АПИНО

ICAIT

10TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2021

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

СБОРНИК НАУЧНЫХ СТАТЕЙ

24–25 ФЕВРАЛЯ 2021 ГОДА

APINO.SPBGUT.RU

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

ГОД НАУКИ И ТЕХНОЛОГИЙ В СПбГУТ

АПИНО

ICAIT

10TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2021

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

Научные направления:

– Радиотехнологии в связи
– Инфокоммуникационные сети и системы
– Информационные системы и технологии
– Теоретические основы радиоэлектроники
– Цифровая экономика и управление в связи
– Гуманитарные проблемы информационного пространства
– Сети связи специального назначения

Партнёры:

КОМПАНИЯ «Т8»

ООО «Т8»

АРГУС НТЦ

ООО «НТЦ АРГУС»

SERTEK

ООО «Сертек»

Информационные партнёры:

ТУЗС

журнал
«Труды учебных заведений связи»

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ ИНФОРМАЦИЯ КОСМОС

журнал
«Информация и космос»

Информационная поддержка:

WWW.IIT.SUT.RU

электронный журнал «Информационные технологии и телекоммуникации»

24–25 ФЕВРАЛЯ 2021

Санкт-Петербург, пр. Большевиков, 22/1,
Английский пр. 3, наб. р. Мойки, 65

APINO.SPBGUT.RU

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная 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, 2021. Т. 1. 770 с.

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

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

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 01.06.2021.
Вышло в свет 30.06.2021. Формат 60×90 1/8.
Уст. печ. л. 96,25. Заказ № 072-ИТТ-2021.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ISBN 978-5-89160-230-4

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

УДК 621.397
ГРНТИ 47.51

ПРОБЛЕМАТИКА ПОДГОТОВКИ ТЕХНИЧЕСКИХ СПЕЦИАЛИСТОВ В СФЕРЕ ТЕЛЕВИДЕНИЯ. СМЕНА ПРИОРИТЕТОВ

А. А. Гоголь[1], И. Ю. Осичев[2], Б. М. Петров[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]АО «ГАТР» (Телеканал «Санкт-Петербург»)

В работе рассмотрены основные изменения направлений подготовки специалистов в настоящее время. Формулировка основных трендов развития телевидения приведена на основе опыта АО "ГАРТ" (телеканал "Санкт-Петербург").

виртуальные студии, дополненная реальность, информационные системы, трёхмерная графика, искусственный интеллект.

Как и многие отрасли, телевидение и радио сегодня очень сильно зависят от компьютерных технологий, и есть тенденция на полное сопряжение. Это касается съемки, технологий производства, хранения, постобработки (монтажа) и сред распространения (OTT сервисы и платформы, видеохостинги и интернет-медиа). Специалисты, глубоко знающие принципы работы и обработки цифровых телевизионных видеосигналов, сегодня нужны в меньшем количестве телекомпаниям, но при этом они по-прежнему востребованы. Основной упор сегодня на кадрах, уверенно ориентирующихся в ИТ технологиях, способных поддерживать сложные компьютерные системы и комплексы. Им достаточно несильно глубоких знаний в области цифрового телевидения, а аналоговые сигналы и системы уже вообще не актуальны. Это также связано и с тем, что все больше производителей обору-

дования переходят на стандартные серверные компоненты, на которых работает Программное обеспечение, а доля собственного разрабатываемого оборудования снижается или вовсе заменяется ПО.

Каждая телекомпания, как правило, обладает той или иной спецификой, которая отражена в технологии производства, и при этом технология меняется с развитием компании. Именно поэтому востребованы специалисты с навыками разработки программного обеспечения, понимающие принципы работы телевидения, которые умеют связывать различные системы, автоматизировать рутинные процессы и могут наладить технологичное, максимально надежное и качественное производство за счет использования программного обеспечения. Скорость работы и надежность на телевидении всегда были важными параметрами, а готовых программных решений зачастую нет, и их приходится писать под конкретные задачи. Также компании часто сталкиваются с тем, что возникает необходимость написать дополнительное программное обеспечение для приобретенного дорогого оборудования, чтобы оно выполняло необходимую задачу или это было удобно, а значит быстро и эффективно.

Активно и прочно вошли в жизнь телекомпаний графические компьютерные системы, работающие в реальном времени (виртуальные студии, дополненная реальность, информационные системы и др.). Это отдельное и глубокое направление, которым занимаются ИТ специалисты на стыке технологий, обладающие знаниями в области телевизионной технологии производства, но гораздо больше разбирающиеся в системах трехмерной графики и трекинга. Такие системы в телевидении имеют тесную интеграцию с внутренними базами данных, с которыми работают пользователи.

По всему миру активно внедряются стандарты IP телевидения, которые пришли на смену технологиям baseband, использовавшим коаксиальные, триаксиальные кабели и оптические волокна для доставки некомпрессированного цифрового видеосигнала. Семейство стандартов SMPTE 2110 [1] – это будущее, которое наступает, и оно позволяет создавать телевизионные инфраструктуры небывалых размеров полностью на стандартных компьютерных технологиях. Для работы с IP технологиями и стандартами необходимы специалисты, уверенно и глубоко знающие принципы работы компьютерных сетей, технологии кодирования видео, а также специалисты, имеющие знания в области информационной безопасности. С приходом подобных технологий становится все более очевидно, почему в перспективе самые востребованные технические специалисты, работающие на телевидении, – это ИТ специалисты, поддерживающие и администрирующие работу сложных ИТ комплексов, нежели ТВ комплексов, основанных на baseband технологиях. Управление и надежное хранение большого количества видеоданных – это также отдельная сложная задача, которая требует глубоких

знаний. Сегодня есть тенденция отходить от дорогостоящих и закрытых систем. Востребованы специалисты, способные поддерживать комплексы, построенные на программном обеспечении (в том числе и open source), способных работать на стандартных серверах, а также и облачных технологиях. Такой подход сегодня является предпочтительным для многих компаний и все больше приближает телекомпании к современным ИТ компаниям.

При развитии и увеличении пропускных способностей компьютерных сетей, повышении скорости публичного интернета, использовании облачных технологий в телевидении обязательно станет неотъемлемой частью ИТ инфраструктур, как центральных, так и региональных каналов.

Такая тенденция явно прослеживается в зарубежной медиаиндустрии, где уже сегодня применяются облачные эфирные сервера (резервные центры вещания) и другие возможности облачных сервисов, которые специально адаптированы для медиа. Сегодня, учитывая геополитические особенности времени, мы не имеем возможности использовать в работе ведущие западные облачные сервисы такие, как Amazon, а отечественные компании пока еще только начали свой путь в этом направлении, но уже достигли неплохих результатов. Тем не менее, специалисты, которые уверенно владеют принципами работы таких сервисов, уже сегодня задействованы в работе многих телекомпаний. И тут речь не про вебсайты компаний, а именно про инфраструктуру вещательного комплекса или обеспечение внестудийного производства, доставки сигналов, мониторинга и др. нужд.

Отдельное перспективное направление – это использование инструментов машинного обучения, алгоритмов искусственного интеллекта. Это создание новых инструментов, автоматизация, обработка больших массивов видеоданных, персонализации контента и др. Как пример, мы сегодня накапливаем огромные архивы данных, с которыми работать традиционными способами будет все сложнее. Технологии Искусственного интеллекта будут помогать в поиске и обработке архивов, восстановлению материалов, улучшению качества архивных видеоматериалов, а также анализу содержимого.

Как некое обобщение данной информации, считаю важным обратить внимание на то, что сегодня решены базовые вопросы в техническом обеспечении телевизионного производства и распространении сигналов, а индустрия находится в стадии трансформации технологий, но это вовсе не значит, что необходимо полностью отказаться от подготовки специалистов по всем существующим дисциплинам. Скорее стоит вопрос в создании новых и значимых направлений.

Развитие телевидения как самостоятельной отрасли со своим специализированным оборудованием сужается с каждым годом, но по-прежнему остается востребована в целом ряде направлений и должна продолжать свое развитие.

Компьютерная индустрия набирает обороты ввиду своей широкой вовлеченности во все отрасли и становится пригодной для тех задач, которые ранее казались недоступными или нерентабельными в медиа. Происходит поиск и замена ТВ оборудования программным обеспечением и более эффективными компьютерными системами. Отсюда следует, что необходимы дополнительно развивать подготовку перспективных специалистов, хорошо понимающих в первую очередь принципы компьютерных технологий и строящихся на них вещательных технологиях, а не наоборот. Специфических компьютерных технологий для телевидения огромное количество и многие из них требуют глубоких знаний и специализации.

Список используемых источников

1. SMPTE ST 2110 FAQ. – URL: https://www.smpte.org/smpte-st-2110-faq

УДК 004.7:621.39
ГРНТИ 49.33; 28.23

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СЕТЯХ СВЯЗИ

А. Е. Кучерявый, А. С. Бородин, А. С. А. Мутханна, А. Р. Абделлах, А. Н. Волков

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

В статье поставлены научно-исследовательские задачи в области искусственного интеллекта для сетей связи. Рассматриваются решения по прогнозированию задержек и трафика для сетей связи пятого и последующих поколений на основе применения машинного и глубокого обучения. Даются рекомендации по применению робастных оценок максимального правдоподобия для сетей автомобильного транспорта VANET (Vehicular Ad Hoc Networks).

искусственный интеллект, машинное обучение, глубокое обучение, прогнозирование, задержки, трафик Интернета Вещей, робастные оценки.

Введение

Предлагаемая вниманию читателей статья основана на опыте научных исследований в области искусственного интеллекта для сетей связи, выполненных на кафедре сетей связи и передачи данных в течение последних двух лет. Эти исследования позволили определить перечень приоритетных задач в области применения искусственного интеллекта для сетей связи пятого и последующих поколений [1, 2, 3], предложить распределенную структуру

искусственного интеллекта для этих сетей в условиях предстоящего широкого использования микросервисов [4, 5], решить ряд задач с использованием машинного [6, 7] и глубокого обучения [8, 9]. Все это вместе взятое позволило университету занять лидирующие позиции в области применения искусственного интеллекта как в Российской Федерации, так и за рубежом [10, 11].

Научно-исследовательские задачи по применению искусственного интеллекта в сетях связи

Сети связи представляют собой чрезвычайно сложное и очень наукоемкое взаимоувязанное для всего земного шара сооружение. Сложность и наукоемкость делают сети связи, в особенности сети связи пятого и шестого поколений, исключительно подходящим полигоном для внедрения технологий искусственного интеллекта. Кроме всего прочего, процессы обслуживания трафика в сетях связи происходят, как правило, в реальном времени, а задержки распространения сигнала могут не превышать 1 мс [12, 13, 14]. Потенциальное число пользователей за счет технологий Интернета Вещей [15, 16] на порядки больше [17], чем число пользователей, например, банков. Эти две характеристики сетей связи пятого поколения, сверх высокая плотность [18, 19] и ультра малые задержки [20, 21] делают внедрение технологий искусственного интеллекта в современных сетях и сетях будущего необходимостью.

При этом основные задачи для сетей связи пятого и последующих поколений состоят в традиционных для любых сетей связи задачах распределения ресурсов [22, 23] и прогнозировании трафика [24, 25].

Именно на основе такого анализа учеными кафедры сетей связи и передачи данных [10] синтезирован перечень приоритетных на сегодняшний день задач в области применения искусственного интеллекта для сетей связи пятого и последующих поколений:

- Идентификация трафика в сети связи, не вносящая дополнительных задержек в поток и обеспечивающая требования сетей связи с ультрамалыми задержками.
- Системный онлайн мониторинг сети связи от потока данных (в том числе виртуального) до многопараметрических моделей сегмента сети с множеством устройств и систем.
- Кратковременное и долговременное прогнозирование нагрузки как на элементы сети, так и на целые сегменты.
- Кратковременное и долговременное прогнозирование поведения потоков ПД на уровне ПД и служебных потоков на уровне управления.
- Долговременное прогнозирование нагрузки на сетевую и вычислительную инфраструктуру с учетом трендов изменения профилей трафика и типов сервисов с целью определения и автоматического формирования

предложения по сокращению или расширению сети, а также ее пороговых характеристиках.

•Эффективное распределение радиоресурсов покрытия 5G с прогнозированием нагрузки на соты.

•Кратковременное и долговременное прогнозирование потребностей пользователей в тех или иных услугах.

•Прогнозирование передвижения пользователя географически, а также формирование модели его предпочтений в контенте.

• Распознавание и прогнозирование атак злоумышленников на систему с формированием опережающей реакции на возможную атаку.

•Применение технологий ИИ для согласованного распределения сервисов по сети на структурах пограничных вычислений (MEC) и туманных вычислений (FoG).

Как видим, в числе задач применения технологий искусственного интеллекта во множестве присутствуют задачи по прогнозированию трафика, чему и посвящен следующий раздел статьи.

Прогнозирование в задачах по сетям связи

Прогнозирование поведения сети в реальном времени достаточно широко использовалось в беспроводных сенсорных сетях [26, 27, 28]. Беспроводные сенсорные сети были предвестником появления высокоплотных и сверх плотных сетей связи в сетях связи пятого и последующих поколений. Число сенсорных узлов на сенсорном поле было достаточно велико, что потребовало кластеризации при построении беспроводной сенсорной сети. При кластеризации беспроводной сенсорной сети одной из важнейших задач стал выбор головного узла кластера. Вследствие всепроникающего характера беспроводных сенсорных сетей [26] практически во все отрасли экономики особенности применения этих сетей в различных областях к настоящему времени разработано достаточно много алгоритмов выбора головного узла. В качестве примеров можно привести алгоритмы LEACH [29, 30] и TEEN [27, 31]. Весомый вклад в разработку алгоритмов выбора головного узла беспроводных сенсорных сетей внесли российские ученые [32, 33, 34, 35].

При этом прогнозирование нашло широкое применение в мобильных беспроводных сенсорных сетях, что было связано с возможностью ухода головного узла кластера из кластера в период сбора и предварительной обработки информации. Первым алгоритмом в этом направлении был алгоритм выбора головного узла с прогнозированием, разработанный в СПбГУТ [36]. Для прогнозирования местоположения головного узла и членов кластера использовались следующие предикторы:

– простой точечный предиктор,

– экстраполяционный предиктор,

– комбинированный предиктор.

На рис. 1 приведены результаты работы предложенного в [36] алгоритма DCA (*Distributed Cluster Algorithm*) при использовании всех трех предикторов и сравнение этих результатов с мобильной версией базового алгоритма LEACH.

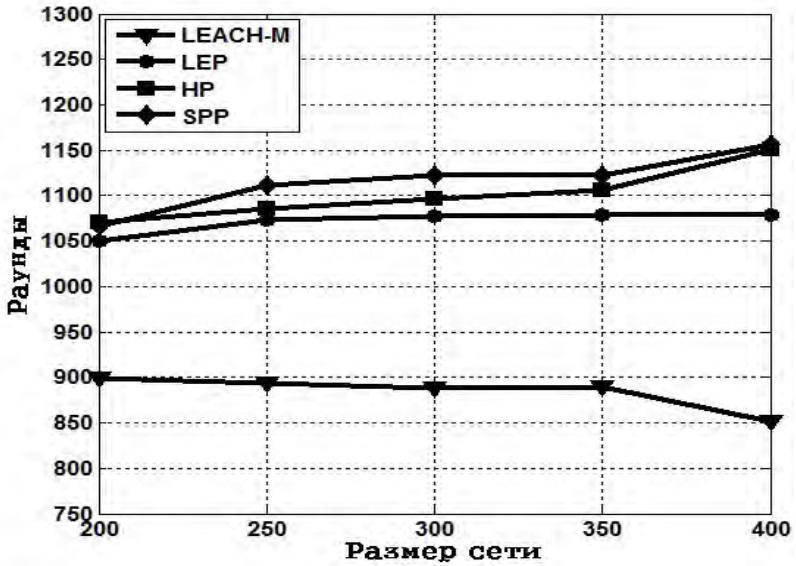


Рис. 1. Жизненный цикл сети с использованием различных версий DCA в сравнении с LEACH-M в случае, когда шлюз расположен в центре сети

На рис. 1 LEACH-M – мобильная версия алгоритма LEACH, LEP – линейный экстаполяционный предиктор, HP – гибридный предиктор, SPP – простой точечный предиктор. Как видим, наилучшие результаты получаются при использовании простого точечного предиктра, что естественно, поскольку прогнозирование осуществляется на достаточно коротком промежутке времени.

Прогнозирование задержки в сетях связи пятого поколения с использованием машинного обучения

Прогнозирование задержки в сетях связи пятого поколения является одной из важнейших задач для обеспечения требуемых параметров по качеству обслуживания и качеству восприятия. Действительно, в целом ряде приложений задержка не должна превышать единицы миллисекунд [37, 38], поэтому краткосрочный прогноз значения задержки в условиях колебания трафика очень важен.

В работах ученых СПбГУТ [6, 7] для решения этой задачи было предложено использовать машинное обучение и следующие нейронную сеть и алгоритмы обучения:

– нелинейная авторегресионная рекуррентная нейронная сеть с внешними входами NARX;

– Trainlm (алгоритм Левенберга-Марквардта с обратным распространением);

– Trainrp (устойчивый алгоритм обучения нейронной сети с обратным распространением);

– Traincgf (алгоритм сопряженных градиентов Флетчера-Ривса для обучения нейронной сети с обратным распространением и обновлениями).

Для сравнения эффективности и выбора того или иного алгоритма обучения использовались значения корня из среднеквадратичной ошибки RMSE (*Root Mean Square Error*) и средней абсолютной ошибки в процентах MAPE (*Mean Absolute Percent Error*).

Результаты моделирования представлены в таблице 1. При этом использовалось как прогнозирование на один шаг вперед, так и на несколько шагов вперед.

ТАБЛИЦА 1. Сравнение эффективности алгоритмов обучения при прогнозировании задержки

Алгоритм обучения	Прогнозирование на один шаг вперед		Прогнозирование на несколько шагов вперед	
	RMSE	MAPE	RMSE	MAPE
Trainlm	0,0551	0,0429	0,0521	0,1301
Traincgf	0,2163	0,5178	0,3704	3,2367
Trainrp	1,4734	0,7245	0,6996	4,7953

Как видим, для прогнозирования задержек высокую эффективность по точности имеют нелинейные рекуррентные сети NARX и алгоритм обучения Левенберга-Марквардта с обратным распространением.

Прогнозирование трафика Интернета Вещей в сетях связи пятого поколения с использованием глубокого обучения

Прогнозирование трафика Интернета Вещей представляет собой также одну из важнейших задач для обеспечения требуемого качества обслуживания и качества восприятия, поскольку Интернет Вещей привносит в сети связи свойства высокой и сверх высокой плотности сетей [39, 40]. В работах ученых СПбГУТ для прогнозирования трафика Интернета Вещей в сетях связи пятого поколения [8, 9] применялось глубокое обучение DL (*Deep Learning*) с использованием нейронной сети долговременной краткосрочной памяти LSTM (*Long Short-Term Memory*). При этом число скрытых нейронов

составляло: 50, 200, 500. На рис. 2, 3 и 4 приведены результаты моделирования из [8, 9] для всех исследуемых значений скрытых нейронов.

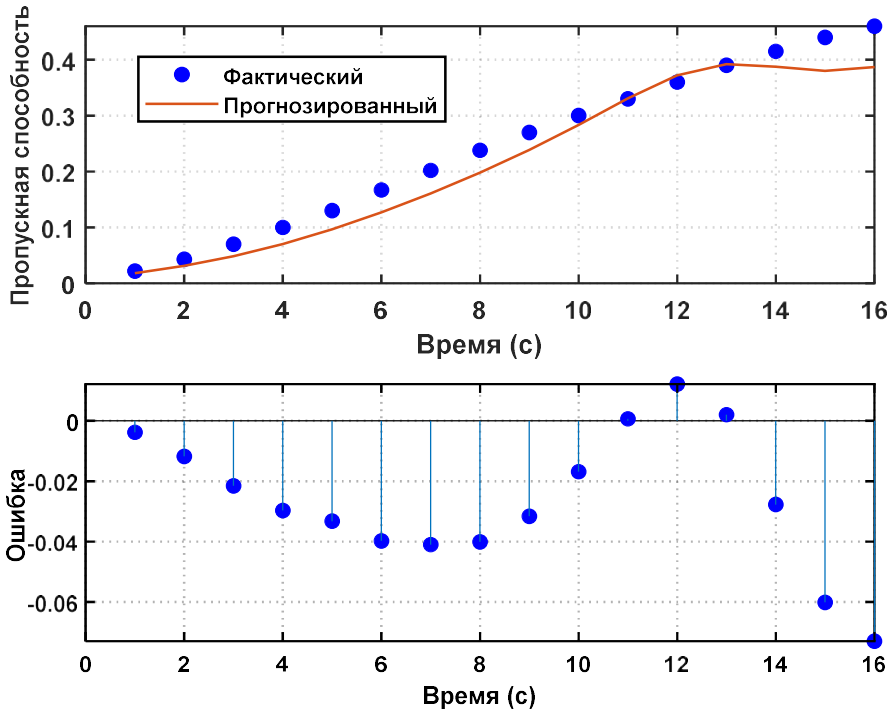


Рис. 2. Прогнозируемая и фактическая пропускная способность и RMSE при 500 скрытых нейронов в слое LSTM

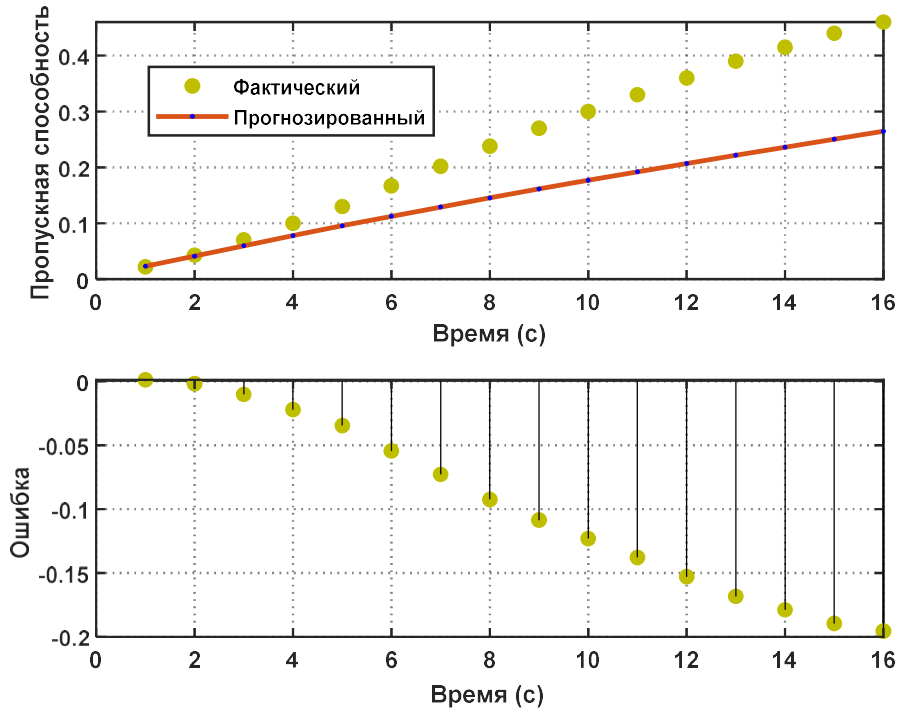


Рис. 3. Прогнозируемая и фактическая пропускная способность и RMSE при 200 скрытых нейронов в слое LSTM

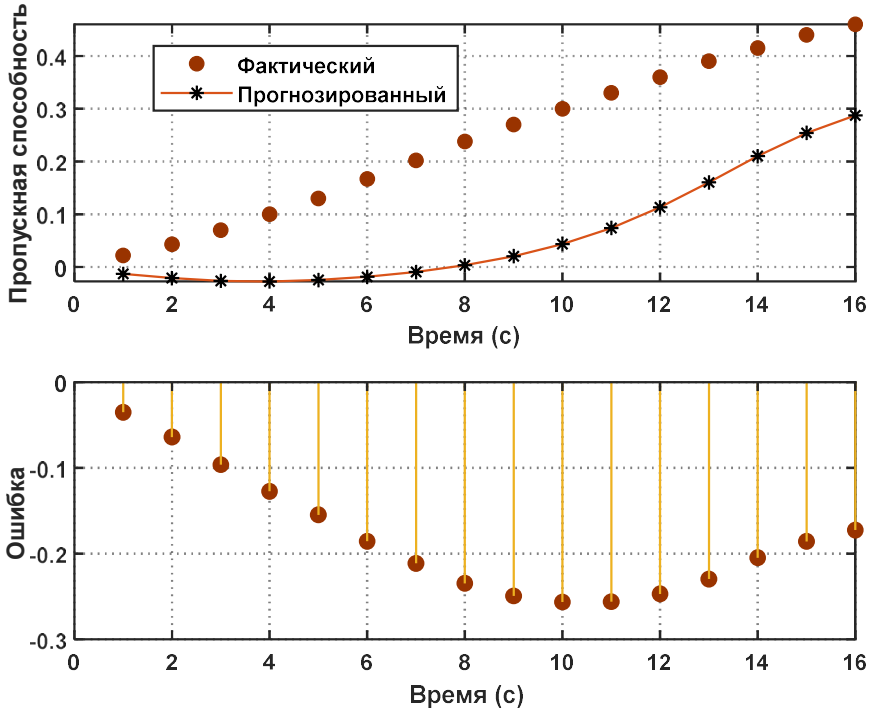


Рис. 4. Прогнозируемая и фактическая пропускная способность и RMSE при 50 скрытых нейронов в слое LSTM

Как видим, использование нейронной сети долговременной кратковременной памяти LSTM при числе скрытых нейронов 500 позволяет прогнозировать пропускную способность с достаточной для практических условий точностью.

Робастные оценки для искусственного интеллекта в сетях связи

Робастные М-оценки (максимального правдоподобия) достаточно успешно использовались в исследованиях по трафику для сетей связи для оценки трафика в часы наибольшей нагрузки (ЧНН). Например, использование кусочно-линейной М-оценки Хампеля [41] позволило с большей точностью определять среднее значение нагрузки и потерь для тридцати самых нагруженных ЧНН в год [42].

В таблице 2 приведены результаты моделирования при использовании различных робастных оценок в исследованиях сетей автомобильного транспорта VANET [43, 44].

ТАБЛИЦА 2. Использование робастных оценок при использовании VANET

Оценка	RMSE	Время обработки
MSE	6,1706e-004	2,6875
Cauchy	5,0916e-004	2,4844
GM	4,4933e-004	2,7500

Оценка	RMSE	Время обработки
Fair	4,8975e-004	2,5000
L1	4,8023e-004	6,0469
LMLS	4,8023e-004	2,5000
Huber	5,0048e-004	2,4531

Оценка L1 являет собой винзоризованную оценку. М-оценка Хьюбера – одна из наиболее часто используемых оценок и, как это будет видно из результатов моделирования, ее применение для машинного обучения сетей VANET весьма эффективно. Кроме того, при исследовании использовались следующие робастные оценки: «справедливая» (*Fair*), Коши (*Cauchy*), GM (*Geman-McLure*) и логарифмическая оценка LMLS [45].

По результатам моделирования [45] можно констатировать, что М-оценка Geman-McLure (GM) обладает наилучшими характеристиками по RMSE со значением 4,4933e-004 по сравнению с другими М-оценками. При этом следует отметить, что значения RMSE для М-оценок L1 и LMLS имеют достаточно близкое значение RMSE 4,8023e-004 с RMSE для оценки GM. Кроме того, «справедливые» оценки, а также оценки Хьюбера и Коши также дают существенно лучшие результаты, чем при традиционной метрике среднеквадратичной ошибки MSE. С точки зрения скорости обучения наилучшие результаты получены с помощью М-оценки Хьюбера – 2,4531 с.

Выводы

1. Определены задачи по использованию технологий искусственного интеллекта в сетях связи.

2. Анализ литературных источников показывает, что СПбГУТ занимает лидирующие позиции в научных исследованиях в Российской Федерации по применению технологий искусственного интеллекта в сетях связи.

3. Существенная часть научно-исследовательских работ по искусственному интеллекту для сетей связи связана с прогнозированием ее характеристик. Исследования СПбГУТ в этих направлениях доказали, что для прогнозирования задержек высокую эффективность по точности имеют нелинейные рекуррентнтные сети NARX и алгоритм обучения Левенберга-Марквардта с обратным распространением.

4. При прогнозировании трафика Интернета Вещей целесообразно использовать методы глубокого обучения, что связано с высокой плотностью таких сетей. Доказано, что использование нейронной сети долговременной краткосрочной памяти LSTM при числе скрытых нейронов 500 позволяет прогнозировать пропускную способность с достаточной для практических условий точностью.

5. При исследовании применения технологий искусственного интеллекта следует обратить внимание на оценку статистических характеристик

с использованием робастных М-оценок, что позволяет улучшить точность оценивания параметров.

Список используемых источников

1. Volkov A., Proshutinskiy K., Adam A. B. M., Ateya A. A., Muthanna A., Koucheryavy A. SDN Load Prediction Algorithm Based on Artificial Intelligence // In Communications in Computer and Information Science. 2019. Vol. 1141 CCIS, pp. 27–40. Springer. https://doi.org/10.1007/978-3-030-36625-43.

2. Атея А. А., Мутханна А. С., Кучерявый А. Е. Интеллектуальное ядро для сетей связи 5G и тактильного интернета на базе программно-конфигурируемых сетей // Электросвязь. 2019. № 3. С. 34–40.

3. Кучерявый А. Е., Бородин А. С., Киричек Р. В. Сети связи 2030 // Электросвязь. 2018. № 11. С. 52–56.

4. Volkov A., Ateya A. A., Muthanna A., Koucheryavy A. Novel AI-Based Scheme for Traffic Detection and Recognition in 5G Based Networks // In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2019. Vol. 11660 LNCS. pp. 243–255. Springer Verlag. https://doi.org/10.1007/978-3-030-30859-921.

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

6. Абделлах А. Р., Махмуд О. А., Парамонов А. И., Кучерявый А. Е. Прогнозирование задержки в сетях интернета вещей и тактильного интернета с использованием машинного обучения // Электросвязь. 2021. № 1. С. 26–30.

7. Abdellah A. R., Abdulkareem Mahmood O., Koucheryavy A. Delay prediction in IoT using Machine Learning Approach // International Congress on Ultra Modern Telecommunications and Control Systems and Workshops. 2020. pp. 275–279.

8. Абделлах А. Р., Кучерявый А. Е. Исследование методов прогнозирования трафика в сетях 5G на основе глубокого обучения // СПбНТОРЭС, Труды ежегодной НТК. 2020. № 1 (75). С. 155–156.

9. Бородин А. С., Абделлах А. Р., Кучерявый А. Е. Глубокое обучение с долговременной краткосрочной памятью для прогнозирования трафика Интернета Вещей // Электросвязь. 2021. № 2. С. 48–52.

10. Бородин А. С., Волков А. Н., Мутханна А. С., Кучерявый А. Е. Искусственный интеллект в сетях связи пятого и последующих поколений // Электросвязь. 2021. № 1. С. 17–22.

11. Khayyat M., Elgendy I. A., Muthanna A., Alshahrani A., Alharbi S., & Koucheryavy A. Advanced Deep Learning-based Computational Offloading for Multilevel Vehicular Edge-Cloud Computing Networks // IEEE Access. 2020. 1–1. URL: https://doi.org/10.1109/access.2020.3011705.

12. Кучерявый А. Е., Маколкина М. А., Киричек Р. В. Тактильный Интернет. Сети связи со сверхмалыми задержками // Электросвязь. 2016. № 1. С. 44–46.

13. Кучерявый А. Е., Выборнова А. И. Тактильный Интернет // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2016. Т. 1. С. 6–11.

14. Атея А. А., Выборнова А. И., Кучерявый А. Е. Многоуровневая облачная архитектура для услуг Тактильного Интернета // Электросвязь. 2017. № 2. С. 26–30.

15. Кучерявый А. Е, Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб.: Типография Любавич, 2011. 312 с.

16. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.

17. Waldner, J.-B. Nanocomputers and Swarm Intelligence. ISTE, John Wiley & Sons, 2008.

18. Тонких Е. В., Парамонов А. И., Кучерявый А. Е. Анализ беспроводной сети интернета вещей высокой плотности // Электросвязь. 2020. № 1. С. 51–55.

19. Тонких Е. В., А. И. Парамонов, А. Е. Кучерявый Свойства самоподобия сетевой структуры и ее моделирование для сети Интернета вещей высокой плотности // Электросвязь. 2020. № 8. С. 18–24.

20. Кучерявый А. Е. Парамонов А. И., Аль-Наггар Я. М. Сети связи с ультра малыми задержками // Электросвязь. 2013. № 12. С. 15–19.

21. Yastrebova A., Kirichek R., Koucheryavy Y., Borodin A., Koucheryavy A. Future Networks 2030: Architecture and Requirements // The 10th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT). November 2018, Moscow. Proceedings, 2018.

22. Ateya A., Muthanna A., Gudkova I., Abuarqoub A., Vybornova A., Koucheryavy A. Development of intelligent core network for Tactile Internet and future smart systems // Journal of Sensor and Actuator Networks. 2018. V. 7. No. 1. P. 1.

23. Ateya Abdelhamied A., Muthanna Ammar, Vybornova Anastasia, Algarni Abeer D., Abuarqoub Abdelrahman, Koucheryavy Y., Koucheryavy Andrey. Chaotic Salp Swarm Algorithm for SDN Multi-controller Networks // Engineering Science and Technology, an International Journal. 2019. Vol. 22. Iss. 4. pp. 1001–1012.

24. Шнепс М. А. Системы распределения информации. М.: Связь, 1979. 344 с.

25. Лившиц Б. С., Пшенишников А. П., Харкевич А. Д. Теория телетрафика. М.: Связь, 1979. 224 с.

26. Аль-Кадами Н. А., Кучерявый А. Е. Адаптивный алгоритм кластеризации для беспроводных сенсорных сетей с мобильными узлами // Электросвязь. 2015. № 3. С. 22–26.

27. Аль-Кадами Н. А. Оценка и сравнительный анализ алгоритмов маршрутизации для гомогенных и гетерогенных беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. Вып. 3 (7). С. 4–22.

28. Al-Qadami N., Laila I., Koucheryavy A., Ahmad A. S. Mobility Adaptive Clustering Algorithm for Wireless Sensor Networks with Mobile Nodes // ICACT-2015, Proceedings, 1–3 July, Phoenix Park, Korea.

29. Heinzelman W., Chandrakasan A., and Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks // Proceedings 33rd Hawaii International Conference on System Sciences (HICSS), Wailea Maui, Hawaii, USA, Jan. 2000.

30. Kim D., Chung Y. Self-Organization Routing Protocol Supporting Mobile Nodes for Wireless Sensor Networks // IMSCCS'06. Proceedings. Zhejiang University, China, June 20–24, 2006.

31. Arati M. A. and Dharma P. A. TEEN: a routing protocol for enhanced efficiency in wireless sensor networks // in Proceedings of the 15th International Parallel & Distributed Processing Symposium, pp. 2009–2015, San Francisco, Calif, USA, April 2001.

32. Koucheryavy A., Salim A. Cluster-based Perimeter-coverage Technique for Heterogeneous Wireless Sensor Networks // Proceedings, ICUMT 2009 International Conference IEEE on Ultra Modern Telecommunications, Saint-Petersburg, Russian. 2009.

33. Кучерявый А. Е., Салим А. Выбор головного узла кластера в однородной беспроводной сенсорной сети // Электросвязь. 2009. № 8. С. 32–36.

34. Мочалов В. А., Турута Е. Н. Построение отказоустойчивой структуры беспроводной сенсорной сети с учетом отказов центров сбора информации // Труды IS&IT'12. Научное издание в 4-х т. М.: Физматлит, 2012. Т. 2.

35. Abakumov P., Koucheryavy A. The Cluster Head Selection Algorithm in the 3D USN // Proceedings, International Conference on Advanced Communication Technology, 2014. ICACT 2014. Phoenix Park, Korea.

36. Koucheryavy A., Salim A. Prediction-based Clustering Algorithm for Mobile Wireless Sensor Networks // Proceedings, International Conference on Advanced Communication Technology. ICACT 2010. Phoenix Park, Korea. 2010.

37. Li Z., Uusitalo M., Shariatmadari H., Singh B. 5G URLLC: Design Challenges and System Concepts. 15th International Simposium on Wireless Communication Systems (ISWCS), October 8–9. Tokio, Japan, 2018. 6 p.

38. Popovski P. and all. Wireless Access for Ultra-Reliable Low Latency Communications. IEEE Network. March-April 2018. V. 32, Iss. 2. pp. 16–23.

39. Бородин А. С., Кучерявый А. Е., Парамонов А. И. Метод построения сети связи на базе D2D-технологий с использованием дополнительных маршрутизаторов // Электросвязь. 2019. № 4. С. 86–92.

40. Бородин А. С., Парамонов А. И. Маршрутизация трафика в сети беспроводной связи, построенной на базе D2D-технологий // Электросвязь. 2019. № 2. С. 38–44.

41. Хампель Ф., Рончетти Э. Робастность в статистике. Подход на основе функций влияния. М.: Мир, 1989. 512 с.

42. Кучерявый А. Е. Робастные оценки нагрузки и потерь на ГТС // Электросвязь, 1986. № 7. С. 12–14.

43. Abdellah A. R., Muthanna A., Koucheryavy A. Robust Estimation of VANET Performance-based Robust Neural Networks Learning // 19th International Conference NEW2AN 2019. LNCS, Springer. Vol. 11660. pp. 402–414.

44. Vladyko A., Khakimov A., Muthanna A., Ateya A. A., Koucheryavy A. Distributed Edge Computing to Assist Ultra-Low-Latency VANET Applications // Future Internet. 2019. Vol. 11. Iss. 6. P. 128.

45. Абделлах А. Р., Кучерявый А. Е. Применение робастных М-оценок для машинного обучения в сетях VANET // Электросвязь. 2020. № 5. С. 41–46.

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 654.739
ГРНТИ 49.33.29

АНАЛИЗ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ НА БАЗЕ ТЕХНОЛОГИИ ПОСТРОЕНИЯ РАСПРЕДЕЛЕННЫХ СЕТЕЙ СВЯЗИ

Э. А. Аббасов[1], **Б. Г. Ибрагимов**[1], **М. Б. Намазов**[2]

[1]Азербайджанский технический университет
[2]Бакинский инженерный университет

Проанализированы показатели эффективности мультисервисных сетей связи, построенные в соответствии с архитектурной концепцией NGN (Next Generation Network) и FN (Future Network) на базе технологии построения распределенных сетей связи. В качестве критерия эффективности функционирования системы выбрана производительность мультисервисных сетей связи с использованием SDN (Software Defined Networking) и NFV (Network Functions Virtualization) технологий. Получены на базе модели аналитические выражения для оценки вероятностно-временных характеристик сети связи.

производительность сети, SDN, технологии построения распределенных сетей связи, NFV, физический ресурс.

Бурное развитие единой информационной инфраструктуры и единой многооператорской среды на основе программы цифровой экономики требуют новые фундаментальные принципы и глобальные подходы к построению высокоэффективных мультисервисных сетей связи на базе архитектурной концепции следующих NGN и будущих сетей FN, использующих инновационные технологии [1].

В настоящее время глубокая интеграция информационных и коммуникационных технологий приводит к новому качеству информационной инфраструктуры – к появлению инфокоммуникационной инфраструктуры, построенной в соответствии с концепцией цифровой трансформации экономики.

К инновационным технологиям относятся прежде всего технологии построения распределенных сетей связи как SDN (*Software Defined Networking*), NFV (*Network Functions Virtualization*), IMS (*Internet Protocol Multimedia Subsystem*), искусственного интеллекта, WDM&DWDM (*Wavelength Division Multiplexing&Dense* WDM), облачных вычислений, мобильных LTE (*Long Term Evolution*) & UMTS (*Universal Mobile Telecommunications System*), IoT (*Internet of Think*), так и квантовых технологий [2, 3].

Стоит отметить, что среди перечисленных передовых технологий для построения мультисервисных сетей связи с повышенной производительностью на базе NGN и FN, особое место занимают SDN и NFV технологии. SDN и NFV были выбраны в качестве ключевых факторов эволюции мультисервисных сетей, направивших процесс стандартизации FN в новом направлении [4, 5].

В работе [2, 4, 6] исследованы эффективности функционирования мультисервисных телекоммуникационных сетей на базе архитектурной концепции NGN и FN с использованием инфокоммуникационных технологий и выявлены их основные сетевые и канальные показатели.

В рекомендации МСЭ-Т Y.3001 заданы основные четыре целевых установки создания Будущих сетей FN с учетом информационных, канальных и сетевых ресурсов [1].

Поэтому, задачи анализа показателей производительности мультисервисных сетей связи на базе архитектурной концепции будущих сетей, использующие передовые инфокоммуникационные SDN и NFV технологии являются наиболее актуальными.

В данной работе рассматривается решение сформулированной выше задачи – исследование комплексных показателей производительности мультисервисных сетей связи на базе SDN и NFV технологии.

Учитывая предложенные целевые установки для создания будущих сетей FN на основе рекомендаций ITU-T, Y.3001 [3, 4, 5, 7], использующие вышеперечисленных технологии SDN и NFV открывают новые возможности для оказания широкого спектра мультимедийных услуг с учетом многочисленных требований параметров качества обслуживания QoS (*Quality of Service*) и качества восприятия QoE (*Quality of Experience*). Кроме того, внедрение новых инфокоммуникационных технологий, необходимость передачи различных потоков пакетов трафика в узлах сети связи, определяют повышенные требования к эффективности функционирования системы.

На основе исследования установлено [3, 7], что мультисервисные сети связи на базе технологии SDN и NFV при оказании мультимедийных услуг и приложений как “Triple Play services” (речи, данные и видео трафиков), интеллектуальные услуги так и «Bandwith» представляют собой многоканальную систему массового обслуживания с N_k аппаратно-программным комплексом. Входящий поток пакетов имеет пуассоновское распределение с параметром λ_i и среднее время обслуживания одного пакета равно μ_i^{-1}, $i=\overline{1,n}$.

Одним из важных критериев эффективности функционирования сети связи выбрана производительность аппаратно-программных комплексов SDN и NFV и описывается следующей зависимостью:

$$E_{\text{эфф.}}(\lambda_i) = W\,[G_{\text{пр.}}(\lambda_i)], \quad i=\overline{1,n}, \tag{1}$$

где $G_n(\lambda_i)$ – производительность системы аппаратно-программных комплексов SDN и NFV с учетом скорости поступления входящего потока λ_i при обработке i-го трафика, $i=\overline{1,n}$.

В (1) отмеченных в качестве аппаратно-программных комплексов SDN и NFV являются коммутаторы и контроллеры SDN с использованием протоколов OpenFlow, виртуализированное ядро сети (компоненты ядро сети EPC и vEPC), а также виртуальные каналы с физическими ресурсами.

В мультисервисных сетях связи производительность системы с учетом показателей эффективности для оказания мультимедийных услуг характеризуется следующим показателем:

- $L_{\text{ср}}(\lambda_i)$ – среднее время ожидания пакета в очереди на обслуживание в системе с учетом скорости поступления входящего потока λ_i при обработке i-го трафика, $i=\overline{1,n}$;
- R_i – коэффициент сохранения отказоустойчивости аппаратно-программных средств при обработке i-го потока трафика, $i=\overline{1,n}$;
- I_i – коэффициент информационной безопасности функционирования аппартно-программных средств при обработке i-го потока трафика, $i=\overline{1,n}$;
- $C_{\max}(\lambda_i)$ – пропускные способности аппаратно-программных комплексов SDN и NFV с учетом скорости поступления входящего потока λ_i при обработке i-го трафика, $i=\overline{1,n}$.

Учитывая вышеизложенные предположения, построим математическую модель мультисервисной сети связи при использовании коммутаторов и контроллеров SDN, а также виртуализированного ядра сети NFV. Широ-

кое использование технологий NFV и SDN позволяет создавать новые сервисы с существенно более высокими скоростями передачи данных и меньшими задержками [7].

Из описания поведения системы видно, что рассмотренная модель является многоканальной системой с N_k обслуживающими приборами и буферным накопителем конечной емкости $N_{\text{вн}}$. В систему поступает пуассоновский поток пакетов трафика с интенсивностью λ_i и длительность обслуживания потоков пакетов распределена экспоненциально с параметром μ_i. Для увеличения эффективности построенной модели предлагается использовать канальные и физические ресурсы.

Математическая формулировка задачи, предлагаемой ММ, для оценки показателей эффективности функционирования систем обработки информационных потоков автомобильных служб описывается следующим функциональным преобразованием трафика:

$$E_{\text{фп}}(\lambda):\{t_{\text{вх}}\}\rightarrow\{\lambda\}\left|\begin{array}{c} R_i \geq R_{i.\text{доп.}}, \quad i=\overline{1,n} \\ L_{\text{ср}}(\lambda_i) \leq L_{\text{ср.др.}}(\lambda_i) \\ C_{\max}(\lambda_i) \leq C_{\max.\text{доп.}}(\lambda_i), i=\overline{1,n} \\ I_i \leq I_{i.\text{доп.}}, \quad i=\overline{1,n} \end{array}\right., \tag{2}$$

при следующих ограничениях

$$C_{\text{ап}}(\lambda_i) \leq C_{\text{ап.дп.д}}(\lambda_i),\ T_{\text{зад.}}(\lambda_i) \leq T^{\text{доп.}}_{\text{зад.}}(\lambda_i),\ P_{\text{отк.}} \leq P^{\text{доп.}}_{\text{отк.}},\quad i=\overline{1,n}, \tag{3}$$

где $C_{\text{ап}}(\lambda_i)$ – величина экономической эффективности и стоимости аппаратно-программных комплексов и терминальных средств системы;

$T_{\text{зад.}}(\lambda_i)$ – время задержки пакета от момента его поступления до момента отправки с учетом скорости поступления входящего потока λ_i;

$P_{\text{отк.}}$ – вероятность отказа в обслуживании пакета поступающего трафика;

$T^{\text{доп.}}_{\text{зад.}}(\lambda_i)$, $P^{\text{доп.}}_{\text{отк.}}$, $L_{\text{ср.др.д}}(\lambda_i)$, $C_{\max.\text{доп.}}(\lambda)$, $R_{i.\text{доп.}}$, $I_{i.\text{доп}}$, $C_{\text{ап.дп.д}}(\lambda_i)$ – соответственно, допустимое значение величины времени задержки пакета, вероятность отказа, среднее время ожидания пакета в очереди на обслуживание, пропускные способности, коэффициент сохранения отказоустойчивости и коэффициент информационной безопасности функционирования программно-аппаратных комплексов и экономической эффективности и стоимости аппаратно-программных комплексов и терминальных средств системы при передаче i-го потока пакетов с интенсивностью λ_i, $i=\overline{1,n}$.

Выражения (1), (2) и (3) определяют сущность рассматриваемого нового подхода с учетом интенсивности потоков пакетов полезного и служебного трафиков, на основе которого предлагается математическая модель

анализа показателей эффективности функционирования мультисервисных сетей связи. Кроме того, выражения (1), (2) и (3) описывают поведения ММ производительности сети связи на базе технологии SDN и NFV при оказании мультимедийных услуг и при установлении соединения.

Одной из ключевых характеристик для оценки производительности мультисервисных сетей связи на базе технологии SDN и NFV, является их максимальная пропускная способность.

В условиях допустимой загрузки $\rho_{i.\text{доп.}} \le 1$, максимальная пропускная способность сети при обслуживании *i*-го потока пакета полезного и служебного трафиков, определяется следующим выражением:

$$C_{i.\max}(\rho_i \le \rho_{i.\text{доп.}}) = \frac{N_k}{L_{i.\text{n}} + L_{i.\text{c}}} \cdot E[V(\lambda_i)] \cdot (\rho_{i.\text{вх}} + \rho_{i.\text{исх}}) \le C_{i.\max.\text{доп.}}(\lambda_i),\ i = \overline{1,n}, \qquad (4)$$

где $E[V(\lambda_i)]$ – средняя скорость работы сетевых терминальных оборудований SDN и NFV с учетом интенсивности λ_i;

$\rho_{i.\text{вх}}, \rho_{i.\text{исх}}$ – соответственно, коэффициент загрузки входящих и исходящих каналов ядра сети NFV и аппаратно-программных комплексов технологии SDN при обслуживании *i*-го потока пакета и $\rho_{i.\text{исх}} \le \rho_{i.\text{вх}} \le 1$;

$L_{i.\text{n}}, L_{i.\text{c}}$ – средняя длина *i*-го потока пакета полезного и служебного трафиков, $L_{i.\text{nc}} = L_{i.\text{n}} + L_{i.\text{c}}$, $i = \overline{1,n}$.

Из (4) видно, максимальное значение пропускной способности сети в зависимости от параметров $E[V(\lambda_i)]$, $L_{i.\text{nc}}$ и N_k при заданном условии коэффициента $\rho_{i.\text{доп.}}$ загрузки ограничена. Эта означает, что также заданы ограничения на суммарную стоимость исследуемой сети, поскольку $C_{\max}(\lambda_i)$ напрямую зависит от $C_{\text{ап}}(\lambda_i)$ с учетом интенсивности входящего потока трафика.

Учитывая совокупности уравнения Линдли и РК-формулы – Полячека-Хинчина среднее время пребывание *i*-го потока пакетов в *j*-й узла коммутации сетей связи на базе SDN и NFV технологий определяется следующим выражением [3, 8]:

$$E[T_{i.\text{в}}(\lambda_i, N_{\text{бн}} \le N_{\text{бн.доп.}})] = \frac{1}{K_{i.\text{c}}} \sum_{j=1}^{N_k} [T_{ij.\text{вых}}(\lambda_i) - T_{ij.\text{вх}}(\lambda_i)],\quad i = \overline{1,n},\ j = \overline{1,N_k}, \qquad (5)$$

где $K_{i.\text{c}}$ – коэффициент сжатия трафика *i*-го потока пакетов.

Выражения (5) определяет среднее время пребывание в системе потоков пакетов полезного и служебного трафиков по сети SDN от момента их поступления в буферного накопителя (БН) входного порта коммутатора

$T_{ij.\text{вх}}(\lambda_i)$ с интенсивностью λ_i до момента прибытия его в граничной БН контроллера $T_{ij.\text{вых}}(\lambda_i)$ выходного порта сети SDN с использованием протоколов OpenFlow. Кроме того, выражения (5) характеризует полную среднюю задержку передачи потоков пакетов по сети и влияние показателей QoS и QoE полезного и служебного трафиков.

В работе на основе исследования и анализа эффективности функционирования мультисервисных сетей на базе технологий построения распределенных сетей связи SDN и NFV, предложена математическая модель для расчета комплексных показателей производительности сети.

Список используемых источников

1. Росляков А. В., Ваняшин С. В. Будущие сети (Future Networks). Самара: ПГУТИ, 2015. 274 с.

2. Джафарова Э. М., Ибрагимов Б. Г., Исмайлова С. Р. Анализ комплексных показателей мультисервисных телекоммуникационных сетей на базе архитектурных концепций FN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ. 2020. Т. 1. С. 399–404.

3. Пшеничников А. П. Теория телетрафика : учебник для вузов. М. : Горячая линия – Телеком, 2017. 212 с.

4. Naumov V. A., Samuilov K. E., Samuilov A. K. On the total amount of resources occupied by serviced customers // Autom Remote Control. 2016. Vol. 77. Iss. 8. pp. 1419–1427.

5. Agyapong P. K., Iwamura M., Staehle D., Kiess W., Benjebbour A. Design considerations for a 5G network architecture // IEEE Communications Magazine. Nov 2014. Vol. 52. No. 11. pp. 65–75.

6. Гасанов М. Г., Аббасов Э. А., Гахраманова Н. Д. Исследование нелинейных эффектов в системе передачи оптической информации в режиме управления дисперсией // Международная студенческая НПК в рамках ассоциации Государственных университетов прикаспийских стран. 30 мая 2019. Атырау: Атырауский университет нефти и газа им. Сафи Утебаева, 2019. С. 99–104.

7. Ibrahimov B. G., Humbatov R. T., Ibrahimov R. F. Analysis performance multiservice telecommunication networks with using architectural concept future networks // T-Comm. 2018. Vol. 12. No. 12. pp. 84–88.

8. Ибрагимов Б. Г., Гасанов А. Г., Алиева А. А., Исаев А. М. Исследование показателей качества функционирования мультисервисных телекоммуникационных сетей на базе архитектурной концепции будущих сетей // Надежность и качество сложных систем. 2019. № 1 (25). С. 88–95.

УДК 004.056.53
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ АТАК И МЕТОДОВ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ ПРИ АУТЕНТИФИКАЦИИ ПО ПРОТОКОЛУ 802.1X

Г. Т. Абраменко, А. А. Миняев, Д. О. Храмцов

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

В данной статье рассматриваются принципы работы стандарта IEEE 802.1x, а также возможные DoS-атаки: EAPOL-Start, EAPOL-Logoff, EAP-Failure, EAP-Success, которые может реализовать активный нарушитель, описанный в нормативно-правовых актах. Определяются методы защиты от представленных атак и исследуются способы их реализации на оборудование различных производителей, таких как TP-LINK, ASUS.

беспроводные сети, атаки на беспроводные сети, WPA2-Enterprise, Radius, 802.1x, DoS, отказ в обслуживании, методы защиты.

В настоящее время всё чаще применяется технология беспроводного доступа в Интернет. Крупные государственные и частные компании из различных отраслей, образовательные учреждения, имеющие зачастую большой список работников, вместо проводной корпоративной сети используют беспроводную. Самым распространённым способом является передача данных с помощью Wi-Fi сетей, что позволяет работникам подключаться в любой точке зоны действия. Для выполнения контролируемого доступа к сети используется RADIUS сервер, который предназначен для обеспечения централизованной аутентификации, авторизации и учёта пользователей [1]. Однако, существуют проблемы безопасности, связанные с использованием сетей семейства стандартов IEEE 802.11. Рассмотрев данные по отчетам Kasperky можно сказать о том, что с каждым годом количество угроз увеличивается. По диаграмме можно заметить, что общее количество DDoS-атак выросло в 1,5 раза по сравнению с 2020 и 2019 годами соответственно (см. рис. 1).

В рамках данной работы рассматривается наиболее распространенный тип построения корпоративной сети. Для исследуемой информационной системы актуальным является внешний нарушитель, не имеющий доступ в контролируемую зону и к средствам вычислительной техники. Схема организации сети представлена на рис. 2 (см. ниже). В ней есть два клиента: один из которых подключен через сетевой кабель, а другой по беспроводной сети. Установлена точка доступа, на которой включен режим WPA2-

Enterprise. Злоумышленник, который отправляет фальшивые сообщения по беспроводной сети, установленный RADIUS сервер на операционной системе на ядре Linux и системный администратор, который следит за беспроводным трафиком с помощью анализатора трафика [2].

Рис. 1. Диаграмма DDoS-атак за 2019 и 2020 года согласно исследованиям Kaspersky

Рис. 2. Исследуемая модель беспроводной корпоративной сети

Корпоративные сети с шифрованием WPA2-Enterprise строятся на аутентификации по протоколу 802.1x через RADIUS-сервер. Протокол 802.1x (EAPOL) определяет методы отправки и приема запроса данных аутентификации и обычно встроен в операционные системы и специальные программные пакеты.

802.1x предполагает три роли в сети:

– клиент (supplicant) – клиентское устройство, которому нужен доступ в сеть;

– сервер аутентификации (RADIUS сервер);

– аутентификатор – устройство (маршрутизатор, коммутатор, точка доступа, беспроводной контроллер), которое соединяет множество клиентских устройств с сервером аутентификации и отключает/подключает клиентские устройства.

Для организованной сети была предложена следующая методика для тестирования беспроводной сети:

1. АРМ атакующего (kali linux);
2. АРМ тестирования (kali linux);
3. Анализатор трафика (wireshark);
4. Перехват пакетов с помощью анализатора трафика;
5. Формирование большого количества пакетов и отправка их;
6. Обработка результатов и принятие решения.

На рис. 3 показан принцип работы протокола 802.1x, а также смоделированные DoS атаки: EAPOL-Start, EAPOL-Logoff, EAP-Failure, EAP-Success по Mitre att&ck matrix, которые состоят из одной тактики и техники: TA0043(Reconnaissance)/T1595(Active Scanning)/Pre-compromise.

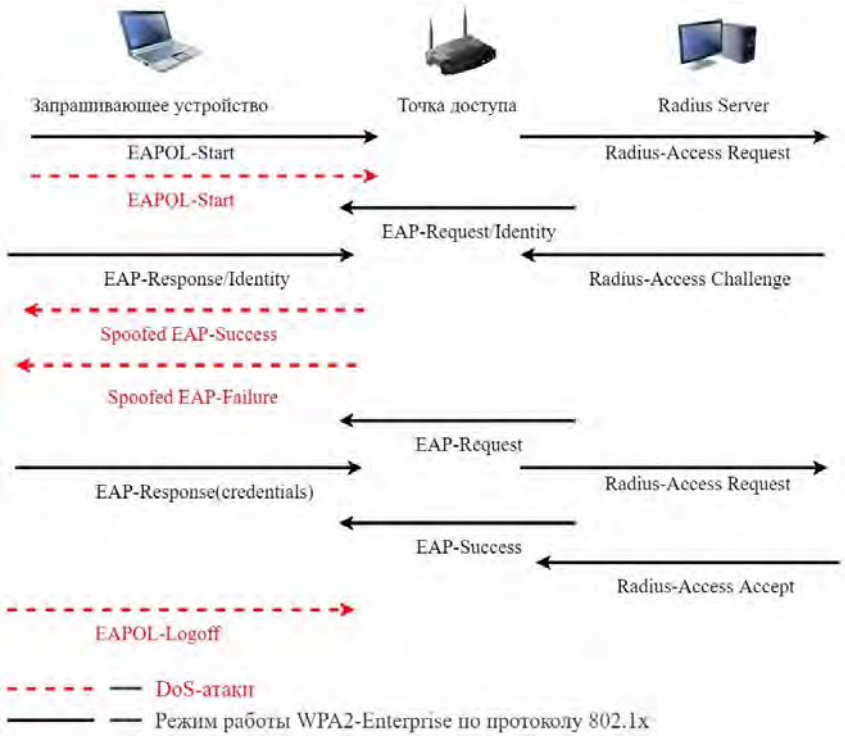


Рис. 3. Схема работы WPA2-Enterprise 802.1x

На двух точках доступа: TP-Link Archer AX50, ASUS WL-520 GU исследовалось, при каком количестве пакетов в секунду запрашивающее

устройство не может аутентифицироваться. Результаты представлены в таблице.

ТАБЛИЦА. Количество пакетов, отправленных в секунду, необходимых для успешной DoS атаки

Точка доступа	EAPOL Logoff, количество пакетов в секунду	Premature EAP-Success, количество пакетов в секунду	Premature EAP-Failure, количество пакетов в секунду	EAPOL Start, количество пакетов в секунду
ASUS WL-520GU	1	5	10	1
TP–LINK Archer AX50	1	1	5	1

Для данных DoS атак существуют следующие механизмы защиты [3, 4]:

1. В настройках маршрутизатора можно устанавливать канал, на котором будет вещаться Wi-Fi сеть.

2. Используется фильтрация MAC-адресов. При фильтрации подключиться к сети могут только устройства, MAC-адреса которых администратор внес в таблицу доверенных на точке доступа.

3. Рекомендуется выбирать оборудование беспроводной сети, поддерживающее стандарт 802.11w. Данный стандарт обеспечивает защиту управляющего трафика между клиентом и точкой доступа.

4. Внедрение WIPS [5]. Это система, которая осуществляет мониторинг окружающего радиоэфира с помощью сенсоров. Они анализируют полученную информацию об источниках радиосигнала, их взаимодействиях и аномальных (необычных) активностях и предотвращает действия, противоречащие настроенной политике предотвращения вторжений.

В заключение можно сказать, что при выполнении работы рассмотрены механизмы защиты от DoS атак, смоделированных по Mitre att&ck matrix, смоделирована типовая корпоративная среда, использующая беспроводные технологии по протоколу 802.1x, а также разработана методика тестирования для проверки корпоративной сети на уязвимости.

Список используемых источников

1. Ковцур М. М., Поляничева А. В. Исследование механизма авторизации пользователей для доступа к IP-ТВ сервисам с применением RADIUS-сервера // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 466–471.

2. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в

науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 24–28.

3. Александрова Е. С., Иванов Г. Н., Ковцур М. М. Анализ механизмов защиты Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 47–51.

4. Казаков Д. Б., Красов А. В., Лоханько Н. О., Подоляк Р. С. Методика защиты сети связи от DDoS атак с помощью BGP FLOWSPEC // 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. 386–390.

5. Зуев И. П., Карельский П. В., Ковцур М. М., Юркин Д. В. Разработка методики проведения испытания IPS модулей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 492–496.

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

УДК 621.391.1
ГРНТИ 49.43.01

ОБЗОР ОСНОВНЫХ ПОНЯТИЙ ИНВАРИАНТНОСТИ В СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ

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

Сибирский государственный университет телекоммуникации и информатики

В статье приведены основные понятия об инвариантности. Рассмотрены формы инвариантности в системах автоматического регулирования, которые отличаются условиями и методами достижения инвариантности. Описана инвариантная система передачи данных. Обозначена роль и значение инвариантных систем в современных системах, устройствах и сетях телекоммуникации.

инвариант, инвариантность, инвариантная система, помехоустойчивость, вероятность ошибки.

Слова «инвариант», «инвариантный» в переводе означают «неизменяющийся». Эти термины первоначально использовались в математике, причем инвариантом называется величина (или математическое выражение, формула), характеризующая некоторый математический или физический объект и не изменяющаяся при определенных преобразованиях его [1, 2].

Например, дисперсия $D(\xi)$ случайной величины ξ не изменяется от прибавления к последней произвольной постоянной величины a, следовательно, величина $D(\xi)$ является инвариантом преобразования вида $\xi + a$. Последнее утверждение можно представить лаконичными записями

$$D(\xi) = in \operatorname{var}(\xi + a) \quad (1)$$

или

$$D(\xi) = in \operatorname{var} a, \quad (2)$$

которые читаются следующим образом: «величина $D(\xi)$ является инвариантом преобразования $\xi + a$» или «$D(\xi)$ инвариантно к воздействию a». В последнее время понятие инвариантности все чаще используется в технических науках для определения свойства устойчивости, нечувствительности технических систем к случайным изменениям их параметров и к различным мешающим воздействиям [1, 2].

В современной теории автоматического регулирования вопросы, вязанные с инвариантностью, занимают одно из центральных мест [1, 2].

Под инвариантностью понимается способность системы автоматического регулирования противостоять мешающим воздействиям. И роли инварианта выступает здесь величина управляющего воздействия по одной из координат (или просто управление). Если управление по некоторой координате не зависит от мешающего о действия, то система автоматического регулирования называется инвариантной [3].

Различают несколько форм инвариантности в системах автоматического регулирования, отличающихся условиями и методами достижения инвариантности.

1. Первая форма предполагает существование двух каналов передачи воздействия, причем воздействие по второму, искусственно введенному каналу компенсирует воздействие по первому каналу. Условием достижения первой формы инвариантности является (помимо существования двух каналов) возможность получения равного нулю суммарного коэффициента передачи по мешающему воздействию от точки приложения воздействия до регулируемой координаты [4].

2. Вторая форма инвариантности связана с использованием глубокой отрицательной обратной связи. Если величина управляющего сигнала по некоторой координате известна, то отклонения от нее, вызванные мешающим возмущением, можно компенсировать при помощи специальной цепи обратной связи. При весьма большом коэффициенте усиления в цепи любые отклонения практически полностью компенсируются [4].

3. Третья форма инвариантности в системах автоматического регулирования достигается при одноканальной передаче возмущения к точке управления путем создания цепи с равной нулю передаточной функцией

для возмущения. Создание подобной цепи возможно только при априорно известной форме возмущающего воздействия [4].

Наряду с инвариантными системами автоматического регулирования существуют и инвариантные системы передачи данных.

Следует сразу же отметить, что термин «инвариантная система» требует доопределения, а именно: необходимо указать, какая числовая характеристика системы является инвариантом и относительно каких преобразований или воздействий. В случае системы связи в роли мешающих воздействий выступают помехи, а характеристикой системы, которая должна быть инвариантом помех, является ее помехоустойчивость, выраженная количественно, например, через вероятность ошибки, если речь идет о системах передачи дискретных сообщений. Термин помеха здесь понимается весьма широко и обозначает не только всевозможные шумы, складывающиеся с полезным сигналом, но и все случайные изменения характеристик и параметров канала связи и сигнала, оказывающие влияние на помехоустойчивость [1, 4, 5].

Систему передачи данных, количественная характеристика помехоустойчивости которой является инвариантом определенного класса помех, будем называть инвариантной по отношению к данным помехам. Это определение инвариантной системы передачи данных можно представить в математической форме [6], аналогичной формулам (1) или (2). Если обозначить через P некоторую количественную характеристику помехоустойчивости связи, например, вероятность ошибки, а через Ξ – множество реализаций рассматриваемой помехи, то в системе, инвариантной к помехе Ξ,

$$P = in \operatorname{var} \Xi. \qquad (3)$$

Запись вида (3) довольно часто используется далее, причем в левой части равенства всегда стоит числовая характеристика помехоустойчивости дайной системы передачи данных, а справа – обозначение помехи, по отношению к которой эта характеристика является инвариантом.

Следует специально отметить отличия в проблематике инвариантных систем передачи данных по сравнению с инвариантными системами автоматического регулирования [2].

В системах автоматического регулирования мешающие воздействия и управляющие сигналы , как правило, пространственно разделены (во всяком случае в рамках, изученных в теории инвариантности ситуаций). Это позволяет измерять мешающее воздействие (даже если оно является случайным) и применять всевозможные компенсационные методы реализации инвариантности.

В системах передачи данных полезный сигнал и помеха действуют в одной и той же точке (например, на входе приемника) и, как правило,

принципиально не могут быть полностью разделены, иначе проблема борьбы с помехой и не существовала бы! В системах передачи данных всегда имеется смесь сигнала с помехой (в частности, аддитивная). Вследствие этого в системах передачи данных, как правило, невозможно или затруднительно использовать компенсационные методы подавления помех, и проблема достижения инвариантности решается другими способами, не характерными для систем автоматического регулирования [2].

Другая особенность проблематики инвариантности систем передачи данных состоит в том, что в роли инварианта здесь выступает не мгновенное значение выходной величины, а некоторая ее статистическая характеристика, например, математическое ожидание. Примером может служить вероятность ошибки, являющаяся математическим ожиданием частности ошибок.

Теперь возникает вопрос, существуют ли инвариантные системы передачи данных и не противоречит ли принцип инвариантности нашим интуитивным представлениям о том, что полностью избавиться от помех невозможно.

Рассмотрим роль и значение инвариантных систем в современных системах, устройствах и сетях телекоммуникаций.

К современным системам передачи данных предъявляются довольно жесткие требования по помехоустойчивости. В системах передачи дискретных сообщений эти требования обычно задаются в виде предельно допустимых значений вероятности ошибки. Требуемое значение вероятности ошибки зависит от вида передаваемой информации и в современных системах колеблется от 10^{-2} до 10^{-6}. Например, при передаче речевых сигналов в дискретной форме вероятность ошибки не должна превосходить 10^{-2}, при передаче телеграфных сигналов – 10^{-4}, при передаче цифровой информации – 10^{-6}. Если вероятность ошибки превышает указанные допустимые значения, то передача соответствующего вида сообщений становится невозможной из-за недопустимо низкого качества, а иногда и вредной, так как могут быть приняты ошибочные решения [2].

В канале связи с постоянными характеристиками вероятности ошибки является постоянной величиной, и, следовательно, можно заранее спроектировать систему так, чтобы ее помехоустойчивость удовлетворяла заданным требованиям.

В каналах связи с переменными характеристиками вероятность ошибки является переменной величиной (неоднородный канал связи). В этом случае, если даже удается обеспечить среднее значение вероятности ошибки ниже заданной допустимой величины, в отдельные интервалы времени вероятность ошибки становится больше допустимого значения. Более того, в нестационарном канале связи, в отличие от стационарного, уменьшение средней вероятности ошибки не свидетельствует однозначно об улучшении

качества функционирования системы. Если, например, наряду с уменьшением средней вероятности ошибки увеличился процент случаев, когда вероятность ошибки больше допустимой, то следует считать, что помехоустойчивость системы не увеличилась, а уменьшилась. Отсюда, в частности, следует, что оптимизация системы передачи данных критерию минимума средней вероятности ошибки не обеспечивает наилучшего качества работы реальных систем в каналах с переменными характеристиками [4].

Таким образом, для обеспечения приемлемого качества работы реальной системы передачи дискретных сообщений в канале с переменными характеристиками необходимо поддерживать вероятность ошибки на уровне, не превышающем некоторой заданной допустимой величины. Эта задача может считаться выполненной, если:

– вероятность ошибки, меньше заданной и остается неизменной, несмотря на наличие помех, вызывающих нестационарность канала связи;

– вероятность ошибки под влиянием помех, вызывающих нестационарность канала, меняется произвольно в области значений, меньших заданного, и не превосходит этого значения ни при каких изменениях характеристик канала связи [6].

В обоих случаях можно говорить, что заданное качество функционирования системы достигается благодаря неизменности вероятности ошибки, ее независимости (полной в первом случае и частичной во втором) от тех причин, которые вызывают нестационарность канала связи. Для обозначения этого свойства уместно использовать термин «инвариантность».

Таким образом, потребность в инвариантных системах передачи данных вызывается необходимостью обеспечения заданного качества передачи сообщений в канале с переменными характеристиками [7].

Список используемых источников

1. Петрова Б. Н., Солодникова В. В., Топчеева Ю. И. Современные методы проектирования систем автоматического управления (раздел первый с библиографией). М.: Машиностроение, 1967. 703 с.

2. Чинаев П. И. Самонастраивающиеся системы / Справочник под ред. П. И. Чинаева. Киев: Наукова думка, 1969. 528 с.

3. Павлов И. И., Макаров В. А. Система управления цифровой радиорелейной системы Pasolink Neo // Материалы российской научно-технической конференции «Информатика и проблемы телекоммуникаций». Новосибирск, 2011. Секция 8. 276 с.

4. Окунев Ю. Б., Яковлев Л. А. Широкополосные системы связи с составными сигналами. М.: Связь, 1968. 167 с.

5. Павлов И. И. Модель сервисной логики (модуль SLU) // Материалы российской научно-технической конференции «Современные проблемы телекоммуникации». Новосибирск, 2012. Секция 4. 79 с.

6. Павлов И. И. Архитектура платформы RTB // Материалы российской научно-технической конференции «Современные проблемы телекоммуникации». Новосибирск, 2012. Секция 4. 78 с.

7. Applebaum S. Adaptive arrays // IEEE Transactions on Antennas and Propagation. 1976. 24 (5). pp. 585–598.

УДК 004.051
ГРНТИ 20.53.23

ВЛИЯНИЕ ТИПОВ ШИФРОВАНИЯ VPN-СОЕДИНЕНИЯ НА СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ ПО ФИЗИЧЕСКОМУ КАНАЛУ

Е. М. Аленников, Н. Н. Васин, А. Ю. Субботская

Поволжский государственный университет телекоммуникаций и информатики

При формировании VPN-туннеля создается логический канал между двумя или несколькими участками сети поверх физического соединения. Это создает дополнительную нагрузку на маршрутизаторы, что приводит к снижению их производительности. В работе проведено исследование влияния VPN-туннеля на пропускную способность канала.

Virtual Private Network, GNS3, VirtualBox, IPSec, пользовательская VPN.

VPN (*Virtual Private Network* – виртуальная частная сеть) – это защищенное соединение – туннель, на одном конце которого компьютер, а на другом – VPN-сервер. VPN-туннель может использоваться, например, для объединений филиалов и офисов компаний, для соединения дата-центров, а также удаленного подключения сотрудника к сети предприятия [1].

Для создания защищенных VPN-туннелей используется протокол ISAKMP (*Internet Security Association and Key Management Protocol*). Для защиты данных, которые будут передаваться по туннелю, протокол ISAKMP настраивается как для IPSec-туннеля, так и для пользовательской VPN. При настройке данного протокола прописываются такие параметры как: алгоритм шифрования (*3des, aes*), алгоритм аутентификации (*md5, sha*), ключ, версия алгоритма Диффи-Хеллмана (используется 1,2 и 5), время жизни туннеля [2].

Рассмотрено два вида туннелирования:

– пользовательский VPN (настраивается только маршрутизатор сервера;

– для доступа клиента к серверу используются специальные программы);

– IPSec – Internet Protocol Security (создается туннель между двумя аналогично настроенными маршрутизаторами) [3].

Для проведения тестов используются две схемы сети, собранные на основе эмулятора сети GNS3. Клиентская часть реализована с помощью VirtualBox [4] с ОС Windows7, а FTP-сервер настроен на физическом ПК.

На первой схеме сети (рис. 1) настроены *IPSec*-туннели: между маршрутизаторами *R1* и *R2* с шифрованием *3des* и хешированием *md5*, между *R3* и *R2* с шифрованием *aes* и хешированием *md5*. Затем меняется тип хеширования на *sha*. Также между всеми маршрутизаторами настроен *OSPF* протокол маршрутизации [5].

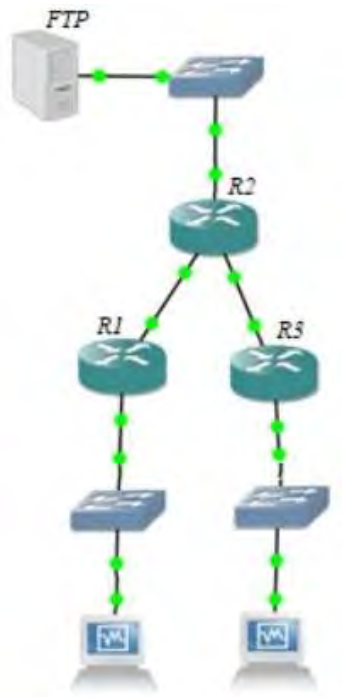


Рис. 1. Схема сети с *IPSec*-туннелем

На второй схеме сети (рис. 2) настроена пользовательская VPN с типами шифрования *3des, aes* и хеширования *md5, sha*. Для подключения клиента к серверу через VPN используется программа VPN Access Manager, данная программа необходима для подключения клиентов к удаленному шлюзу. Между всеми маршрутизаторами настроен протокол OSPF [5].

На каждой схеме проведено по два теста:

Первый тест включает в себя тесты скорости при помощи программы TamoSoft Throughput Test – это утилита, которая посылает TCP- и UDP-потоки данных между клиентом (*Tamosoft Client*) и сервером (*Tamosoft Server*) и отображает текущую скорость передачи данных. Данная программа устанавливается на каждый ПК в схеме: на одном из ПК – Tamosoft Server, а на другом – Tamosoft Client. Tamosoft Server ожидает соединения от Tamosoft Client, как только клиент посылает на сервер сгенерированные программой пакеты, сервер принимает их, обрабатывает и отправляет ответ. Получив ответ, Tamosoft Client показывает среднюю скорость передачи пакетов [6].

Второй тест включает в себя скачивание реального файла с FTP-сервера. Для этого заранее был загружен на FTP-сервер архив весов 574 Мбайта. При загрузке этого файла с ПК клиента скорость передачи можно посмотреть в браузере в разделе «Загрузки».

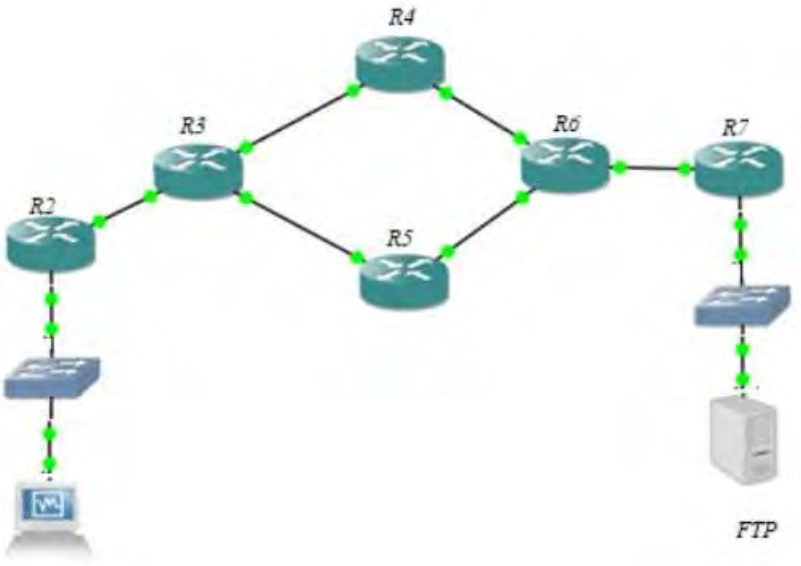


Рис. 2. Схема сети с пользовательской VPN

На рис. 3 приведен результат теста при настроенном типе шифрования *3des* и хеширования *sha* на схеме 1. На графике показаны изменения скоростей передачи TCP и UDP пакетов в направлениях клиент-сервер (*Upstream*) и сервер-клиент (*Downstream*): по оси *X* откладывается значение времени между отправлением и приемом пакета, по оси *У* – значение скорости в Мб в соответствующий момент времени. Так как графики имеют неравномерный характер (в разные моменты времени наблюдаются разные значения скоростей), то для нашего исследования мы брали среднее значение скорости (указанное в скобках с пометкой “*Ave*”) на данный момент соединения. Главным параметром, который анализировался в данной работе, является значение в поле TCP Down, так как именно оно показывает среднюю скорость сети у клиента.

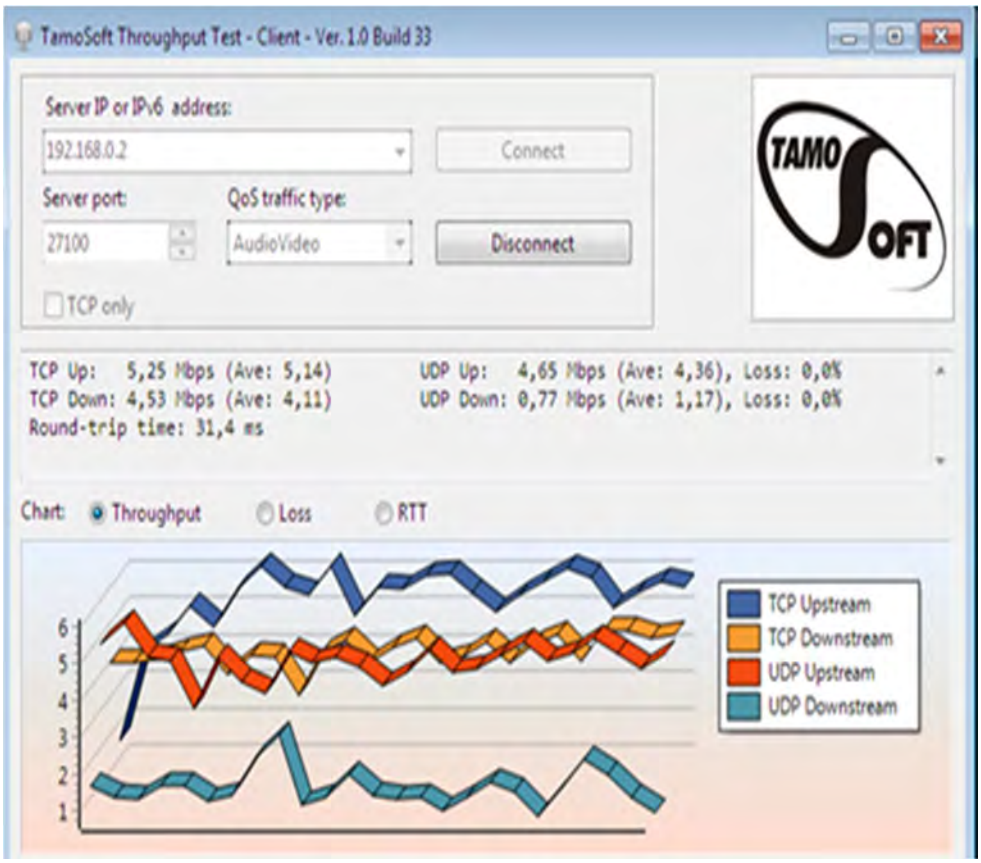


Рис. 3. Результаты теста при настроенном типе шифрования *3des* и хеширования *sha* на схеме 1

Данные тесты повторялись для каждого типа шифрования и хеширования, а также в схемах без настроенных VPN-туннелей, результаты тестов сведены в таблицу 1 и таблицу 2.

ТАБЛИЦА 1. Скорости передачи пакетов через TamoSoft Throughput Test

	3des/sha	*3des/md5*	*aes/sha*	*aes/md5*
Скорость в пользовательской VPN, Мб/с	11,64	12,60	12,78	12,85
Скорость в IPSec-туннеле, Мб/с	4,11	5,26	3,79	6,31
Скорость без VPN-туннеля, Мб/с	11,43			

ТАБЛИЦА 2. Скорости передачи пакетов при загрузке файла с FTP-сервера

	3des/sha	*3des/md5*	*aes/sha*	*aes/md5*
Скорость в пользовательской VPN, Мб/с	1,10	1,00	1,01	1,06

	3des/sha	*3des/md5*	*aes/sha*	*aes/md5*
Скорость в IPSec-туннеле, Мб/с	0,55	0,48	0,70	0,79
Скорость без VPN-туннеля, Мб/с	1,08			

Значения скоростей для наглядности приведены в виде столбчатой диаграммы (рис. 4). По ней видно, что самые высокие показатели скорости у пользовательской VPN при использовании программы TamoSoft Throughput Test; самые низкие – у IPSec-туннеля при загрузке файла с FTP-сервера. Лучшим сочетанием шифрование/хеширование является *aes/md5*, так как оно показывает самые высокие скорости передачи разных типов трафика.

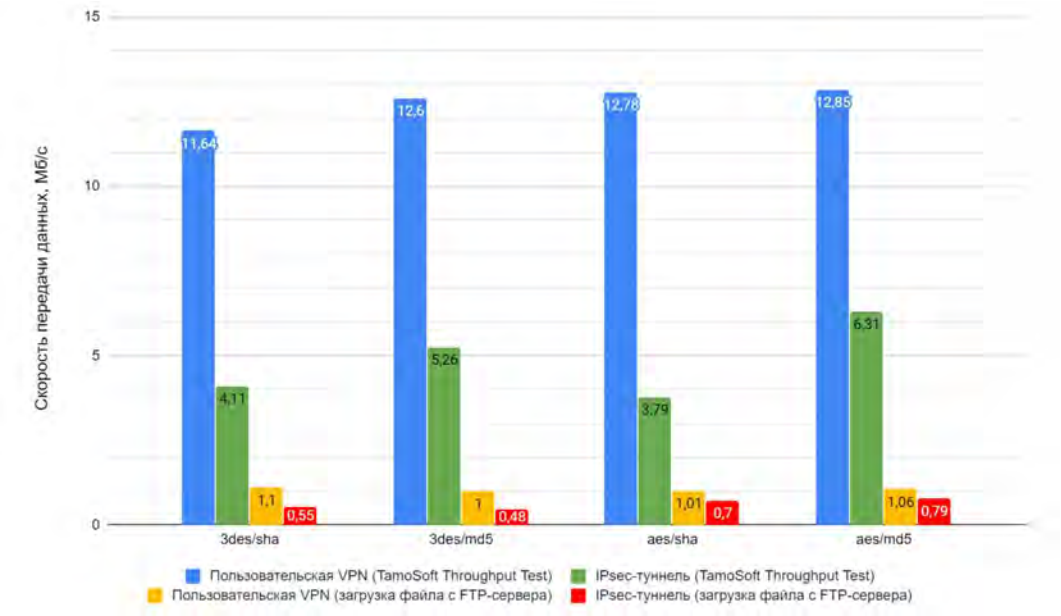


Рис. 4. Скорости передачи разных типов трафика при различных комбинациях шифрование/хеширование

По результатам первого теста можно сделать вывод, что скорость передачи искусственно сгенерированных пакетов по сети с пользовательской VPN в 2–3 раза превышает скорость по сети с настроенным IPSec-туннелем. Второй тест показал, что в любой схеме скорость передачи реального файла в 10 раз ниже, чем скорость передачи пакетов, сгенерированных программой TamoSoft Throughput Test. Также видим, что скорость в схеме с IPSec-туннелем в 2 раза ниже, чем в схеме с пользовательской VPN. Вышеперечисленные выводы справедливы для всех типов шифрования и хеширования, рассмотренных в данной работе. Также отметим, что лучшие показатели скорости предоставляет сочетание *aes/md5*. Наиболее предпочтительно

использовать его в *IPsec*-туннеле, потому что в обоих тестах данная комбинация даёт выигрыш в скорости в 1,5 раза.

Пользовательская VPN в обоих тестах не уступает в скорости каналу связи без VPN-туннеля, а при генерации пакетов с помощью TamoSoft Throughput Test скорость передачи пакетов по VPN-туннелю выше на 1 Мб/с. Это объяснимо тем, что данный вид туннелирования применяется именно для пользователей, которым важна скорость интернет-соединения, а не для организаций, где во главу угла ставится безопасность соединения.

По IPSec-туннелю скорость в 2–3 раза ниже, чем по каналу без VPN-туннеля. Так как данный вид туннелирования применяется в основном для объединения филиалов одной компании в единую сеть, то акцент в организации туннеля делается больше на безопасности, чем на скорости. Поэтому такая разница исследуемых значений по сравнению с пользовательской VPN логична.

Список используемых источников

1. Егоров А. Н., Журавлев А. Е., Базунов А. А., Румянцев О. В. Моделирование компьютерных сетей: учебно-методическое пособие. СПб.: Изд-во ГУМРФ имени адмирала С. О. Макарова, 2015. URL: https://studfile.net/preview/5851940/page:35/

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 876 с.

3. Настройка IPsec на маршрутизаторах Cisco. URL: http://xgu.ru/wiki/IPsec_%D0%B2_Cisco

4. Oracle VM VirtualBox. 2016. URL: https://www.virtualbox.org

5. Васин Н. Н. Технологии пакетной коммутации: Учебник. СПб. : Лань, 2019. 196 с.

6. TamoSoft Throughput Test. 1998–2021. URL: https://www.tamos.ru/products/throughput-test/

Статья представлена заведующим кафедрой ССС ПГУТИ, доктором технических наук, профессором А. В. Росляковым.

УДК 654.739
ГРНТИ 49.33.29

АНАЛИЗ ПОКАЗАТЕЛЕЙ ПРОПУСКНЫХ СПОСОБНОСТЕЙ МУЛЬТИСЕРВИСНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА БАЗЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ

А. А. Алиева[1], **Б. Г. Ибрагимов**[2], **Ф. В. Мамедова**[2]

[1]Мингечаурский государственный университет
[2]Азербайджанский технический университет

Проанализированы показатели эффективности функционирования мультисервисных телекоммуникационных сетей, построенных в соответствии с архитектурными концепциями NGN (Next Generation Networks) и FN (Future Networks). На основе исследования предложен новый подход к построению математической модели с учетом свойства самоподобия передаваемого трафика для оценки показателей пропускной способности мультисервисных телекоммуникационных сетей на базе инновационных технологий. На базе модели получены аналитические выражения для анализа вероятностно-временных характеристик сетей связи при оказании мультимедийных услуг.

пропускная способность, SDN, самоподобие трафика, мультимедийные услуги, NFV, мультисервисная сеть, канальные ресурсы, управление трафика.

Настоящий период развития нового сектора единого информационного пространства и единой многооператоской среды на основе архитектурных концепций сети следующего NGN (*Next Generation Networks*) и будущего FN (*Future Networks*) поколения требует построения мультисервисных телекоммуникационных сетей с использованием инновационных технологий построения распределенных сетей связи [1, 2].

Концепция и архитектура NGN и FN на базе технологии построения распределенных сетей связи обеспечивает переход на IP-стандарт (ITU-T, Y.1542 и Y.3001) и рост доходов операторов связи за счет предоставления широкого спектра телекоммуникационных основных, дополнительных и интеллектуальных новых услуг [3, 4].

Одной из наиболее важных задач является эффективное распределение и управление канальными ресурсами в узлах мультисервисных телекоммуникационных сетей с повышенной пропускной способностью и поддержка качества мультимедийных услуг и приложения. При этом, в первую очередь необходимо улучшить показатели надежности функционирования и информационной безопасности, а также показатели вероятностно- временных характеристик доступа к любым мультимедийным услугам.

На основе исследования установлено [1, 2, 3, 4, 5], что широкое использование инновационных технологий и внедрения многообразных мультимедийных услуг, бурное развитие сетей Internet, появление центров обработки данных, массовое внедрение мобильных систем 5G/IMT-2020 и приложений, требуют высокой пропускной способности и передовых технологий высокоскоростной передачи потоков пакетов полезного и служебного трафиков.

Для построения мультисервисных телекоммуникационных сетей с повышенной пропускной способностью на базе инновационных технологий, в настоящее время на первый план выходит способность этих технологий обеспечить заданное качество обслуживания QoS (*Quality of Service*) и воспроизведение QoE (*Quality of Experience*) при передаче потоков пакетов трафика мультимедийных услуг и приложенй. К таким технологиям, обладающим данными характеристиками [3, 4, 5], необходимо в первую очередь отнести программно-конфигурируемые сети SDN (*Software-Defined Networking*), асинхронный режим передачи ATM (*Asynchronous Transfer Mode*), спектральный WDM/DWDM (*Wavelength Division Multiplexing/Dense* WDM) технологии, подсистемы IMS (*Internet Protocol Multimedia Subsystem*), многопротокольные коммутации меток MPLS (*Multi-Protocol Label Switching*), виртуализацию сетевых функций NFV(*Network Functions Virtualization*).

Проведенный анализ [2, 3] и опубликованные работы при исследовании мультисервисных телекоммуникационных сетей показали [4, 5], что в ранее проведенных исследованиях данной тематике уделялось недостаточное внимание.

В данной работе рассматривается решение выше сформулированной задачи – исследование и анализ нового подхода к построению модели для оценки показателей эффективности функционирования мультисервисных телекоммуникационных сетей, построенной в соответствии с концепцией сети NGN и FN.

Для решения поставленной задачи предлагается новый подход к построению математической модели (ММ) оценки эффективности функционирования мультисервисных телекоммуникационных сетей на базе концепции сети NGN и FN, использующих инновационные технологии SDN, IMS и NFV. Исследуемые модели учитывают характер передаваемого информационного потока пакетов λ_i, наличие множества канальных ресурсов $\eta_k(t)$ и свойства самоподобия трафика H.

Системно-технический анализ показал [4, 6], что исследуемые мультисервисные телекоммуникационные сети связи представляют собой непрерывный стохастический процесс и являются сложными объектами анализ которых требует учета большого количества параметров.

Непрерывный стохастический процесс $X = \{X(t), t > 0\}$, считается статистически самоподобным с параметром Херста H, $0{,}5 \le H \le 1$, если для любого положительного числа a, процессы $X(t)$ и $a^{-H} \cdot X(at)$ будут иметь идентичные распределения, где H – параметр Херста, a –положительное число и $0 < a \le 2$. Здесь параметр Херста показывает степень самоподобности передаваемого полезного и служебного трафика [6].

На основе исследования установлено [4, 7], что рассматриваемые мультисервисные сети связи представляют собой систему массового обслуживания (СМО), которая по кодировке Башарина-Кендалла, соответствует общему типу $M/G/1/N_{бн}$ с одним обслуживающим аппаратно-программным комплексом и терминальным сервером.

Допустим, что входящий поток пакетов в систему обслуживания имеет пуассоновские законы распределения с параметром λ_i, длительность обслуживания i-го трафика имеет произвольную функцию распределения $B(t)$ с моментами b_i. Здесь, предполагаем, что при критической загрузке $\rho_i = (\lambda_i \cdot b_i) \le 1$, $i = \overline{1,n}$ в системе число мест для ожидания ограничено $N_{бн}$.

Тогда, изучаемая ММ представляет собой одноканальную систему массового обслуживания общего типа $M/G/1/N_{бн}$ с ограниченными очередями.

Проведенный анализ показал [4, 7], что важным и полноценным критерием, исследуемых характеристик эффективности функционирования мультисервисных телекоммуникационных сетей является пропускная способность аппаратно-программных комплексов и терминальных серверов. Пропускная способность сети определяется максимальным количеством передаваемых потоков пакетов трафиков в единицу времени в условиях заданной надежности функционирования и информационной безопасности, которые функционально описываются следующей зависимостью:

$$C_{\max}(\lambda_i, H) = W[V_k(\lambda_i), B(\lambda_i, H), \eta_k(\Delta F, t), \quad i = \overline{1,n}, \tag{1}$$

где $\eta_k(\Delta F, t)$ – коэффициент эффективного использования канальных ресурсов частотный полосы пропускания ΔF с учетом требования от условия обслуживания потоков пакетов трафика в момент времени t;

$B(\lambda_i, H)$ – функция, учитывающая показатели вероятностно-временных характеристик сетей связи с учетом коэффициента самоподобности потоков пакетов полезного и служебного трафиков H и интенсивности поступления входящего потока λ_i при передаче потоков пакетов i-го трафика, $i = \overline{1,n}$;

$V_k(\lambda_i)$ – скорость работы аппаратно-программных средств и терминальных серверов системы с учетом интенсивности поступления входящего потока λ_i при передаче самоподобного H потоков пакетов i-го трафика, $i = \overline{1,n}$;

$C_{\max}(\lambda_i, H)$ – максимальное значение пропускной способности мультисервисных телекоммуникационных сетей связи с использованием инновационных технологий SDN, IMS и FN при оказании мультимедийных услуг и при установлении соединений.

Выражение (1) определяет сущность рассматриваемого нового подхода к построению математической модели эффективности передачи потоков пакетов полезного и служебного трафиков. Далее, предлагаемое выражение (1) характеризует комплексные показатели эффективности функционирования мультисервисных телекоммуникационных сетей на базе архитектурных концепций

NGN и FN с использованием инфокоммуникационных технологий при оказании мультимедийных [8].

На базе (1), в качестве показателя эффективности функцинирования мультисервисных телекоммуникационных сетей на базе архитектурной концепции FN выбрана пропускная способность сети связи с использованием технологий SDN, IMS и NFV.

С учетом свойств самоподобия служебного и полезного трафиков, параметров информационной безопасности системы, пропускная способность аппаратно-программных комплексов сети связи $C_{\max}(\lambda, H)$ определяется следующим образом:

$$C_{\max}(\lambda, H) = \sum_{i=1}^{n} \beta_i \cdot \frac{\lambda_i}{b_i} \cdot \frac{1}{F_{i.}(\lambda)} \cdot \frac{f(H_i)}{\mu_i}, \quad i = \overline{1,n}, \tag{2}$$

где b_i – время передачи i-го потока пакета трафика и характеризует i-й момент времени обслуживания трафика;

μ_i – параметр процесса обслуживания i-го пакета трафика;

$F_i(\lambda)$ – функция штрафа при использовании злоумышленником кибератак на коммутатор и контроллер SDN с использованием протоколов OpenFlow;

β_i – коэффициент штрафа, который определяет время задержки при обработке i-го потока пакета, $i = \overline{1,n}$;

$f(H) = 2H$ – функция, учитывающая свойство самоподобия поступающих пакетов полезного и служебного трафиков;

H – коэффициент Хэрста для потока трафика [6] и равно

$$H = 1 - 0{,}5\beta, \quad 0 < \beta < 1,$$

Выражение (2) характеризует показатели пропускных способностей системы с учетом параметров угрозы информационной безопасности в сетях связи, использующие технологий SDN, IMS и NFV с помощью которых можно предотвратить возможные кибератаки и несанкционированный доступ нелегальных пользователей.

Одним из важных показателей эффективности МТС с использованием технологий SDN, IMS и NFV является эффективное использование и распределение канальных ресурсов в узлах сети FN [4, 6] при критической загрузке СМО, $\rho_i(H) \le 1$, $i = \overline{1,n}$.

На основании данного предположения, коэффициент эффективного использования канальных ресурсов в мультисервисных телекоммуникационных сетях при обслуживании потоков пакетов i-го трафика выражается следующим образом [7]:

$$\rho_i(\lambda_i, H) = [\lambda_i / V_k(\lambda)] \cdot L_{i.n} \cdot f(H) \cdot / \mu_i \le 1, \quad i = \overline{1, n}, \tag{3}$$

где $L_{i.n}$ – длина передаваемого пакета *i*-го трафика;

$V_k(\lambda)$ – средняя скорость работы коммутатора, маршрутизатора и контроллера сети SDN с интенсивностью поступающих пакетов трафиков.

Выражение (3) является необходимым и достаточным условием существования стационарного режима СМО типа $fBM/G/1/N_{бн}$ с учетом свойства самоподобного трафика.

Учитывая (2), (3) и коэффициент загрузки узлов коммутации МТС, скорость работы аппаратно-программных средств и терминальных серверов технологии SDN, IMS и NFV с интенсивностью поступления входящего потока λ_i при передаче самоподобного *H* потоков пакетов *i*-го трафика находится следующим образом:

$$V_k(\lambda) = \sum_{i=1}^{n} f(H)[(L_{i.n} + L_{i.c}) \cdot \lambda_i / \rho_i(\lambda_i, H)], \quad H \neq 0.5, \quad i = \overline{1,n}. \qquad (4)$$

В результате исследования предложена модель эффективности функционирования сети связи с помощью которого получены аналитические выражения для оценки показателей QoS, пропускные способности аппаратно-программных комплексов и веротяностно-временных характеристик системы.

Список используемых источников

1. Семенов Ю. В. Проектирование сетей связи следующего поколения. СПб.: Наука и техника, 2005. 105 с.

2. Ibrahimov B. Q., Humbatov R. T., Ibrahimov R. F. Analysis of Performance Multiservice Telecommunication Systems Using Architectural Concept Future Networks // Proceedings of the XXI International Scientific Conference Russia on the “Distributed Computer and Communication Networks: Control, Computation, Communications” (DCCN-2018). Russian Academy of Sciences V. A. Trapeznikov Institute of Control Sciences of RAS. Moscow, 2018. pp. 379–386.

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

4. Джафарова Э. М., Ибрагимов Б. Г., Исмайлова С. Р. Анализ комплексных показателей мультисервисных телекоммуникационных сетей на базе архитектурных концепций FN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 399–404.

5. Сергеева Т. П. Повышения эффективности сетевой инфраструктуры при взаимодействии мультисервисных и оптческих транспортных сетей // Электросвязь. 2018. № 3. С. 41–47.

6. Шелухин О. И. Моделирование информационных систем. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2018. 516 с.

7. Ibrahimov B. G., Humbatov R. T., Ibrahimov R. F. Analysis performance multiservice telecommunication networks with using architectural concept future networks // T-Comm. 2018. Vol. 12, No.12. pp. 84–88.

8. ITU-T Y. 1542. Framework for achieving end to end IP performance objectives.

УДК 681.7
ГРНТИ 49.44.31

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ВОЛОКОННЫХ СВЕТОВОДОВ РАЗЛИЧНЫХ СТАНДАРТОВ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Е. И. Андреева, А. С. Калашников

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

Для передачи высококачественного видеосигнала по волоконно-оптическому кабелю необходимо подобрать параметры волоконного световода как непосредственной среды передачи таким образом, чтобы обеспечить требуемую дальность с одной стороны, и защиту от несанкционированного доступа с другой. Проведенное исследование позволяет сравнить защищенность от утечки информации системы с различными типами световодов.

волоконно-оптические сети, волоконный световод, оптические потери, изгибные потери.

Для решения конкретных задач подбираются компоненты с такими параметрами, чтобы характеристики системы в целом были оптимальны. Зачастую оптимизация системы по одному параметру сопряжена с трудностями сохранения на должном уровне других рабочих параметров. Одним из ключевых вопросов в проектировании системы видеонаблюдения является выбор типа волоконного световода как непосредственной среды передачи сигнала [1, 2, 3, 4, 5, 6, 7]. Характеристики волоконного световода должны обеспечивать и максимальную дальность линии, и защищенность передаваемых данных от несанкционированного доступа. Как правило, дальность передачи цифрового оптического сигнала определяется энергетическим бюджетом и влиянием дисперсионных эффектов.

Известно, что качественный видеосигнал сам по себе широкополосен, поэтому для передачи такого сигнала на дальнее расстояние наряду с низким уровнем энергетических потерь желательно уменьшить влияние хроматической дисперсии в световоде. В волоконно-оптических системах видеонаблюдения, как и в линиях оптической связи, наиболее часто используются стандартные волоконные световоды (SSMF, *Standard Single Mode Fiber*, стандарт G652). Одно из преимуществ этих световодов в возможности использовать спектральное уплотнение CWDM (*Coarse Wavelength Division Multiplexing*) в широком диапазоне длин волн (от 1270 до 1610 м) [4]. В то же время оптимальные параметры по потерям и дисперсии в третьем окне

прозрачности (вблизи длины волны 1550 нм) обеспечивают волоконные световоды NZDSF (*Nonzero Dispersion Shifted Fiber*) стандарта G655.

Конфиденциальность передачи данных обеспечивается защищенностью к наиболее распространенным способам перехвата информации. Наиболее доступными с точки зрения технической реализации являются методы перехвата с использованием изгиба волоконного световода и утечки оболочечных мод в непосредственной близости от передающей аппаратуры. Если защита пунктов установки активного оборудования обеспечивается, как правило, на высоком уровне, то контроль за кабельной системой на трассе оказывается более сложной задачей. Для того, чтобы минимизировать риск перехвата передаваемого сигнала методом изгиба надо правильно подобрать тип волоконного световода в оптическом кабеле.

Для прокладки в условиях, предполагающих многократные изгибы с малыми радиусами, используются световоды BLIF (*Bending Loss Insensitive Fiber*) стандарта G657. Чаще всего это касается монтажа оптического кабеля в составе системы видеонаблюдения непосредственно на объекте. Наиболее часто используются световоды типа G657.A2, так как они могут стыковаться со стандартными световодами в магистральном кабеле.

Кроме того, конфиденциальность передачи данных в системах со спектральным уплотнением осложняется возможностью перекачки части передаваемого сигнала из рабочего канала в соседние спектральные каналы вследствие нелинейных эффектов.

Целью данной работы было сравнительное исследование защищенности передаваемого видеосигнала от несанкционированного доступа по таким критериям как:

– чувствительность к изгибу световодов стандартов G652, G655 и G657.A2;

– вероятность перекачки части передаваемого сигнала в другие спектральные каналы в системах с WDM при использовании световодов стандартов G652, G655.

Для оценки чувствительности световодов к изгибу использовалась методика [1], позволяющая сравнить степень уязвимости разных спектральных каналов в системе CWDM в одномодовых световодах разных типов. Экспериментальное исследование проводилось на образцах кабеля со световодами стандартов G652, G655 и G657.A2. На рис. 1. приведены результаты ослабления передаваемого сигнала α в зависимости от рабочей длины волны λ при укладке 5 витков на оправке диаметром $d = 12{,}5$ мм одножильного оптического кабеля со световодом: 1 – NZDSF (G655), 2 – SSMF (G652), 3 – BLIF (G657.A2). Как показали исследования, волоконные световоды NZDSF (G655) имеют повышенную чувствительность к изгибу. Это может приводить к дополнительным потерям при прокладке оптического

кабеля и повышенному риску несанкционированного доступа. Для снижения вероятности этих рисков могут использоваться волоконные световоды стандартов G652D и G657, которые, как и ожидалось, продемонстрировали существенно меньшую чувствительность к изгибу. Таким образом, при необходимости осуществить передачу качественного видеосигнала на максимально большое расстояние в случае использования световодов со смещенной дисперсией необходимо более тщательно продумать вопрос конфиденциальности.

В системах со спектральным уплотнением при большом числе рабочих каналов возникают перекрестные помехи. При необходимости передачи сигнала на большое расстояние необходимо обеспечить высокую входную мощность в канале. Вследствие этого на эволюцию цифрового сигнала оказывают влияние не только линейные (потери, дисперсия), но и нелинейные эффекты. Одним из наиболее существенных нелинейных эффектов становится эффект четырехволнового смешения (FWM, *four wave mixing*). Как результат этого эффекта часть мощности из рабочих каналов может перекачиваться в каналы на комбинационных частотах. Конфиденциальность информации, передаваемой по рабочим каналам, снижается. Как показывают численные оценки [3] и результаты компьютерного моделирования в программе OptiSystem, наиболее подвержены этому эффекту световоды со смещенной дисперсией – NZDSF (G655).

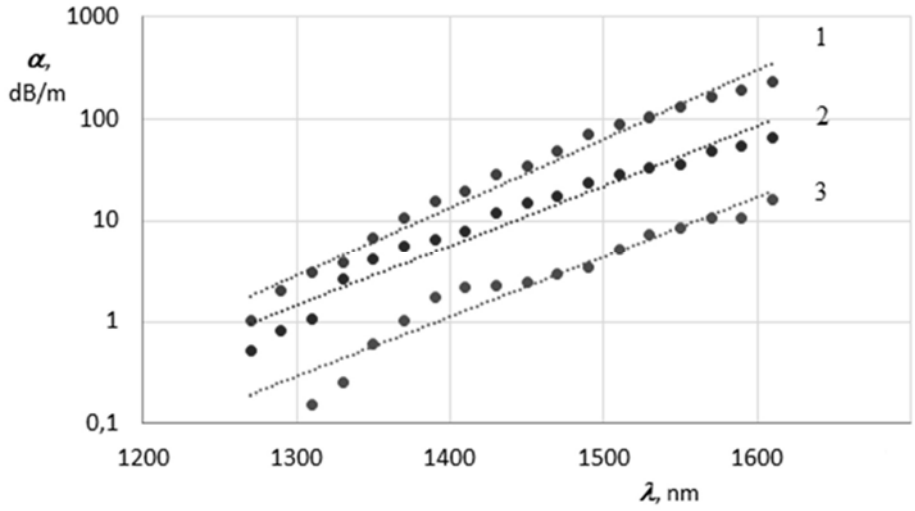
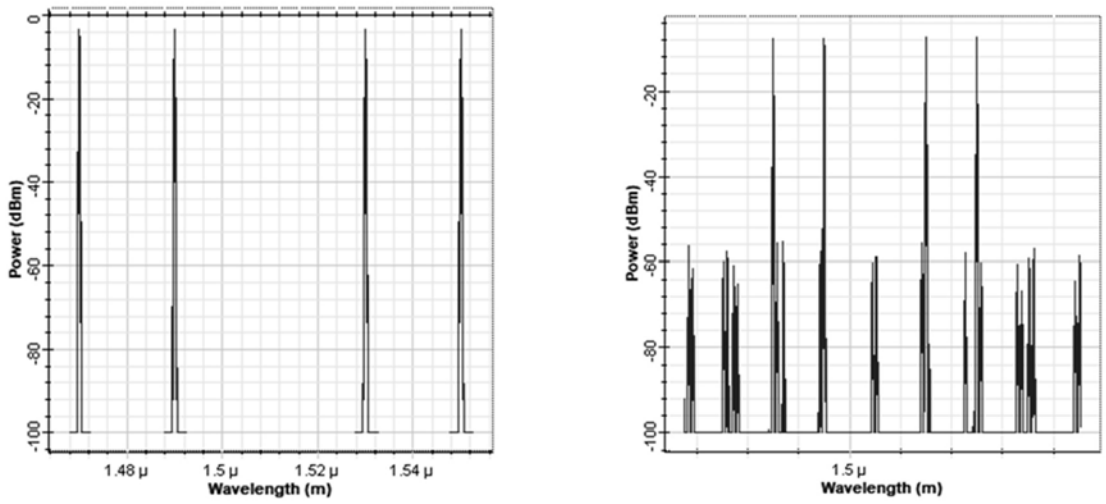


Рис. 1. Потери на макроизгибе α от длины волны λ рабочего канала для оптического кабеля с волоконным световодом:
1 – NZDSF (G655), *2* – SSMF (G652), *3* – BLIF (G657.A2)

На рис. 2 (см. на сл. стр.) представлены спектры сигналов на входе в линию (а) и после прохождения расстояния 20 км (б), соответствующего эф-

фективной длине проявления потерь, для NZDSF (G655). Стандартные световоды – SSMF (G652), характеризуются большими значениями дисперсии и меньшими значениями нелинейных коэффициентов, так как диаметр модового поля в этих световодах больше. Поэтому с точки зрения перехвата передаваемой информации световоды NZDSF (G655) оказываются более уязвимыми.

Таким образом показано, что при использовании спектрального уплотнения стандартные световоды SSMF (G652) характеризуются большей защищенностью от несанкционированного доступа, чем световоды NZDSF (G655). Экспериментально подтверждено, что волоконные световоды со смещенной дисперсией стандарта G655 отличаются повышенной чувствительностью к изгибу, вследствие чего требуют большей защищенности для исключения перехвата трафика передаваемого сигнала. Для передачи видеосигнала высокой конфиденциальности могут быть использованы специальные методы модуляции, например частотные [3], или добавляться дополнительные шумовые сигналы.



(а) (б)

Рис. 2. Результаты моделирования FWM в программе OptiSystem при использовании в качестве рабочих спектральных каналов с рабочей длиной волны λ = 1470, 1490, 1530 и 1550 нм. Сигнал на входе в линию (а) и на выходе (б) при использовании световода NZDSF (G655)

Список используемых источников

1. Андреева Е. И., Купцов В. Д., Валюхов В. П., Сумкин В. Р., Копалин К. Р. Влияние изгиба оптического кабеля в волоконно-оптических системах видеонаблюдения и абонентского доступа со спектральным уплотнением: методика // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 68–72.

2. Андреева Е. И., Купцов В. Д., Валюхов В. П., Сумкин В. Р. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 2. Тестирование // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 61–66.

3. Андреева Е. И., Купцов В. Д., Валюхов В. П. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 1. Активное оборудование // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 57–61.

4. Андреева Е. И., Валюхов В. П., Купцов В. Д., Сумкин В. Р. Система видеонаблюдения на волоконной оптике с использованием спектрального уплотнения. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 60–65.

5. Гришачев В. В. Перехват трафика в оптических сетях: информативные паразитные электромагнитные излучения // Фотоника. 2019. Т. 13. № 3. С. 280–294.

6. Купцов В. Д., Валюхов В. П. Чувствительность фотоприёмных устройств волоконно-оптических линий связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. № 6 (113). С. 31–36.

7. Андреева Е. И., Купцов В. Д., Валюхов В. П. Передача высококачественного видеосигнала по волоконно-оптической сети с CWDM // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 56–60.

УДК 004.732
ГРНТИ 49.43.29

ИССЛЕДОВАНИЕ РАБОТЫ СМАРТФОНОВ APPLE В СЕТЯХ WI-FI

А. Д. Антоненко, Р. А. Дунайцев

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

Согласно последним исследованиям, одними из наиболее популярных смартфонов являются мобильные телефоны компании Apple, работающие под управлением операционной системы iOS. Помимо сетей сотовой связи, данные устройства часто используются для подключения к беспроводным локальным сетям Wi-Fi. В статье рассмотрен алгоритм, используемый в смартфонах Apple для сканирования каналов Wi-Fi и выбора точки доступа, а также алгоритм, отвечающий за осуществление роуминга между точками доступа.

Wi-Fi, Apple, iPhone, смартфон, роуминг, точка доступа.

В настоящее время большинство жителей мегаполисов едва ли смогут обойтись без смартфона с выходом в глобальную сеть Интернет. При этом, согласно исследованиям [1], одними из наиболее популярных смартфонов являются мобильные телефоны компании Apple, работающие под управлением операционной системы iOS.

Наиболее доступным и широко распространенным способом доступа в Интернет является использование беспроводной локальной сети Wi-Fi. При обнаружении поблизости нескольких сетей Wi-Fi операционная система iOS использует алгоритм, который выбирает сеть, исходя из уровня принимаемого сигнала, категории и безопасности сети [2]. В таблице приведены приоритеты по автоматическому выбору сети Wi-Fi. При прочих равных приоритет отдается сети Wi-Fi с более высоким уровнем принимаемого сигнала (*Received Signal Strength Indicator*, RSSI).

ТАБЛИЦА. Приоритеты по выбору сети Wi-Fi

Приоритет	Категория сети	Безопасность сети
1	Частная	EAP
2	Частная	WPA3
3	Частная	WPA2/WPA
4	Частная	WEP
5	Частная	Незащищенная/открытая
6	Публичная	Hotspot 2.0/Passpoint
7	Публичная	EAP
8	Публичная	WPA3
9	Публичная	WPA2/WPA
10	Публичная	WEP
11	Публичная	Незащищенная/открытая

Для выбора точки доступа операционная система iOS сканирует все доступные каналы, посылая широковещательные кадры Probe Request (в неподключенном состоянии) или одноадресные кадры Probe Request (в подключенном состоянии) в каждый из проверяемых каналов для обнаружения точки доступа с наибольшим уровнем сигнала. В ответных кадрах Probe Response, передаваемых точками доступа, содержится информация об имени сети (*Service Set Identifier*, SSID), поддерживаемых скоростях передачи и т. п. В результате клиент может получить ответ от нескольких точек

доступа одновременно, после чего должен будет решить, к какой из них следует подключиться. Операционная система iOS пробует подключиться к сетям Wi-Fi в следующем порядке:

1) наиболее предпочтительная сеть,
2) последняя частная сеть, к которой подключался смартфон,
3) частная сеть,
4) публичная сеть.

Начиная с версии 8, операционная система iOS отправляет широковещательные кадры Probe Request, заменяя в них свой настоящий MAC-адрес на рандомизированный (так называемый «частный адрес»). В 2020 году вышла версия 14, новой функцией которой стала рандомизация MAC-адреса для каждой сети Wi-Fi (т. е. для каждого SSID) [3]. На рис. 1 приведен пример, в котором Wi-Fi роутер TP-Link вместо настоящего MAC-адреса видит рандомизированный.

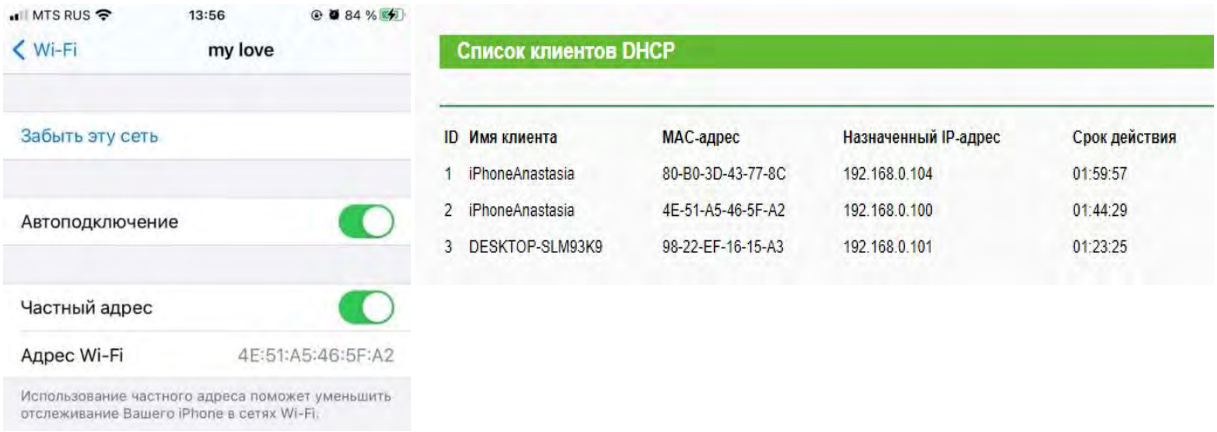


Рис. 1. Рандомизированный MAC-адрес и список клиентов, подключенных к сети Wi-Fi

Для осуществления более плавного перехода от одной точки доступа к другой в рамках одной сети Wi-Fi операционная система iOS поддерживает стандарты IEEE 802.11k, IEEE 802.11r и IEEE 802.11v [4]. Также эти стандарты поддерживает большинство производителей и поставщиков оборудования для сетей Wi-Fi корпоративного класса. Если по каким-либо причинам стандарты IEEE 802.11k/r/v не поддерживаются, то при сигнале от –70 дБм и ниже операционная система iOS начнет заново сканировать все каналы в надежде найти точку доступа с высоким уровнем сигнала. Полный алгоритм, отвечающий за осуществление роуминга между точками доступа, представлен на рис. 2 [5].

Рис. 2. Критерии выбора потенциальной точки доступа для роуминга

Список используемых источников

1. Global Smartphone Market Share: By Quarter. URL: https://www.counterpointresearch.com/global-smartphone-share/ (дата обращения 31.03.2021).

2. Порядок выбора iOS беспроводной сети для автоматического подключения. URL: https://support.apple.com/ru-ru/HT202831 (дата обращения 31.03.2021).

3. Использование частных адресов Wi-Fi в iOS 14, iPadOS 14 и watchOS 7. URL: https://support.apple.com/ru-ru/HT211227 (дата обращения 31.03.2021).

4. Роуминг в сетях Wi-Fi при использовании стандартов 802.11k, 802.11r и 802.11v в ОС iOS. URL: https://support.apple.com/ru-ru/HT202628 (дата обращения 31.03.2021).

5. О беспроводном роуминге для корпоративных клиентов. URL: https://support.apple.com/ru-ru/HT203068 (дата обращения 31.03.2021).

УДК 004.056.55
ГРНТИ 81.96

ИССЛЕДОВАНИЕ АФФИННОЙ ЭКВИВАЛЕНТНОСТИ В БЛОКАХ ПОДСТАНОВОК РАЗМЕРНОСТИ 3x3

М. Э. Ахметшина[1], Н. П. Борисенко[2], В. А. Яковлев[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]АО «РЦЗИ ФОРТ»

Проведено исследование блоков подстановок размерности 3x3 *(S-блоков), выполняющих нелинейные преобразования, при построении криптографических систем, с целью определения количества и состава аффинно-эквивалентных классов. С использованием разработанной программы, использующей переборный алгоритм, произведен полный расчет аффинно-эквивалентных множеств. Найдено четыре аффинно-эквивалентных класса и полностью определен их состав. Данный результат может использоваться для выявления взаимосвязей внутри классов и служит основой для поиска алгоритма нахождения аффинно-эквивалентных классов S-блоков больших размерностей.*

криптографические преобразования, S-блоки, булевы функции, аффинно-эквивалентные преобразования.

В состав современных криптографических стандартов ГОСТ Р 34.12-2015, AES и многих других входят нелинейные преобразования, именуемые *S*-блоками. Каждый такой блок задается *n*-мерной векторной булевой функцией, представляющей собой отображение $GF(2^n) \to GF(2^m)$.

С ростом числа входов/выходов (*n/m*) количество блоков и их разнообразия сильно возрастают, соответственно их сложнее исследовать.

Выбор булевых функций (БФ) для построения *S*-блока важная до конца нерешенная задача. Обычно булевы функции, используемые в *S*-блоках, характеризуются следующими показателями [1]:

- Вес Хэммина БФ *wt(f)* – количество единиц в векторе значений этой функции. БФ является уравновешенной, когда половина значений БФ равна единице.
- Расстояние Хэмминга между двумя функциями определяется как количество различающихся позиций в векторах значений функций.
- Алгебраическая нормальная форма (АНФ) – представление БФ в виде суммы по модулю *2* из 2^n произведений возможных входов. Максимальное количество сомножителей в любом слагаемом АНФ называется алгебраической степенью БФ.
- Преобразование Уолша-Адамара – функция вида

$$W_f(a) = \sum_{x \in Z_2^n} (-1)^{f(x) \oplus (a,x)}, \quad (1)$$

где *(a,x)* – скалярное произведение двух векторов длины *n*.

- Нелинейность БФ величина N_f, равная минимальному расстоянию до класса аффинных функций той же размерности. Нелинейность влияет на стойкость к линейному и дифференциальному криптоанализу, чем выше показатель нелинейности, тем лучше.
- Автокорреляционная функция называется функция, зависящая от векторного параметра *a*:

$$R_a(f) = \sum_x (-1)^{f(x) \oplus f(x \oplus a)}. \quad (2)$$

В последнее время для характеризации БФ и *S*-блоков используют также такие показатели как аффинная эквивалентность БФ и аффинная эквивалентность *S*-блока [3].

Свойство аффинной эквивалентности позволяет разделить S-блоки на множества, в которых будут находиться блоки со схожими свойствами, что упрощает описание и изучение их свойств, в том числе, поиск блоков

с наилучшими характеристиками. В работе исследованы отношения аффинной эквивалентности для блоков подстановок для $n = 3$, $m = 3$.

Булевы функции $f(x)$ и $h(x)$ от n переменных называются аффинно-эквивалентными, если для них выполняется равенство

$$h(x) = f(D \cdot x^T \oplus a^T) \oplus bx^T \oplus c, \quad (3)$$

где D – невырожденная матрица с элементами из $GF(2)$ размера n×n,

$a, b \in GF(2^n)$ – векторы,

c – константа $GF(2)$,

$bx^T = b_{n-1}x_{n-1} \oplus \ldots \oplus b_0x_0$ –скалярное произведение векторов b, x.

Проведенное исследование показало, что все 256 БФ при $n = 3$ можно в соответствии с (3) разделить на 3 класса. Причем отличительной особенностью класса является величина нелинейности БФ:

- 1 класс – аффинные функции – не обладают нелинейностью $N_f = 0$, мощность класса равна 16.
- 2 класс – нелинейные функции с $N_f = 1$, мощность класса – 128.
- 3 класс – нелинейные функции с $N_f = 2$, мощность класса – 112.

Для S-блоков аффинная эквивалентность задаётся уравнением

$$S_2 = B \cdot S_1(A \cdot x \oplus a) \oplus b, \quad (4)$$

где S_1 и S_2 – аффинно-эквивалентные блоки подстановок задаваемые отображением $GF(2^n) \to GF(2^n)$,

A и B – невырожденные матрицы с элементами из $GF(2)$ размера $n \times n$,

a и b – двоичные вектора размера n.

Интерес к исследованию аффинной эквивалентности S-блоков объясняется следующим обстоятельством. Современные SD-шифры имеют многораундовую структуру [2]. Каждый раунд это три преобразования: умножение входного вектора на матрицу – линейное преобразование (L); сложение с раундовым ключом (X); нелинейное преобразование с помощью S-блока.

Эти преобразования могут быть описаны правой частью соотношения (4). Действительно, входной вектор x в первом раунде умножается на матрицу A, суммируется с подключом раунда a и далее выполняется нелинейное преобразование S_1. Затем выполняются еще два преобразования следующего раунда умножение на матрицу (B) и сложение с подключом (b). То есть равенство в (4) означает, потерю в раунде операций сложения с ключом и линейного преобразования, что создает предпосылки к ослаблению стойкости шифра.

Нами проведено исследование аффинной эквивалентности всех S-блоков (3/3), удовлетворяющих следующим ограничениям. При построении блоков использовались только уравновешенные БФ. Существует 70 уравновешенных

функций, в ходе исследований выяснено, что среди них – 14 являются линейными и относятся к 1 классу аффинной эквивалентности булевых функций, остальные 56 функций относятся к 3 классу с показателем нелинейности 2.

Общее число блоков, которые получаются путем составления комбинаций из подобных булевых функций, составляет 40320. Были также исключены блоки, в состав которых входят линейные комбинации этих функций, повторяющиеся и инверсные функции, так как очевидно, что наличие таких функции в составе блока уменьшает показатель нелинейности блока до нуля.

Для выполнения преобразования (4) существует 168 невырожденных матриц (*A, B)* размера 3×3 и 8 векторов *(a,b)* длины 3. Для нахождения аффинно-эквивалентных множеств использовался переборный алгоритм. Суть алгоритма заключается в следующем. Вначале случайно выбирается блок из множества 40 320 блоков. Производится преобразования с использованием матриц *A* и векторов *a* (назовем эти преобразования внутренними преобразованиями). При этом полагаем, что $B = I$, где I – единичная 3×3 матрица, $b = 000$. В результате генерируется подмножество S-блоков, которое назовем первым *классом*. Для определения следующего класса выбирается блок, который отсутствует в первом классе. Этот цикл продолжается пока не классифицируются все блоки. В результате было получено 30 классов, в состав каждого входит по 1 344 блока.

Далее выполнялось внешнее преобразование – умножение на матрицу *B* и сложение с вектором *b*. Так как внутреннее преобразование не влияет на переход между полученными аффинно-эквивалентными классами, то для внешнего преобразования было взято только по одному *S*-блоку из каждого класса. После внешнего преобразования над блоками все аффинно-эквивалентные классы разделились на 4 множества, которые назовем *множествами классов* (рис., см. на сл. стр.).

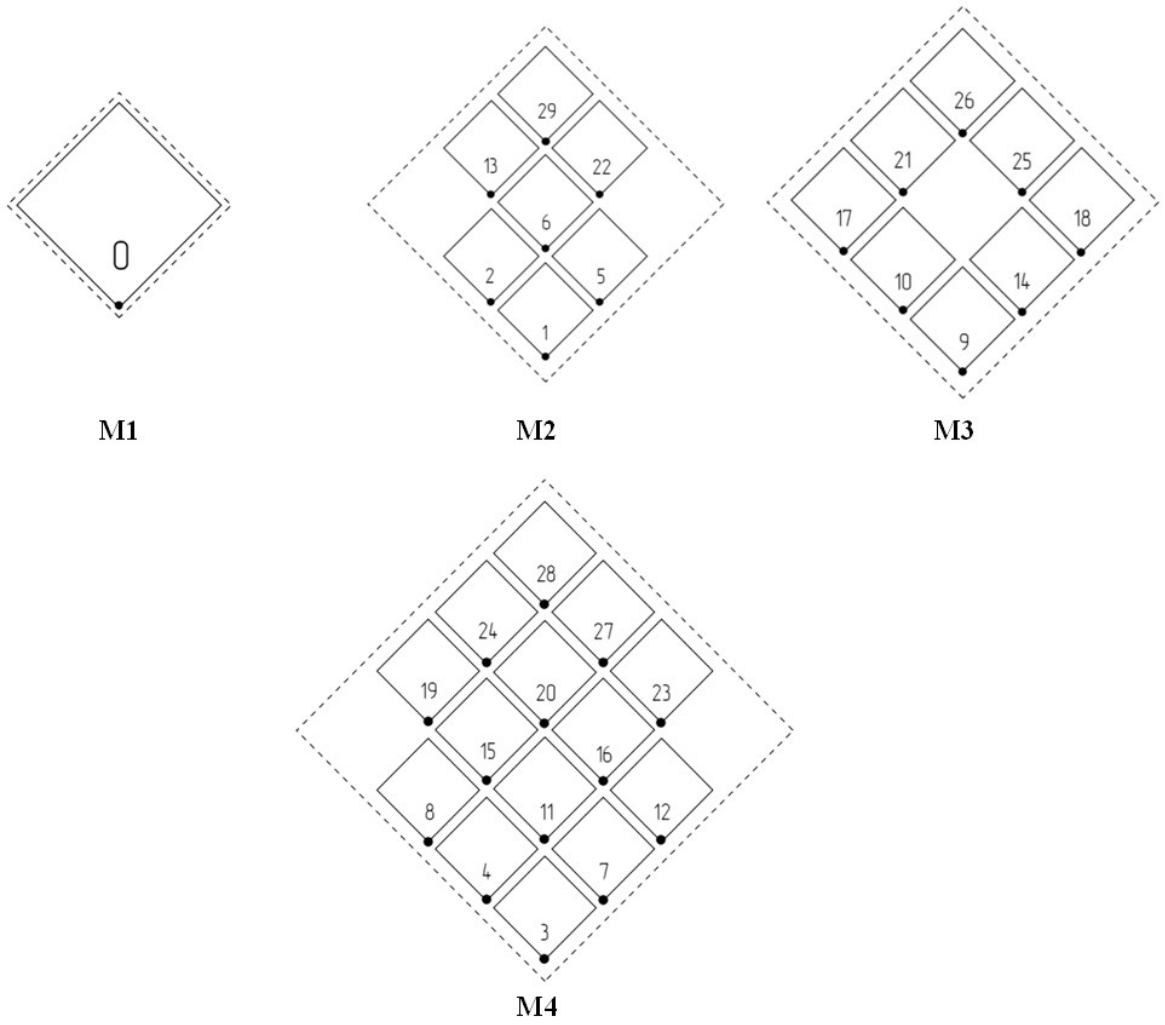


Рис. Разбиение блоков на множества классов

- 1-е множество классов – в состав *S*-блока входят только линейные булевы функции, нелинейность *S*-блока $N_S = 0$, мощность 1 класс и 1 344 блока.
- 2-е множество классов – в состав *S*-блока входят 2 линейные и нелинейная функция, $N_S = 0$, мощность 7 классов и 9 408 блоков.
- 3-е множество классов – в состав *S*-блока входят нелинейные функции, $N_S = 2$, мощность 8 классов и 10 752 блока.
- 4-е множество классов – в состав *S*-блока входят линейная и 2 нелинейные функции, $N_S = 0$, мощность 14 классов и 18 816 блоков.

Известен способ генерации *S*-блоков на основе обращения элементов поля $GF(2^n)$ по модулю неприводимого многочлена, в таких шифрах как Shark, Square, Rijndael и др. [1]. Считается, что такой способ генерации *S*-блоков дает наилучшие результаты с точки зрения линейного и дифференциального криптоанализа [2]. При $n = 3$ существует 2 неприводимых многочлена. Оба блока, получившихся в результате такой генерации, относятся к

3-му множеству классов, то есть имеют максимальную нелинейность, хотя с другой стороны, все БФ этого блока являются аффинно-эквивалентными.

Полученные результаты открывают некоторую перспективу дальнейших исследований аффинной эквивалентности *S*-блоков размера 4x4. Всего существует ≈21 триллион таких блоков, поэтому переборным алгоритмом эту задачу не решить. Вместе с тем возможен подход построения *S*-блоков путем комбинирования БФ, взятых в различных сочетаниях из «представителей» аффинно-эквивалентных классов БФ. Для $n = 4$ таких классов 8 [1]. Вычислений при этом существенно меньше по сравнению с переборным алгоритмом.

Результаты исследования и разработанная программа классификации *S*-блоков по подмножествам классов могут быть использованы в учебном процессе при постановке новых лабораторных работ и в курсовом проектировании при изучении дисциплины «Криптографические методы защиты информации».

Список используемых источников

1. Fuller J., Millan W. Linear Redundancy in S-Boxes // Information Security Research Centre, Queensland University of Technology, GPO Box 2434, Brisbane, Queensland 4001, Australia.

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

3. Нгуен В. Н., Григорян Д. Р. Влияние группы инерции S-блока на дифференциальную характеристику блочного шифра // Доклады Томского государственного университета систем управления и радиоэлектроники. Томск, 2019. Т. 22. № 1. С. 45–49

4. Панкратова И. А. Булевы функции в криптографии: учебное пособие. Томск: Издательский Дом Томского государственного университета, 2014. 88 с.

УДК 004.056.53
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ОБОРУДОВАНИЯ MIKROTIK К АТАКАМ НА БЕСПРОВОДНЫЕ СЕТИ

К. А. Ахрамеева, Г. Е. Ворошнин, М. М. Ковцур

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

Вместе с популярностью сети Интернет, в мире растет и количество производителей сетевого оборудования. Сетевое оборудование от компании MikroTik является популярным в связи с низким ценовым диапазоном, при этом предоставляя достаточно

широкий функционал. Оборудование данной компании часто является выбором для малых корпоративных сетей, в частности для организации сети Wi-Fi. Данная технология получила большое распространение из-за удобства, но, из-за повсеместного использования беспроводных сетей, становятся все более распространены беспроводные атаки. Некоторые из них могут быть реализованы достаточно легко, при этом атакуемое оборудование может обладать большим количеством уязвимостей. В связи с этим теме беспроводных атак, а также защиты от них, посвящено огромное количество научных статей и докладов. Однако, несмотря на это, влияние беспроводных атак на оборудование конкретных производителей исследовано крайне мало. В статье исследовано влияние атак на беспроводные сети на оборудовании производителя MikroTik, а также предложены методы их обнаружения.

информационная безопасность, безопасность беспроводных сетей, MikroTik.

Беспроводные сети имеют большую популярность как в обычных домашних помещениях, так и в общественных местах, и в корпоративном сегменте. При этом они обладают одной серьезной уязвимостью: они используют общедоступную среду передачи данных. Она приводит к возможности реализации множества атак на сеть [1, 2]. На сегодняшний день большое количество атак достаточно просты в реализации, так как злоумышленнику достаточно только скачать и запустит определенное программное обеспечение. Поэтому все больше становится актуальным исследование атак на беспроводные сети, с целью создания методов по их обнаружению и предотвращению. Мировые вендоры, такие как Cisco, Ruckus, Huawei [3, 4, 5], реализуют системы IPS и IDS. Также существует множество других методов [6], например honeypot [7]. Несмотря на то, что оборудование компании MikroTik не обладает такими системами, оно достаточно популярно в корпоративных сетях. Популярность обусловлена более низким ценовым диапазоном, по отношению к оборудованию названных мировых вендоров, и гораздо большим функционалом, чем у обычных домашних точек доступа. Также стоит заметить, что исследованию уязвимостей и защиты оборудования MikroTik уже посвящено несколько статей [8, 9, 10], но тема в части атак на беспроводную сеть остается малоизученной. Приняв во внимание вышесказанное и изучив статистику из базы данных общеизвестных уязвимостей информационной безопасности CVE [11], представленную на рис. 1, можно заключить, что исследование уязвимостей оборудование MikroTik к атакам на беспроводные сети является актуальным.

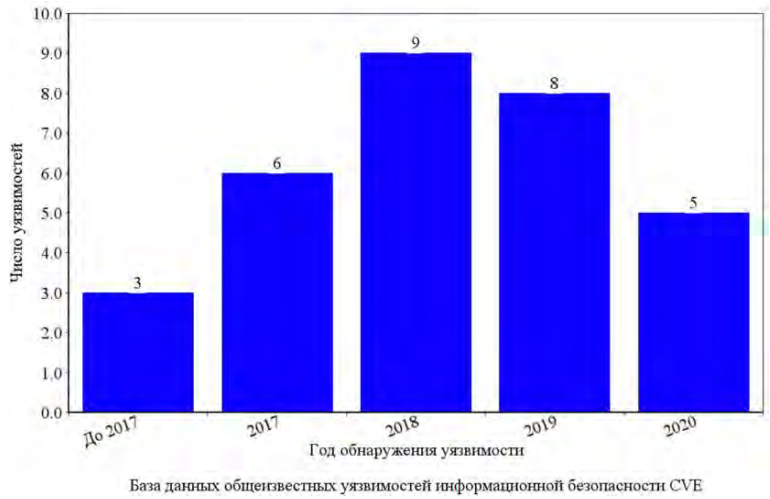


Рис. 1. Статистика обнаружения уязвимостей оборудования MikroTik

Типовая беспроводная сеть семейства стандартов IEEE 802.11 состоит из точки доступа и беспроводных клиентов. Один из них может оказаться злоумышленником – клиентом, пытающемся нарушить целостность, доступность сети или конфиденциальность передаваемых по ней данных.

Для исследования было отобрано 4 атаки: authentication flood, deauthentication food, probe request flood и ARP inject. Первые три были выбраны из-за простоты реализации, четвертая из-за серьезности возможных последствий. Для начала рассмотрим суть и механизм работы атак.

При рассмотрении первых двух атак обратимся к рис. 2. На нем схематично представлен процесс подключения клиента к точке доступа. Для успешного соединения клиенту необходимо пройти аутентификацию и ассоциацию, а при отключении – деассоциацию и деаутентификацию. При поддержании беспроводной необходимо оставаться в состоянии 3.

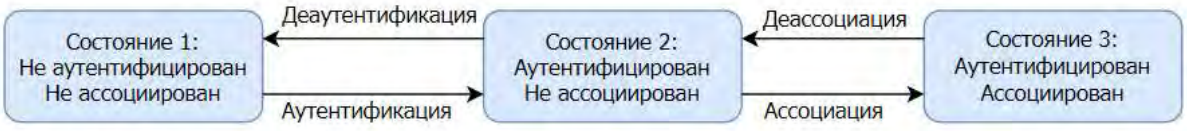


Рис. 2. Схема подключения клиента к точке доступа.

Основная цель атаки Authentication flood – заполнить таблицу ассоциаций точки доступа, тем самым не давая подключаться легальным клиентам. Как изображено на рис. 3, выполняется это путем отправки злоумышленником большого количества кадров authentication (type/subtype 0x000b) с различными MAC-адресами.

Рис. 3. Схема атаки authentication flood

Цель Deauthentication flood – отключить клиента(ов) от точки доступа. Существует 3 разных способа реализации этой атаки:

1. Злоумышленник отправляет клиенту фреймы deauthentication (type/subtype 0x000c) от имени точки доступа (указывая ее MAC-адрес в поле MAC-адреса отправителя), отключая его.

2. Злоумышленник отправляет на широковещательный адрес фреймы deauthentication от имени точки доступа, тем самым отключая всех клиентов.

3. Злоумышленник от имени клиента отправляет фреймы деаутентификации точке доступа, после чего она отключает клиента.

Также возможно применение нескольких способов в комбинации. На рис. 4 показана комбинация первого и третьего способов.

Рис. 4. Схема атаки deauthentication flood

Как показано далее в статье – исследуемые атаки по-разному влияли на сетевое оборудование. Для оценки влияния были выделены некоторые критерии:

1. Успешность атаки – получилось ли у злоумышленника добиться цели атаки.

2. Показатели оборудования (CPU, записи в log-файле и др.).

3. Показатели клиента (возможность подключения к сети, сетевые данные и др.).

Name	CPU	Usage
cpu0		10.0
ethernet	0	0.0
firewall	0	0.0
management	0	2.0
networking	0	0.5
profiling	0	4.0
unclassified	0	1.0
winbox	0	1.0
wireless	0	1.5

Рис. 7. Загрузка CPU при атаке authentication flood

В ходе эксперимента было выяснено, что атаки authentication flood в первую очередь влияет на точку доступа. Из рис. 7 видно, что загруженность CPU увеличилась больше, чем в 3 раза, и стала достигать 10 %.

В это время в таблице зарегистрированных клиентов поддерживалось порядка 50 записей, что можно увидеть на рис. 8.

Wireless Tables

WiFi Interfaces | W60G Station | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | Channels

00 Reset

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx Rate	Rx Rate
	12:81:09:39:E3:87	wlan1	00:00:03	no	no	2.830	-40	1Mbps	
	64:5B:EC:CA:B7:08	wlan1	00:00:03	no	no	2.710	-39	1Mbps	
	B0:9C:8C:E2:76:F3	wlan1	00:00:03	no	no	2.680	-39	1Mbps	
	C0:59:BE:F9:29:53	wlan1	00:00:03	no	no	2.680	-39	1Mbps	
	EA:01:59:64:72:69	wlan1	00:00:03	no	no	2.640	-40	1Mbps	
	84:95:11:11:77:87	wlan1	00:00:03	no	no	2.600	-39	1Mbps	
	04:37:E1:C3:30:0A	wlan1	00:00:02	no	no	2.480	-40	1Mbps	
	70:5E:AF:82:6F:26	wlan1	00:00:02	no	no	2.330	-39	1Mbps	
	48:C2:38:F7:44:A7	wlan1	00:00:02	no	no	1.770	-39	1Mbps	
	08:2D:A0:B0:2E:5D	wlan1	00:00:02	no	no	1.670	-39	1Mbps	
	16:1B:0C:70:7F:7E	wlan1	00:00:01	no	no	1.240	-42	1Mbps	
	D8:AD:F4:11:1D:E2	wlan1	00:00:01	no	no	1.140	-39	1Mbps	
	68:DD:35:FB:DA:1A	wlan1	00:00:01	no	no	1.030	-38	1Mbps	
	34:17:39:33:45:8A	wlan1	00:00:01	no	no	1.030	-40	1Mbps	
	D2:96:CA:25:FE:F2	wlan1	00:00:01	no	no	0.980	-39	1Mbps	
	08:89:95:20:86:11	wlan1	00:00:01	no	no	0.940	-39	1Mbps	
	EC:A3:DE:08:1D:16	wlan1	00:00:01	no	no	0.910	-39	1Mbps	

48 items

Рис. 8. Таблица зарегистрированных пользователей точки доступа во время атаки authentication flood

В log-файле ежесекундно добавлялись десятки записей об удалении и добавлении клиентов, также нужно заметить, что беспроводные клиенты не могли подключиться, а значит цель атаки была достигнута.

В отличие от authentication flood – deauthentication flood не оказала влияния на загруженность CPU, но, как видно из log-файла на рис. 9, цель ее была достигнута.

12	Feb/20/2021 11:34:26	memory	wireless, info	D0:37:45:81:3E:48@wlan1: disconnected, received deauth: class 3 frame received (7)
13	Feb/20/2021 11:34:30	memory	wireless, info	D0:37:45:81:3E:48@wlan1: connected, signal strength -45
14	Feb/20/2021 11:34:30	memory	wireless, info	D0:37:45:81:3E:48@wlan1: disconnected, received deauth: class 3 frame received (7)
15	Feb/20/2021 11:34:42	memory	wireless, info	D0:37:45:81:3E:48@wlan1: connected, signal strength -45

Рис. 9. Log-файл оборудования во время атаки deauthentication flood

При этом после нескольких попыток подключения клиентское оборудование прекратило попытки подключения и сообщило об ошибке, что и видно из рис. 10.

В ходе экспериментов было выяснено, что, несмотря на низкую стоимость, оборудование компании MikroTik является достаточно устойчивым к нагрузкам на беспроводную сеть в виде DoS-атак.

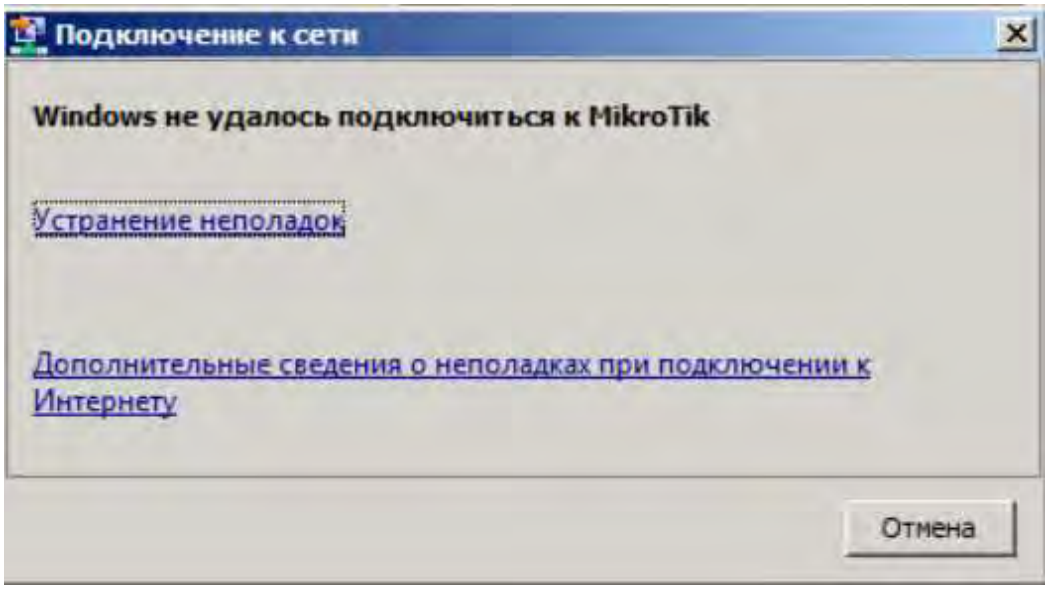


Рис. 10. Сообщение клиента при атаке deauthentication flood

При этом оно обеспечивает низкий уровень безопасности, так как не имеет достаточных средств не только для противодействия, но также и для обнаружения многих видов беспроводных атак.

Список используемых источников

1. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 24–28.

2. Герлинг Е. Ю., Кулишкина Е. И. Модели нарушителей информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 214–219.

3. Wireless Access Controller (AC and Fit AP) V200R019C10 CLI-based Configuration Guide. URL: https://support.huawei.com/enterprise/en/doc/EDOC1100156624/ 4d68bbca/ wids-profile (дата обращения: 08.03.2021).

4. WIPS. URL: https://docs.ruckuswireless.com/unleashed/200.1.9.12/c-WIPS.html (дата обращения: 08.03.2021).

5. Cisco Wireless Controller Configuration Guide, Release 8.5. URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/wireless_intrusion_detection_system.html#ids-signatures (дата обращения: 08.03.2021).

6. Миняев А. А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информация и связь. 2020. № 6. С. 29–36.

7. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86–97. DOI: 10.31854/1813-324X-2019-5-3-86-97.

8. Шамсутдинов Р. Р. Использование маршрутизаторов Mikrotik Rb-951 в качестве средств защиты информационной инфраструктуры малых организаций // European research: innovation in science, education and technology: XXXVII INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE, London, United Kingdom, 07-08 февраля 2018 года. – London, United Kingdom: PROBLEMS OF SCIENCE, 2018. С. 26–28.

9. Васин Н. Н., Кондаков А. С. Исследование стабильности работы маршрутизатора Mikrotik с большим объемом маршрутной информации // III Научный форум телекоммуникации: теория и технологии ТТТ-2019: Материалы XXI Международной научно-технической конференции, Казань, 18-22 ноября 2019 года. Казань: Казанский государственный технический университет им. А.Н. Туполева, 2019. С. 61–62.

10. Давидюк Н. В. Обеспечение безопасности абонентского телетрафика путём конфигурирования и настройки маршрутизатора (на примере MikroTik RouterBOARD) : Практикум. Санкт-Петербург : Общество с ограниченной ответственностью "Издательский центр "Интермедия", 2020. 68 с. ISBN 9785438301950.

11. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org (дата обращения: 08.03.2021).

УДК 004.056.5
ГРНТИ 81.93.29

ИСПОЛЬЗОВАНИЕ СТЕГАНОГРАФИИ В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

Е. Ю. Герлинг, К. А. Ахрамеева

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

Социальные сети и мессенджеры прочно вошли в нашу жизнь. Они дают широкие возможности для общения с людьми, находящимися в самых разных уголках Земли. Для обмена информацией через социальные сети и мессенджеры можно использовать, помимо непосредственно текста, файлы различных форматов. Что, в свою очередь, позволяет использовать не просто файлы, а файлы с вложенными в них методами стеганографии скрытыми сообщениями. В данной работе рассматривается возможность использования стеганографии обмена скрытой информацией через современные социальные сети и мессенджеры.

стеганография, социальные сети, мессанджеры, вложение информации, извлечение информации.

В современной жизни для общения и обмена информацией часто применяются социальные сети и мессенджеры. Они позволяют поддерживать связь людям из разных уголков планеты. События 2020 года, карантин, закрытые границы показали, насколько важно иметь возможность связаться с близкими и друзьями, находящимися на расстоянии, или даже в соседнем доме.

Социальные сети и мессенджеры могут быть также использованы и для незаконных действий, таких как террористическая и экстремистская деятельность, незаконная торговля наркотиками и оружием.

Так, согласно Ежемесячному сборнику Генеральной прокуратуры Российской федерации «Состояние преступности в России» за январь-декабрь 2020 г. [1]: «В сравнении с прошлым годом более чем на 42 % увеличилось количество выявленных преступлений экстремистской направленности (833). Большинство преступных проявлений экстремизма связаны с публичными призывами к осуществлению экстремистской деятельности (+34,9 %, 367), значительная часть из которых совершена с использованием сети «Интернет» (339)».

Неуклонно растет количество преступлений, так или иначе связанных с инфотелекоммуникационными технологиями. Согласно упомянутому выше сборнику [1]: «В целом на деяния, совершенные с использованием информационнотелекоммуникационных технологий или в сфере компьютерной информации, по-прежнему приходится одно из четырех регистрируемых в текущем году преступлений (+73,4 %, 510,4 тыс.). За последние пять лет число таких преступлений увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8 до 25 %. Большинство «киберпреступлений» совершается с использованием сети «Интернет» (300,3 тыс.) или при помощи средств мобильной связи (218,7 тыс.)».

Также отметим, что согласно тому же сборнику всего зарегистрировано 300 337 (1 место) преступления (любого характера), совершенных с использованием или применением сети «Интернет» [1].

Рис. 1. Число зарегистрированных преступлений, совершенных с использованием или применением различных инфотелекоммуникационными технологиями

Актуальность проблемы возможного использования Интернет пространства и отдельных его компонентов, таких как социальные сети и мессанджеры, подтверждается тенденцией развития современного Интернета в Российской Федерации, которая представлена в следующих явлениях:

- Принятие Закона о «суверенном интернете» (№ 608767-7) от 16 апреля 2019 года [2, 3], который предусматривает поправки в действующий 149-ФЗ («Об информации, информационных технологиях и о защите информации» [4, 5]);
- Смена владельца социальной сети ВКонтакте на компанию «Mail.ru group» (2017 год), политика которой позволяет предоставлять данные о пользователях, в том числе об имеющихся у них данных и переписок органам исполнительной власти [6].

К сожалению, нет собранной статистики об использовании методов стеганографии для передачи информации через сеть «Интернет», в том числе для совершения незаконной деятельности. Но отдельные случаи все-таки освещены в научных статьях.

Так, по мнению специалистов, террористы, связанные с бэн Ладеном и группировкой Аль-Кайда передавали друг другу карты местностей, диаграммы, важные фотографии и текстовые послания, используя методы стеганографии, скрывая информацию в изображениях, которые потом, размещались, например, на сайтах с фотогалереями или в социальных сетях [7].

Также американские и британские СМИ утверждают, что русские нелегалы, задержанные в США в июне 2010 года (в том числе Анна Чапман), использовали стеганографию для передачи секретной информации, спрятанной в неподвижных изображениях [7].

В научных статьях также прослеживается повышенный интерес к использованию стеганографии для передачи скрытой информации через социальные сети и мессенджеры. При этом авторы статей регулярно предлагают новые методы вложения. Например, в 2018 году в журнале «Вычислительная технология» (входит в перечень ВАК) был предложен метод сокрытия информации в графоподобных структурах социальной сети [8].

Отметим, что самыми популярными покрывающими объектами на сегодняшний день остаются файлы различных форматов с неподвижными изображениями и файлы формата PDF [9, 10], которые также можно легко передавать через социальные сети и мессенджеры.

Результаты проведенных исследований показали, что применив свободно распространяемое программное обеспечение, включающее в себя методы стеганографии, можно использовать социальные сети и мессенджеры для передачи стеганограмм. Результаты экспериментов для различных методов стеганографии при передаче стеганограмм через социальную сеть

ВКонтакт и мессанджер Telegram приведены в таблицах 1 и 2 соответственно.

ТАБЛИЦА 1. Результаты исследования для социальной сети ВКонтакте («+» – успешное вложение и последующее извлечение, «−» – неуспешное вложение и последующее извлечение)

Формат ПО	RAR архив	DeEggerEmbedded	НЗБ	Outguess	F5
JPEG	−	−	+	+	−
PNG	+	+	+	+	+
BMP	+	+	+	+	+
PDF	+	+	+	+	+

ТАБЛИЦА 2. Результаты исследования для Telegram («+» – успешное вложение и последующее извлечение, «−» – неуспешное вложение и последующее извлечение)

Формат ПО	RAR архив	DeEggerEmbedded	НЗБ	Outguess	F5
JPEG	−	+	+	+	+
PNG	+	+	+	+	+
BMP	+	+	+	+	+
PDF	+	+	+	+	+

Как видно из проведенных исследований социальная сеть «ВКонтакте» и мессенджер Telegram в подавляющем большинстве случаев позволяют успешно передавать стеганограммы, для которых в качестве покрывающего объекта использовались файлы различных форматов с неподвижными изображениями и файлы формата PDF. При этом возможность передачи стеганограммы зависит от выбранного метода стеговложения.

Стоить также отметить, что на данный момент в законодательстве Российской Федерации нет ограничений на длину ключей, используемых в стеганографии, хотя такое ограничение есть для криптографических ключей. Поэтому использование стеганографии один из законных и эффективных способов защитить информацию от посторонних глаз, что делает ее особенно привлекательной для использования при передаче незаконной информации.

На сегодняшний день проблема выявления скрытой передачи информации через сеть Интернет, в том числе по средствам социальных сетей и мессенджеров, является актуальной. Отсутствие достоверной статистики применения методов стеганографии, а также достаточно надежных методов выявления скрытых каналов передачи только повышает интерес к данной проблеме.

Список используемых источников

1. «Состояние преступности в России». Генеральная прокуратура Российской Федерации. Главное управление правовой статистики и информации. Ежемесячный сборник за декабрь 2020. URL: http://crimestat.ru/analytics (дата обращения 27.03.2021).
2. Обзор: "Госдума приняла закон о суверенном Рунете: к чему готовиться операторам связи" (КонсультантПлюс, 2020). URL: http://www.consultant.ru/ document/ cons_doc_LAW_322703 (дата обращения 25.02.2021)
3. Публикация Закона о «суверенном интернете» (КонсультантПлюс, 2020). URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 24.02.2021)
4. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция) (КонсультантПлюс, 2020) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 24.02.2021)
5. Перечень законов, регулирующий использование криптографии в РФ. URL: https://www.cryptocom.ru/law/ (дата обращения 24.02.2021)
6. ВКонтакте» упразднила должность гендиректора и назначила Рогозова управляющим директором. URL: https://tjournal.ru/flood/40797-vkontakte-uprazdnila-dolzhnost-gendirektora-i-naznachila-rogozova-upravlyayushchim-direktorom (дата обращения 24.02.2021)
7. Jesse, D. D. Tactical Means, Strategic Ends: Al Qaeda's Use of Denial and Deception // Terrorism and Political Violence. 2006. Vol. 18. pp. 367–388.
8. Нечта И. В. Метод сокрытия информации в графоподобных структурах социальной сети // Вычислительные технологии. 2018. Т. 23. № 2. С. 55–62.
9. Ахрамеева К. А., Герлинг Е. Ю., Ковцур М. М., Галецкая А. В. Стегоанализ объектов полученных с помощью стеганографических программ, распространенных в сети Интернет // StudNet. 2020. Т. 3. № 9. С. 1023–1030.
10. Герлинг Е. Ю., Ахрамеева К. А. Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи. 2019. № 3 (13). С. 51–58.

УДК 004.056
ГРНТИ 20.53.19

ОБЗОР ЖАНРОВ КОМПЬЮТЕРНЫХ ИГР ДЛЯ СОЗДАНИЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

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

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

В статье представлены результаты исследования, целью которого является анализ основных жанров компьютерных игр, классифицированных по способам получения информации во время игры, по типу совершаемых действий, использованию игрового

окружения, перемещения по игровому миру, по типу контроля и управления игровыми сущностями (игры информации, игры действий и игры контроля). Рассматриваются возможности и особенности создания стеганографических систем в играх определенных жанров. Предложены способы создания стеганографических систем для популярных игровых жанров. Дается сравнение возможностей создания стеганографических систем с помощью геймплейных элементов жанров и различных комбинаций этих элементов в гибридных игровых жанрах.

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

Введение

Зарождение компьютерных игр произошло в середине прошлого века (более 60 лет назад), а игровые жанры появились лишь около 20 лет назад.

И, не смотря на это, каждая игра была уникальна и неповторима на начальном этапе развития игровой индустрии. Но со временем игр становилось всё больше и больше. Для того, чтобы ориентироваться во всём многообразии игр, люди стали разделять игры на различные категории.

Критерии разделения на категории были самые разные: количество игроков, вид игровой камеры, сюжет. Но наибольшую популярность получил способ разделения на игровые жанры.

Классификация

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

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

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

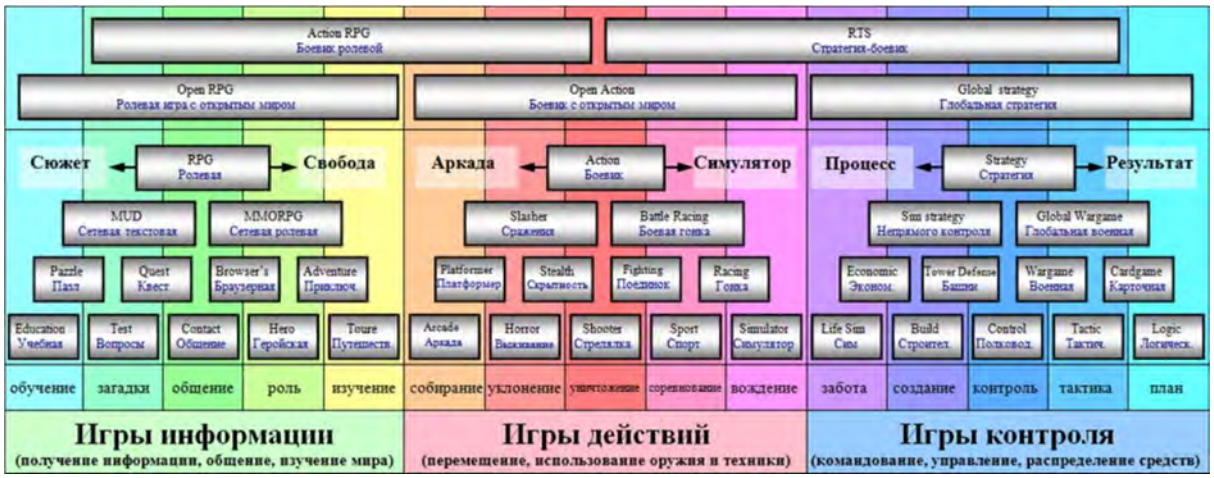


Рис. 1. Схема классификации игровых жанров

1. Игры информации

Главное в играх этой группы – получение информации во всех ее проявлениях. Пример – жанр «Ролевая игра» (RPG – *RolePlaying Game*), игры, в которых можно «вживаться» в роль персонажа. В таких играх в качестве главных достоинств выставляют атмосферу, сюжет, игровой мир

2. Игры действий

Отличительная особенность – движения, которые необходимо совершать каким-либо телом (чаще всего человеческим или гуманоидным), либо технчиеским средством. Это наиболее динамичные игры, которые принято хвалить за то, что они развивают скорость реакции. Примером может служить жанр «Экшн» (*Action*).

3. Игры контроля

Группа «игры контроля» состоит из тех игр, главная суть которых — планирование событий и управление для достижения преимущества в дальнейшем. Сюда попадают все виды стратегий, различные экономические игры, варгеймы, тактики.

Возможности создания стеганографических систем

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

Игры информации

1. Обучение

Главное действие – получение новой информации, а точнее – обучение. Самые простейшие из них – изучение цифр, алфавита, названий вещей. Сле-

довательно объектом, в который можно вложить необходимую информацию, будет информация, подаваемая игроку при обучении – текст, аудио, видео.

2. Загадки

Главное действие – проверка знаний (ранее полученной информации). Задается вопрос, игрок должен выбрать единственно верный ответ из предложенных вариантов, либо, при отсутствии готовых вариантов, создать свой ответ. В этом случае информацию можно вкладывать в ответы тестов, в сами вопросы, либо с помощью последовательности неверных ответов открывать доступ к скрываемой информации. К примеру, во всех вопросах может быть 4 варианта ответа, 3 из которых верные, а последовательность из порядковых номеров неверных ответов является вложенной информацией.

3. Изучение

Главное действие – изучение окружающего мира. Игрок ходит где хочет, общается с кем хочет, и занимается тем, чем хочет. Нет ничего обязательного к выполнению. В данном случае будет эффективным метод построения стеганографических систем с учетом содержимого [2] (*content aware steganography*) – вложение информации с сюжет, структуру игрового мира. Игровой мир может быть большим, поэтому вероятность случайного извлечения становится ниже, а знающий человек может спокойно извлекать необходимую информацию, выполняя, на первый взгляд, рядовые игровые действия.

Игры действий

Собирание

Главная задача – собрать все особые объекты на уровне. Довольно часто игры бывают бесконечны, а целью игры является набор наибольшего количества очков. В играх этой группы можно вкладывать информацию в разнообразие игровых предметов, которые при определенных последовательностях будут давать доступ к скрытой информации.

Игры контроля

1. Создание

Главное действие – распределение доступных ресурсов для развития. В подчинении игрока находятся ресурсы (деньги, стройматериалы, строители, свободная для застройки земля), их нужно с умом использовать для развития (обычно, постройка города). Такие игры еще называют «песочницами» (*“Sandbox”*). Данный жанр обладает большим количеством возможностей создания стеганографических систем. Почти все игры этого жанра

имеют конструктор, который позволяет менять окружающий мир [3], а онлайн-игры этого жанра позволяют делиться игрокам собственными построенными мирами в сети Интернет. Таким образом получается целая система передачи стеговложений. На примере игры *“Minecraft”* – игрок создал игровую карту с городом, в котором по определенным координатам спрятал сундук с письмом с важной информацией. Игрок выложил эту карту в свободный доступ. Другие игроки могут играть на этой карте и модифицировать ее, а знающий человек может провести извлечение информации, так как координаты ему были известны заранее.

1. План

Главное действие – планирование всех последующих действий. Логические игры очень абстрактны: в них используются различные кубики, шарики, карты – ничего реального. Примером таких игр являются “Tetris”, “Zuma”, пасьянсы. К примеру, в игре “Tetris” можно вкладывать информацию в изображение, которое получается при построении игровых блоков (рис. 2).

Рис. 2. Игровое поле Tetris

Сравнение возможностей создания стеганографических систем

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

Игры группы жанров «Игры информации» хоть и нацелены на работу с информацией, но в них может быть проблема с гибким построением стегосистем – под каждую новую стегостистему придется создавать отдельную игру.

А «Игры контроля» и, в особенности, жанр «Строительство» обладают большим потенциалом и наибольшей эффективностью создания стеганографических систем. В таких играх нет необходимости что-то менять и дополнять, чтобы создать новую стегостистему взамен старой, так как внутриигровой конструктор чаще всего содержит все необходимое для удобного

редактирования игрового уровня. При этом многие игры этого жанра предлагают игрокам возможность обмена своими творениями по сети, что упрощает передачу стеговложений.

Заключение

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

Список используемых источников

1. Киризлеев А. А. Жанры компьютерных игр (общая схема). URL: https://gamesisart.ru/TableJanr.html

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

3. Воробьев Д. Б., Шабалкин Л. Э., Музыкантов М. А. Симуляторы строительства и управления. История развития и особенности жанра. URL: https://cyberleninka.ru/article/n/simulyatory-stroitelstva-i-upravleniya-istoriya-razvitiya-i-osobennosti-zhanra

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ ЭФФЕКТИВНОСТИ SIEM-СИСТЕМЫ В ОРГАНИЗАЦИИ

И. Н. Бабков

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

Применение систем класса SIEM позволяет значительно повысить уровень защиты информационных ресурсов и эффективность контроля информационной безопасности в организациях. В статье анализируются основные задачи, преимущества и недостатки таких систем. Особое внимание уделяется вопросам выбора наиболее эффективных систем на основе критериев, учитывающих особенности организаций. Рассматриваются способы повышения эффективности SIEM-систем в организации.

Security Information and Event Management, SIEM, информационная безопасность.

Введение

В настоящее время большинство крупных компаний и организаций в целях обеспечения безопасности своих информационных ресурсов и непрерывности бизнеса создают мощные комплексные системы защиты информации (КСЗИ). При создании КСЗИ по возможности используются современные эффективные подсистемы информационной безопасности. Выбор механизмов защиты осуществляется специалистами подразделений информационной безопасности (ИБ) и информационных технологий (ИТ), как правило, с учетом модели угроз информационной безопасности, актуальной для конкретной компании.

Согласно аналитическим отчетам, публикуемым различными ИБ-компаниями, количество компьютерных атак постоянно возрастает. Так, например, в отчете компании Positive Technologies «Актуальные угрозы: III квартал 2020 года» отмечается, что в III-м квартале 2020 года число атак возросло на 54 % за год по сравнению с прошлым периодом.

Устойчивая тенденция роста числа атак, в том числе их новых видов, вынуждает компании модернизировать или внедрять новые системы защиты. Соответственно возрастает нагрузка на подразделения ИБ и ИТ.

В этих условиях возникают проблемы:

– обслуживание большого числа систем;

– проведение локального контроля настроек;

– сложность оценки событий ИБ в реальном времени и анализа данных из журналов аудита различных информационных систем и средств защиты;

– снижение оперативности оповещения администратора безопасности о возникающих событиях ИБ;

– повышение риска пропуска важных событий и инцидентов ИБ.

SIEM-системы

На сегодняшний день значительно повысить эффективность управления современными комплексами защиты можно с помощью SIEM-систем [1]. Эти системы позволяют автоматизировать: процессы управления событиями безопасности, подготовку отчетов по оценке соответствия состояния безопасности нормативным требованиям, а также принятие решений по реагированию на инциденты информационной безопасности.

SIEM (*Security Information and Event Management system*) – «Система управления информацией и событиями в безопасности» включает два механизма: SIM – управление ИБ (сбор, хранение и анализ данных из журналов; подготовка отчетов по выполнению нормативных требований) и SEM – управление событиями ИБ (мониторинг событий безопасности в реальном времени; выявление и реагирование на инциденты безопасности).

Решение SIEM может внедряться как самостоятельная система или, при наличии в организации Центра оперативного управления ИБ (*Security Operations Center*, SOC), входить в его состав [2].

Механизмы SIEM-системы позволяют производить сбор, нормализацию, агрегацию, фильтрацию, корреляцию, хранение и визуализацию данных, относящихся к безопасности, как для изучения в режиме реального времени, так и за прошлые периоды [3]. Источниками событий ИБ для SIEM-системы являются: межсетевые экраны, системы обнаружения и предотвращения вторжений, антивирусные системы, системы предотвращения утечек информации, сканеры уязвимостей, СКУД, сетевое оборудование, журналы аудита серверов и рабочих станций, а также другие системы, влияющие на безопасность. Данные от источников автоматически или по запросу поступают на серверы системы SIEM, где осуществляется их централизованная обработка.

К основным задачам SIEM-системы относятся:

– сбор и централизация данных;
– консолидация и хранение журналов событий;
– реагирование на инциденты безопасности в реальном времени;
– оповещение об инцидентах администратора ИБ;
– анализ данных с учетом корреляции событий по установленным правилам;
– анализ событий и инцидентов безопасности, хранящихся в журналах, подготовка отчетов;
– визуализация;
– оценка соответствия КСЗИ нормативным и другим документам.

Основные задачи носят общий характер, но их конкретные решения в разных компаниях будут определяться спецификой объекта внедрения: областью его деятельности, информационной инфраструктурой, бизнес-процессами, квалификацией ИБ и ИТ-персонала, а также требованиями регуляторов по обеспечению безопасности (в частности, наличием у системы сертификата соответствия ФСТЭК России). Поэтому важной целью организаций является выбор и внедрение SIEM-системы, способной обеспечить наиболее эффективное решение вышеперечисленных задач при минимальных затратах и с учетом специфики объекта.

Выбор SIEM-системы

Выбор приемлемой SIEM-системы для внедрения в организации сейчас довольно широкий. Достаточно назвать такие известные системы как IBM QRadar, HP ArcSight, PT MaxPatrol SIEM, Ankey SIEM.

Основные этапы внедрения и использования SIEM-системы включают: предпроектное обследование корпоративной сети организации, проектиро-

вание (выбор конкретной SIEM-системы), проведение настроек, оценку работоспособности системы, опытную эксплуатацию (внесение исправлений в систему), промышленную эксплуатацию, проведение планового аудита, модернизацию.

При выборе SIEM-системы необходимо учитывать недостатки, снижающие её эффективность. К ним относятся:

– высокая стоимость владения SIEM-системой (включает стоимость самой системы, проекта, продления лицензий и технической поддержки);

– неточное определение масштабов внедрения (состава SIEM-системы) в ходе предпроектного обследования;

– продолжительное время реализации проекта внедрения;

– возможные проблемы при сопряжении системы с источниками событий (для специфического оборудования и ПО, применяемого в сети организации, требуется разработка специальных коннекторов);

– недостаточная защищенность самой SIEM-системы.

В целях повышения эффективности SIEM-системы можно использовать ряд способов, позволяющих компенсировать отмеченные недостатки, и более полно задействовать её инструменты.

Способы повышения эффективности SIEM-системы

1. *Четкое формулирование целей и задач внедрения SIEM-системы.* На этапе предпроектного обследования информационной инфраструктуры организации следует собрать необходимые данные для определения масштабов и этапов внедрения. На основе полученных данных можно выбрать приоритетные источники информации, определить требуемые параметры SIEM-системы (технические характеристики, базовые настройки), подготовить техническое задание. Проведение этих работ позволит выбрать приемлемый вариант внедрения системы с учетом специфики компании и лимита финансирования, рисков и ущербов, которые может понести организация в случаях серьёзных инцидентов ИБ.

2. *Выбор SIEM-системы на основе сравнительного анализа решений.* Сравнение решений SIEM, основанное на методе экспертного анализа, является важным инструментом выбора наиболее эффективной системы для организации. Существуют различные варианты этого метода. В частности, в [4] при проведении сравнения применяются блоки критериев, для которых введены веса, определяющие важность каждого критерия. Критерии разрабатываются на основе полного набора выполняемых SIEM-системой задач. Каждый блок критериев включает различные параметры также с весовыми коэффициентами. Вводятся оценки степени выполнения критериев. Результаты сравнения тестируемых систем рассчитываются по специальной методике с учетом введенных весовых коэффициентов и оценок. Для каждой организации, выбирающей систему, следует использовать индивидуальный

подход. Критерии могут меняться в зависимости от реальных задач, весовые коэффициенты должны выбираться с учетом специфики организации.

3. *Корреляция событий.* Корреляция является наиболее важным механизмом SIEM-системы. Она позволяет идентифицировать атаки, которые сложно выявить по одному событию. В отличие от обычных средств защиты информации, фиксирующих событие ИБ, с её помощью можно получить дополнительную уточняющую информацию о событии. Благодаря механизму корреляции, можно снизить вероятности пропуска и ложного обнаружения атаки и тем самым повысить точность её идентификации. Соответственно повышается эффективность SIEM-системы. В состав SIEM-системы входит набор базовых правил корреляции, позволяющих идентифицировать основные угрозы, атаки, инциденты безопасности. В ходе настройки и эксплуатации системы в организации можно создавать собственные правила, в том числе по выявлению новых видов атак [5, 6].

4. *Визуализация событий и отчетов.* Визуализация является эффективным механизмом SIEM-системы, позволяющим отображать на графических панелях большие объемы информации о состоянии безопасности в форме компактных видеоизображений (диаграмм, гистограмм, таблиц, графиков и т. д.). Функционал визуализации отличается у разных SIEM-систем. Можно формировать отчеты с различной степенью детализации. Детальные отчеты о событиях безопасности сокращают время реагирования на инциденты ИБ, что повышает эффективность мониторинга состояния ИБ в организации. Визуализация также позволяет получить наглядную информацию об общем состоянии ИБ в организации и ИТ-инфраструктуре. Благодаря ей, удается сократить трудозатраты персонала и время принятия решений по поступающей информации.

5. *Контроль защищенности SIEM-системы.* На SIEM-систему ложится основная нагрузка по управлению и контролю состояния ИБ в организации, поэтому обеспечение защиты и непрерывности работы системы является приоритетной задачей. Для поддержания защищенности необходимо проводить периодический аудит SIEM-системы, в том числе тесты на проникновение в целях выявления критических уязвимостей.

Выводы

SIEM-системы оптимизируют процессы управления и контроля ИБ организации. Они наиболее эффективны для крупных компаний с мощными КСЗИ. При правильном их использовании можно снизить общие затраты на безопасность. На малых предприятиях применение таких систем не столь выигрышно, поэтому при принятии решения о внедрении системы можно ограничить его масштабы наиболее приоритетными задачами.

При выборе SIEM-системы целесообразно проводить сравнительный анализ различных систем с использованием соответствующих методик по критериям, учитывающим специфику организации.

В целях повышения эффективности функционирования SIEM-системы необходимо максимально использовать возможности: механизмов корреляции и визуализации, выявления уязвимостей, обнаружения новых видов атак, подготовки отчетов о состоянии ИБ в организации и его соответствии требованиям нормативных документов.

Список используемых источников

1. Кузнецова А. Д., Сахаров Д. В. Обзор состояния исследований информационной безопасности и применения SIEM-систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 626–631.

2. Казанцев А. А., Красов А. В., Катасонов А. И., Гельфанд А. М. Создание и управление Security Operations Center для эффективного применения в реальных условиях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 590–595.

3. Котенко И. В., Саенко И. Б. SIEM-система для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5. С. 54–65.

4. Ниязов Т. Сравнение SIEM-решений для построения SOC // Jet Info. 2015. № 8. URL: https://www.jetinfo.ru/sravnenie-siem-reshenij-dlya-postroeniya-soc/ 2015 (дата обращения: 29.01.2021).

5. Kovtsur M. M., Mikhailova A. V., Potemkin P. A., Ushakov I. A., Krasov A. V. Guidelines for using machine learning technology to ensure information security // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT): сб. науч. ст., 2020. С. 285–290.

6. Гамидов Т. О., Виткова Л. А., Ковцур М. М. Разработка моделей и алгоритмов анализа данных для исследования хода инцидентов и кризисов в социальных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 3–10.

УДК 004.056.53
ГРНТИ 49.33.35

ВОЗМОЖНОСТИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ВОЛОКНАМ В ПАССИВНЫХ ОПТИЧЕСКИХ СЕТЯХ

А. В. Балина, М. С. Былина

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

В работе исследуется возможность несанкционированного доступа к оптическому волокну в пассивных оптических сетях посредством создания акустооптического канала утечки. Рассмотрены физические причины формирования акустооптических каналов утечки в волоконно-оптических системах связи и проведена оценка эффективности данного канала утечки, критерием эффективности выбрана глубина модуляции оптического сигнала, подвергнутого акустическому воздействию.

пассивные оптические сети (PON), акустическая модуляция, акустооптический канал утечки, оптическое разъемное соединение, френелевское отражение, глубина модуляции.

В пассивных оптических сетях (*Passive Optical Network*, PON), широко применяемых в современных домах и офисах, передача оптического сигнала между центральным и абонентскими узлами осуществляется исключительно пассивными компонентами. В здании, охваченном сетью PON, по всем помещениям проходят оптические кабельные каналы, что создает совершенно новые, на данный момент недостаточно изученные и исследованные условия для несанкционированного доступа (НСД). Одна из угроз связана с воздействием акустических полей на проходящее по оптическому волокну (ОВ) излучение, что создает возможность извлечения звуковой информации (например, подслушивания разговоров) [1]. Данное исследование наиболее актуально для обеспечения безопасности в коммерческих, ведомственных и административных помещениях.

Акустооптический канал утечки формируется следующим образом: акустическая волна речевого диапазона частот, распространяясь в воздухе, взаимодействует с окружающими объектами, в том числе с ОВ, оказывая на них механическое воздействие. В результате возникает паразитная модуляция проходящего по ОВ света по амплитуде, частоте, фазе и поляризации [2]. Модулированное звуком световое излучение распространяется по ОВ за пределы охраняемой зоны, и может быть принято и демодулировано нарушителем.

Формирование акустооптического (волоконного) канала утечки информации практически невозможно без физического доступа к оптическому кабелю, проходящему через выделенные помещения. Кроме того, кабельная сеть должна быть свободна от активного волоконно-оптического оборудования на участке между нарушителем и источником акустической информации, что связано с восстановлением формы штатных сигналов и подавлением шумовых составляющих излучения в активном оборудовании. Между нарушителем и источником акустической информации должен располагаться оптический кабель с пассивными оптическими элементами, которые не изменяют существенным образом модуляцию светового потока [3].

Эффективность модуляции зависит от места взаимодействия акустического поля и оптического потока. Воздействию подвергаются все пассивные элементы волоконно-оптической кабельной системы. Обычно выделяют три типа канала утечки: свободный участок оптического кабеля (ОК); ОК, имеющий виброакустический контакт с конструкциями здания (например, в месте его крепления к элементам конструкций здания) и место механического (разъемного) соединения ОВ. Именно последний тип канала утечки будет подробно рассмотрен в данной работе.

Между торцами ОВ в разъемном соединении (коннекторе) всегда имеется небольшой зазор (осевое смещение), в котором возникают многократные переотражения излучения. В результате их интерференции формируются прошедшее соединение и отраженное от него излучения, описываемые соотношениями для интерферометра Фабри-Перо [4] и позволяющими определить вносимые и возвратные потери в соединении. Для вносимых a_{vn} и возвратных a_{vz} потерь соединения с осевым смещением двух одинаковых стандартных одномодовых ОВ с плоскими торцами, перпендикулярными оптическим осям, справедливо [1, 2]:

$$a_{vn} = -10 \lg K_{vn} = -10 \lg \frac{4 * n_c^2 * n^2}{4 * n_c^2 * n^2 + (n^2 - n_c)^2 \sin^2(\frac{2\pi}{\lambda} * n * s)}, \quad (1)$$

$$a_{vz} = -10 \lg K_{vz} = -10 \lg \frac{(n^2 - n_c^2)^2 * \sin^2(\frac{2\pi}{\lambda} * n * s)}{4 * n^2 * n_c{}^2 + (n^2 - n_c{}^2)^2 \sin^2(\frac{2\pi}{\lambda} * n * s)}, \quad (2)$$

где K_{vn}, K_{vz} – коэффициенты вносимых и возвратных потерь,

n_c – показатель преломления сердцевин соединяемых волокон,

n – показатель преломления среды в зазоре,

s – ширина зазора,

λ – длина волны излучения. Из выражений (1) и (2) видно, что потери зависят от соотношения s/λ.

Для увеличения $a_{вз}$ применяется соединение типа «физический контакт», предполагающее придание торцам соединяемых ОВ сферической

формы с радиусом R (рис. 1). В таком соединении ширина зазора s будет зависеть от расстояния от оптической оси волокна r:

$$s(r) = 2 * (R - \sqrt{R^2 - r^2}) + s_0, \quad (3)$$

где $s_0 = s(r)$ – ширина зазора на оптической оси.

Для идеального контакта величина s_0 равна нулю, в таком положении волокна касаются друг друга высшими точками сфер, расположенными на их оптических осях. В реальном разъемном соединении максимальная допустимая величина s_0 составляет 0,1 мкм. Далее будем считать, что в разъеме, не подвергнутом внешнему воздействию, s_0 составляет половину максимальной величины (0,05 мкм).

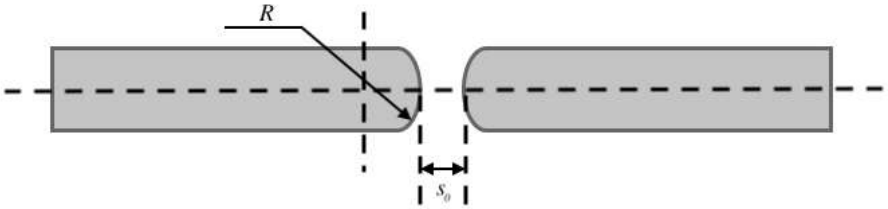


Рис. 1. Соединение типа «физический контакт»

На рис. 2 представлены результаты расчета $s(r)$ при R = 15 мм. Видно, что при увеличении расстояния r от оптической оси зазор между ОВ увеличивается.

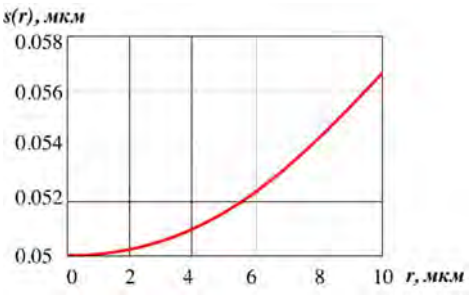


Рис. 2. Зависимость ширины зазора между ОВ от расстояния от оптической оси при физическом контакте

Из (1)–(3) следует, что коэффициенты K_{vn} и K_{vz} в соединении типа «физический контакт» зависят от r. Для расчета вносимых и возвратных потерь такого соединения K_{vn} и K_{vz} необходимо усреднить по поперечному сечению ОВ:

$$A_{vn} = -10 \lg \left[\frac{2}{w^2} \int_0^w K_{vn}(r) \cdot r \cdot dr \right], A_{vz} = -10 \lg \left[\frac{2}{w^2} \int_0^w K_{vz}(r) \cdot r \cdot dr \right], \quad (4)$$

где w – радиус модового пятна ОВ, определяемый выражением:

$$w = r_c \cdot (0{,}65 + 1{,}619/V^{1.5} + 2{,}879/V^6), V = 2\pi \cdot r_c \cdot NA/\lambda. \quad (5)$$

В (5) r_c – радиус сердцевины ОВ, V – нормированная частота ОВ, NA – числовая апертура ОВ.

На рис. 3 представлены результаты расчета по (1)–(5) зависимостей A_{vn} и A_{vz} от длины волны λ для соединения стандартных одномодовых ОВ, не подвергнутого внешнему воздействию. Расчеты проведены при R = 15 мм, r_c = 5 мкм, NA = 0,14.

Акустическое воздействие с частотой f вызывает вибрацию соединенных ОВ, то есть изменение s_0 с этой частотой, приводящее к модуляции мощности прошедшего и отраженного излучения. Возникающими под воздействием вибрации угловыми и радиальными смещениями соединяемых ОВ пока пренебрегаем.

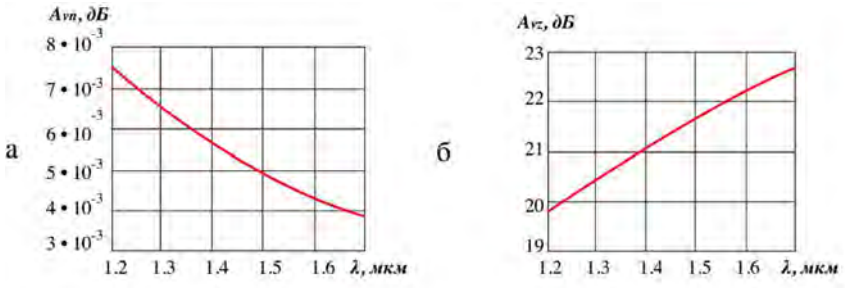


Рис. 3. Зависимость вносимых (а) и возвратных (б) потерь от длины волны в невозмущенном соединении

На рис. 4 представлены результаты расчетов минимальных и максимальных A_{vn} и A_{vz} от длины волны λ для соединения, подвергнутого виброакустическому воздействию. Полагалось, что амплитуда S_m колебаний ОВ вдоль оптической оси составляет 25 нм – 50 % от величины s_0 для соединения, не подвергнутого внешнему воздействию.

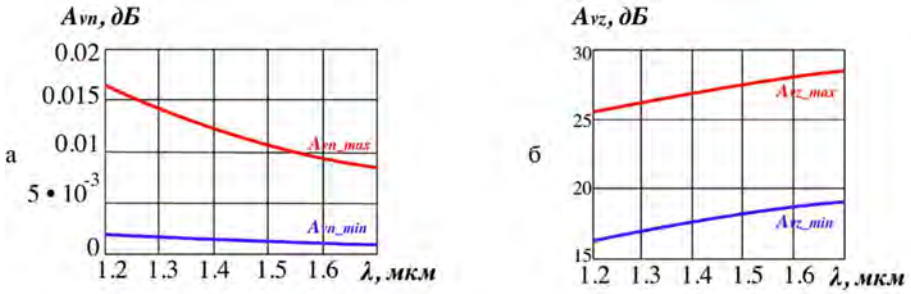


Рис. 4. Зависимости минимальных и максимальных вносимых (а) и возвратных (б) потерь от длины волны в соединении, подвергнутом виброакустическому воздействию

Для оценки эффективности модуляции проходящего и отраженного излучения определим глубину модуляции:

$$\textit{для прошедшего излучения:}\quad m_t = \frac{\delta P_{\text{пр}}}{P_{\text{пр}}} * 100\% \qquad (6)$$

$$\textit{для отраженного излучения: } m_r = \frac{\delta P_{\text{отр}}}{P_{\text{отр}}} * 100\% \qquad (7)$$

где $P_{\text{пр}}$ и $P_{\text{отр}}$ – мощности прошедшего и отраженного излучений.

Были проведены расчеты глубины модуляции прошедшего и отраженного излучений для амплитуд S_m, составляющих 20–50 % от величины s_0 для соединения, не подвергнутого внешнему воздействию. Результаты расчетов для $S_m = 0{,}2s_0$ представлены на рис. 5.

Расчеты показали, что в результате акустического воздействия наибольшую глубину модуляции приобретает мощность отраженного излучения. При изменении ширины зазора с амплитудой 20–50 % от номинального значения (ширины зазора s_0 в невозмущенном соединении) она составляла от 30 до 80 %, в то время как глубина модуляции прошедшего излучения не превышала 2 %. Таким образом, глубина модуляции отраженного излучения m_r вполне достаточна, чтобы нарушитель мог демодулировать изменения его амплитуды с помощью технического средства разведки – достаточно чувствительного фотоприемного устройства.

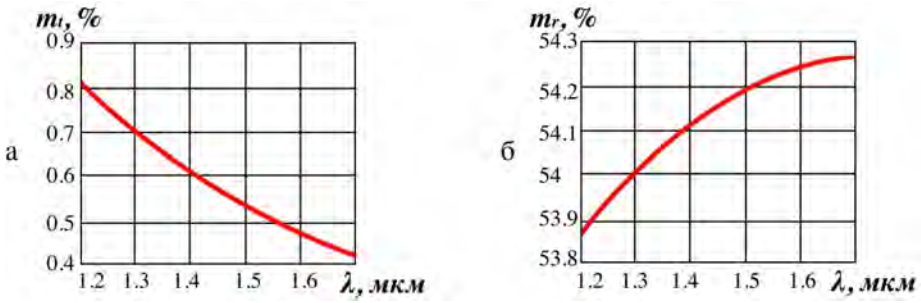


Рис. 5. Зависимости глубины модуляции прошедшего (а) и отраженного излучения (б) от длины волны

В заключение отметим, что при проведении исследования полагалось, что соединяемые волокна полностью идентичны и учитывались потери в соединении, обусловленные только френелевскими отражениями. Учет нефренелевских потерь из-за различия параметров соединяемых ОВ (например, в результате технологического разброса) может привести к некоторому снижению рассчитанной глубины модуляции m_r.

Отметим также, что в работе проанализировано только возникновение амплитудной модуляции излучения под воздействием акустического поля. Анализ частотной, фазовой и поляризационной модуляции излучения является предметом дальнейших исследований.

Тем не менее, даже с учетом указанных особенностей исследования, можно считать доказанной возможность НСД к конфиденциальной акустической информации через канал утечки на основе излучения, отраженного от соединения ОВ.

Список используемых источников

1. Балина А. В. Угрозы несанкционированного доступа к информации путем формирования акустооптического канала утечки в волоконно-оптических линиях связи // Глобальные трансформации технологических и научных систем: перспективы развития. Сборник докладов Международной научно-практической конференции. Санкт-Петербург, 2020. С. 34–37.
2. Панов М. Ф., Соломонов А. В., Филатов Ю. В. Физические основы интегральной оптики. М.: Академия, 2010. 432 с. ISBN 978-5-7695-5976-1.
3. Гришачев В. В. Выявление угроз утечки речевой информации через волоконно-оптические коммуникации // Фотоника. 2011. № 4. С. 32–39.
4. Былина М. С., Глаголев С. Ф., Павлова Н. Н. Теоретическое исследование потерь в соединениях одномодовых волокон // Фотон-Экспресс. 2007. № 3 (63). С. 36–38.

УДК 519.718:004.722
ГРНТИ 49.33.35

АНАЛИЗ ВРЕМЕННЫХ ЗАТРАТ НА ФОРМИРОВАНИЕ СЕЧЕНИЙ ПУТЕМ ПОСЛЕДОВАТЕЛЬНОГО ПЕРЕБОРА ВСЕХ СОЧЕТАНИЙ ВЕРШИННЫХ СЕЧЕНИЙ

К. А. Батенков

Академия ФСО России

Рассматривается подход к формированию сечений, базирующийся на методе, использующем в качестве основы матрицу связностей, и, по сути, предполагающий последовательный перебор всех сочетаний вершинных сечений, начиная с истока и стока. Показано, что время выполнения подобных вычислений не слишком велико и не превысило десяти секунд для тестовой сети.

сеть связи, сечение, временные затраты, двухполюсная сеть, граф.

Рассматриваемый подход базируется на методе, использующем в качестве основы матрицу связностей, и, по сути, предполагающий последовательный перебор всех сочетаний вершинных сечений, начиная с истока и стока [1, 2]. Отметим, что данный способ приводит к включению в общий состав сечений не минимальных, что потребовало введения дополнительной процедуры проверки добавляемого сечения на безызбыточность [3, 4].

Формально процедуру формирования множества минимальных двухполюсных сечений целесообразно разбить на три этапа. На первом синтези-

руют $v-1$ множество вершинных сечений, выделяя в отдельный блок сечение истока и стока, на втором находят декартово произведение сечений, не являющихся истоком и стоком, вплоть до $v-3$ полученного множества с учетом неповторяемости ребер, отсутствием ребер, принадлежащих истоку, и невключенности всех ребер сечения стока в получаемое множество, а на третьем вычисляют декартово произведение полученных ранее произведений на сечение истока, контролирую уникальность ребер [1, 5, 6, 7].

В качестве тестовой сети связи используется магистральная сеть Ростелеком, развернутая с целью формирования потоков в направлении «Европа – Азия». Помеченный граф рассматриваемой сети связи представлен на рис. 1 [7, 8].

Для двухполюсной связности оказывается возможным провести анализ для магистральной сети (рис. 1) целиком даже на основе сечений. На рис. 2 представлены результаты формирования множества сечений для всех пар узлов, образующих направления связи. Нумерация *n* сечений задана сначала по номеру стока *j* при фиксированном истоке *i*, а затем и по номеру истока *i*, то есть номер сечения вычисляется по формуле:

$$n = j + v(i-1) - \frac{i(i+1)}{2}, i = 1, 2, \dots, v-1, j = i+1, i+2, \dots, v.$$

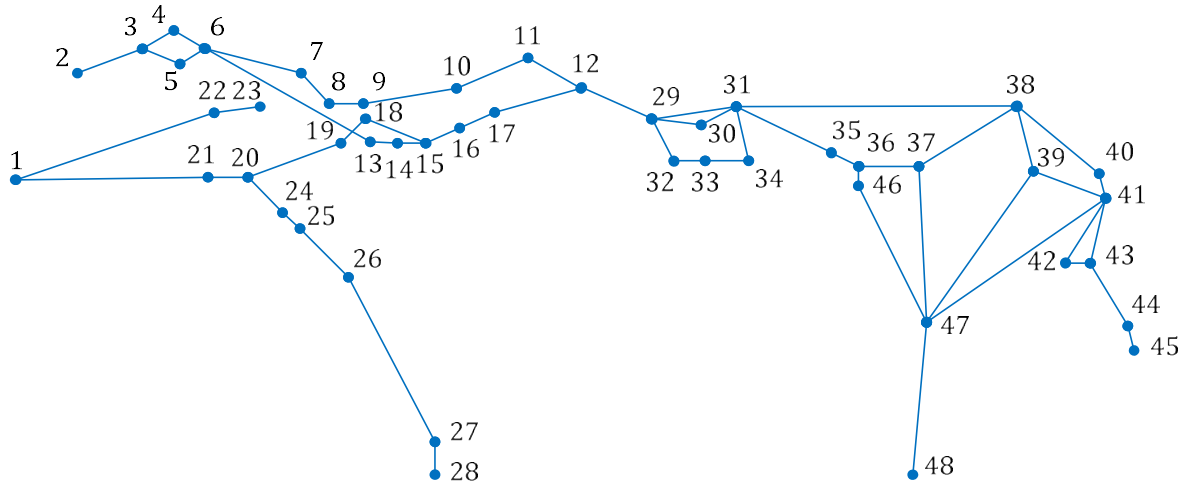


Рис. 1. Граф – модель магистральной сети Ростелеком

Отметим, что максимальное количество сечений равно 105 в направлении связи 2 – 48 ($n = 92$).

Временные затраты на формирование сечений представлены на рис. 3. Стоит отметить, что здесь также время выполнения подобных вычислений не слишком велико и не превысило десяти секунд (максимальное значение характерно для наиболее богатых сечениями направлений связи) и составляет 8,238 с. Тем не менее, несмотря на почти в четыре раза меньшее число сечений, чем путей, максимальное время расчетов возросло более, чем на

порядок, что связано, прежде всего с более затратной процедурой перебора вершинных сечений.

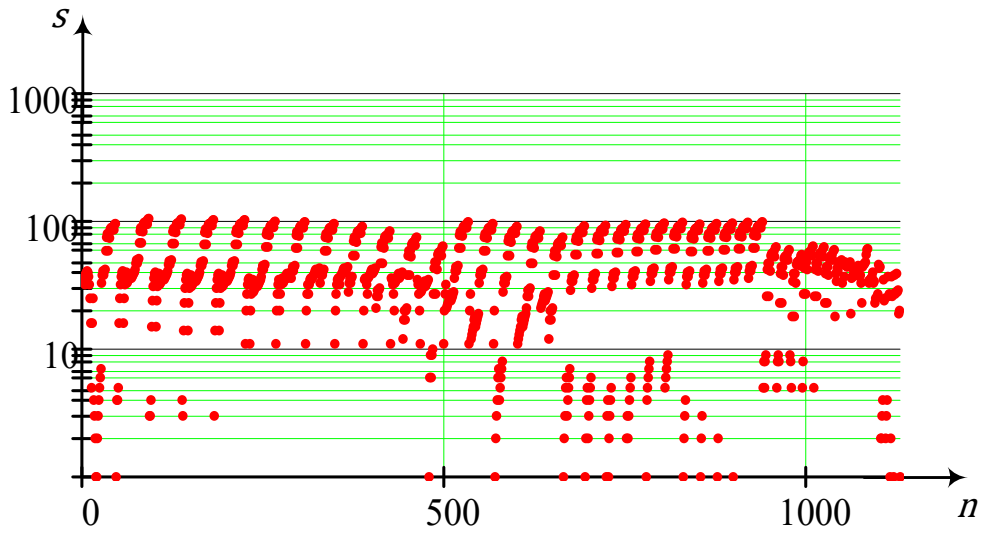


Рис. 2. Зависимость числа *s* сформированных сечений между заданными парами вершин от порядкового номера *n* сечения

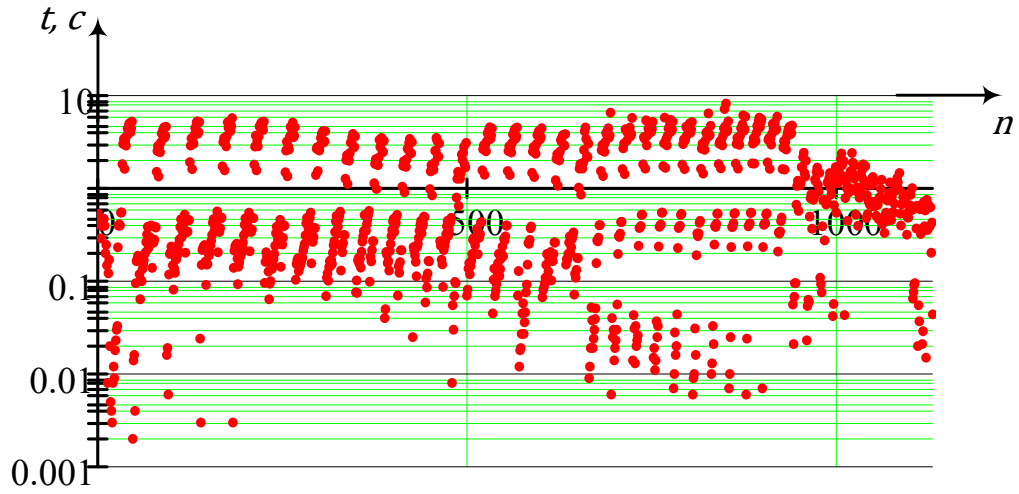


Рис. 3. Зависимость времени *t* выполнения процедуры формирования путей от их порядкового номера *n*

Список используемых источников

1. Chaturvedi S. K. Network Reliability Measures and Evaluation. Scrivener Publishing LLC. 2016. 237 p.

2. Ahmad S. H. Enumeration of Minimal Cutsets of an Undirected Graph // Microelectronics Reliability. 1990. Vol. 30 (1). pp. 23–26.

3. Батенков К. А. Числовые характеристики структур сетей связи // Труды СПИИРАН. 2017. № 4 (53). С. 5–28.

4. Батенков К. А. Общие подходы к анализу и синтезу структур сетей связи // Современные проблемы телекоммуникаций: Материалы Российской научно-технической конференции. 2017. С. 19–23.

5. Батенков К. А. К вопросу оценки надежности двухполюсных и многополюсных сетей связи // Современные проблемы радиоэлектроники: сб. науч. тр. Красноярск: Сиб. федер. ун-т. 2017. С. 604–608.

6. Батенков К. А. Анализ и синтез структур сетей связи по детерминированным показателям устойчивости / К. А. Батенков, А. А. Батенков // Труды СПИИРАН. 2018. № 3 (58). С. 128–159.

7. Батенков А. А. Методы формирования множеств состояний телекоммуникационных сетей для различныхмер связности / А. А. Батенков, К. А. Батенков, А. Б. Фокин // Труды СПИИРАН. 2020. Т. 19. № 3. С. 644–673.

8. Батенков К. А. Точные и граничные оценки вероятностей связности сетей связи на основе метода полного перебора типовых состояний // Труды СПИИРАН. 2019. Т. 18. № 5. С. 1093–1118.

УДК 621.391.82
ГРНТИ 49.33.29

МОДЕЛЬ КОГНИТИВНОЙ РАДИОСЕТИ НА ОСНОВЕ ТЕОРИИ СТОХАСТИЧЕСКОГО СЕТЕВОГО ИСЧИСЛЕНИЯ

А. В. Белов, В. А. Липатников, И. В. Федоров

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

Доступные ресурсы частотного спектра становятся более ограниченными. Предлагается применение когнитивного радио для решения по использованию ограниченного спектра более эффективным способом. Теория стохастического сетевого исчисления способна по полученным вероятностным характеристикам настраивать параметры когнитивной радиосети.

когнитивная радиосеть, стохастическое, сетевое исчисление, вероятностные граничные характеристики.

Техническое развитие сферы информационных услуг способствовало существенному расширению рынка телекоммуникационных устройств. В результате в свободном доступе оказались и радиоэлектронные системы, обеспечивающие прием и передачу информации по радиоканалам.

В статье приводится направление моделирования и анализа инфокоммуникационных сетей и систем – научно-методический аппарат с возможностью практического применения для оценки граничных характеристик,

который позволит синтезировать радиосети когнитивного характера [1]. Целью является получение граничных характеристик исследуемых показателей когнитивной радиосети [2]. С граничными оценками показателей применяются такие понятия как нижняя и верхняя границы, инфимум и супремум [3].

Свойства предлагаемой модели когнитивной радиосети (рис.) заключаются в динамическом изменении параметров функций управления, которые проявляются на различных уровнях иерархий принятия решения в зависимости от качественного изменения информации о когнитивной радиосети.

Для выполнения требований Service Level Argeement (SLA), воспользуемся теорией сетевого исчисления Network Calculus (NC), благодаря которой получим оценочные показатели основных сетевых характеристик, при анализе задержек трафика из конца в конец в радиолинии когнитивной радиосети [3]. Её используют в качестве удобного аппарата для оценки различных сетей, за счет получения детерминированных или стохастических граничных характеристик.

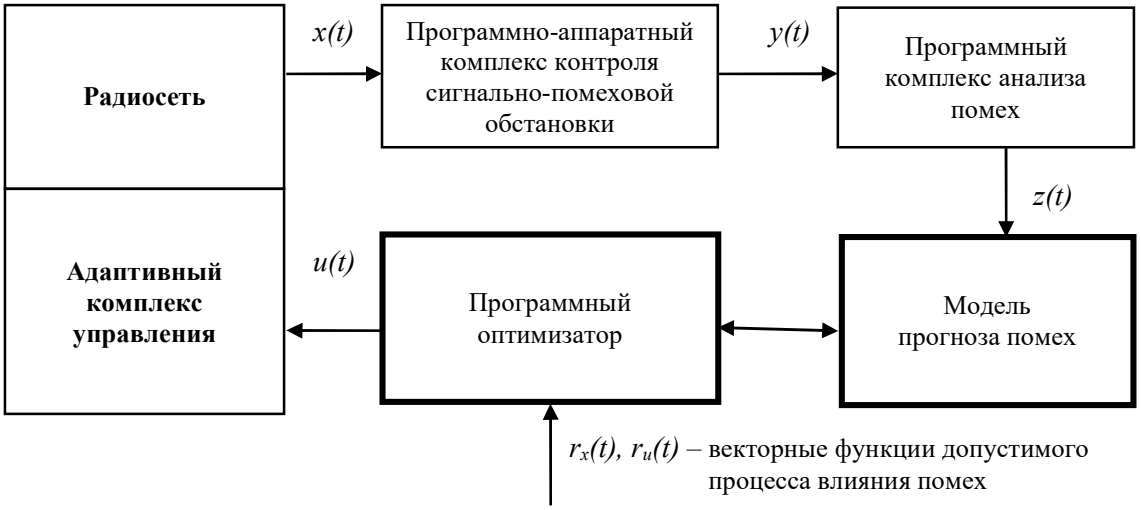


Рис. Структура модели когнитивной радиосети
с прогнозированием сигнально-помеховой обстановки

По настоящее время прогнозирующая модель – Model Predictive Control (MPC) является перспективным направления анализа систем управления в теории управления динамических объектов [4, 5].

В 60-х годах данный метод начал развиваться в различных энергетических сферах для управления процессами и оборудованием, где ранее применяемые методы расчёта приносили неудобство из-за большого объема вычислений математических моделей [6].

Упрощенный алгоритм представлен в таком виде:

1) За основу берётся математическая модель, с начальными условиями которой является её текущее состояние. Программное управление производит интегрирование уравнений данного метода, в следствии чего на определенном конечном отрезке времени выводится динамика изменения движения объекта [6].

2) Для приблизительной регулировки переменных данной модели к задающим сигналам, на конечном отрезке времени происходит оптимизация программного управления, и проектируется комплекс ограничений, добавленных к управляемым и регулируемым переменным.

3) Производится выполненное вычисления оптимального управления и фактического состояния объекта на последнем этапе, на определённом малым горизонте прогноза.

4) Далее цикл повторяется со смещением на следующий отрезок времени.

В данной модели выделяются следующие особенности:

1. Использование нелинейных систем обыкновенных дифференциальных уравнений.

2. Принимаются во внимание ограничения, добавленные на управляющие переменные и компоненты вектора состояния.

3. Качество процесса управления оценивается в динамическом режиме с минимальными ресурсами.

4. Динамический режим позволяет одновременно измерять и оценивать текущее состояние объекта.

5. Прогноз движения объекта не совпадает с реальным движением.

6. Оптимизация задачи управления должно быть рассчитано достаточно быстро, чтобы не превышать допустимый предел запаздывания.

Характеристики потоков поступающих и обслуживающих заявок в системе являются основой данной модели когнитивной радиосети. Анализ и обеспечение гарантий качества обслуживания удобнее осуществить с помощью сетевого исчисления Network Calculus (NC) [7, 8]. Математическая основа сетевого исчисления базируется на идемпотентной математики, позволяющая осуществить свертку и развертку функции моделирования характеристик [9].

На практике использование детерминированной модели неприемлем, в виду завышенных требований гарантий QoS к радиочастотной передачи, а стохастическая модель принимает во внимание случайную природу поступления пакетов с вероятностными ошибками в потоке. Любые, даже малые, всплески (бёрстность трафика) на кривой поступления уже сказываются на её пропускную способность, указывающие на неэффективность использования сетевых ресурсов при передаче мультимедийного трафика. В добавок, линейная зависимость между кривой поступления и количества

потоков не позволяет реализовать мультиплексированных ресурсов многоканальных транспортных сетей.

Идемпотентная математика удобна тем, что может заменять обычные арифметические операции более простыми, основанными на максимальных и минимальных функциях, где их числовые поля заменяются идемпотентными полукольцами и полуполями. В поле вещественных чисел (***R***) возможно можно вывести пример на основе идемпотентной max-плюс алгебры (max ***R***) и min-плюс алгебры (min ***R***). Где Max ***R*** представляет диоид с операциями $x \vee y = \max\{x,y\}$ и $x \times y = x + y$, где максимум равен новому сложению, а новое умножение равнозначно обычному сложению. Также min ***R*** будет являться диоидом с операциями $x \wedge y = \min\{x,y\}$ и $x \times y = x + y$. В $\boldsymbol{R}_{\max}$ алгебре и $\boldsymbol{R}_{\min}$ алгебре представлены две операции, следственно, являются диоидами.

Поток имеет стохастическую кривую поступления α, которая учитывает объем трафика, с граничной функцией *f*, для всех значений $0 \leq s \leq t$ и $x \geq 0$ отсюда вытекает неравенство:

$$P\{A(s,t) - \alpha(t-s) > x\} \leq f(x).$$

Анализ характеристик стохастического обслуживания представлен множеством стохастических моделей. Например, для модели (σ(θ),ρ(θ)) стохастическая кривая поступления заявок представляет граничную функцию $e^{-\theta x}$, где θ – является некоторым заданным параметром.

Выводы

Представленная модель позволяет понизить ошибки при передаче на больших горизонтах прогноза, и применение данных моделей с малым горизонтом оказывается не выгодным в практических целях. Благодаря чему отпадает проблема в выборе горизонта прогноза, и вид переходного процесса достаточно осуществить за счет этих качеств эталонной моделью. За счет этих качеств построение когнитивной радиосети на основе программно-определяемой радиосистемы набирает рост актуальности [10].

В теоретическом аспекте использование теории сетевого исчисления имеет самостоятельное значение и может быть распространено на более широкий класс объектов. Применение теории сетевого исчисления на более широкий класс объектов может стать универсальной методологией при анализе различных систем и сетей [3].

Направление дальнейших исследований авторы связывают с разработкой временных циклов управления ресурсами разработанной модели помехозащищенных радиосетей с прогнозированием сигнально-помеховой обстановки.

Список используемых источников

1. Макаренко С. И. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты: Монография. СПб.: Свое издательство, 2013. 166 с.
2. Липатников В. А., Царик О. В. Методы радиоконтроля. Теория и практика: Монография. СПб.: Военная академия связи, 2018. 607 с.
3. Росляков А. В., Лысиков А. А. Сетевое исчисление Network Calculus. Часть 2. Практическое применение // Инфокоммуникационные технологии. 2020. Т. № 3. С. 237–248.
4. Camacho E. F., Bordons C. Model Predictive Control. Springer, 1999.
5. Maciejowski J. M. Predictive control with constraints. Prentice Hall, 2002.
6. Веремей Е. И., Еремеев В. В. Введение в задачи управления на основе предсказаний // Проектирование научных и инженерных приложений в среде MATLAB: материалы всерос. науч. конф., Москва, 2004. С. 98–115.
7. Jiang Y., Liu Y. Stochastic Network Calculus. London: Springer-Verlag, 2008. 229 p.
8. Cruz R. L. A Calculus for Network Delay, Part I: Network Elements in Isolation // IEEE Transactions on Information Theory. 1991. V. 37. № 1. pp. 114–131.
9. Литвинов Г. Л., Маслов В. П. Идемпотентная математика: принцип соответствия и его компьютерные приложения // Успехи математических наук: сб. науч. тр. / 1996. Т. 51., Вып. 6 (312). С. 209–210.
10. Алекаев А. Е., Липатников В. А., Ряскин Р. Ю., Капкин Ю. А. Модель многоступенчатой адаптации низкоэнергетической радиолинии коротковолнового диапазона с учетом затрачиваемых ресурсов радиолинии и прогнозирования сигнально-помеховой обстановки // Системы управления, связи и безопасности. 2020. № 3. С. 158–183. DOI: 10.24411/2410-9916-2020-10305.

УДК 004.056.53
ГРНТИ 81.93.29

РАЗРАБОТКА БАЗЫ ДАННЫХ ВЫБОРА ПРОТИВОДЕЙСТВУЮЩИХ МЕР ДЛЯ СИСТЕМ ВЫЯВЛЕНИЯ ВРЕДОНОСНОЙ ИНФОРМАЦИИ

Е. О. Березина[1], **Л. А. Виткова**[1,2]

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

Информационные технологии и онлайн взаимодействие сегодня являются частью нашей жизни. Вопрос разработки системы выявления и противодействия вредоносной информации представляется актуальным. В работе рассматривается структура базы данных контрмер и информационных угроз и методика построения подобной базы данных. Предполагается, что такая база данных может взаимодействовать с модулем

выбора контрмер и поддержки принятия решений о противодействии в системах мониторинга и противодействия вредоносной информации.

вредоносная информация, база данных контрмер, системы мониторинга и противодействия, СППР.

Сложно представить современную жизнь без информационного взаимодействия. Сейчас интернет и социальные сети представляют собой крупномасштабную и разнородную информационно-телекоммуникационную среду. Объем информации, с которой пользователи взаимодействуют каждый день, только растет. При этом социальные сети содержат значительное количество разнородной информации, которая может быть истолкована как вредоносная по смыслу и может нанести вред здоровью индивида или побудить к противоправному поведению. Такая информация может стать серьезной угрозой личной, общественной и государственной информационной безопасности [**Ошибка! Источник ссылки не найден.**, 1]. И вопрос разработки системы выявления и противодействия вредоносной информации представляется актуальным.

Сегодня системам противодействия приходится фильтровать трафик на основе политик безопасности, что не всегда является эффективным методом. В основном существующие платформы социальных сетей обеспечивают защиту от вредоносной информации на основании требований законодателя, если веб-страница профиля или сообщества внесены в black-лист, и при этом системы противодействия анализируют только страницы, с которыми взаимодействует пользователь. Ключевой принцип, лежащий в основе работы этих систем, может быть описан как: 1) проверка страницы по списку, 2) ограничение доступа к ресурсу с информацией.

На данный момент существует достаточно большое количество систем реагирования на вредоносную информацию. Эти системы опираются на использование некоторого устоявшегося набора контрмер, таких как фильтрация, блокировка доступа, уведомление.

Поскольку существующие системы зачастую используют только один подход из набора вышеупомянутых контрмер, очевидно, что существует необходимость в классификации контрмер, а также разработке единой базы данных на основе этих контрмер и информационных угроз, на которые они призваны реагировать. База данных, описываемая в данной статье, предназначается главным образом для хранения признаков информационных угроз, информационных объектов с вредоносной информации и мер противодействия, доступных в системе.

Исходными данными для такой базы данных являются html-страницы – сетевые информационные объекты трех категорий в соответствии с «размером» [3]:

– SIO (*Small Information Object*) – малый информационный объект, блок текста на html-странице (она же веб-страница; прим.: комментарий на веб-странице);

– MIO (*Medium Information Object*) – средний информационный объект, отдельная веб-страница некоторого веб-ресурса (несколько веб-страниц, объединенных общей темой и дизайном и связанных между собой ссылками; прим.: веб-страница домена третьего уровня [4]);

– BIO (*Big Information Object*) – большой информационный объект (прим.: веб-сайт домена первого, второго уровня).

Под контрмерой понимается действие (противодействие), направленное на нейтрализацию угрозы информационной безопасности или прекращение доступа к ней пользователю системы. Под соответствующей применимой контрмерой подразумевается такая контрмера, которая наиболее эффективна в противодействии текущей рассматриваемой угрозе, а также является возможной для реализации.

Формальный вид соответствующей применимой контрмеры Measure может быть представлен следующим образом:

$$Measure = \langle Threat, Countermeasure \rangle ,$$

где Threat – рассматриваемая угроза, Countermeasure – соответствующая контрмера, учитывающая атрибуты ее реализации и тип применимого сетевого информационного объекта.

Представим выделенные атрибуты и их взаимосвязи формально:

$$Threat = \langle Definition, Token, Keys\_words \rangle .$$

Перечислим элементы, входящие в этот кортеж:

– Definition – описание угрозы в человекопонятном виде;

– Token – некоторые признаки угрозы информационной безопасности, позволяющие некому оператору, однозначно классифицировать угрозу;

– Keys_words – семантические признаки угрозы для упрощения классификации угрозы.

Аналогичным образом опишем атрибуты контрмеры и их взаимосвязи:

$$Countermeasure = \langle Object, Agent, Implementation\_type, Phase \rangle .$$

Перечислим элементы, входящие в этот кортеж:

– Object – сетевой информационный объект, к которому применима контрмера;

– Agent – агент реализации, через который может быть реализована контрмера (прим.: оператор связи, браузер и т. д.);

– Implementation_type – тип реализации контрмеры (прим.: ручной, авто и т. д.);

– $Phase = \langle Static/Dynamic \rangle$ – этап реализации контрмеры; контрмеры могут применяться на этапе реагирования на вредоносную информацию (т. н. динамические контрмеры) в социальной сети, а также на этапе предотвращения ее распространения (т. н. статические контрмеры).

На рис. представлена диаграмма базы данных вредоносной информации и соответствующих применимых контрмер, цветом выделены справочники в базе данных:

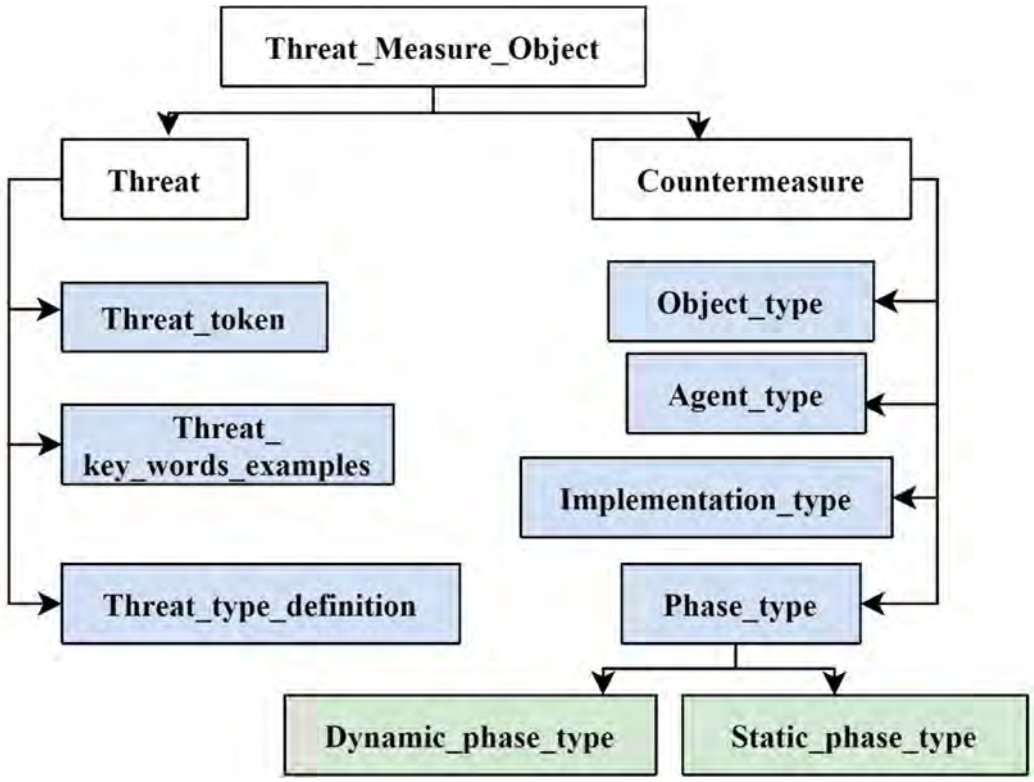


Рис. Диаграмма базы данных
для учета вредоносной информации совместно с мерами противодействия

Структура базы данных состоит из следующих 12 взаимосвязанных реляционных таблиц:

1. Threat_Measure_Object – содержит список угроз и соответствующих им контрмерам;

2. Threat – содержит список угроз в соответствии с атрибутами нежелательной информации;

3. Threat_type_definition – содержит список с описаниями типов угроз;

4. Threat_token – содержит список признаков типов угроз;

5. Threat_key_words_examples – содержит список ключевых слов в соответствии с типами угроз;

6. Countermeasure – содержит список контрмер в соответствии с атрибутами их применения;

7. Object_type – содержит список объектов, к которым применимы контрмеры;

8. Agent_type – содержит список неких агентов реализации, агентов, через которые реализуется контрмера;

9. Implementation_type – содержит список типов реализации контрмер;

10. Phase_type – содержит список категории этапов реализации контрмер;

11. Static_phase_type – содержит список статических этапов реализации контрмер;

12. Dynamic_phase_type – содержит список динамических этапов реализации контрмер.

Выводы

Предложенная база данных может быть использована для улучшения систем противодействия нежелательной информации. К ее преимуществам относится то, что база данных контрмер вредоносной информации содержит информацию о следующих элементах: (1) информационные объекты; (2) угрозы, сопровождающиеся соответствующими признаками и списком характерных ключевых слов; (3) контрмеры, ранжированные в соответствии со способом и типом их реализации. Предложенная база данных может найти применение в области классификации сетевых информационных объектов, угроз нежелательной информации, а также для исследований и разработок решений для поддержки принятия решения о противодействии нежелательной информации.

Работа выполнена при финансовой поддержке Гранта РНФ (проект № РНФ 18-11-00302) в СПб ФИЦ РАН.

Список используемых источников

1. Паращук И. Б., Котенко И. В., Островерхий С. М. Оценка корреляции понятий мониторинга в интересах обнаружения вредоносной информации и положений менеджмента качества информационно-аналитических систем // Информация и космос. 2019. № 2. С. 50–55.

2. Виткова Л. А. Место и роль мониторинга и противодействия нежелательной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 209–212.

3. Валиева К. А., Виткова Л. А., Чечулин А. А. Предварительная обработка информационных объектов в системах мониторинга сети интернет // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 197–201.

4. Какие бывают домены? Виды доменов. Уровни доменов. URL: https://www.domenus.ru/support/help/group/1343472/question/kakie-byvayut-domeny (дата обращения: 05.11.2020).

Статья представлена доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Чечулиным.

УДК 004.056.53
ГРНТИ 81.93.29

РАЗРАБОТКА ДИАГРАММЫ ПОСЛЕДОВАТЕЛЬНОСТИ ТРАФИКА В СЕТЯХ IoT

Л. Н. Богданова[1], **Л. А. Виткова**[2]

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

С каждым годом Интернет вещей (IoT) приобретает большую популярность во многих отраслях жизни, открывая новые формы коммуникации между людьми и вещами. Информация передаётся с помощью датчиков, интегрированных в «умные» приборы. Рост популярности IoT подразумевает разработку решений и алгоритмов обеспечения информационной безопасности Интернета вещей и, в частности, защиты пользовательских данных, передающихся в сетях связи. Проектирование методов защиты информации предполагает наличие чёткого представления о системе, работающей в нормальном режиме. Таким образом, разработка алгоритмов сетевой безопасности IoT подразумевает предварительное описание нормального прохождения трафика. Для наглядного представления обмена пакетами данных составляется диаграмма последовательности, отображающая элементы сети связи. В докладе представлено описание составления диаграммы, описаны сетевые узлы, участвующие в процессе передачи данных и указаны сообщения, обмен которыми осуществляется во время прохождения трафика.

сети IoT,безопасность IoT, угрозы безопасности IoT, анализ трафика, диаграмма последовательности.

Архитектура Интернета вещей охватывает множество технологий. Сложность IoT-систем связана с сочетанием различных, часто не связанных между собой типов архитектур. На 2019, согласно [1], в мире существует более 700 IoT-провайдеров, предлагающих облачные хранилища, системы управления IoT-устройствами, SaaS-компоненты, системы безопасности и любые виды анализа данных.

Ядро IoT-сетей состоит из двух типов устройств: датчиков, собирающих данные, и исполнительных механизмов, получающих команды управления. Организация систем IoT может быть разделена на три уровня: конечные устройства (вещи), сетевые шлюзы (сеть) и облако [1]. Трехуровневая архитектура сети IoT представлена на рис. 1.

Физический уровень состоит из реальных устройств Интернета Вещей, которые являются исполнительными устройствами, подключенными к системе.

Уровень виртуализации действует как промежуточное программное обеспечение между клиентскими приложениями и физическими устройствами. Виртуальные объекты создаются для каждого подключенного устройства Интернета Вещей и используются клиентскими приложениями [2]. Сеть виртуализации IoT устанавливается между связанными устройствами интернета вещей в соответствии с требованиями клиентского приложения и желаемыми настройками. Виртуальные объекты предоставляют интерфейск реальному устройству Интернета Вещей для использования его услуг в клиентских приложениях [3].

Уровень приложения служит для использования услуг уровня виртуализации [4]. Приложения из любого домена могут иметь доступ к общимресурсам через уровень виртуализации. Приложения отображают необходимое количество IoT-устройств с желаемыми настройками подключения через выделенный интерфейс, а логика отражается в виде виртуальной сети среди связанных виртуальных объектов [5].

Основные компоненты системы и взаимодействия между элементами сети IoT отображены на рис. 2 в виде диаграммы последовательности.

Процесс инициируется командой «Запрос о регистрации». Каждое IoT-устройство отправляет информацию о своем профиле на предварительно настроенный сервер виртуализации, отправляя запрос на регистрацию. После проверки информации о профиле устройства создается виртуальный объект для соответствующего устройства Интернета Вещей и на соответствующее устройство отправляется подтверждающее сообщение [6]. Виртуальный объект используется сервером виртуализации для дальнейшей связи с устройством Интернета Вещей.

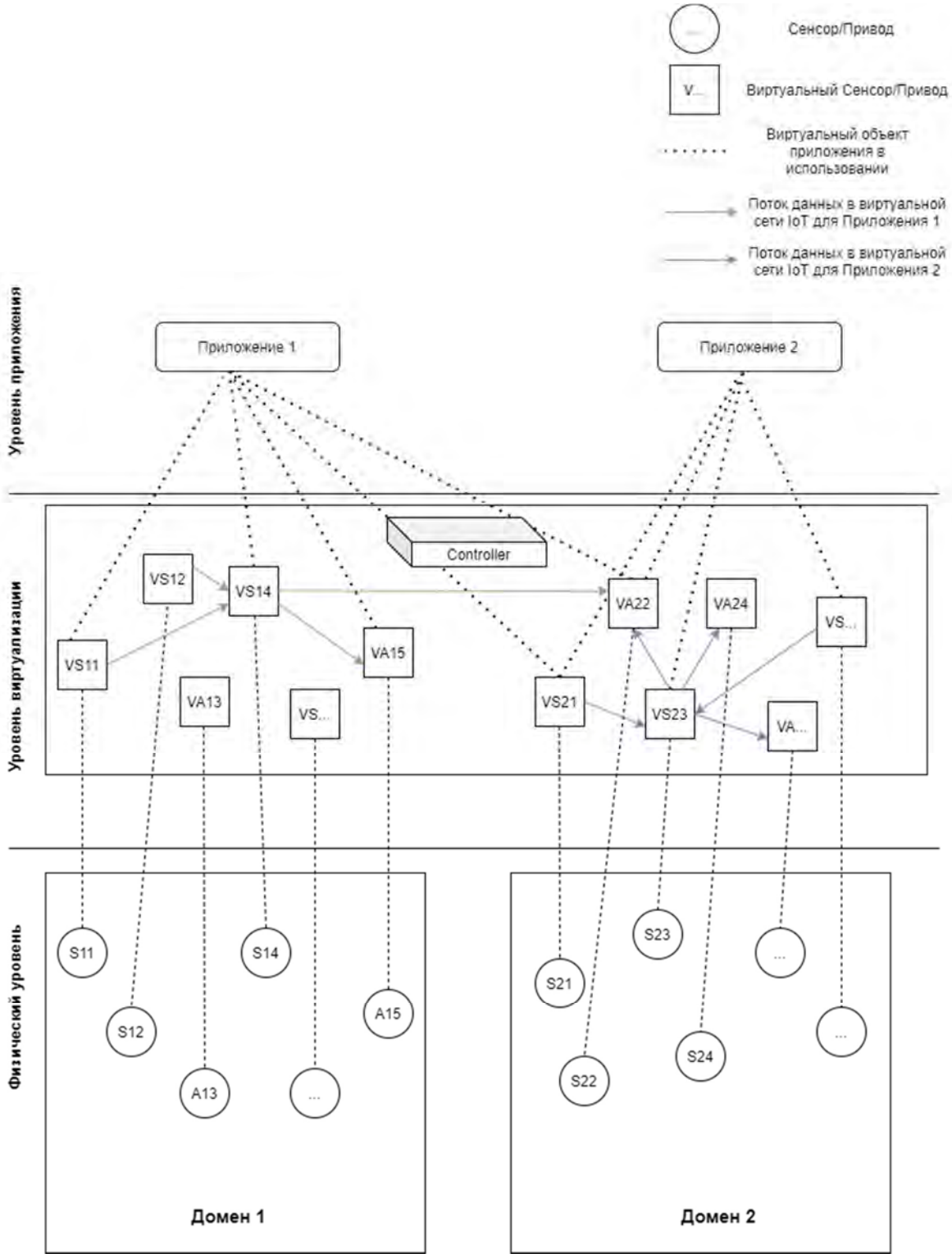


Рис. 1. Трехуровневая архитектура IoT-сетей

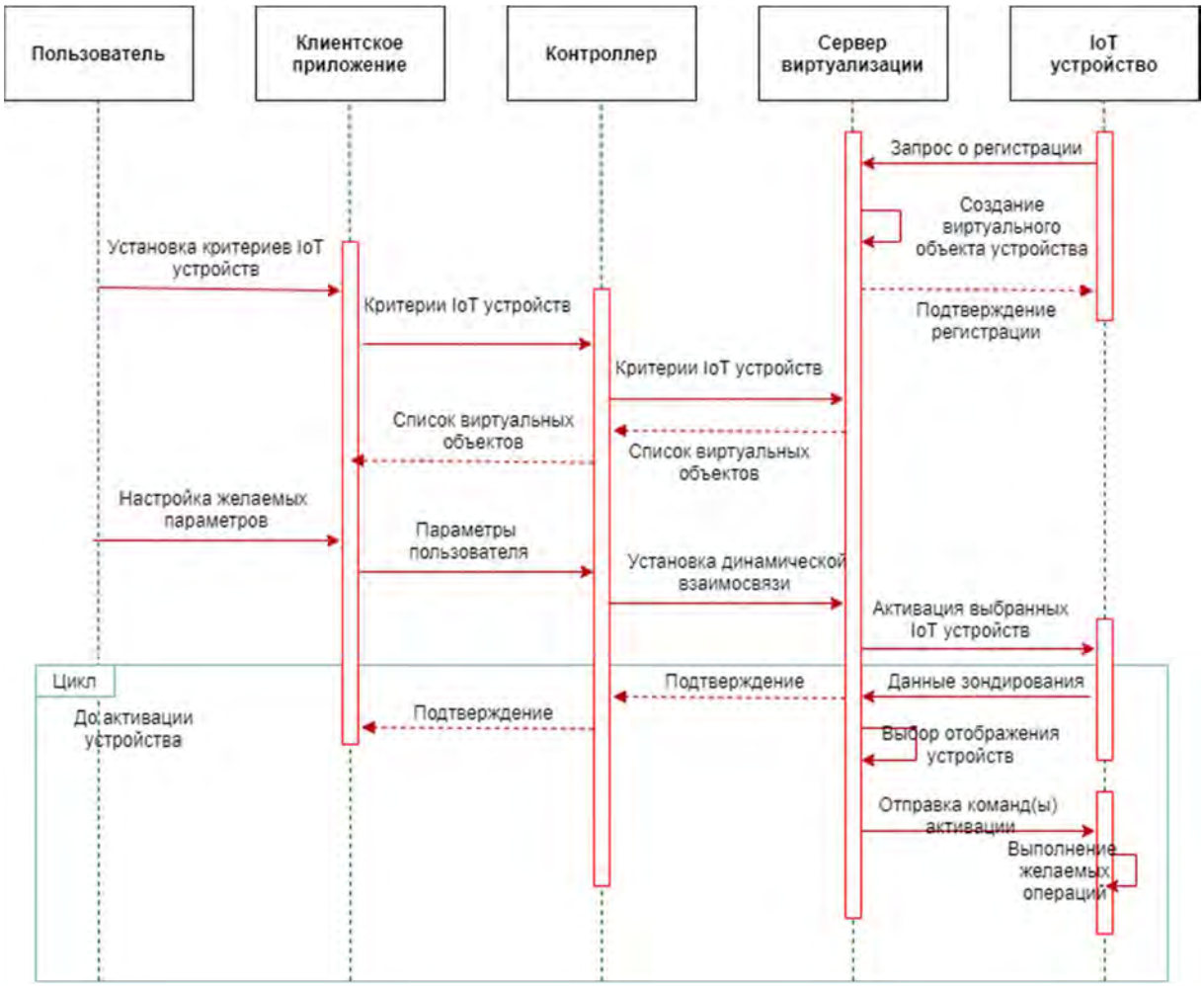


Рис. 2. Диаграмма последовательности трафика в IoT-сети

Далее пользователь инициирует запрос через клиентское приложение на желаемый тип и количество IoT-устройств. Контроллер обрабатывает запрос и извлекает профили виртуальных объектов соответствующих устройств Интернета Вещей в соответствии с заданными пользователем критериями. Получив списки виртуальных объектов в клиентском приложении, пользователь задает и настраивает нужные параметры. После этого нужные пользователю настройки развертываются через клиентское приложение, и запрос передается контроллеру.

Контроллер отвечает за установление желаемых параметров сети путем манипулирования виртуальными объектами на сервере виртуализации [7]. Динамические соединения выполняются между связанными виртуальными объектами в соответствии с желаемыми настройками пользователя путем обновления списка сопоставлений. После этого команда активации отправляется соответствующим датчикам IoT для инициирования передачи данных. Данные принимаются виртуальными объектами, после чего команда активации передается следующему подключенному виртуальному объекту

после выбора отображаемого устройства из списка отображений. Исполнительное устройство выполняет требуемую операцию, и в клиентское приложение отправляется подтверждающее сообщение.

Процесс продолжается до тех пор, пока не закончится время активации устройства. Информация о подключении конкретной виртуализированной сети Интернета Вещей удаляется из списка сопоставления по истечении времени ее активации.

Диаграмма последовательности отображает основные элементы архитектуры Интернета Вещей с учетом актуальных особенностей передачи данных и взаимодействия. Анализ схемы позволяет получить информацию о нормальном прохождении трафика в сети, необходимую при проектировании систем и определения методов обеспечения безопасного соединения.

Список используемых источников

1. Перри Ли Архитектура Интернета Вещей. М.: ДМК, 2019. С. 44–45, 46–50.

2. Shafique K, Khawaja B, Sabir F, Qazi S, Mustaqim M. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios // IEEE Access Special section on antenna and propagation for 5G and beyond. 2020. V. 10

3. Ullah I, Sohail Khan M, Kim D. IoT Services and Virtual Objects Management in Hyperconnected ThingsNetwork // Mobile Infrastructure System. 2018. V.2018

4. Березина Е. О., Виткова Л. А. Модель угроз IoT в программно-конфигурируемых сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 130–134.

5. Tao M, Ota Tao M K, Dong M. Ontology-based data semantic management and application in IoT-andcloud-enabled smart homes // Future Generation Computer System. 2017. V. 76. pp. 528–539

6. Ullah I, Ahmad S, Mehmood F, Kim D Cloud Based IoT Network Virtualization for-Supporting Dynamic Connectivity amongConnected Devices // Electronics MDPI. 2019. V. 8, №. 742, pp. 7–10.

7. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Исследование распределенного механизма безопасности для устройств Интернета Вещей с ограниченными ресурсами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПБГУТ, 2020. С. 321–326.

Статья представлена доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Браницким.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДИКА КЛАССИФИКАЦИИ СООБЩЕСТВ В СОЦИАЛЬНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

А. А. Браницкий[1,2], **И. В. Котенко**[1,2], **Е. В. Федорченко**[1,2]

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

В работе описывается методика классификации сообществ в социальной сети по степени их деструктивного воздействия на пользователей, принадлежащих к социально-демографической группе «молодежь», с использованием текстовых классификаторов, классификаторов, построенных на основе искусственных нейронных сетей, а также их ансамблей. Классификация сообществ в социальных сетях осуществляется на основе данных, полученных в результате проведения теста Аммона среди участников этих сообществ. Результаты экспериментов демонстрируют применимость предложенной методики для выявления деструктивных воздействий в социальной сети.

деструктивное воздействие, социальная сеть, тест Аммона, нейронная сеть, классификация.

В настоящее время социальные сети представляют собой популярные Интернет-сервисы, которые предоставляют как возможность поиска новых друзей и общения с ними, так и создания группы единомышленников для обмена интересующей их информацией. Помимо положительных преимуществ социальных сетей, они могут рассматриваться как источник распространения информации, которая может оказывать деструктивное влияние на их пользователей. Задача выявления групп, содержащих такую информацию, является важной и требует разработки такой методики, которая позволит определить степень их деструктивного воздействия на пользователей. Практическая значимость разработанной методики заключается в том, что построенная на ее основе автоматизированная система может быть использована как вспомогательный инструмент для специалистов-психологов.

Для диагностирования изменений структуры личности используются специальные тесты. В данной статье в качестве такого теста рассматривается тест Аммона [1, 2], который представляет собой список из 220 вопросов, ответы на которые могут быть сформулированы в виде «да» или «нет». Результатом прохождения теста являются измеренные величины Т-баллов

для 18 психологических шкал (например, деструктивной тревоги). В зависимости от значения Т-балла выделяют низкий, средний и высокий уровень соответствующей психологической шкалы.

В разработанной методике в качестве входных данных используются текстовые посты, размещенные на стене сообществ в социальной сети. В рамках данной методики выделяются следующие этапы [3]: (1) прохождение теста Аммона определенной группой пользователей (представителями социально-демографической группы «молодежь»), (2) классификация текстового наполнения сообществ, участниками которых являются исследуемые пользователи, (3) анализ полученных результатов с привлечением специалистов-психологов. Второй этап, выполняемый с использованием текстовых классификаторов и нейронных сетей, состоит из трех шагов: (1) сбор и предобработка текстовых постов из открытых групп, (2) обучение классификаторов, (3) классификация групп в зависимости от выходного значения классификатора.

В качестве классификаторов экспериментально исследовались текстовые классификаторы: (1) простой мешок слов, (2) взвешенный мешок слов, (3) непрерывный мешок слов; классификаторы на основе искусственных нейронных сетей: (4) классификатор skip-gram, (5) классификатор fastText [4]; ансамбли этих классификаторов: (6) простое голосование, (7) взвешенное голосование, (8) мягкое голосование. Использование ансамблей классификаторов подразумевает такое объединение классификаторов, которое позволяет повысить их показатели обоснованности. В данном исследовании объединение классификаторов выполняется таким образом, что их выходные результаты рассматриваются в качестве входных данных для ансамблей, которые, в свою очередь, формируют окончательный результат классификации.

В качестве показателей обоснованности для оценки функционирования классификаторов и их ансамблей использовались (1) аккуратность, (2) точность, (3) полнота, (4) F-мера. Второй, третий и четвертый показатели усреднялись по всем трем рассматриваемым классам («низкий уровень», «средний уровень», «высокий уровень»), соответствующим определенной психологической шкале, поскольку они характерны только для бинарной классификации.

При проведении эксперимента использовалась 10-блочная перекрестная проверка. Исходный набор данных, содержащий посты, представленные в 250 группах социальной сети, разбивался на десять частей. На этапе обучения использовалось 90 % записей, на этапе тестирования – оставшиеся 10 %. Этапы обучения и тестирования выполнялись десять раз, при этом обучающий набор данных замещался одним из девяти кусков, взятым из тестового набора данных. Показатели обоснованности, полученные в рамках десяти этапов тестирования, усреднялись.

На рис. представлены вычисленные значения выбранных показателей обоснованности. Эксперимент выполнялся для классификации сообществ по трем уровням внутри психологической шкалы «деструктивная тревога», при этом в качестве входных данных использовалось только текстовое наполнение постов, которые размещаются на стене этих сообществ. Среди текстовых классификаторов наибольшие значения данных показателей принадлежат простому мешку слов, а среди классификаторов, построенных на основе искусственных нейронных сетей, – классификатору skip-gram. За счет использования ансамбля, построенного на основе мягкого голосования, показатель F-меры увеличился на 0,89 %, показатель точности увеличился на 3,52 %, а показатель полноты уменьшился на 1,48 % по сравнению с наилучшим значением аналогичных показателей, демонстрируемых простым мешком слов.

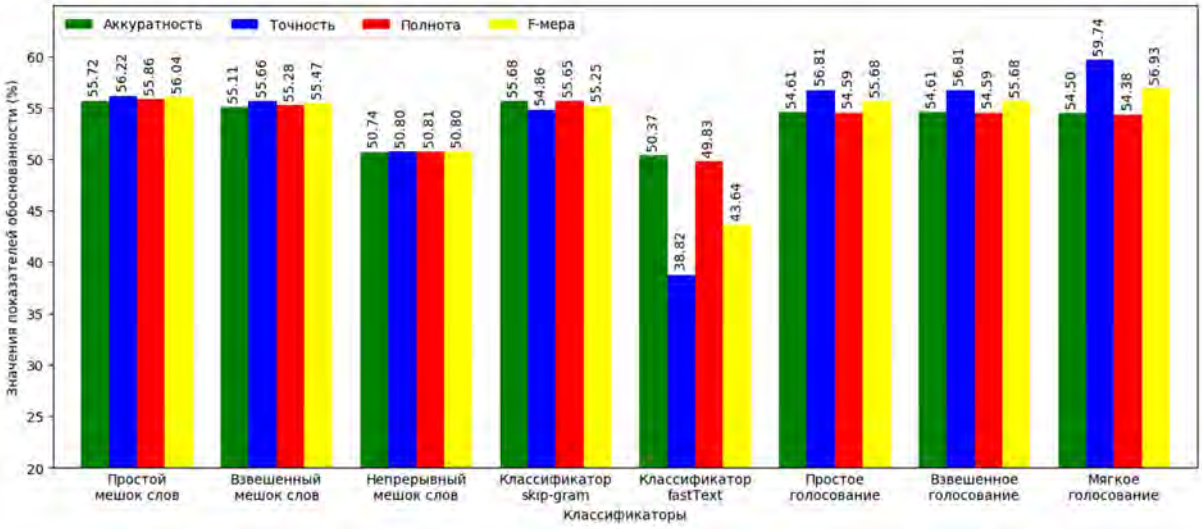


Рис. Показатели обоснованности, вычисленные для текстовых классификаторов, классификаторов, построенных на основе искусственных нейронных сетей, и их ансамблей

Результаты выполненных экспериментов подтверждают возможность применения разработанной методики для классификации сообществ в социальных сетях. Дальнейшая работа может быть связана с повышением эффективности алгоритмов анализа текста и, в частности, алгоритмов обучения классификаторов и построения их ансамблей.

Работа выполнена при финансовой поддержке РФФИ (проект 18-29-22034 мк).

Список используемых источников

1. Кабанов М. М., Незнанов Н. Г. Очерки динамической психиатрии: Транскультуральное исследование. СПб.: Институт им. В. М. Бехтерева, 2003. 438 с.

2. Браницкий А. А., Ванчакова Н. П., Дойникова Е. В., Котенко И. В., Красильникова Н. В., Саенко И. Б., Тишков А. В. Общий подход к выявлению деструктивных информационных воздействий и негативных личностных тенденций молодого поколения с использованием методов нейросетевой обработки Интернет-контента // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 164–167.

3. Браницкий А. А., Дойникова Е. В., Котенко И. В. Использование нейросетей для прогнозирования подверженности пользователей социальных сетей деструктивным воздействиям // Информационно-управляющие системы. 2020. N 1 (104). С. 24–33. DOI: 10.31799/1684-8853-2020-1-24-33.

4. Joulin A., Grave E., Bojanowski P., Douze M., Jégou H., Mikolov T. Fasttext. zip: Compressing text classification models // arXiv preprint arXiv:1612.03651. 2016.

УДК 004.9
ГРНТИ 76.01.85

МЕТОДИКА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Л. Б. Бузюков, Н. Ш. Гусейнов

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

В связи с пандемией коронавирусной инфекции в 2020 году во всех сферах жизни человека остро возникла необходимость в переходе на дистанционное обслуживание, что не обошло стороной и сферу медицинских услуг. Поэтому возрос спрос на медицинские информационные системы (МИС). С ростом потребности медицинских учреждений в МИС появилась необходимость в повышении безопасности подобных сервисов.

цифровое здравоохранение, медицинские информационные системы, база данных, электронные медицинские карты, веб-сервис.

В настоящее время системы здравоохранения развиваются всесторонне, позволяя объединить существующие больничные активы («традиционную больницу»), безопасность и защищённость конфиденциальной информации, а также удобство работы для конечных пользователей. Кроме того, из-за массового перехода в 2020 году многих систем обслуживания на дистанционный формат, на рынке стали весьма актуальны системы онлайн обслуживания пациентов, а также услуги телемедицины.

Возросший поток информации внутри больниц, между ними и клиентами создаёт риски, которые включают в себя возможные угрозы безопасности пациента или потерю конфиденциальной информации и могут быть

вызваны не только злонамеренными действиями, но также человеческими ошибками, сбоями системы [1].

Особую ценность для киберпреступников имеют персональные данные, ведь медицинские карты содержат в себе всю критическую информацию – номер социального страхования, дату рождения и т. д. Это позволяет злоумышленникам использовать эти данные для получения кредитов на стороннее лицо, для налоговых махинаций, выставления фиктивных счетов страховым компаниям, получения лекарственных препаратов строгой отчетности и других [2].

За 2016 год в США было украдено 27 млн. медицинских записей, что в 9 раз больше, чем финансовых. Это почти 10 % населения США. Кроме того, данный тип краж ПД опасен еще тем, что может привести к причинению вреда здоровью человека. Американский альянс по борьбе с мошенничеством в сфере медицины (*Medical Identity Fraud Alliance*) подсчитал, что 20 % жертв кражи медицинских данных получили неверные диагнозы или курсы лечения [3].

В конце 2020 года стало известно об утечке данных 300 тыс. переболевших коронавирусом *COVID-19* москвичей. По данным издания *Readovka*, неизвестные выложили в интернет Ф.И.О., адреса, сведения о течении болезни, анализах и другие данные пациентов, а также ключи к системе учета коронавирусных больных. Газета отметила, что закрытые чаты больниц, доступ к которым также открыли злоумышленники, были «оперативно удалены». Архив с данными больных был выложен в *Google Docs,* откуда его мог скачать любой желающий, что привело к распространению базы данных по сети Интернет [4].

Из этого следует, что для использования МИС в учреждениях системы здравоохранения необходимо решить ряд программных, организационно-технических вопросов, в первую очередь связанных с соблюдением врачебной тайны и защитой персональных данных.

МИС – это электронная база данных (БД), которая помогает эффективно выстраивать работу с пациентами, контролировать административные и финансовые вопросы. Отличительной чертой медицинских информационных систем можно назвать изменение локального способа работы с медицинской информацией к системе, в которой, вся необходимая информация, проходящая через медучреждение, может быть доступна из единой информационной среды.

Типовая МИС предназначена для поддержки деятельности лечебно-профилактического учреждения (ЛПУ) и отличается от других программных продуктов прежде всего тем, что в ней хранится и обрабатывается персональная и конфиденциальная информация. Юридически медицинские сведения о пациентах относятся к информации, составляющей профессиональную тайну, доступ к ней ограничен и регламентируется действующим

законодательством. В соответствии с этим в МИС обязательно должен быть реализован ряд мер по обеспечению безопасности. Структура и схема данных МИС приведена на рис. 1 и рис. 2 соответственно.

Рис. 1. Структура данных в МИС

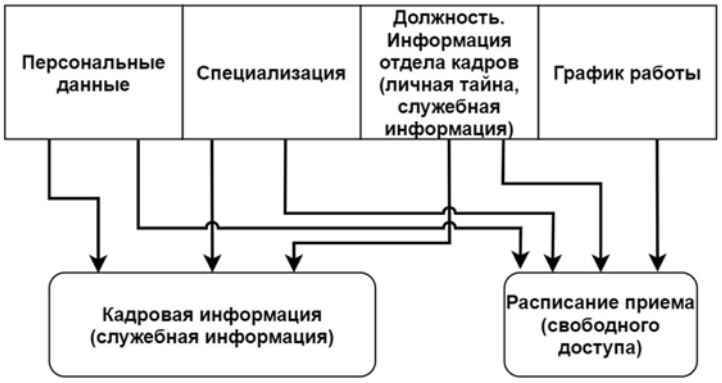


Рис. 2. Схема данных о сотрудниках клиники в МИС

В МИС содержится информациях о пациентах и работниках клиники. Например, история посещения, диагноз, рекомендации по лечению и т. д. Персональные данные отнесены законодательством к личной тайне человека. Более того, они выделены в особую категорию, охраняемую специальным образом. Основными типами совокупностей медицинской информации являются:

– информация пациента;
– информация сотрудника ЛПУ;
– справочная информация, описывающая ЛПУ;
– справочная информация, описывающая предметную область.

Информационная безопасность (ИБ) при функционировании медицинской информационной системы обеспечивается за счет взаимоувязанного

комплексного использования организационных мер, программных и технических средств защиты. Основными направлениями возможных нарушений ИБ являются:

– утечка данных (нарушение конфиденциальности);
– утрата данных;
– несанкционированная модификация данных.

При включении в МИС средств обеспечения информационной безопасности необходимо помнить, что наращивание требований по ИБ неизбежно накладывает ограничения на доступность данных для пользователей МИС.

Есть три вектора информационной безопасности:

– конфиденциальность,
– целостность,
– доступность данных.

Ниже приведен список видов угроз в зависимости от уровня модели OSI и их возможный метод решения:

• На физическом уровне – выведение из строя аппаратных средств хранения, обработки и передачи информации, отказ, уничтожение носителей информации. Основной источник угроз – техногенные аварии, нарушение правил эксплуатации.

• На сетевом уровне и уровне сетевых приложений и сервисов – блокирование работы серверов МИС, несанкционированный доступ к информационному ресурсу в результате ошибочных настроек сетевых сервисов. Угрозы ведут к потере доступности и конфиденциальности информации. Для защиты данных необходимо использование протоколов HTTPS и TLS. Обеспечение защищенности сайта, на котором работает МИС, посредством SSL-сертификата безопасности, которая работает поверх протокола HTTPS с использованием шифрованием данных (логина и пароля) при работе с сайтом.

• На уровне операционных систем – нарушение работы прикладного ПО, уничтожение информации в результате заражения вредоносным ПО (вирус, троянский конь, черви и т. д.). Для обеспечения защиты и стабильной работы МИС необходимо производить регулярные обновления ОС и поддерживать актуальную базу антивируса.

• На уровне управления БД наиболее опасной угрозой является несанкционированный доступ к БД в результате получения административных паролей системы управления базами данных (СУБД), паролей администраторов МИС и т. д. Результатом воздействия таких угроз может быть потеря доступности данных вследствие нарушения работоспособности СУБД и удаления (изменения) объектов или настроек, нарушение целостности, нарушение конфиденциальности данных. Для повышения безопасности БД необходима фильтрация не нужных символов при работе с БД для предотвращения кибератак посредством SQL-инъекции.

- На уровне технологического процесса – ввод фиктивной информации, неправомерный вывод и разглашение конфиденциальной информации. Основное воздействие данных угроз – на целостность и конфиденциальность информации [7]. Необходимо, чтобы все, кто работает с ПД понимали важность конфиденциальности и ответственность за их разглашение или ввод неверной информации

При создании МИС необходимо продумать каждый уровень таким образом, чтобы они соответствовали всем требованиям безопасности при работе с конфиденциальными данными, проводить тщательное тестирование каждого этапа. Ведь от каждого уровня будет зависеть работоспособность всей системы, насколько она будет защищена и обеспечена стабильная работа при ее эксплуатации. Тем самым уменьшив количество «лазеек» для несанкционированного доступа до минимума.

Список используемых источников

1. Суслина Алена Умные больницы: как обеспечить защиту от угроз и безопасность инфраструктуры? // Anti-Malware.ru – информационная безопасность для профессионалов. URL: https://www.anti-malware.ru/practice/methods/Smart-hospitals-how-to-provide-threat-protection-and-infrastructure-security

2. Вахонин Сергей Как защитить от утечки медицинские данные // Anti-Malware.ru – информационная безопасность для профессионалов. URL: https://www.anti-malware.ru/practice/methods/how-protect-medical-data-from-leakage

3. Статистика кражи персональных данных // Медиацентр Panda Security – Вся информация об информационной безопасности. URL: https://www.cloudav.ru/mediacenter/tips/identity-theft-statistics/

4. Утечки данных в медицинских учреждениях // Zdrav.Expert – Издание о новых технологиях в здравоохранении. URL: https://zdrav.expert/index.php/Статья:Утечки_данных_в_медицинских_учреждениях

5. Что такое медицинская информационная система (мис) и ее помощь в работе клиники // Управление медицинской клиникой в Санкт-Петербурге – решения от «Первого БИТа». URL: http://spb.bit-medic.ru/articles/chto-takoe-mis/

6. Карабаев М. К. Абдуманонов А. А. Алгоритмы и технологии обеспечения безопасности информации в медицинской информационной системе ExterNET // Международный журнал "Программные продукты и системы". URL: http://swsys.ru/index.php?page=article&id=3404

7. Гулиев Я. И., Фохт И. А., Фохт О. А., Белякин А. Ю. Медицинские информационные системы и информационная безопасность. Проблемы и решения // Программные системы: теория и приложения. Переславль-Залесский, 2009. ISBN 978-5-901795-18-7. URL: http://skif.pereslavl.ru/psi-info/psi/psi-publications/e-book-2009/volume2/175-Guliev.Healthcare_Information.pdf

УДК 004.9
ГРНТИ 76.01.85

АНАЛИЗ ПРОБЛЕМ ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ КЛИЕНТОВ В СФЕРЕ МЕДИЦИНЫ

Л. Б. Бузюков, М. Л. Клочков

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

В 2020 году в связи с пандемией COVID-19 многие сферы услуг были вынуждены перейти на дистанционный формат обслуживания. По этой причине среди медицинских организаций возрос спрос на медицинские информационные системы (МИС), особенно на комплексные системы (КМИС). Их главным преимуществом является способность контролировать оптимизацию затрат и улучшать качество обслуживания пациентов.

цифровое здравоохранение, электронные медицинские карты, телемедицина, комплексные медицинские информационные системы, база данных, электронные медицинские карты, лечебно-профилактические учреждения, веб-сервис.

Активный тренд современного рынка – это цифровое здравоохранение или digital healthcare. Данный тренд не случайно пользуется повышенным вниманием в последние годы: его задача включает заботу о развитии взаимосвязанных систем здравоохранения. Цель – повысить эффективность использования вычислительных технологий, интеллектуальных устройств, методов компьютерного анализа и средств связи в сфере здравоохранения [1].

Больше всего рынок телемедицинских услуг развит в США. Согласно исследованию компании Grand View Research, мировой рынок электронных медицинских карт (ЭМК) еще в 2016 году составлял 23 млрд, а к 2025 году вырастет до 33 млрд. Также активно ведутся разработки в этом направлении в Бразилии, Индии, России и странах Азии [2].

В 2011–2012 году в России началась масштабная информатизация медицины: был запущен проект создания «Единой государственной информационной системы здравоохранения» (ЕГИСЗ). За восемь месяцев 2020 года по данным аналитической платформы Dsight число медицинских онлайн-консультаций выросло в два раза по сравнению с 2018 годом, когда законом было разрешено проводить консультации пациентов удаленно [3].

Пандемия коронавируса показала необходимость ускорить цифровизацию здравоохранения. Пациенты в ситуации локдауна были значительно ограничены в возможности получить медицинские услуги. Только на Дальнем Востоке из-за пандемии число профосмотров на туберкулез снизилось

на 35 %, число плановых госпитализаций – на 38 % и на 36 % – число хирургических вмешательств.

По данным Всемирной организации здравоохранения (ВОЗ) 68 % государств столкнулись с перебоями в предоставлении медуслуг, включая мониторинг диабета, гипертонии, скрининга рака. Такие сбои грозят ростом смертности от тяжелых заболеваний, отмечают в ВОЗ. Начиная от «красных» зон реанимаций с тяжелыми пациентами с COVID-19, дистанционным обменом опытом врачей и заканчивая сопровождением больных на амбулаторном лечении – во всех этих случаях стала остро востребована телемедицина [4].

Поэтому все чаще стали прибегать к использованию медицинских онлайн-платформ для всех секторов здравоохранения с целью повышения оперативной эффективности системы. Повышается ценность медицинских информационных систем (МИС).

МИС – это важный инструмент автоматизации документооборота для лечебно-профилактических учреждений. В ней объединены система поддержки принятия медицинских решений, электронные медицинские карты пациентов, данные медицинских исследований в цифровой форме, данные мониторинга состояния пациента с медицинских приборов, средства общения между сотрудниками, финансовая и административная информация.

Преимущества такой системы заключаются в следующем:

- Для директора клиники – удобное отображение статистики по работе клиники и конструктор построения отчетов.
- Для администратора клиники – удобная система отображения расписания каждого специалиста, ведение бухгалтерии и печать необходимых документов по клику мыши.
- Для врачей – напоминания о записи на прием, полная история болезни, различные планы лечения и прейскуранты на услуги [3].
- В целом – система экономит время врача и пациентов. Кроме того, дистанционная консультация чаще всего дешевле очной (в России в среднем на 20–50 %) [5]. Электронные карты хранят всю историю болезни пациента, что дает полную картину врачу в постановке диагноза и организации лечения.

Таким образом, МИС упрощает и оптимизирует управление больницами без использования лишних ресурсов, помогает формировать кадры, распоряжаться финансами, материальными ресурсами. Цифровизация медицинской отрасли способствует развитию телемедицины в стране, массовому внедрению удаленного консультирования, скорой помощи онлайн [2].

В России основоположником системной классификации медицинских информационных систем (МИС) является С. А. Гаспарян, который опубликовал три варианта классификации за период 1978–2001 годов. В последней своей версии он рассматривал пять основных групп МИС. В том же году

Г. А. Хай предложил свой вариант классификации и структурировал МИС по типам (рис.).

Рис. Классификация МИС

Важнейшая роль в развитии информационных технологий в здравоохранении принадлежит Федеральным законам «Об обязательном медицинском страховании» и «Об основах охраны здоровья граждан в Российской Федерации». В концепции создания единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ) изложены основные параметры, цели и задачи информатизации [6].

Рассмотрим наиболее значимые проблемы при внедрении МИС и их возможные пути их решения:

1. Проблема организации системы. Сюда входит отсутствие организованного подхода к внедрению и эксплуатации системы, а также недостаточно развитая нормативная база. Законодательство тормозит внедрение МИС, отсутствие стандартов и несовместимость оборудование ведет к неоптимизированной работе. Возможное решение: реформа законов, под необходимости МИС, проведение программы обучения данной системой среди медперсонала, организовать доступность обращения к системе пациентов;

2. Невозможность полного перехода на электронный документооборот. У некоторых организаций сложился консервативный подход, связанный с документооборотом [7]. Возможное решение: проведение поэтапного внедрения ЭДО, введение единого стандарта электронных документов. Требуется перестройка бизнес-процессов организации. Также необходимо создание мощных дата-центров для хранения информации системы;

3. Переоценка или недооценка возможностей МИС. Переоценка возможностей МИС ведет к неоптимизированной работе, как и недооценка, связанная с нежеланием полностью овладеть всеми функциями системы [8].

Решением этой проблемы будет проведение полного инструктажа по работе МИС, чтобы каждый сотрудник, работающий с системой, понимал ее возможности и знал, как с ней работать. Как при решении первой проблемы, необходимо наличие среди персонала технического специалиста для сопровождения системы и помощи персоналу в работе с ней;

4. Внедрение МИС весьма затратно и требует дорого оборудования, а в некоторых больницах порой нет даже современных компьютеров. Более того, даже при наличии компьютера по данным IT-компании АРМИТ около 40 % врачей не имеет доступа к сети Интернет. Также требуется должное обучение медицинского персонала для эксплуатации электронной системы, на что опять же требуются большие денежные затраты и время. Решением проблемы является помощь со стороны государства. Активное финансирование подобных проектов и их продвижение. Проведение дополнительной программы по обучению персонала;

5. Надежность системы. Это не только надежность защиты конфиденциальных данных пациентов и всей клиники, а также закрытый доступ к управлению всей базой, но и бесперебойность системы и ее эффективность при работе в форс-мажорном режиме. Решение проблемы: перед закупкой систем данного типа следуют тщательно смотреть исходный код ПО и результаты тестирования. Надежность МИС МО должна обеспечиваться следующими способами: надежность системы электропитания; возможность реализации механизма восстановления баз данных; сохранение резервных копий базы на независимые носители информации и т. д. [9].

В качестве прототипа МИС, обеспечивающей решение вышеуказанных проблем, предлагается комплексная МИС (КМИС), что является неким симбиозом Технологической информационной медицинской системы и Банка информации медицинских служб. Предполагаемая среда эксплуатации – частная клиника. Система представляет из себя специализированное программное обеспечение, которое ставится на сервере в клиники (или удаленно). Пользование системой осуществляется с помощью авторизации, для которой имеется три типа доступа: врач, пациент, администратор. Назначение системы заключается в организации онлайн-записи пациента к врачу, а также информировании клиента о ходе лечения.

В данной статье были проанализированы основные проблемы внедрения МИС в сфере здравоохранения и приведен ряд возможных решений. Подводя итоги, можно сказать, что телемедицина и МИС – одни из быстрорастущих и очевидных сейчас векторов развития медицины. В нынешних внезапных условиях пандемии данный вектор набрал дополнительную популярность. В случае поддержки в развитии данной отрасли со стороны государства (разрешении на деятельность и обеспечении гарантий для пациента) данное направление будет активнее расширяться и привлекать все

больше клиентов. Данная сфера еще молодая и у нее есть большой потенциал в развитии.

Список используемых источников

1. Цветкова А. Переходим на цифровое лечение: как пандемия меняет рынок медицинских услуг? // Новости 33. URL: http://novosti33.ru/2020/11/perehodim-na-tsifrovoe-lechenie-kak-pandemiya-menyaet-rynok-meditsinskih-uslug/ (дата обращения: 05.12.2020)

2. Резник И. Цифровизация сделает здравоохранение эффективным // Партнерские приложения и тематические проекты РБК+ Санкт-Петербург и область. URL: https://plus.rbc.ru/news/5f6e921e7a8aa9bebb4f7e6b (дата обращения: 05.12.2020)

3. Кузовков С. Обзор медицинских информационных систем (МИС) в 2020 году // Симметрия Medical – комплексные решения для медицинских компаний. URL: http://symmetria-med.ru/blog/obzor-meditsinskih-informatsionnyh-sistem-mis-v-2020-godu.html (дата обращения: 10.12.2020)

4. Цифровая медицина как способ сократить бумажную работу в сфере здравоохранения // Конференция M-Health Congress – телемедицина, технологии и инновации для здоровья, медицинская конференция. URL: https://mhealthcongress.ru/ru/article/tsifrovaya-meditsina-kak-sposob-sokratit-bumagnuyu-rabotu-v-sfere-zdravoohraneniya-96477 (дата обращения: 20.12.2020)

5. Телемедицина в России: деньги, риски и искусственный интеллект // vc.ru – бизнес, технологии, идеи, модели роста, стартапы. URL: https://vc.ru/services/126485-telemedicina-v-rossii-dengi-riski-i-iskusstvennyy-intellekt (дата обращения: 18.12.2020)

6. Кошкаров А. А., Рубцова И. Т., Семенов А. Б., Халафян А. А. Автоматизация медицинской экспертизы назначения льготных лекарств // Научная электронная библиотека Монографии, изданные в издательстве Российской Академии Естествознания. URL: https://www.monographies.ru/ru/book/section?id=13847 (дата обращения: 20.12.2020)

7. Как перейти на ЭДО: пошаговая инструкция // Электронный документооборот ДИАДОК – СПБ Контур. URL: https://kontur.ru/diadoc/spravka/275-perehod_na_edo (дата обращения: 22.12.2020)

8. Гарнец А. А. Проблемы внедрения медицинских информационных систем и подходы их решения // Вестник Восточноукраинского национального университета имени Владимира Даля. 2013. Ч. 2. № 4 (193).

9. Рекомендации по надежности // Методические рекомендации по обеспечению функциональных возможностей медицинских информационных систем медицинских организаций (МИС МО) (утв. Минздравом России 01.02.2016).

УДК 004.422.81
ГРНТИ 50.41.25

АНАЛИЗ ПРОБЛЕМ И КОНЦЕПЦИЯ СИСТЕМЫ КОНТРОЛЯ РАБОТЫ СОТРУДНИКОВ

Л. Б. Бузюков, А. В. Сударев

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

В настоящее время многие компании внедряют у себя системы учета рабочего времени. Главная цель при этом экономическая — повышение эффективности труда. Но побочным эффектом часто становится недовольство работников. Потому что попытку контроля они воспринимают как явное недоверие со стороны руководства, и даже как стремление «закрутить гайки». Как избежать ухудшения отношений и не остаться без работников?

отслеживание сотрудников, менеджмент, WinAPI, C++, Winsock, база данных.

Данная тема интересна тем, что во время карантина вырос спрос на специальные программы, позволяющие контролировать работу удаленных сотрудников [1, 2].

Спрос на инструменты контроля работы сотрудников растет во всем мире. По данным газеты The New York Times, продажи софта компании Hubstaff (компания, которая обеспечивает мониторинг персонала) с марта до начала мая подскочили в три раза [1]. Программа раз в несколько минут делает скриншоты монитора и подсчитывает, сколько времени пользователь печатал или пользовался компьютерной мышкой, фиксирует сайты, на которые заходит сотрудник, и его GPS-координаты.

Контроль как часть мониторинга рабочего времени позволяет решать несколько задач [3]:

1. Фиксировать время прихода на работу, чтобы вычислить систематически опаздывающих и отсутствующих.
2. Проверять своевременное возвращение работника после обеденного перерыва и присутствие на рабочем месте в течение всего дня.
3. Определять время окончания работы.
4. Выявлять прогульщиков.
5. Разделять оплачиваемые периоды рабочего времени на фактически отработанные часы, отпуск, больничный, простой по вине нанимателя и т. д.

Главная проблема удаленного контроля – вопросы приватности. Многие программы содержат кейлоггеры (программное обеспечение регистрирующее различные действия пользователя), могут записывать звук и видео,

перехватывать изображение с веб-камеры, сообщения почты. Поэтому внедрение программы учета, особенно внезапное, может вызвать снижение лояльности сотрудников. У сотрудников растет стресс и снижается мотивация: «Они отвлекаются на мысли о «взломе системы» и ухода от контроля» [2].

Как видно из таблицы, до 37 % рабочего времени сотрудники отсутствуют за персональным компьютером [4]. Поэтому самым легким в плане реализации и безболезненным для личной конфиденциальности сотрудников способом контроля работы сотрудников будет отслеживание их присутствия на рабочем месте: для этого не понадобятся технологии, ставящие под вопрос приватность сотрудников. Для этого можно использовать встроенные в операционные системы технологии отслеживания активности пользователя, такие как: отслеживание движения курсора мыши и нажатие клавиш клавиатуры. То есть если пользователь никак не взаимодействует с ПК, то он считается неактивным.

ТАБЛИЦА. Статистика эффективности использования рабочего времени

Дата: 25.11.2017	**В среднем**	**По профессии**				
		бухгалтеры	**ИТ-персонал**	**секретари**	**продавцы**	**колл-центр**
Общая информация						
Продуктивно затраченное время	18%	17%	11%	12%	22%	18%
Нейтрально затраченное время	16%	16%	9%	8%	16%	22%
Непродуктивно затраченное время	39%	29%	27%	73%	43%	34%
Простой (отсутствие за ПК)	17%	21%	37%	3%	14%	16%
Опоздания	6%	12%	13%	3%	2%	9%
Переработки	3%	5%	3%	1%	3%	1%

В наборе базовых функций интерфейсов программирования приложений операционных систем семейств Microsoft Windows (WinAPI) присутствует функция, которая возвращает время с момента последнего входного события пользователя: BOOL GetLastInputInfo (PLASTINPUTINFO plii) [5].

Чтобы узнать сколько времени простаивал ПК, необходимо вызвать функцию GetTickCount [6], которая возвращает количество миллисекунд, прошедших с момента запуска системы, и вычесть из полученного значения время GetLastInputInfo. Получится текущее время бездействия пользователя, которое можно сравнивать с заданным максимально допустимым значением. Если оно будет больше максимально допустимого значения, можно сделать следующее: вывести, например, сообщение с предупреждением и где-нибудь сохранить это событие, чтобы руководитель мог видеть, что его

сотрудник бездействует. Пример реализации данного алгоритма приведён на рис. 1.

```
#include <windows.h>

#define TIME_AFK 60 // Время отстутствия в секундах

int main() {
    LASTINPUTINFO* afk = new LASTINPUTINFO;
    afk->cbSize = sizeof(PLASTINPUTINFO);
    GetLastInputInfo(afk);

    //Вычисление текущего времени бездействия пользователя
    ULONGLONG current_afk = (GetTickCount64() - afk->dwTime) / 1000;

    // Если пользователь отсутствовал больше заданного времени TIME_AFK
    if (current_afk > TIME_AFK) {
        // Выполнение какого-либо действия
    }

    return 0;
}
```

Рис. 1. Пример алгоритма вычисления времени бездействия пользователя

Сохранять данные на ПК сотрудника не безопасно: он может взять и удалить записи и смысл в этой программе пропадёт. Поэтому понадобится централизованное хранилище базы данных. То есть сообщение о бездействии сотрудника будет отправляться на сервер и там сохраняться. Администратор сможет подключиться к серверу и изучить сведения о бездействии сотрудников. Передачу данных лучше всего организовать по сетевой модели TCP/IP, которая реализована через сокеты Беркли в WinAPI [7].

Для удобства просмотра записей из сервера можно разработать ещё одну специальную программу (рис. 2), которая будет получать данные из базы MySQL и выводить их на экран. Для этого предусмотрена библиотека MySQL Connector/C++ X DevAPI [8].

Подключившись к базе данных и получив оттуда необходимые данные, их можно вывести на экран, используя любую библиотеку построения графического интерфейса пользователя: Qt, wxWidgets и другие.

```
#include <mysqlx/xdevapi.h>
#include <iostream>
#include <string.h>
int main(){
    {
        mysqlx::Session mySession("localhost", 33060, "eyeserver", "Borrow145!");
        mysqlx::Schema db = mySession.getSchema("education");
        mysqlx::Table myTable = db.getTable("Salespeople");

        myTable.insert("sname", "city", "comm").values("Ivan", "Moscow", 0.01).execute();

        mysqlx::RowResult res = myTable.select("*").execute();

        for (mysqlx::Row row : res.fetchAll()) {
            std::cout << "snum: " << row[0] << std::endl;
            std::cout << "sname: " << row[1] << std::endl;
            std::cout << "city: " << row[2] << std::endl;
            std::cout << "comm: " << row[3] << std::endl;
        }
```

Рис. 2. Пример подключения к серверу MySQL

В результате проделанной работы можно сделать следующие выводы в предлагаемом программном обеспечении:

- программа такого класса будет проста в написании,
- требует мало вычислительных ресурсов,
- практически не нуждается в обслуживании,
- сохраняет конфиденциальность сотрудников,
- помогает решить проблему отсутствия сотрудников за ПК.

Список используемых источников

1. The New York Times. How My Boss Monitors Me While I Work From Home. URL: https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html (дата обращения 24.12.2020).

2. РБК+. Бизнес на удаленке включает тотальный контроль. URL: https://plus.rbc.ru/news/5fbbba267a8aa9f2975810a4 (дата обращения 29.12.2020).

3. СёрчИнформ. Методы контроля рабочего времени. URL: https://searchinform.ru/kontrol-sotrudnikov/uchet-rabochego-vremeni/metody-kontrolya-rabochego-vremeni/ (дата обращения 24.12.2020).

4. Kickidler. Статистика эффективности использования рабочего времени. URL: https://www.kickidler.com/ru/statistics.html

5. Microsoft documentation. GetLastInputInfo function. URL: https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-getlastinputinfo (дата обращения 24.12.2020).

6. Microsoft documentation. GetTickCount function. URL: https://docs.microsoft.com/en-us/windows/win32/api/sysinfoapi/nf-sysinfoapi-gettickcount (дата обращения 24.12.2020).

7. Microsoft documentation. Winsock Network Protocol Support in Windows. URL: https://docs.microsoft.com/en-us/windows/win32/winsock/network-protocol-support-in-windows (дата обращения 24.12.2020).

8. MySQL. Connector/C++ Documentation. URL: https://dev.mysql.com/doc/dev/connector-cpp/8.0/

УДК 004.056.52
ГРНТИ 49.41.01

РАЗРАБОТКА МЕТОДА ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ДЛЯ ЗАЩИТЫ ОТ АТАКИ КЛОНИРОВАНИЯ БУМАЖНЫХ СЕРТИФИКАТОВ

И. Д. Букшин, В. И. Коржик

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

Используются бумажные сертификаты различных изделий для защиты оригинальности продуктов и доказательства прав их собственников. Для защиты от фальсификации сертификатов обычно используются штрих-коды или дата-коды. Однако, этой меры может оказаться недостаточно, особенно от таких злоумышленных действий, как клонирование и изготовление копий сертификаций для её использования с контрафактной продукцией. В настоящей работе для подлинности надёжности защиты от такой атаки, которую мы называем «клонированием» сертификатов, предлагается использовать вложение в них цифровых водяных знаков. Приводится алгоритм обнаружения такого клонирования и теоретически рассчитываются вероятности ошибочного обнаружения и ложной тревоги для данной атаки, в зависимости от параметров системы.

сертификаты продукции, клонирование, цифровые водяные знаки, вероятности пропуска атаки клонирования и ложной тревоги.

Защита различных изделий от подделок или фальсификация их характеристик и производителей является важной задачей, понимаемой в широком смысле информационной безопасностью.

Для решения этой задачи большое распространение получил метод бумажных сертификатов, где при помощи использования штрих-кода или, в более общем случае Data Matrix, делается полное решение данной задачи. Однако, не для всех атак злоумышленников она может оказаться успешной. Так, при выполнении атаки «клонирование сертификата», злоумышленник копирует (фотографирует) сертификат, а затем производит его копирование (возможно и с изменением) и печать нового сертификата, который затем прикрепляется к изделию пониженного качества, но содержание сертификата говорит о его высоком качестве и, следовательно, требует пониженной цены продукта. В настоящем докладе рассматривается метод повышенной надёжности сертификатов, при помощи вложения в них цифровых водяных знаков (ЦВЗ), подлинность которых подтверждается использованием специального конфиденциального цифрового ключа, который имеется только

у собственника этого продукта [1]. Однако такой подход не может защитить от атаки «клонированием сертификатов».

В настоящей работе предлагается метод защиты сертификатов от подобной атаки, который использует факт увеличения мощности шума в цифровой копии сертификата, вследствие появления дополнительных операций считывания и печати, выполненных злоумышленником.

Вложение одного бита ЦВЗ "b_i" в "n"-й частотный (DCT) коэффициент дата-матрикса производится по правилу:

$$C_w^{b_i}(n) = C(n) + \delta(-1)^{b_i} \times \pi(n),\ n = 1,2..N_0,$$

где δ – глубина погружения,

$b_i \in (0, 1)$ бит ЦВЗ с номером "i",

$\pi(n)$ – ПСП для ШПС (на одном бите),

N_0 – длина ШПС для одного бита, причём так делается для всех бит ЦВЗ, причём величины $C_w^{b_i}(n),\ n = 1, 2..N,\ i = 1,2..S$, необходимо предварительно запомнить для последующего использования. Если всего вкладывается S бит, т. е. $i = 1,2..S$, то общая «длина» покрывающего объекта (ПО) с ЦВЗ будет $N = S \times N_0$. Рассмотрим математическую модель клонирования сертификата. Обозначим ЦВЗ $C_t^i(n)$ – отсчёты теста, извлекаемого легитимным пользователем.

Тогда, если клонирования не было, то:

$$C_t^{\prime,i}(n) = C_w^{b_i}(n) + N_{p1}(n) + N_{s1}(n), n = 1, 2..N, i = 1,2..S, \qquad (1)$$

где $N_{p1}(n)$ – шумы, при печати цифрового сертификата легитимным пользователем,

$N_{s1}(n)$ – шумы, возникающие на бумаге при сканировании сертификата легитимным пользователем в процессе тестирования.

Если же было осуществлено клонирование, то тогда получим:

$$C_t''(n) = C_w^{b_i}(n) + N_{p1}(n) + N_{s2}(n) + N_{p2}(n) + N'_{s1}(n),\ n = 1, 2..N, \qquad (2)$$

где $N_{s2}(n)$ – шумы при сканировании сертификата злоумышленником,

$N_{p2}(n)$ – шумы при печати клона злоумышленником,

$N'_{s1}(\mathrm{n})$ – шумы при сканировании сертификата легитимным пользователем при тестировании.

Сравнивая выражения (1) и (2), видим, что при клонировании добавляются две новых компоненты аддитивного шума N_{p2}, N'_{s1}, которые возникают из-за того, что злоумышленник должен дополнительно считать и отпечатать сертификат. В нашей модели все шумы полагаются гауссовскими

случайными величинами с нулевыми средними и дисперсиями одинаковыми для принтера и сканера, но с разными для легитимного пользователя и злоумышленника т. е. $Var(N_{p1}) = Var(N_{s1}) = Var(N'_{s1}) = \sigma^2$, $Var(N_{s2}) = Var(N_{p2}) = r\sigma^2$, где $r \leq 1$ – некоторый коэффициент, который показывает, что злоумышленник может иметь мощность шума в "r" раз меньше, чем легитимный пользователь.

Ранее предполагалось, что легитимный пользователь запоминает в своём ПК дата-код сертификата с вложением ЦВЗ, т. е. $C_w^{bi}(n)$, n = 1,2..N. Затем он, получив от сканера результаты тестирования $C_t(n)$, n = 1,2..N находит величину $\lambda(n) = C_t(n) - C_w^{bi}(n)$, n = 1,2..N.

Если клонирования не было, то проверяющий вычисляет:

$$\lambda'(n) = C'_t(n) - C_w^{bi}(n) = C_w^{bi}(n) + N_{p1}(n) + N_{s1}(n) - C_w^{bi}(n) = N_{p1}(n) + +N_{s1}(n), \quad n = 1, 2..N. \tag{3}$$

Если же клонирование было, то проверяющий получит:

$$\lambda'(n) = C_t^{\prime\prime,i}(n) - C_w^{bi}(n) = C_w^{bi}(n) + N_{p1}(n) + N_{s2}(n)+N_{p2}(n) + N'_{s1}(n) - C_w^{bi}(n) = \\ = N_{p1}(n) + N_{s2}(n)+N_{p2}(n) + N'_{s1}(n). \tag{4}$$

Суммарная мощность шумов будет тогда:

для случая без клонирования – $E\{\lambda_{nc}^2(n)\} = 2\sigma^2$,
для случая с клонированием – $E\{\lambda_c^2(n)\} = 2\sigma^2 r'$,

где $r' = \frac{r+1}{r}$, r – это величина, которая показывает во сколько раз дисперсия шумов у атакующего меньше дисперсии шумов у легального пользователя. (Мы, таким образом, даём некоторую «фору» атакующему)

Далее измеряется нормированная мощность шумов:

$$\Omega = \frac{1}{N}\sum_{n=1}^{N} \lambda^2\,(n).$$

Решение о клонировании принимается по правилу:

$$\begin{aligned} &\Omega \geq \Omega_0 \Rightarrow \text{клонирование есть,} \\ &\Omega < \Omega_0 \Rightarrow \text{клонирования нет,} \end{aligned} \tag{5}$$

где Ω_0 – некоторый заранее заданный порог.

При принятии решения могут появится два вида ошибок: P_m – вероятность пропуска клонирования, когда оно в действительности было и P_{fa} – вероятность ложной тревоги, когда клонирования не было, но по правилу (5)

было принято решение, что оно было. Определим полную вероятность ошибки $P_e = \frac{1}{2}\left(P_m + P_{fa}\right)$ и будем называть оптимальным порогом такую величину $\Omega = \Omega_0$, которая обеспечивает минимум P_e.

Определим гауссовскую аппроксимацию Ω, т. е. когда $\Omega \in N(E\{\Omega\}, Var\{\Omega\})$, согласно ЦПТ(центральной предельной теоремы [2]) при больших N. Рассчитаем величины $E\{\Omega\}, Var\{\Omega\}$ без клонирования и с ним:

Без клонирования.

$$E\{\Omega\} = \frac{1}{N}\sum_{n=1}^{N} E\{\lambda_n^2\} = 2\sigma^2,$$
$$Var\ \Omega = \frac{1}{N}\sum_{n=1}^{N} Var\ \lambda^2(n) = \frac{8}{N}\sigma^4, \quad (6)$$

поскольку λ_n – это гауссовские случайные величины с нулевым средним и дисперсией $2\sigma^2$ и тогда $Var\ \lambda^2(n) = 8\sigma^4$ [2].

С клонированием.

$$E\{\Omega\} = 2\sigma^2 r',$$
$$Var\ \Omega = \frac{8}{\mathrm{N}}\sigma^4 (r')^2. \quad (7)$$

Тогда вероятности ошибок $P_{m,} P_{fa,}$ и P_e будут:

$$P_m = \int_{-\infty}^{\Omega_0} w_\Omega^c(\mathrm{x})\, d\mathrm{x};\ P_{fa} = \int_{\Omega_0}^{\infty} w_\Omega^{nc}(\mathrm{x})\, d\mathrm{x};\ P_e = \frac{1}{2}\ \left(P_m + P_{fa}\right). \quad (8)$$

Эти вероятности можно выразить при помощи функции Лапласа [2]

$$\Phi(\mathrm{x}) = \frac{1}{\sqrt{2\pi}}\int_0^x exp^{\left(-\frac{t^2}{2}\right)}\mathrm{dt},$$

Тогда,

$$P_e = \frac{P_m + P_{fa}}{2} = \frac{1}{2}\left(1 + \Phi\left(\sqrt{N}\,\frac{\Omega_0 - 2\sigma^2\frac{r+1}{r}}{\sigma^2 2\sqrt{2}}\,\frac{r}{r+1}\right) - \Phi\left(\sqrt{N}\,\frac{\Omega_0 - 2\sigma^2}{\sigma^2 2\sqrt{2}}\right)\right). \quad (9)$$

Для нахождения оптимального порога Ω_0 необходимо вычислить производную $P_e'(N)$ в (9), а затем приравнять её к нулю и после преобразований получим:

$$\Omega_0 \approx 4\sigma^2\,\frac{r+1}{2r+1}. \quad (10)$$

Далее, приводим конечную формулу для P_e при оптимальном пороге Ω_0 (10), которую можно доказать:

$$P_e = \frac{P_m + P_{fa}}{2} \approx \frac{1}{2}\left(1 + \Phi\left(-\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right) - \Phi\left(\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right)\right) = \\ = \frac{1}{2} - \Phi\left(\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right). \quad (11)$$

Для того, чтобы рассчитать вероятность ошибки P_e при конечных величинах N и r, можно воспользоваться следующим приближением функции $\Phi(\cdot)$:

$$\Phi(x) \approx \frac{1}{2} - \frac{1}{\sqrt{2\pi}}\frac{e^{-\frac{x^2}{2}}}{x}. \quad (12)$$

Подставляя (12) в (11), получаем:

$$P_e \approx \Phi\left(\frac{1}{2\pi}\frac{e^{-\frac{x^2}{2}}}{x}\right), \text{ где } x = \frac{\sqrt{N}}{\sqrt{2}(2r+1)}. \quad (13)$$

На рис. показана зависимость P_e от N для различных величин r = 1, 2, 4, 8, 16.

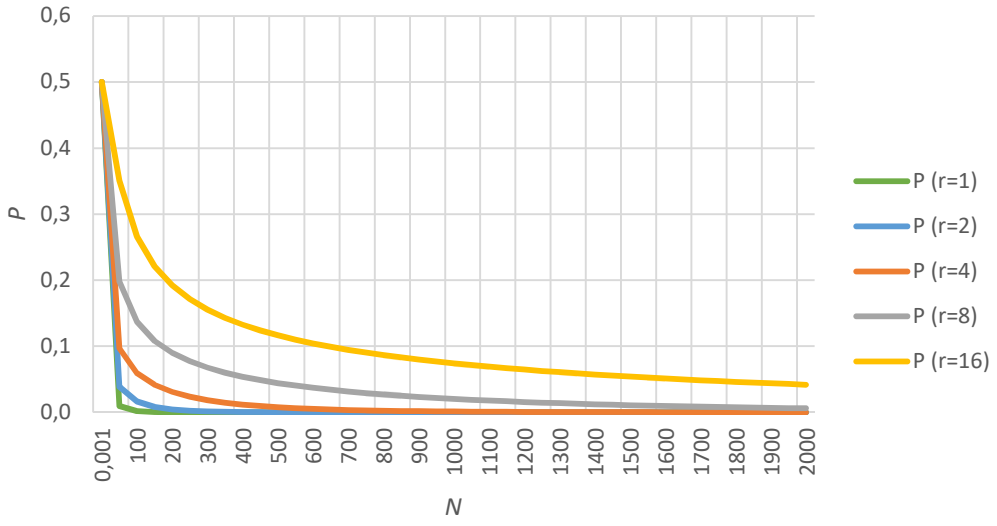


Рис. Зависимости полной вероятности ошибки обнаружения атаки клонирования от длины ЦВЗ N

Список используемых источников

1. Коржик В. И., Анфиногенов С. О., Кочкарёв А. И., Федянин И. А., Жувикин А. Г., Флаксман Д. А., Алексеев В. Г. Цифровая стеганография и цифровые водяные

знаки. Часть 2. Цифровые водяные знаки: [монография] / под общей редакцией В. И. Коржика; СПбГУТ. СПб, 2017. 198 с. ISBN-978-5-89160-125-3.

2. Ван дер Варден Б. Л. Математическая статистика. М.: Изд-во иностранной литературы, 1960. 435 с.

3. Коржик В. И., Финк Л. М., Щелкунов К. Н. Расчёт помехоустойчивости систем передачи дискретных сообщений: Справочник / Под ред. Л.М. Финка. М.: Радио и связь, 1981. 232 с.

4. Ho A. T. S., Shu F. A print-and-scan resilient digital watermark for card authentication // Fourth International Conference on Information, Communications and Signal Processing. IEEE 2003 and The Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint. Vol. 2. pp. 1149–1152.

5. Коржик В. И., Флаксман Д. А. Система цифровых водяных знаков с возможностью их извлечения из бумажных копий цифровых документов // Труды учебных заведений связи. 2019. Т. 5. No 3. С. 75–85. DOI: 10.31854/1813-324X-2019-5-3-75.

УДК 621.39; 534.8; 535.8
ГРНТИ 49.44.31; 59.39.33

ПОТЕНЦИАЛЬНЫЕ ВОЗМОЖНОСТИ КОНТРОЛЯ ПРОЧНОСТИ ОПТИЧЕСКИХ ВОЛОКОН ПО ОЦЕНКАМ НЕЛИНЕЙНОЙ АКУСТИЧЕСКОЙ ЭМИССИИ ПРИ ИСПОЛЬЗОВАНИИ ТЕСТИРУЕМЫХ ВОЛОКОН В КАЧЕСТВЕ АКУСТИЧЕСКОГО СЕНСОРА

А. В. Бурдин[1,2], В. А. Бурдин[1], М. В. Дашков[1], А. О. Нижгородов[1]

[1]Поволжский государственный университет телекоммуникаций и информатики
[2]Научно-производственное объединение Государственный оптический институт им. С. И. Вавилова

В представленной работе приведены результаты эксперимента, демонстрирующие возможность контроля прочности оптических волокон на основе использования тестируемого оптического волокна в качестве акустического сенсора для измерений спектральных характеристик сигналов нелинейной акустической эмиссии, формируемых при воздействии на тестируемое оптическое волокно с микротрещинами на поверхности оболочки акустического сигнала одной частоты.

оптическое волокно, оптоволоконный акустический сенсор, прочность оптического волокна, акустическое воздействие, нелинейная акустическая эмиссия, спектральная характеристика.

Задача неразрушающего контроля прочности оптических волокон (ОВ) крайне актуальна на сегодняшний. Во многом это объясняется тем, что на волоконно-оптических линиях связи, построенных в конце прошлого века

срок службы оптических кабелей приблизился или даже превысил значения, декларированные производителем. Прогноз же оставшегося срока службы кабелей, прослуживших на линии 20–30 лет, требует знания прочности ОВ кабеля на момент прогноза [1]. К сожалению, на сегодняшний день регламентированных неразрушающих методов контроля прочности ОВ нет. При этом, хорошо известно применение для определения наличия дефектов и их местоположения в различных структурах методов, базирующихся на измерениях параметров сигналов нелинейной акустической эмиссии [2]. В приложении к ОВ применение данных методов пока ограничивается фиксацией момента разрушения ОВ в реализациях разрушающих методов контроля [3]. Вместе с тем, хорошо известно, что ОВ является сверхвысокочувствительным акустическим сенсором [4, 5]. Это позволяет предположить, что при использовании тестируемого ОВ в качестве акустического сенсора его чувствительности будет достаточно для измерения оценок нелинейной акустической эмиссии, по которым можно будет оценить прочность тестируемого ОВ. В данной работе представлены результаты эксперимента, которые наглядно демонстрируют такую возможность.

Для измерений спектральных характеристик сигналов нелинейной акустической эмиссии была собрана экспериментальная установка, общая схема которой приведена на рис. 1. На тестируемое ОВ воздействовали непрерывным синусоидальным звуковым сигналом одной частоты (1–2 кГц). В качестве источника акустических воздействий был использован динамик с диафрагмой 40 см, подключенный к генератору сигналов. Образцы ОВ помещали непосредственно над диафрагмой динамика без натяжения и фиксировали в двух точках по концам.

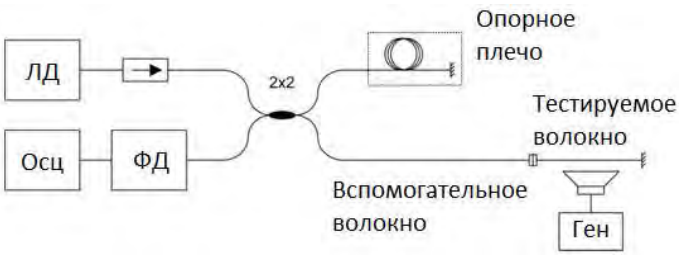


Рис. 1. Общая схема экспериментальной установки

Оптоволоконный интерферометр Майкельсона реализован на разветвителе 2×2 с коэффициентом деления 50/50. Опорное плечо интерферометра представляет собой бухту ОВ соответствующей длины, помещенную в теплоизолированный корпус с защитой от вибрации. В качестве источника оптического излучения использован лазерный диод с распределенной обратной связью (ЛД) с центральной длиной волны 1 550 нм и полосой пропускания менее 1 МГц. Лазерный диод подключен через оптический изолятор с изоляцией 25 дБ. Детектирование оптического сигнала осуществляется с помощью p-i-n фотодиода (ФД). Выделенный на приеме сигнал через трансимпедансный усилитель вводится в запоминающий осциллограф (Осц). Спектральные характеристики принятого сигнала получены

методом быстрого преобразования Фурье. Для уменьшения паразитных воздействий система опроса с опорным плечом интерферометра и тестовое ОВ были размещены в разных лабораториях. Для соединения ОВ с системой опроса между лабораториями был проложен оптический кабель со стандартным одномодовым ступенчатым оптическим ОВ. Общая длина оптического кабеля составляет 85 метров. Предварительно были проведены испытания образца стандартного одномодового ступенчатого ОВ (Рекомендация ITU-T G.652). Образец был взят с катушки с аттестованным оптическим ОВ. По завершению испытаний на образец оптического волокна ручкой-скалывателем был нанесен дефект оболочки. На рис. 2 приведены фотографии в двух плоскостях участка образца ОВ с поверхностным дефектом. Затем, повторили испытания для образца с дефектом. На рис. 3 представлены нормированные спектральные характеристики сигналов нелинейной акустической эмиссии для образца без дефекта и образца с дефектом. Здесь, низкочастотные составляющие, включая компоненту на частоте воздействующего акустического сигнала, были отфильтрованы.

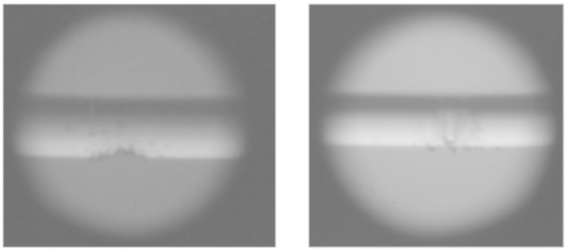


Рис. 2. Фотографии участка ОВ с нанесенным дефектом оболочки

Хорошо видно, что амплитуды спектральных компонент сигнала нелинейной акустической эмиссии для образца волокна с дефектом существенно превышают амплитуды спектральных компонент сигнала нелинейной акустической эмиссии образца без дефекта, что подтверждает заявленное предположение.

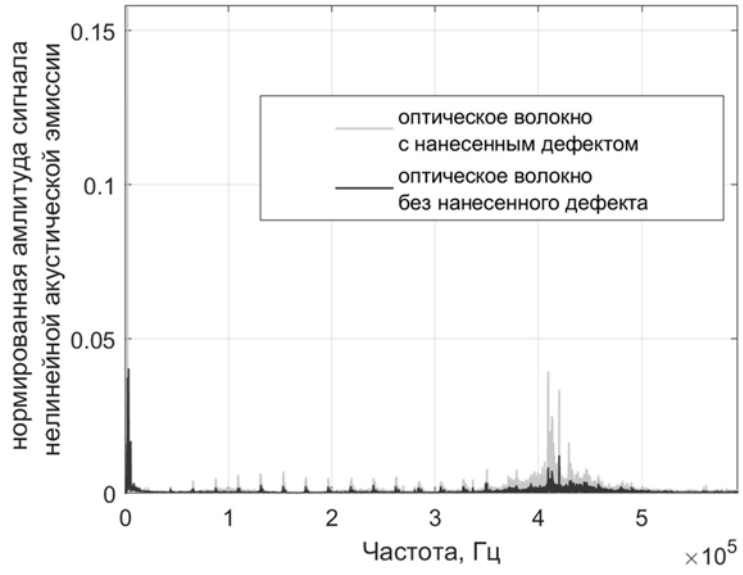


Рис. 3. Нормированные спектральные характеристики сигналов нелинейной акустической эмиссии образцов с нанесенным дефектом и без дефекта

Список используемых источников

1. ITU-T G-series Recommendations. Supplement 59, Series G: Transmission systems and media, digital systems and networks, Guidance on optical fibre and cable reliability, (02/2018).
2. Gholizadeh S., Leman Z., Baharudin B. T. H. T. A review of the application of acoustic emission technique in engineering // Structural Engineering and Mechanics. 2015. V. 54. pp. 1075–1095.
3. R'Mili M., Moevusm M., Godin N. Statistical fracture of E-glass fibres using a bundle tensile test and acoustic emission monitoring // Composites Science and Technology. 2008. V. 68. pp. 1800–1808.
4. Teixeira J. G. V., Leite I. T., Silva S., Frazão O. Advanced Fiber-Optic Acoustic Sensors // Photonic sensors. 2014. V. 4. pp. 198–208.
5. Muanenda Y. Recent Advances in Distributed Acoustic Sensing Based on Phase-Sensitive Optical Time Domain Reflectometry // Hindawi Journal of Sensors. 2018. pp. 1–16.

УДК 004.056
ГРНТИ 81.93.29

РЕАЛИЗАЦИЯ ТУННЕЛИРОВАНИЯ SSH-СОЕДИНЕНИЯ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА WEBSOCKET

М. Д. Бурмистров, А. Ю. Цветков

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

С развитием облачных технологий число устройств в рамках инфраструктуры сервиса значительно увеличивается. В связи с этим возникает потребность в централизованном управлении ими. Современные веб-технологии, в свою очередь, позволяют реализовать доступ к узлам сети через единый графический интерфейс, доступный с любого пользовательского устройства, подключенного к сети.

веб-разработка, туннелирование, соединение, удаленное управление, информационная безопасность.

Введение

С развитием облачных технологий число устройств в рамках инфраструктуры сервиса значительно увеличивается. В связи с этим возникает потребность в централизованном управлении ими [1]. Современные веб-технологии, в свою очередь, позволяют реализовать доступ к узлам сети через единый графический интерфейс, доступный с любого пользовательского устройства, подключенного к сети [2].

Анализ используемых технологий

На данный момент существуют несколько распространенных способов установления удаленного подключения к устройствам. Сравнение характеристик некоторых из них представлено в таблице.

ТАБЛИЦА. Сравнение протоколов удаленного управления устройствами

Протокол	Достоинства	Недостатки
Telnet	Широкий спектр поддерживаемых устройств.	Полное отсутствие шифрования трафика.
SSH	Шифрование трафика; наиболее широкий спектр поддерживаемых устройств среди перечисленных протоколов.	–
RDP	Шифрование трафика; управление через графический интерфейс удаленной ОС.	Не поддерживается сетевыми устройствами ввиду отсутствия графической оболочки ОС.

Анализируя данные, представленные в таблице, можно сделать вывод о том, что среди описанных средств наиболее предпочтительным является протокол SSH, так как поддерживает шифрование входящего и исходящего трафика [3], поддерживается широким спектром различных устройств, включая коммутаторы, маршрутизаторы и прочие сетевые устройства, а также практически не имеет недостатков.

Как было упомянуто ранее, с увеличением количества используемых различных сетевых устройств, к примеру, в корпоративной сети, растет необходимость управления через единый интерфейс, так как это позволяет компаниям значительно сократить расходы на администрирование сети, а вследствие этого, и на персонал, непосредственно занимающийся администрированием.

Выбор стека веб-технологий для построения такого интерфейса также решает множество проблем безопасности, которые могут возникнуть в процессе его создания, поскольку клиентское веб-приложение не зависит от аппаратной платформы или операционной системы конкретного устройства пользователя, а значит, задача обеспечения безопасности среды выполнения приложения на каждой отдельной поддерживаемой платформе ложится на разработчиков данного программного обеспечения (в данном случае, веб-браузера), которые в большинстве случаев обладают огромными ресурсами для анализа и устранения уязвимостей своих продуктов [4].

Впрочем, стек веб-технологий хоть и имеет множество преимуществ, облегчающих разработку ПО, но также подразумевает использование ограниченного набора технологий для реализации клиент-серверного взаимодействия между пользователем и удаленным устройством [5].

В частности, установить прямое SSH-соединение между клиентским веб-приложением и удаленным устройством не представляется возможным, поскольку ни один из существующих на сегодняшний день браузерных движков не поддерживает и не обязан поддерживать использование данного протокола ввиду множества проблем безопасности, которые может породить внедрение такого функционала.

Тем не менее, соединение между клиентом и сервером может быть установлено при помощи туннелирования SSH-соединения с использованием протоколов, поддерживаемых средой веб-браузера, в качестве транспорта. Использовать основной протокол для взаимодействия веб-клиента с сервером – HTTP – не удастся, так как HTTP не поддерживает длительные соединения, а также не позволяет удаленному серверу передавать данные без запроса клиента.

Для создания туннеля между клиентским веб-приложением и удаленным устройством требуется использовать протокол, обеспечивающий длительное дуплексное соединение и передачу сообщений в реальном времени. Под выдвинутые требования подходит протокол WebSocket, поддерживающий вышеупомянутый функционал. При использовании WebSocket в качестве транспорта для SSH достигается взаимодействие пользователя с терминальной сессией удаленного устройства в реальном времени.

Изначально протокол WebSocket не обеспечивает защищенное соединение между клиентом и сервером, так как работает поверх протокола HTTP, но позволяет использовать в качестве транспорта его защищенную версию – HTTPS, что позволяет шифровать весь трафик [6].

При туннелировании SSH-соединения необходимо использовать промежуточный веб-сервер, принимающий HTTP/WebSocket-запросы и имеющий встроенный SSH-клиент для подключения к целевым устройствам [7]. Его использование обусловлено невозможностью управления устройством только по протоколу WebSocket, так как протокол предназначен для передачи произвольных сообщений, а также в большинстве случаев не поддерживается целевыми устройствами ввиду отсутствия в них настроенного веб-сервера.

Реализация туннелирования соединения

Процесс реализации туннелирования SSH-соединения состоит из трех шагов:

1. Запрос на промежуточный сервер, служащий мостом между клиентом и целевым устройством;

2. Установление SSH-соединения между промежуточным сервером и целевым устройством;

3. Установление WebSocket-соединения между клиентом и промежуточным сервером и последующая передача данных через сервер от клиента к устройству и обратно.

Условная схема взаимодействия узлов при туннелировании соединения представлена на рис.

Рис. Условная схема взаимодействия узлов при туннелировании.

Реализация промежуточного сервера выполнена на языке Python с использованием веб-фреймворка FastAPI и библиотеки для установления SSH-соединения Paramiko. Представленный в листинге 1 участок кода демонстрирует обработку входящего WebSocket-соединения, установление SSH-соединения и последующее перенаправление данных между клиентом и целевым устройством.

Листинг 1

```
from fastapi import FastAPI, WebSocket
import paramiko
app = FastAPI()
@app.websocket("/ws")
async def websocket_endpoint(websocket: WebSocket):
    await websocket.accept()
    data = await websocket.receive_json()
    host = data.get("host")
    port = data.get("port")
    username = data.get("user")
    password = data.get("pass")
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.client.WarningPolicy)
    ssh.connect(host, port, username, password)
    term = ssh.invoke_shell("xterm")
    term.setblocking(False)
    while True:
        data_out = term.recv()
        if data_out:
            await websocket.send_bytes(data_out)
```

```
        data_in = await websocket.receive_bytes()
        if data_in:
            if term.send(data_in) == 0:
                break
    await websocket.send_bytes(b"Connection closed")
    await websocket.close()
```

На листинге 2 представлена реализация взаимодействия клиентского веб-приложения с промежуточным сервером с использованием протокола WebSocket, написанная на языке Javascript.

Листинг 2

```
const sendToSocket = (ws, data) => {
    if (ws.readyState < 2) {
        ws.send(data);
    }
}
const ws = new WebSocket(`wss:\/\/${agentHost}/ws`);
ws.onopen = () => {
    ws.send(JSON.stringify({
        host: deviceHost,
        port: devicePort,
        user: deviceUser,
        pass: devicePass
    }));
};
ws.onmessage = (event) => {
    // Обработка принятого сообщения
}
```

Заключение

Описанный способ туннелирования SSH-соединения обеспечивает защищенное подключение к удаленным устройствам из браузерной среды клиентского веб-приложения [8]. В зависимости от поставленных требований при выполнении конкретной задачи при различных усовершенствованиях исходного кода клиента и промежуточного сервера возможно также туннелирование упомянутых выше протоколов Telnet, RDP и других протоколов удаленного управления.

Список используемых источников

1. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 2. С. 329–334.

2. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.

3. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернбородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 525–527.

4. Построение доверенной вычислительной среды: монография / Красов А. В., Гельфанд А. М., Коржик В. И., Котенко И. В., Петрив Р. Б., Сахаров Д. В., Ушаков И. А., Шариков П. И., Юркин Д. В. СПб.: Индивидуальный предприниматель Петрив Р. Б., 2019. 108 с.

5. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 321–326.

6. Волкогонов В. Н., Казанцев А. А., Катасонов А. И., Орлов Г. А. Анализ безопасности wi-fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 270–275.

7. Гельфанд А. М., Лансере Н. Н., Ложкина А. А., Фадеев И. И. Организация концептуальной модели критической информационной инфраструктуры // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 39–40.

8. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 2. С. 262–266.

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

УДК 004.94+621.391
ГРНТИ 49.33.29

АНАЛИЗ СПОСОБОВ ПОВЫШЕНИЯ КАЧЕСТВА ОБСЛУЖИВАНИЯ ПРИЛОЖЕНИЙ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Ю. О. Бусаров, Н. М. Редругина, А. А. Швидкий

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

Целью статьи является моделирование услуги электронной коммерции для расчета качественных характеристик системы. Сформированы подходы по улучшению качества обслуживания пользователей, включающие в себя прогнозирование возрастающей нагрузки и возможность манипуляций объемом серверного оборудования.

система массового обслуживания, качество обслуживания, QoS, инфокоммуникационные услуги, имитационное моделирование, распределение серверных ресурсов

Электронная коммерция является одним из самых популярных и быстроразвивающихся направлений инфокоммуникационных услуг. Данный термин включает в себя продажи, покупки, платежи, которые были проведены через глобальную сеть. В существующих публикациях [1, 2] описываются методы расчета вероятностно-временных характеристик для определения качества обслуживания и варианты улучшения качества обслуживания для отдельных инфокоммуникационных услуг. В статье [3] определяются подходы к моделированию обслуживания нагрузки для другого типа услуг – игровых многопользовательских сервисов. Однако построенная модель не предусматривает возможность потерь по истечению времени ожидания в очереди что является основным критерием качества обслуживания.

Для рассматриваемого в данной статье типа услуг мы используем метод сравнительной оценки показателей качества обслуживания сервиса с самим собой на коротких промежутках времени для определения проблемы качественного предоставления услуг, связанной с периодическим ростом нагрузки на сервис. Услуга электронной коммерции может стабильно предоставляться работать в будние дни, но возросшая нагрузка в вечер пятницы или выходные может значительно ухудшить показатели качества. Такую услугу сложно назвать быстрой или доступной.

Рассмотрим работу услуги электронной коммерции на примере модели интернет магазина в обычном и критическом состоянии для определения возможности улучшения качества обслуживания. На рис. 1 представлена функциональная схема такого сервиса, который состоит из четырех СМО: «Каталог», «Корзина», «Оплата» и система денежных транзакций «Банки». Пользователи при переходе по ссылку имеют возможность попасть только

на страницу каталога продукции или услуг данного интернет магазина. Далее запрос поступает на страницу «Корзина», где пользователь имеет выбор либо вернуться в каталог продукции и выбрать что-то еще, либо оплатить то что он выбрал. В системе оплаты пользователь заполняет данные связанные с доставкой и выбором типа оплаты и переводится на страницу банка, после чего покидает систему безвозвратно.

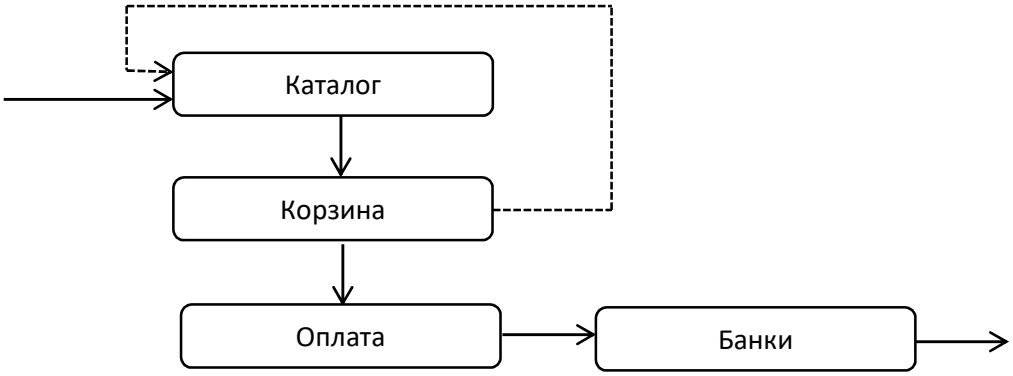


Рис. 1. Схема сервиса интернет магазина

Интернет-эквайринг добавляет в нашу схему сеть массового обслуживания, состоящую из систем онлайн-банков через которые проходят денежные переводы. Так как не существует ограничений и лимитов от банка на производимые транзакции, то при разработке системы мы не можем повлиять на качество обслуживания после прохождения СМО «Оплата».

Для приведенного примера моделирования осуществлено с использованием открытой сети систем массового обслуживания. Так же учитывается возможность выхода заявки из очереди в первой СМО.

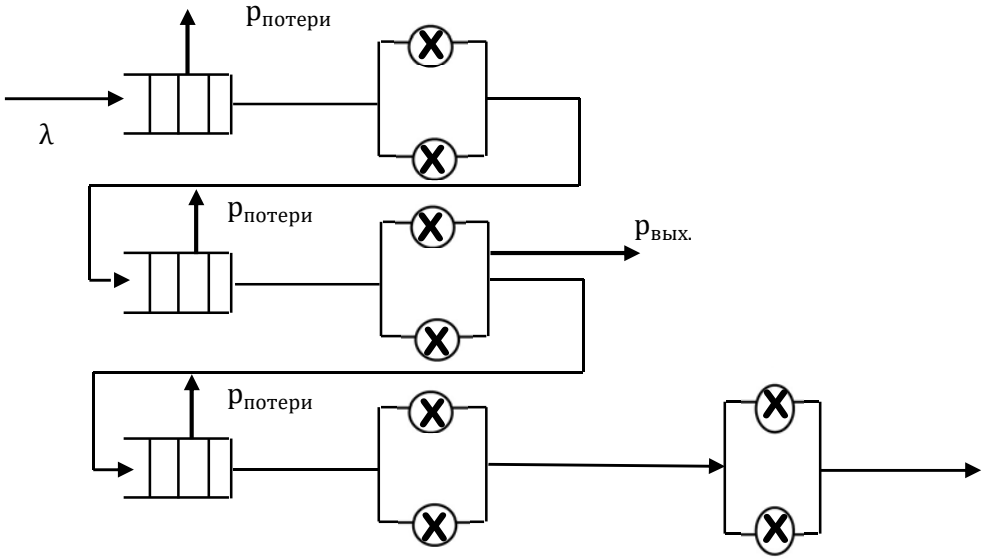


Рис. 1. Схема модели интернет магазина

Где $p_{потери}$ вероятность выхода заявки из очереди первого узла.

Интенсивность поступления заявок на обслуживающие приборы первого узла определяется уравнением:

$$\lambda_1 = \lambda - \lambda * p_{потери}. \quad (1)$$

Имитационная модель сети массового обслуживания была построена в программе AnyLogic 8 Personal Learning Edition 8.7.2.

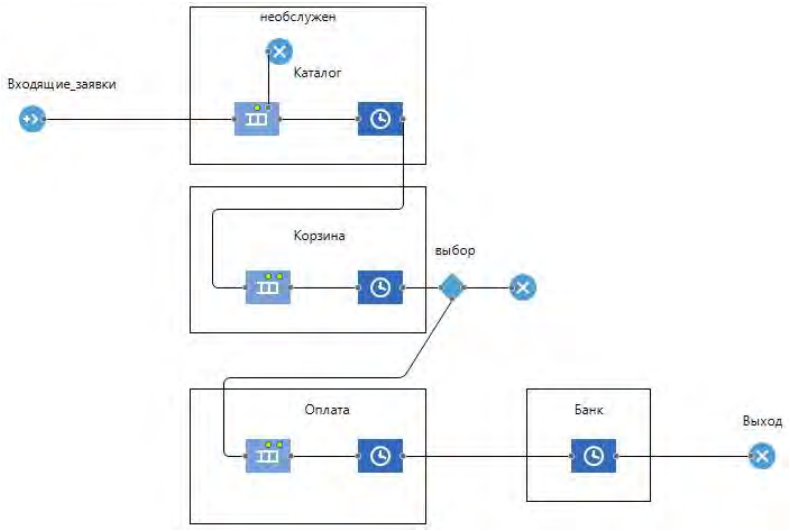


Рис. 2. Схема имитационной модели интернет магазина

Качественная характеристика – неявные потери, определена в данной модели как вероятность потери заявок при выходе из очереди по истечению времени. Критичность потерь для каждого сервиса и компании индивидуальные. Как показано на рис. 4 при увеличении входящей нагрузки, увеличивается и количество потерянных заявок. Данную проблему можно решить либо увеличением объема серверного оборудования, либо уменьшением времени обслуживания, что решается лишь упрощением выбора товаров либо услуг. Ведь невозможно напрямую повлиять на время, проведенное пользователем на данной странице.

На графике представленном ниже показана возможность контролировать объем предоставляемых ресурсов для нашего сервиса. Светло-серым на графике отмечен объем серверных ресурсов которое могут занимать пользователи, зашедшие на страницу «Каталог». Темно-серым на графике указано реальное количество пользователей на сервере в каждый момент модельного времени. Если прогнозируется увеличение количества пользователей на определенный процент, потеря которого является критической в обслуживании, то решением может быть аренда серверного оборудования на это время. Постоянное использование большого количества незадействованных ресурсов финансово не выгодно для любой компании.

В настоящее время нейросети помогают спрогнозировать скачки нагрузки, например, как в случае электронной коммерции: крупные распродажи, появление на рынке инновационной продукции (промежуток 30–50 модельного времени на рис. 5).

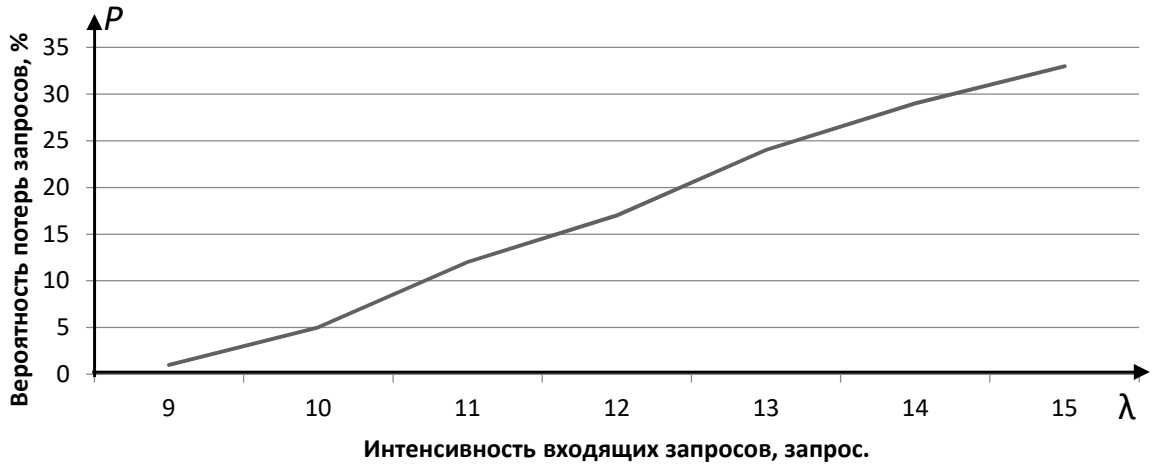


Рис. 4. Зависимость доли потерянных запросов
от интенсивности входящего потока пользователей

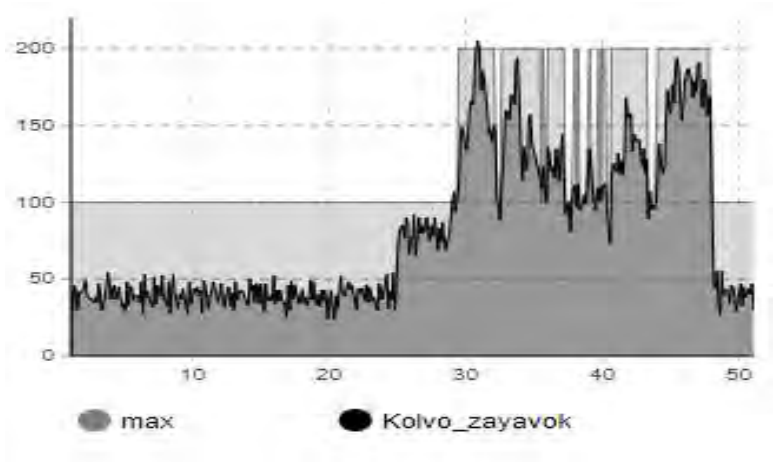


Рис. 5. Зависимость загрузки сервера от времени

Качество обслуживания один из главных ориентиров на которые следует ссылаться при разработке, эксплуатации и работе с ошибками. Возрастание популярности сервиса, приводит к увеличению входящих запросов при котором может увеличиваться количество потерянных заявок, время ожидания в очереди. Системы управления и мониторинга позволят разработчикам предсказать и исправить моменты критических ошибок.

Список используемых источников

1. Зарубин А. А. Изменение организационно-технической парадигмы современных инфокоммуникационных услуг // Вестник связи. 2017. № 12. С. 25–30.

2. Зарубин А. А., Кызюров О. Е., Савельева А. А. Разработка моделей и методов оценки качества цифровых услуг // Вестник связи. 2018. № 5. С. 37–40.

3. Зарубин А. А., Редругина Н. М. Моделирование игровых многопользовательских сервисов // Вестник связи. 2020. № 8. С. 11–16.

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.05
ГРНТИ 81.93.29

ВЫЯВЛЕНИЕ НЕСАНКЦИОНИРОВАННЫХ ИНФОРМАЦИОННЫХ ПОТОКОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В. В. Бухарин[1], **А. В. Казачкин**[2]

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

В статье рассматривается подход по выявлению несанкционированных информационных потоков в информационно-телекоммуникационной сети с использованием идентификаторов, образованных деструктивными программными возможностями или недекларированными возможностями программного обеспечения, от узлов сетей.

несанкционированные информационные потоки, недекларированные возможности, защита информационно-телекоммуникационных сетей.

В настоящее время под событием безопасности в информационно-телекоммуникационной сети понимается операция или действие, совершенное пользователем или программой, приводящее к изменению потоков данных в информационно-телекоммуникационной сети. Событием безопасности является идентифицированное появление определённого состояния системы, сервиса или сети, указывающего на возможное нарушение политики безопасности или на отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [1]. Событием информационной безопасности являются проявления недекларированных возможностей программного обеспечения, функционирующего в телекоммуникационном оборудовании. Недекларированными возможностями называют функциональные возможности программного обеспечения, не описанные или не соответствующие описанным

в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации [2].

Кроме того, несанкционированные информационные потоки в информационно-телекоммуникационных сетях могут организовываться под видом легитимных потоков данных, зачастую создаваемых для организации канала передачи данных из защищаемого сегмента злоумышленнику, находящемуся во внешнем сегменте сети, или канала управления извне (рис. 1).

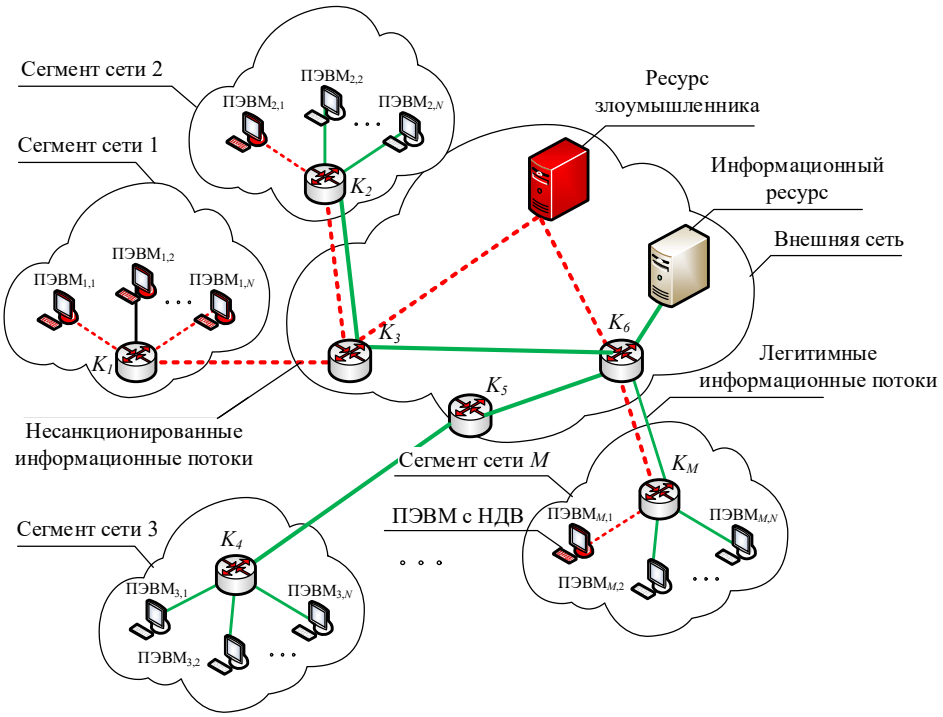


Рис. 1. Пример информационно-телекоммуникационной сети с несанкционированными потоками данных

Существует достаточно большое количество способов защиты информационных систем от несанкционированных потоков [3, 4, 5]. Однако, общими их недостатками являются отсутствие взаимосвязи между протоколами верхнего прикладного уровня и целью функционирования телекоммуникационных сетей, а также низкая защищенность, определяемая тем, что управление трафиком и конфигурирование сетью осуществляется после выявления несанкционированных попыток нарушителя.

Представленный на рис. 2 алгоритм реализует управление трафиком в информационно-телекоммуникационной сети [6].

Первоначально создается массив коммутации M. В массиве коммутации имеющемуся атрибуту передаваемых данных прописываются соответствующий номер порта телекоммуникационного оборудования [7].

После этого создают таблицу сетевых элементов L_i и соответствующих программ K_R, которые используются определенными сетевыми элементами абонентов N_i, передающие информационные пакеты данных P_k.

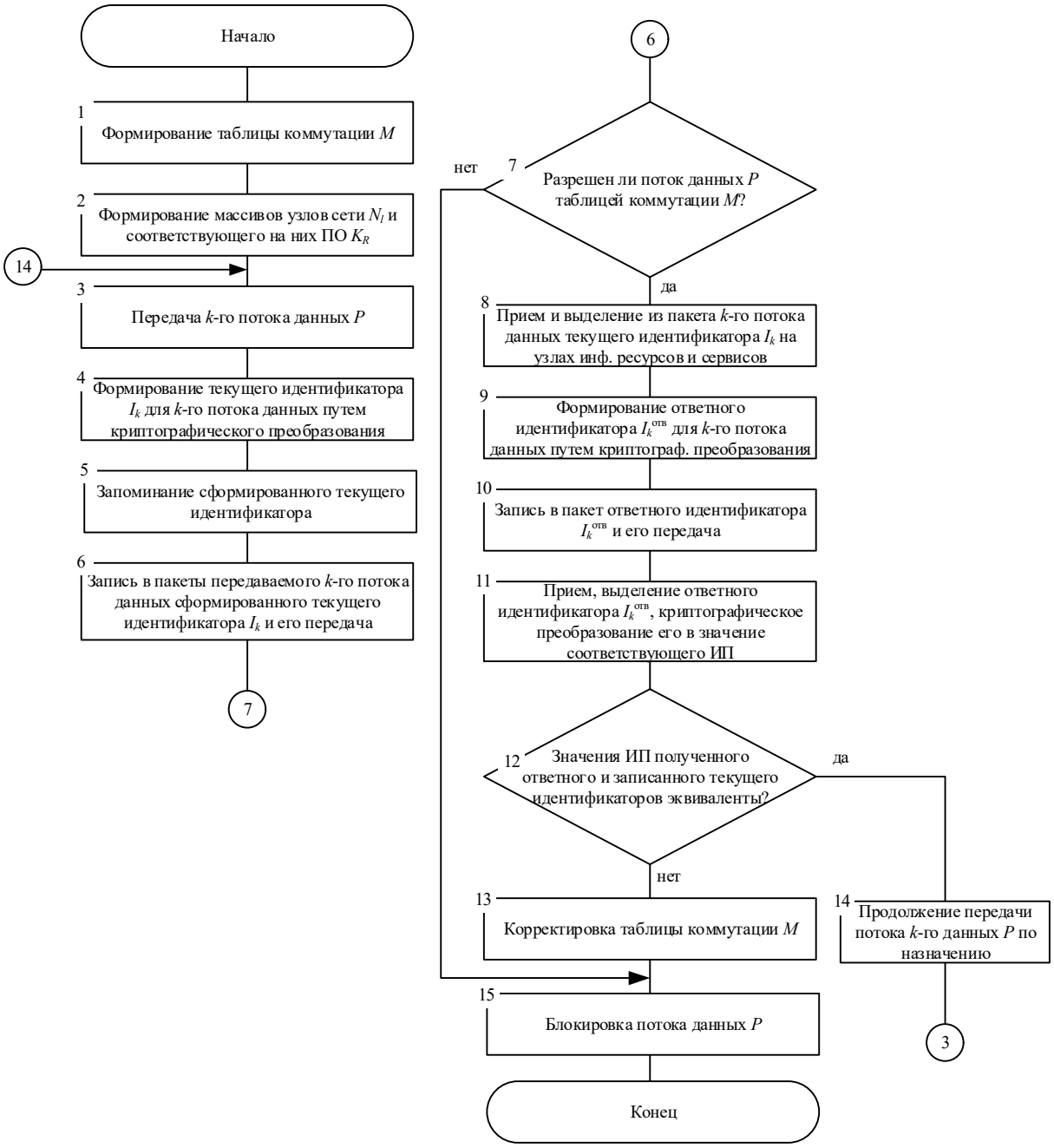


Рис. 2. Алгоритм управления трафиком в информационно-телекоммуникационной сети

Затем на приемной стороне записывается k-й информационный пакет данных P определенного сетевого элемента L_i, и создается текущий атрибут

$I_{тек}$ за счет кодирования номера сетевого элемента абонента N_i, номера программы телекоммуникационного оборудования K_r, и номера сетевого элемента, располагающего ресурсом S_j.

Закодированный текущий атрибут $I_{тек}$ помещается в соответствующее поле *IP*-пакета информационных данных P_k. Запись текущего атрибута возможно в поле данных *IP*-пакета [8].

На приемной стороне телекоммуникационной сети из *IP*-пакета информационных данных P_k считывается текущий атрибут $I_{тек}$ и декодируется. Далее создается ответный атрибут $I_{отв}$, путем кодирования номера сетевого элемента, располагающего ресурсом S_j, номера программы телекоммуникационного оборудования K_r и номера сетевого элемента абонента N_i и имеющий отличительные признаки от текущего атрибута.

После этого закодированный ответный атрибут $I_{отв}$ помещается в соответствующее поле *IP*-пакет информационных данных P_k. На приемной стороне телекоммуникационной сети из *IP*-пакета информационных данных считывается ответный атрибут $I_{отв}$, и декодируется. При этом получаются ответные (созданные на взаимодействующей сетевом элементе): номер сетевого элемента абонента N_i, номер программы телекоммуникационного оборудования K_r, номер сетевого элемента, располагающего ресурсом S_j.

Далее необходимо сравнить номер сетевого элемента абонента N_i, номер программы телекоммуникационного оборудования K_r, номер сетевого элемента, располагающего ресурсом S_j, которые созданы на передающей и приемной стороне в соответствующих текущих и ответных атрибутах. При этом если они не совпадают, то необходимо изменить массив коммутации M, за счет дополнительной записи признаков нового информационного направления, имеющего явное воздействие нарушителя, что в дальнейшем позволит управлять трафиком в информационно-телекоммуникационной сети с учетом ее реконфигурации для обеспечения информационной безопасности.

В качестве выводов необходимо отметить, что предлагаемый подход управления трафиком в информационно-телекоммуникационной сети за счет выявления несанкционированного воздействия нарушителей и ее реконфигурации с учетом событий информационной безопасности позволит повысить как защищенность информационно-телекоммуникационной сети.

Список используемых источников

1. ГОСТ Р ИСО/МЭК 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М.: Изд-во стандартов, 2007.

2. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением

председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999. № 114

3. Бирюков А. А. Информационная безопасность: защита и нападение. 2-е изд. Москва: ДМК Пресс, 2017. 434 с.

4. Добрышин М. М. Предложение по совершенствованию систем противодействия DDoS-атакам // Телекоммуникации. 2018. № 10. С. 32–38.

5. Grechishnikov E. V. Algorithmic model of functioning of the system to detect and counter cyber attacks on virtual private network // International conference "Applied mathematics, computational science and mechanics: current problems", AMCSM 2018 Voronezh, 17–19 декабря 2018.

6. Бухарин В. В., Казачкин А. В. Способ и устройство управления потоками данных распределенной информационной системы с использованием идентификаторов. Пат. 2710284 Российская Федерация; № 2019118659; заявл. 17.06.2019: опубл. 25.12.2019.

7. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. СПб.: Питер, 2016. 992 с.

8. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. СПб.: БХВ-Петербург, 2003. 671 с.

УДК 004.043
ГРНТИ 81.93.29

АНАЛИЗ МОДЕЛЕЙ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ЗАДАЧИ ОБНАРУЖЕНИЯ КИБЕР-ИНСАЙДЕРОВ

И. С. Быстров, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В статье анализируются модели поведения пользователей, используемые для задачи обнаружения кибер-инсайдеров. Обнаружение кибер-инсайдеров осложнено тем, что злоумышленник, являясь сотрудником и находясь внутри защищенной сети, исполняет должностные обязанности. Это обстоятельство затрудняет идентификацию злоумышленника. Ключевым фактором для решения задачи является выбор моделей поведения пользователей. Выбор моделей непосредственно определяет возможности дальнейшего обнаружения злоумышленника. Рассматривается широкий спектр моделей: от анализа действий пользователя в одном приложении на персональном устройстве до анализа трафика с помощью специальных сетевых устройств.

модель поведения пользователей, аналитика поведения пользователей, обнаружение кибер-инсайдеров.

Более половины утечек информации из организаций происходит из-за намеренных действий сотрудников [1]. Помимо утечек информации дей-

ствия кибер-инсайдеров могут быть выражены в модифицировании, удалении, повреждении защищенной информации, нанесении ущерба инфраструктуре [2, 3]. Кибер-инсайдеры - это сотрудники или бывшие сотрудники организации, подрядчики, бизнес-партнеры, которые имеют или имели авторизованный доступ компьютерным сетям организации, системам или данным и намеренно злоупотребили доступом таким образом, что это негативно сказалось на конфиденциональности, целостности или доступности информации или информационных систем [4].

Кибер-инсайдеров трудно обнаружить по следующим причинам: небольшое число инсайдеров внутри организации; выполнение инсайдерами повседневных обязанностей, которые нужно отличать от инсайдерской активности; небольшой объем данных, доступных для анализа в связи с нежеланием организаций делать тему утечек публичной. Соответственно, для задачи обнаружения кибер-инсайдеров модели поведения пользователей должны учитывать то, что злоумышленник выполняет повседневные обязанности [5]. Поэтому нужно использовать такую информацию о пользователях, которая будет в наибольшей степени полезна в дальнейшем для выявления кибер-инсайдеров.

Поведение пользователя можно определить последовательностью событий. Событие - это простейший элемент модели поведения пользователя. Определение типов событий, которые будут использоваться в модели поведения пользователя происходит с учетом специфики организации (топология сети, программное обеспечение, законы и стандарты), могут быть использованы экспертные оценки.

Примеры событий, которые могут быть включены в модель поведения пользователя: системный вызов; запуска и завершение процесса; доступ к файлу в локальном хранилище; доступ к файлу на сетевом хранилище; обращение к базе данных; отправка и получение email; печать документов; использование USB устройства.

Для получения событий используются логи приложений, операционных систем, серверов и сетевых устройств. В общем случае несколько записей в логах могут характеризовать одно и то же событие. Например, обращение к базе данных может присутствовать в логе клиента базы данных, в логе сервера

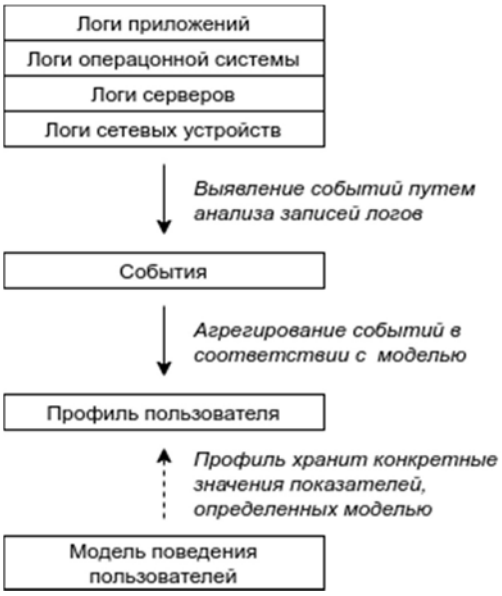


Рис. Взаимосвязь логов, событий, профиля пользователя и модели поведения пользователей

и в логе сетевого устройства. Также несколько записей в логе могут означать одно и то же событие. Например, доступ к ресурсу может происходить посредством выполнения серии команд, которые будут представлены отдельными записями в логе сервера.

Набор событий используется для построения профиля пользователя в соответствии с моделью поведения пользователей. Модель определяется таким образом, чтобы сделать возможным обнаружение кибер-инсайдеров. В модели могут использоваться различные методы [6]: количественные; статистические; последовательности (n-grams). Простая модель, например, может содержать количество случаев использования USB-устройства или количество исходящих писем на внешние почтовые адреса.

На рис. (см. выше) представлена взаимосвязь логов, событий, профиля пользователя и модели поведения пользователей.

Профили пользователей могут быть проанализированы с помощью методов машинного обучения и искусственного интеллекта на предмет наличия аномалий. В таблице ниже представлены некоторые показатели моделей, используемые для построения профилей пользователей.

Таблица. Примеры показателей моделей,
используемых в работах по обнаружению кибер-инсайдеров

Работа	Логи	События	Показатели модели
[7]	Логи, содержащие системные вызовы	Системные вызовы	Последовательность вызовов Гистограмма вызовов Системный вызовы с параметрами
ELICIT [8]	Анализ сетевого трафика (SMB, FTP, HTTP, SMTP)	Поисковые запросы Загрузки документов на устройство Размер документа	Наличие поисковых запросов с определенными ключевыми словами Количество загруженных документов Суммарный размер документов, использованных пользователем за определенный период времени
[9]	Программный комплекс SureView [10]	URL посещенной страницы Использование принтера Отправка электронных писем	Количество вложений в электронном письме Количество распечатанных документов
[11]	Insider Threat Test Dataset[12]	Отправка электронных писем	Количество часов использования устройства

Работа	Логи	События	Показатели модели
	Синтетические данные	URL посещенной страницы	Время окончания работы пользователя на устройстве
BAIT [1]	Данные получены с помощью игровой имитации	Просьба к коллеге отослать электронное письмо	Число действий, связанных с отсылкой информации
		Сохранение данных на USB	Число действий, связанных с получением информации

На основе вышеизложенного, можно предложить следующий подход к определению модели поведения пользователей:

1. Определение желаемых типов событий. Типы событий определяются сетевой инфраструктурой и программным обеспечением организации, способами доступа к информации и взаимодействием сотрудников друг с другом.

2. Обеспечение доступности и достаточности данных в логах для выявления событий.

3. Использование модели поведения пользователей, выбранной с учетом используемых типов событий.

Следует заметить, что различные модели поведения пользователей могут быть построены на основе одних и тех же событий. В дальнейшем они могут быть испытаны с различными методами обнаружения аномалий и выявлены наиболее эффективные методики обнаружения.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Azaria A. [et al.] Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data // IEEE Transactions on Computational Social Systems. 2014. Vol. 1. Behavioral Analysis of Insider Threat. № 2. pp. 135–155.

2. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7–10 August 2006. pp. 339–344.

3. 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, Springer-Verlag. V. 3685. 2005. pp. 311–324.

4. Cappelli D., Moore A., Trzeciak R. The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). Upper Saddle River, NJ: Addison-Wesley, 2012. 389 p.

5. Le D. C., Zincir-Heywood A. N. Machine learning based Insider Threat Modelling and Detection. 2019. p. 9.

6. Liu L. [et al.] Detecting and Preventing Cyber Insider Threats: A Survey // IEEE Communications Surveys & Tutorials. 2018. Vol. 20. Detecting and Preventing Cyber Insider Threats. No. 2. pp. 1397–1417.

7. Liu A. [et al.] A comparison of system call feature representations for insider threat detection // Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. West Point, NY, USA: IEEE, 2005. pp. 40–347.

8. Maloof M. A., Stephens G. D. ELICIT: A System for Detecting Insiders Who Violate Need-to-Know // Recent Advances in Intrusion Detection : Lecture Notes in Computer Science / eds. C. Kruegel, R. Lippmann, A. Clark. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007. Vol. 4637. pp. 146–166.

9. Ted E. [et al.] Detecting insider threats in a real corporate database of computer usage activity. 2013. pp. 1393–1401.

10. SureView™. URL: https://www.raytheon.com/ capabilities/rtnwcm/groups/iis/documents/content/rtn_iis_sureview_datasheet.pdf.

11. Legg P. A. [et al.] Automated Insider Threat Detection System Using User and Role-Based Profile Assessment // IEEE Systems Journal. 2017. Vol. 11. No. 2. pp. 503–512.

12. Insider Threat Test Dataset. URL: https://resources. sei.cmu.edu/library/asset-view.cfm?assetid=508099.

УДК 004.056
ГРНТИ 81.93.29

АРХИТЕКТУРА СИСТЕМЫ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ОТ КИБЕР АТАК И ВЫБОРА ЗАЩИТНЫХ МЕР С ИСПОЛЬЗОВАНИЕМ СЕМАНТИЧЕСКОЙ МОДЕЛИ ДАННЫХ И МЕТРИК

И. С. Быстров[1], А. В. Федорченко[1], Е. В. Федорченко[1,2]

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

В работе описывается предложенная архитектура системы оценивания защищенности от кибер атак и выбора защитных мер. В основе системы лежат методики оценивания защищенности и выбора защитных мер с использованием семантической модели данных и метрик. Разработанная семантическая модель объединяет источники данных для оценивания защищенности и выбора защитных мер, сами данные и метрики, и предназначена для формирования интегральных метрик защищенности на основе первичных метрик, вычисленных с использованием «сырых» данных. Разработанные методики включают этап формирования семантической модели на основе статической информации об анализируемой информационной системе, этап динамического формирования семантической модели путем обработки данных, получаемых в процессе

функционирования анализируемой информационной системы, и этап вычисления метрик с учетом сформированных вопросов оценивания защищенности и выбора защитных мер. Предлагаются алгоритмы интеграции разрабатываемой системы с системами управления информационной безопасностью с использованием методов обработки больших данных.

оценивание защищенности, кибер атака, защитные меры, семантическая модель, метрики, данные.

В настоящее время актуальны вопросы мониторинга и объективного оценивания защищенности с целью своевременного обнаружения и адекватного реагирования на кибер атаки. При этом способы формирования значимых интегральных метрик защищенности должны быть прозрачными и объяснимыми. Для этого предлагается система оценивания защищенности от кибер атак и выбора защитных мер на основе семантической модели данных и метрик. В данной работе описывается архитектура предлагаемой системы.

Разработанная архитектура системы оценивания защищенности от кибер атак и выбора защитных мер включает следующие компоненты:

1. Компонент сбора и предобработки данных, включая подкомпонент сбора условно статических данных из открытых источников данных безопасности (таких как база уязвимостей NVD [1]) и подкомпонент сбора динамической информации, поступающей от системы управления информационной безопасностью (например, журналы событий).

2. Компонент формирования семантической модели, включая подкомпонент формирования семантической модели на основе условно статической информации и подкомпонент формирования семантической модели на основе динамической информации.

3. Компонент оценивания защищенности, включая подкомпонент формирования списка вопросов по оцениванию защищенности, подкомпонент определения доступных данных и соответствующих объектов семантической модели и подкомпонент вычисления интегральных метрик защищенности.

4. Компонент выбора защитных мер, включая подкомпонент формирования списка вопросов по выбору защитных мер, подкомпонент определения доступных данных и соответствующих объектов семантической модели, подкомпонент определения списка доступных защитных мер и подкомпонент выбора оптимальных защитных мер.

5. База данных, содержащая результаты работы компонентов.

В основе предлагаемой системы лежат методики оценивания защищенности и выбора защитных мер с использованием семантической модели данных и метрик.

Разработанная методика формирования семантической модели включает этап формирования модели на основе статической информации об анализируемой информационной системе и этап динамического формирования

модели путем обработки данных, получаемых в процессе функционирования анализируемой информационной системы. Семантическая модель формируется в рамках компонента 2. Она объединяет источники данных для оценивания защищенности и выбора защитных мер, сами данные и метрики [2]. Отдельно выделяется группа концептов инфраструктуры, предназначенная для связи семантической модели с конкретной информационной системой. Данная группа концептов формируется динамически путем анализа событий и сетевого трафика, получаемых от системы управления информационной безопасностью в рамках подкомпонента формирования семантической модели на основе динамической информации. Семантическая модель предназначена для формирования интегральных метрик защищенности на основе первичных метрик, вычисленных с использованием «сырых» данных.

Компонент 3 предложенной архитектуры предназначен для реализации методики оценивания защищенности [3], включающей следующие шаги: определение набора доступных данных (и соответствующих экземпляров семантической модели) для ответа на вопрос оценивания защищенности; расширение знаний с использованием отношений между концептами семантической модели и вычисление интегральной метрики защищенности. Особенностью методики является использование логических отношений между концептами для построения формулы вычисления интегральной метрики на основе первичных метрик.

Компонент 4 предложенной архитектуры предназначен для реализации методики выбора защитных мер [4]. Разработанная методика работает с учетом обнаруженных событий безопасности и различных профилей атакующих, и использует методы интеллектуального анализа данных. Методика включает следующие шаги: определение набора доступных данных (и соответствующих экземпляров семантической модели) для ответа на вопрос, связанный с выбором защитных мер; определение списка доступных защитных мер путем логического вывода с использованием отношений между концептами разработанной семантической модели; выбор оптимальной меры за счет оптимизации коэффициента выбора защитных мер, рассчитанного для доступных мер.

Интеграция разрабатываемой системы с системами управления информационной безопасностью происходит на этапе сбора и предобработки собираемых ими данных, а также на этапе вывода результатов. В рамках архитектуры предполагается использовать нереляционную базу данных, и платформы Hadoop и Spark, поскольку современные системы управления информационной безопасностью обрабатывают большие объемы данных безопасности.

Практическая значимость разработанной архитектуры заключается в том, что построенная на ее основе автоматизированная система может быть

использована как компонент систем управления информационной безопасностью для повышения их эффективности.

Работа выполнена при финансовой поддержке РФФИ (проект 19-07-01246 А).

Список используемых источников

1. База уязвимостей NVD. URL: https://nvd.nist.gov/ (дата обращения 30.03.2021).

2. Doynikova E., Fedorchenko A., Kotenko I. A Semantic Model for Security Evaluation of Information Systems // Journal of Cyber Security and Mobility. 2020. Vol. 9. No. 2. pp. 301–330. DOI: 10.13052/jcsm2245-1439.925.

3. Дойникова Е. В., Федорченко А. В., Котенко И. В., Новикова Е. С. Методика оценивания защищенности на основе семантической модели метрик и данных // Вопросы кибербезопасности. 2021. № 1 (41). С. 29–40. DOI: 10.21681/2311-3456-2021-1-29-40.

4. Дойникова Е. В., Федорченко А. В., Гайфулина Д. А. Методика выбора мер противодействия кибератакам с использованием онтологии метрик безопасности // XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28–30 октября 2020 г. Часть 1. С. 137–138.

УДК 47.59
ГРНТИ 654.16

ПОДХОД К МОДЕЛИРОВАНИЮ ТОПОЛОГИЧЕСКОГО РАЗМЕЩЕНИЯ АБОНЕНТОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Е. В. Вершенник, С. П. Тесля

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

В статье излагается решение, которое может использоваться для моделирования сети связи при ее проектировании, модернизации, эксплуатации, в частности, для формирования оптимального варианта топологического размещения множества информационно взаимосвязанных абонентов на заданном фрагменте сети связи общего пользования.

модель сети связи, моделирование информационно-телекоммуникационных сетей, адекватность моделирования.

Технологической основой любой системы управления являются информационно – телекоммуникационные сети [1]. В современных условиях развёртывание под каждую систему управления собственной системы связи

не рационально и экономически не выгодно, так как имеющаяся развернутая и функционирующая сеть связи общего пользования Единой сети электросвязи имеет достаточные ресурсы и технологические возможности для подключения новых абонентов.

Таким образом, множество систем управления могут одновременно использовать общую транспортную сеть, при этом непосредственно влиять друг на друга. Необходимо также учитывать, что различными системами управления предъявляются различные требования к сети связи. Поэтому в целях определения оптимального варианта топологического размещения множества абонентов заданной системы управления на заданном фрагменте сети связи общего пользования необходимо оценить возможности, предоставляемые транспортной сетью, с учётом выдвигаемых требований к сети связи, а также учетом влияние на нее других систем управления.

Данная задача может быть выполнена при помощи использования метода имитационного моделирования.

Анализ существующих моделей и способов моделирования [2 - 7] показал, что в них не учитывается разнородность абонентов и их нагрузки, также не учитываются требования абонентов к сети связи, а также возможность их перемещения.

Авторами статьи предлагается способ, позволяющий определить оптимальный вариант топологического размещения множества информационно взаимосвязанных абонентов на заданном фрагменте сети связи общего пользования, что позволит минимизировать расход сил и средств связи на обеспечение доступа подключаемых абонентов, минимизировать их влияние на качество услуг, предоставляемых уже подключенных абонентов, минимизировать потребность в изменении реализуемых вариантов маршрутизации; максимизировать качество предоставляемых услуг подключаемым абонентам.

Способ заключается в следующем [8]:

На первом этапе задают исходные данные, к которым можно отнести площадь реального фрагмента сети связи, количество подключаемых абонентов, количество и структуру информационных направлений между подключаемыми абонентами, требуемые значения допустимых интервалов взаимного удаления между абонентами, требуемые значения показателей качества связи, характеристики узлов и линий связи сети связи, критерии ранжирования узлов и линий связи, количественный состав и характеристики резерва сил и средств связи.

Далее формируют состав и структуру сети связи, инвариантной реальному фрагменту сети связи. Формирование такой структуры сети может быть осуществлено по способам, описанным в [2, 9].

Подключаемым абонентам присваивают приоритеты и осуществляют их ранжирование в соответствии с присвоенным приоритетом.

Под приоритетом понимается преимущественное право абонента перед другими, определяющее его относительную важность на доступ к ресурсам коллективного пользования для передачи информации или прерывания.

Ранжируют узлы и линии связи в зависимости от заданным критериям.

Моделируют первоначальный вариант топологического размещения подключаемых абонентов с учетом их важности, значимости узлов и линий связи, допустимых интервалов взаимного удаления.

Приступают к формированию множества маршрутов между подключаемыми абонентами с учетом заданной структуры информационных направлений.

Моделируют функционирование сети связи с учётом нагрузки от пользователей. Моделирование функционирования сети связи, с учётом нагрузки от пользователей может быть реализовано согласно способу по патенту [3].

Моделируют процессы воздействия множества дестабилизирующих факторов на элементы сети связи [10, 11, 12].

Рассчитывают показатели качества связи для каждого информационного направления. Например, качество связи может характеризоваться своевременностью, достоверностью и скрытностью связи [13].

Своевременность характеризует способность системы связи передавать сообщения определенной длины в сроки, не превышающие заданные значения. Это означает, что система связи способна обеспечить передачу и доставку сообщений или ведение переговоров в заданное время, обусловленное оперативно-тактической обстановкой.

Достоверность связи характеризуется максимальным значением вероятности ошибочного приема знака при заданной максимальной вероятности ошибочного приема бита, что обеспечивает воспроизведение передаваемых сообщений в пунктах приема с заданной точностью.

Критерии оценки и количественные показатели своевременности и достоверности описаны в [13].

Количественным показателем своевременности может быть вероятность своевременной передачи сообщений, которая может быть рассчитана согласно выражению:

$$P_{\text{св}} = \frac{N_{\text{св}}}{N},$$

где $N_{\text{св}}$ – количество своевременно переданных сообщений,

N – количество всех переданных сообщений.

Количественным показателем достоверности может выступать вероятность правильного приема сообщений, которая может быть рассчитана согласно выражению:

$$P_{\text{пс}} = \frac{N_{\text{пс}}}{N},$$

где $N_{\text{пс}}$ – количество правильно принятых сообщений,

N – количество всех переданных сообщений.

Скрытность связи – это способность связи противостоять раскрытию содержания передаваемой информации, факта, места ее передачи и принадлежности объекта передачи.

Количественным показателем скрытности может выступать разведзащищенность.

Затем последовательно сравнивают значения рассчитанных показателей качества связи с заданными требуемыми значениями.

Если значения рассчитанных показателей качества больше или равны заданным требуемым значениям, то фиксируют места топологического размещения информационно взаимосвязанных абонентов, значения показателей качества связи информационных направлений которых равны или больше требуемых.

Если значения рассчитанных показателей качества ниже заданных требуемых, то информационно взаимосвязанным абонентам последовательно присваивают координаты ближайшего последующего узла сети связи с учетом заданного допустимого интервала взаимного удаления и повторяют действия по выбору мест топологического размещения информационно взаимосвязанных абонентов до достижения значений показателей качества связи каждого информационного направления требуемым.

Если значения показателей качества связи информационных направлений при переборе всех узлов связи в пределах заданного интервала удаления не равны требуемым, то реконфигурируют систему связи за счет резерва сил и средств связи,

Реконфигурация системы связи заключается в изменении ее структуры, топологии, режимов работы (введении в работу резервных каналов (линий) и средств связи, восстановлении поврежденных и отказавших средств связи, изменении частот передачи, приема, мощности передачи, видов обработки сигналов, маршрутов прохождения и т. д.).

Повторяют действия по выбору мест топологического размещения подключаемых абонентов до достижения значений показателей качества связи каждого информационного направления требуемым.

На заключительном этапе выводят полученные результаты.

Результатами моделирования являются: географические координаты мест топологического размещения информационно взаимосвязанных абонентов; количество и характеристики использованных для реконфигурации средств связи; количество и характеристики используемых сил и средств привязки.

Таким образом, за счет определения оптимального варианта топологического размещения множества подключаемых на заданном фрагменте сети связи общего пользования, происходит минимизация расхода сил и средств связи на обеспечение доступа множества абонентов; минимизация влияния подключаемых абонентов на качество услуг, предоставляемых уже подключенным абонентам; минимизация потребности в изменении реализуемых вариантов маршрутизации; максимизация качества предоставляемых услуг подключаемым абонентам.

Список используемых источников

1. Боговик А. В., Игнатов В. В. Теория управления в системах военного назначения: Учебн. ВАС, 2008. С. 35.

2. Алисевич Е. А., Синев С. Г., Стародубцев П. Ю., Сухорукова Е. В., Чукариков А. Г., Шаронов А. Н. Способ моделирования сетей связи. Пат. 2546318 Российская Федерация ; заявитель и патентообладатель ФГБОУ ВПО «СПГТЭУ». – № 2014103873; заявл. 04.02.2014; опубл. 10.04.2015.

3. Анисимов В. В., Бегаев А. Н., Стародубцев Ю. И., Сухорукова Е. В., Федоров В. Г., Чукариков А. Г. Способ целенаправленной трансформации параметров модели реального фрагмента сети связи. Пат. 2620200 Российская Федерация ; заявитель и патентообладатель Бегаев А. Н. – № 2016119980; заявл. 23.05.2016; опубл 23.05.2017.

4. Бречко А. А., Вершенник А. В., Вершенник Е. В., Львова Н. В., Первов М. С., Стародубцев Ю. И. Способ моделирования двусторонних воздействий при использовании конфликтующими системами управления общего технологического ресурса. Пат. 2692423 Российская Федерация ; заявитель и патентообладатель Львова Н. В., Стародубцев Ю. И. – № 2018122181; заявл. 15.06.2018, опубл. 24.06.2019.

5. Бречко А. А., Бухарин В. В., Вершенник А. В., Вершенник Е. В., Львова Н. В., Стародубцев Ю. И. Способ моделирования преднамеренных повреждений элементов сети связи, функционирующей в интересах разнородных, в том числе анатагонистических систем управления. Пат. 2655466 Российская Федерация ; заявитель и патентообладатель Бречко А. А. – № 2017127332; заявл. 31.07.2017; опубл 28.05.2018.

6. Сухорукова Е. В., Закалкин П. В., Андреянов С. Н. Моделирование торговых бизнес-процессов: способы задания модельного времени // Проблемы экономики и управления в торговле и промышленности. 2013. № 1 (1). С. 104–109.

7. Алисевич Е. А., Закалкин П. В., Кириллова Т. В., Стародубцев Ю. И., Сухорукова Е. В., Чукариков А. Г. Способ адаптивного повышения адекватности модели. Пат. 2562767 Российская Федерация ; заявитель и патентообладатель ФГБОУ ВПО «СПГТЭУ». – № 2014111876; заявл. 27.03.2014; опубл. 10.09.2015.

8. Вершенник А. В., Вершенник Е. В., Латушко Н. А., Стародубцев Ю. И. Способ моделирования оптимального варианта топологического размещения множества информационно взаимосвязанных абонентов на заданном фрагменте сети связи общего пользования. Пат. 2690213 Российская Федерация. – № 2018118104; заявл. 16.05.2018; опубл 31.05.2019.

9. Беликова И. С., Закалкин П. В., Стародубцев Ю. И., Сухорукова Е. В. Моделирование сетей связи с учетом топологических и структурных неоднородностей // Информационные системы и технологии. 2017. № 2 (100). С. 93–101.

10. Синев С. Г., Сорокин М. А., Стародубцев П. Ю., Сухорукова Е. В. Способ определения оптимальной периодичности контроля состояния процессов. Пат. 2623791 Российская Федерация; заявитель и патентообладатель Стародубцев П. Ю. – № 2015108734; заявл. 25.01.2016; опубл 29.06.2017.

11. Стародубцев П. Ю., Стародубцев Ю. И., Вершенник Е. В., Чеснаков М. Н. Способ мониторинга состояния электрических сетей и сетей связи. Пат. 2646321 Российская Федерация ; заявитель и патентообладатель Стародубцев Ю. И., Вершенник Е. В. – № 2017105612; заявл. 20.02.2017; опубл 02.03.2018.

12. Starodubcev U. I., Vershennik E. V., Balenko E. G. Method of monitoring the state of communication networks // 2019 International Science and Technology Conference "EastConf", EastConf 2019. 2019. P. 8725400.

13. Ермишян А. Г. Теоретические основы построения систем военной связи в объединениях, соединениях. Часть 1. Методологические основы организационно-технических систем военной связи. ВАС, СПб. 2005, 741 с., С. 335–339.

УДК 004.056.55; 535.14
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ МОДИФИЦИРОВАННОГО ПРОТОКОЛА BB84-DS ДЛЯ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ (QKD)

К. В. Вершинина, А. Р. Салтыков

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

Одним из перспективных решений для защиты сетей доступа от возможных атак является применение технологии квантового распределения ключей (Quantum Key Distribution), которая позволяет пользователям обмениваться секретными ключами с безусловной безопасностью, гарантированной законами квантовой механики.

В сетях QKD актуальна проблема защиты от атаки на расщепление числа фотонов (Photon Number Splitting). В стандартном протоколе QKD-BB84 гарантируется безопасность только сигналов, исходящих от одиночных фотонных импульсов. Поэтому для борьбы с PNS-атакой предлагается более совершенная версия протокола – BB84-DS, усиленного состояниями-ловушек (decoy-states). В статье рассмотрено, как состояния-ловушки протокола BB84-DS способны усилить безопасность квантовых сетей. А также, какие перспективы у протокола BB84-DS в разрезе глобальных квантовых коммуникационных сетей.

квантовое распределение ключей, QKD, протокол BB84, BB84-DS, состояния-ловушки, PNS-атака, поляризация фотонов.

Квантовое распределение ключа (QKD) представляет собой инновационную комбинацию традиционной криптографии и квантовой механики,

позволяя удалённым пользователям обмениваться конфиденциальной информацией с безусловной безопасностью.

В предыдущем исследовании [1] был описан алгоритм и физические особенности протокола BB84, а также более подробно рассмотрена формула (1) для определения скорости генерации ключей [2]. На рис. 1 показана упрощённая схема работы протокола BB84.

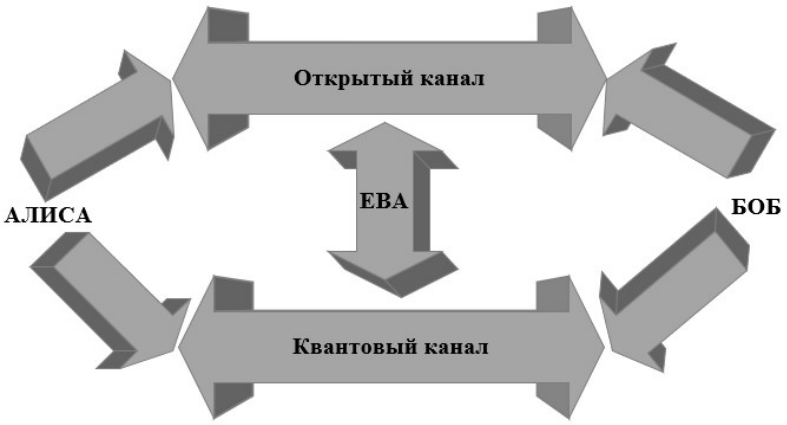


Рис. 1. Структурная схема работы протокола BB84

Согласно представленной схеме (рис. 1), по открытому каналу от отправителя (Алисы) к получателю (Бобу) передаётся служебная информация, а по квантовому каналу – секретные состояния поляризации фотонов, которые пытается перехватить злоумышленник (Ева).

$$R \geq q\{Q_{\mu} f(E_{\mu}) H_2(E_{\mu}) + Q_1[1 - H_2(e_1)]\}, \quad (1)$$

где индекс μ – среднее число фотонов в сигнальном импульсе (интенсивность),

Q_{μ} – коэффициент усиления состояний сигнала,

E_{μ} – частота квантовых битовых ошибок (QBER) состояний сигнала,

Q_1 – коэффициент усиления одиночных фотонных состояний,

e_1 – частота ошибок в однофотонных состояниях,

$f(x)$ – скорость коррекции ошибок,

q – базисный коэффициент просеивания,

$H_{2(x)}$ – двоичная информационная функция Шеннона.

В протоколе BB84 Алиса использует многофотонный источник излучения – сильно ослабленный лазер, который создает слабокогерентные состояния [3], что создаёт условия для атаки на расщепление числа фотонов (PNS-атаки). В стандартном протоколе BB84 гарантируется безопасность только сигналов, исходящих от однофотонных источников, поэтому необходима интеграция состояний-ловушек [4].

Состояния-ловушки используется для обнаружения подслушивающих атак, в то время как стандартные состояния протокола BB84 используются только для генерации ключей. Отличие между состояниями-ловушек и стандартными состояниями протокола BB84 заключается в их интенсивностях,

т. е. в распределениях фотонных чисел. В таблице показано наглядное представление типов поляризаций фотонов и соответствующих интенсивностей.

ТАБЛИЦА. Представления поляризаций фотона и интенсивностей состояний в протоколе BB84-DS

Тип поляризации	Графическое обозначение	Интенсивность
Горизонтальная		I_0
Веритикальная		
Диагональная (135º)		I_1
Диагональная (45º)		I_2

На рис. 2 проиллюстрирован результат реализации атаки на расщепление числа фотонов по протоколу *BB84-DS* и обнаружение Алисой и Бобом факта атаки Евы. В случаях «1», «2», «3», «4» и «5» (рис. 2) передачи интенсивностей были выполнены корректно – интенсивности соответствуют заданным *поляризациям фотонов*. Но в случаях «6» и «7» очевиден факт нарушения согласования в передаче фотонных состояний между Алисой и Бобом, что говорит о постороннем вмешательстве в квантовый канал и необходимости повторных согласований об обмене секретными ключами.

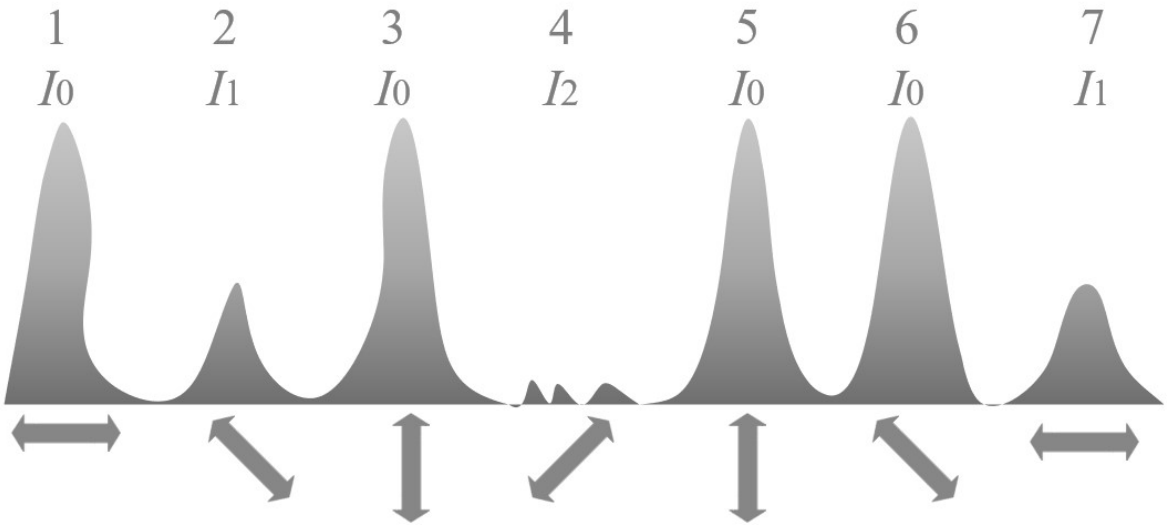


Рис. 2. Распределение интенсивностей поляризационных состояний по протоколу BB84-DS

Таким образом, получая неправильные интенсивности света на стороне получателя секретного ключа – Боба, мы можем удостоверится в факте атаки на квантовую сеть со стороны Евы

Атмосферное свободное пространство и оптическое волокно уже широко эксплуатируются как каналы для межконтинентальных и междугородних квантовых коммуникаций. В таких каналах уже многократно доказана эффективность использования протокола BB84-DS [5, 6].

Актуальной задачей в строительстве глобальных квантовый сетей связи стала разработка воздушно-морского канала свободного пространства, реализуемого спутниковым соединением квантового ресурса с подводным транспортным средством. Однако длинная квантовая коммуникационная водная сеть чрезвычайно сложна из-за неизбежно высоких потерь. Поэтому, китайские учёные в своём исследовании [7] предложили экспериментальную демонстрацию подводной технологии квантового распределения ключей с состояниями-ловушками для предотвращения высоких потерь, сохраняя низкую квантовую частоту ошибок по битам – меньше, чем 2,5 % на разных расстояниях. Используя сине-зеленые лазеры на высокой скорости 50 МГц и протокол BB84-DS, Cheng-Qiu Hu (и др.) смогли показать реализацию QKD на дальних расстояниях для воздушно-водных квантовых коммуникаций. Важно отметить, что в экспериментальной установке Cheng-Qiu Hu (и др.) для водно-воздушной коммуникации используется генератор произвольных волн AWG (*Arbitrary Wave Generator*), в отличие от классической реализации с оптическим волокном, где применяются мультиплексоры с технологией многослойной волноводной решетки типа AWG (Arrayed Waveguide Grating) [8].

Данный эксперимент для воздушно-водных квантовых коммуникаций был основан на использовании аттенюаторов и регулируемого модуля полуволновых пластин HWP (*Half Wave Plates*), чтобы сделать точными три интенсивности состояний-ловушек, для которых среднее число фотонов на импульс составляет: 0.9, 0.3 и для вакуума – 0. Смешивая случайным образом несколько состояний-ловушек различной интенсивности с определенной пропорцией в источнике передатчика, пользователи (Алиса и Боб) удостоверяются, что любая PNS-атака Евы будет обнаружена.

Таким образом, существуют большие перспективы для интеграции модифицированного протокола BB84-DS в глобальные квантовые коммуникационные сети. Секретные ключи, передаваемые по протоколу BB84-DS, являются защищёнными от PNS-атак, т. е. с помощью дополнительных состояний-ловушек возможно осуществлять безопасную реализацию технологии *QKD* с использованием слабокогерентного лазерного источника.

Список используемых источников

1. Вершинина К. В. Применение протокола BB84 для квантового распределения ключей (QKD) // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2020). Региональная научно-методическая конференция магистрантов и их руководителей; сборник лучших докладов конф. СПб.: СПбГУТ, 2021. С. 166–171. ISBN 978-5-89160-204-5. URL: http://pkm.sut.ru/documents/best_pkm2020.pdf
2. Ali S., Saharudin S., Wahiddin R. Decoy State Quantum Key Distribution // IIUM Engineering Journal. 2009. Vol. 10. No. 2. pp. 81–86.
3. Lo H.-K., Ma X., Chen K. Decoy State Quantum Key Distribution // Physical Review Letters. 2005. Vol. 94. No. 23. p. 230504.
4. Hwang W.-Y. Quantum key distribution with high loss: toward global secure communication // Physical Review Letters. 2003. Vol. 91. No. 5. p. 057901.
5. Schmitt-Manderbach T., Weier H., Furst M., Ursin R., Tiefenbacher F., Scheidl T., Perdigues J., Sodnik Z., Kurtsiefer C., Rarity J. G., Zeilinger A., Weinfurter H. Experimental demonstration of freespace decoy-state quantum key distribution over 144 km // Phy. Rev. Lett. 2007. Vol. 98. No. 1. p. 010504.
6. Dixon A. R., Yuan Z. L., Dynes J. F., Sharpe A. W., Shields A. J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate // Optics Express. 2008. Vol. 16. No. 23. pp. 18 790–18 979.
7. Hu C. Q., Yan Z. Q. et al. Decoy-state quantum key distribution over a long-distance high-loss underwater free-space channel // Phys. Rev. Applied. 2020. Vol. 1. pp. 1–9.
8. Вершинина К. В., Салтыков А. Р. Применение квантового распределения ключей (QKD) в сетях WDM PON // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 225–230. ISBN 978-5-89160-197-0. URL: http://apino.spbgut.ru/

Статья представлена заведующим кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной.

УДК 65.012.8
ГРНТИ 10.19.61

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ ПРЕДПРИЯТИЙ

А. Ю Викулова[1], В. А. Волостных[2], П. А. Кононов[1], В. А. Парфиров[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Военная академия связи им. Маршала Советского Союза С. М. Буденного

В настоящее время значительный ряд предприятий размещается на различных территориях и для обмена информацией между обособленными структурными подразделениями используются телекоммуникационные системы. При этом, для обеспечения

управленческих процессов необходимо обмениваться информацией конфиденциального характера, в том числе персональными данными. В статье рассматриваются способы защиты персональных данных при их передаче с между структурными подразделениями территориально-распределенного предприятия. Приведены основные подходы к выбору средств криптографической защиты информации для защиты персональных данных. Статья может быть полезна специалистам подразделений технической защиты информации.

защита персональных данных, электронный документооборот, средства защиты информации, средства криптографической защиты информации, несанкционированный доступ к информации, территориально-распределенное предприятие.

К числу важных задач, стоящих перед руководством предприятий, организаций и учреждений (далее предприятия) с 2006 года относится задача обеспечение безопасности обработки персональных данных [1]. Эту задачу чаще всего возлагают на службы корпоративной защиты информации или на подразделения информационной безопасности (ИБ). Известно, что законодательством Российской Федерации установлены достаточно жесткие требования к обеспечению безопасностиперсональных данных и установлена ответственность должностных лиц за ненадлежащее выполнение этих требований. Исходя из этого, возникает необходимость разработки мероприятий, обеспечивающих требуемый уровень защищенности персональных данных при их обработке в информационных системах территориально распределенных предприятий.

Несмотря на значительный опыт обеспечения безопасности обработки персональных данных в системах электронного документооборота, который специалисты подразделений ИБ приобрели методом проб и ошибок, а также в ходе обучения в специализированных образовательных организациях и на научно-практических конференциях, некоторые аспекты проблемы остаются «за кадром».

Известно, что ряд крупных предприятий размещаются на нескольких территориях, которые могут быть расположены как на незначительном расстоянии друг от друга (назовем их группой А), так и на значительном расстоянии (группа Б). Отнесем к группе А предприятия, все площадки которых можно обеспечить информационными коммуникациями посредством кабельных линий, принадлежащих предприятию на праве собственности или арендованных у телекоммуникационных кампаний России. К группе Б отнесем предприятия, которые осуществляют документальный обмен, содержащий персональные данные между подразделениями предприятия размещенными на удаленных друг от друга территориях и ведут этот обмен информацией посредством сетей связи общего пользования – т. е. с использованием сети Интернет. Согласно [2] оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры по обеспечению безопасности обработки персональных

данных. Эти меры должны быть разумно-достаточными и соответствовать требованиям законодательства Российской Федерации. Очевидно, что для предприятий типа А стоит задача воспретить физический доступ третьих лиц к линии связи между площадками и съем информации с этой линии. Очевидно, защищенность информации передаваемой по линии связи будет зависеть от вида линии, ее протяженности, способа ее прокладки и от применяемого кабеля.

Известно, что к наиболее защищенным, относится способ подземной прокладки кабельных линий, а кабельная линия выполнена на основе оптоволокна [3]. В этом случае съем информации с такой линии существенно затруднен и можно полагать что информация, содержащая персональные данные работников производственного предприятия надежно защищена. В этом случае подразделение связи (информатизации) должны совместно с подразделением ИБ выработать организационные меры по контролю за трассой прокладки кабельной линии. При использовании кабельных линий на медной основе без применения средств уплотнения необходимо предусмотреть использование средств защиты от несанкционированных подключений ккабельной линии, которые могут включать в себя устройства сигнализации о несанкционированном подключении к линии.

Способ использования кабельных линий для осуществления коммуникаций между структурными подразделениями, находящимися на территориях, расположенных в различных контролируемых зонах приемлем для предприятий структурные подразделениям которых находятся на незначительном удалении. Однако, для большинства территориально-распределенных предприятий это нехарактерно и для осуществления передачи информации и в том числе персональных данных чаще всего используется сеть общего пользования. В таком случае возможности нарушителя существенно возрастают. И для защиты информации требуются средства криптографической защиты информации (СКЗИ). Поскольку перечень типов СКЗИ весьма значителен, то предлагаются следующие подходы к их выбору.

Очевидно, что специалистам подразделений ИБ необходимо уяснить категории персональных данных, обрабатываемых в информационной системе и передаваемых между территориально-удаленными структурными подразделениями и на этой основе определить требуемый уровень защищенности персональных данных в информационной системе [3]. Далее в соответствии с [4]. разработать Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определить на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ. Авторы полагают, что специалистам понятно, что СКЗИ должны быть только Российского производства и иметь соответствующую лицензию ФСБ России, и в ряде случаев ФСТЭК России.

Исходя из этого целесообразно тип и модификацию СКЗИ выбирать на официальном сайте ФСБ России.

В целях выбора оптимального решения предлагается следующая последовательность.

На 1-м этапе необходимо уяснить информационные потоки на информационных направлениях между структурными подразделениями, которые требуют защиты средствами криптографической защиты информации. Если таких подразделений несколько, то необходимо уяснить параметры максимального потока с учетом перспектив развития предприятия.

На 2-м этапе из Перечня средств защиты информации, сертифицированных ФСБ России, с учетом требуемого класса СКЗИ и необходимой производительности СКЗИ, необходимо составить список СКЗИ, возможных для применения на предприятии. При этом необходимо обратить внимание на окончание срока действия сертификата ФСБ России и включать в список только те СКЗИ, у которых срок действия сертификата максимальный или имеются ссылки на возможность его продления.

На 3-м этапе из составленного списка предлагается выбрать те СКЗИ, которые имеют дополнительные функции, необходимые для защиты информационных систем предприятия. К числу таких функций относится функция межсетевого экранирования и ряд СКЗИ такую функцию выполняют.

На 4-м этапе целесообразно выделить те СКЗИ, производители или их представители которых имеют опыт установки СКЗИ и находятся в близкой доступности, что имеет значение для обеспечения надежности функционирования системы защиты информационных систем предприятия.

На завершающем этапе, как правило, проводится оценка стоимости приобретения СКЗИ и дополнительного оборудования, их установки, ввода в эксплуатацию и сопровождения [5].

На основе анализа функционирования ряда предприятий и возможностей рынка Северо-Западного региона авторами был сделан вывод о целесообразности для защиты персональных данных и другой информации конфиденциального характера применения СКЗИ типа «Континент».

Аппаратно-программный комплекс шифрования «КОНТИНЕНТ» версии 3.9 предназначен для защиты сетевой инфраструктурыи создания VPN-сетей с использованием алгоритмов ГОСТ.

Предназначен для решения следующих задач:

- Защита периметра сети.
- Объединение филиалов организации в виртуальную частную сеть (VPN).
- Защищенный удаленный доступ.

Сертификация ФСТЭК России:

− 4 класс МЭ тип «А» (включает сертификацию по НДВ);

− 4 класс сетевой СОВ (ИТ.СОВ.С4.ПЗ).

Сертификация ФСБ России:

− СКЗИ КС3;

− 4 класс по РД МЭ.

СКЗИ сертифицировано для защиты информационных систем персональных данных (ИСПДн) до уровня защищенности УЗ1. включительно. Некоторые характеристики которого приведены в таблице.

ТАБЛИЦА. Некоторые характеристики СКЗИ АПКШ «Континент»

Модель	Спецификация
АПКШ «Континент» IPC-3000F	Количество подключённых устройств АПКШ «Континент»: до 3000. Количество подключённых клиентов «Континент-АП»: до 3000. Доступен в модификациях: ЦУС, КШ, КК, ДА.
АПКШ «Континент» IPC-500	Количество подключённых устройств АПКШ «Континент»: до 500. Количество подключённых клиентов «Континент-АП»: до 500. Доступен в модификациях: ЦУС, КШ, КК, ДА.
АПКШ «Континент» IPC-25	Количество подключённых устройств АПКШ «Континент»: до 10. Количество подключённых клиентов «Континент-АП»: до 25. Доступен в модификациях: ЦУС, КШ, КК, ДА.
АПКШ «Континент» IPC-10	Количество подключённых устройств АПКШ «Континент»: до 5.

Выводы и рекомендации:

1. Защита персональных данных территориально-распределенного предприятия может быть эффективной только при комплексном подходе к созданию системы защиты информации, включая технические, организационные решения, а также подготовку должностных лиц подразделений информационной безопасности.

2. При создании системы защиты персональных данных передаваемых между структурными подразделениями территориально-распределенного предприятия наиболее оптимальным решением является использование средств криптографической защиты информации.

3. В целях принятия эффективного решения о выборе СКЗИ предлагаются подходы, изложенные в настоящей статье.

4. К числу наиболее приемлемых типов СКЗИ, по мнению авторов, можно отнести СКЗИ АПКШ Континент. Данное решение обуславливается широкой линейкой СКЗИ, наличием дополнительных функций по защите информации, существенным временем нахождения на рынке СКЗИ, либеральными ценами и положительной репутацией производителя. (Просьба –

данный вывод не считать рекламой, так как данное заключение основано на большом опыте применения СКЗИ для защиты информационных ресурсов предприятий и организаций.)

Список используемых источников

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».

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

3. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). М. Гостехкомиссия России, 2001.

4. Приказ ФСБ России от 10 июля 2014 года N 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

5. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ МОДЕЛЕЙ ДАННЫХ ПОПУЛЯРНЫХ СОЦИАЛЬНЫХ СЕТЕЙ

Л. А. Виткова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Существующие подходы к построению моделей социальных сетей можно условно разделить на три концепции: модели представления данных, модели информационного обмена в социальных сетях, модели распространения информации. Каждая концепция по-своему уникальна и позволяет описывать различные характеристики. В основе анализа и синтеза структур данных популярных социальных сетей используется концепция представления данных.

социальные сети, модели данных, структуры данных социальных сетей, вредоносная информация, распространение информации.

Модели данных (МД) – это совокупность правил создания и взаимосвязи структур данных социальных сетей в базе данных, возможных операций, а также ограничений (например количество взаимных друзей

в Facebook, VK) [1]. Модель данных всех социальных сетей состоит из трех наборов: (1) набор типов структур данных; (2) операторов и правил вывода; (3) набор общих правил целостности.

В основе структуризации данных СС лежат концепции «агрегации» и «обобщения». При этом наименьшей единицей в модели данных социальной сети (МДСС) является «элемент данных» (сетевая модель данных (версия CODASYL) [2]) или «атрибут» (реляционная модель данных (РМД) [3]). Поименованная совокупность всех элементов данных внутри МДСС, которую можно рассматривать как единое целое называется «агрегат данных» (CODASYL). В МД социальной сети «запись» (CODASYL) или «кортеж» (РМД) может иметь несколько атрибутов. Так, например запись: пользователь <user> имеет несколько элементов данных (связанный друг, связанный пост (репост), пол) и несколько агрегатов: простые агрегаты – ФИО, адрес и повторяющиеся агрегаты – интересы.

Среди атрибутов МДСС выделяются одно или несколько ключевых полей в качестве основного ключа, именно они характеризуют домены (классы) МДСС. Если модель данных описывает класс реципиента, тогда основной ключ – это имя или идентификатор. Для МД социальной сети основными ключами будут идентификатор источника и идентификатор сообщения.

Рассмотрим три основных структуры данных социальных сетей.

Первый тип СС – это сети, структура которых представляет собой полносвязный граф (Полносвязанные СС). К таким сетям относятся Facebook, VK, OK и другие схожие (рис. 1). Особенностью таких сетей является связь между идентификаторами страниц двунаправленная или однонаправленная (на рисунке – не прерывистые линии), которая позволяет сторонним страницам (будь то страница пользователя или группы) взаимодействовать с сообщениями или страницами, с которыми они не связаны – косвенная связь (на рисунке – прерывистые линии).

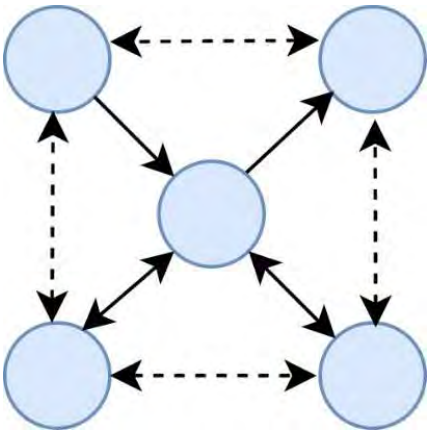


Рис. 1. Структура данных полносвязных социальных сетей

Второй тип – социальные сети, медиа-трансляторы информации (будь то пользователь или организация). По своей сути структура данных таких СС также, как и первого типа содержит связи между идентификаторами страниц, однако медиа-транслятор имеет свою отличительную особенность – это сторонний информационный канал, формируемый системой на основе анализа предпочтений получателей и связанных с ними идентификаторов (рис. 2). Но если в сетях первого типа вершинами графа могут быть как сообщения, так и страницы пользователей,

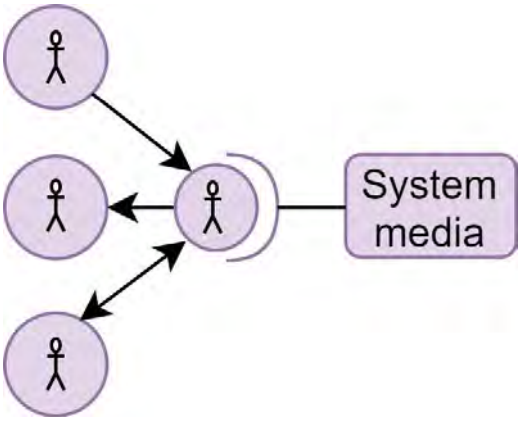


Рис. 2. Структура данных социальных сетей медиа-трансляторов

групп, то в СС второго типа связь устанавливается только между пользователями или стоящими за их страницами организациями. Одним из ярких примеров таких СС является Instagram. Новая сеть медиа-транслятор – Tik Tok.

К третьему типу сетей относиться СС структура данных, которых однонаправленная от многих источников (сообщений) ко одному реципиенту (рис 3). Отличительной особенностью таких сетей является то, что получатель информации выбирает набор источников, с которыми он связан (подписан на них), система предлагает получателю схожие сообщения и источники по теме. Однако источники не связаны с получателями обратной связью и не видят созданный ими контент (исключения составляют комментарии, но и они находятся на странице источника). Яркими примерами таких СС являются Youtube и Telegram.

Все три типа структур СС содержат общие атрибуты, отличие одной структуры от другой начинается на уровне отношений.

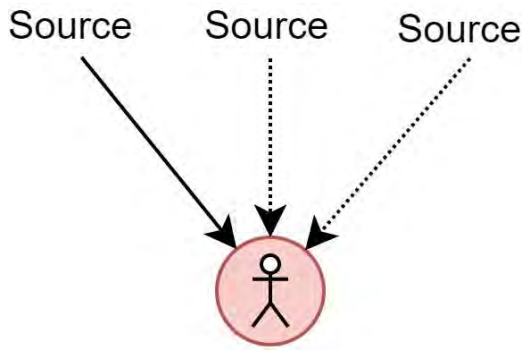


Рис. 3. Структура данных однонаправленных социальных сетей

В процессе анализа основных структур данных СС можно выделить общие атрибуты, которые могут быть применимы для описания взаимосвязи между источником, реципиентом и информацией в социальных сетях. Анализ и синтез структур данных популярных СС позволяет сформировать требования к алгоритмам оценки источников информации и выбора мер противодействия распространению вредоносной информации [4, 5].

Работа выполнена при финансовой поддержке Гранта РНФ (проект РНФ № 18-71-10094) в СПб ФИЦ РАН.

Список использованных источников

1. ГОСТ 20886-85 Организация данных в системах обработки данных. Термины и определения (с Изменениями N 1, 2). 1986 г. // Электронный фонд правовых и нормативно-технических документов. URL: https://beta.docs.cntd.ru/document/1200015708

2. Taylor R. W., Frank R. L. CODASYL Data-Base Management Systems // ACM Comput. Surv. 1976. Vol. 8. Iss 1. pp. 67–103.

3. Codd E. F. The Relational Model for Database Management : Version 2 // Database. 1990. 538 p.

4. Виткова Л. А. Место и роль мониторинга и противодействия нежелательной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференцияи : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 209–212.

5. Виткова Л. А., Сахаров Д. В., Голузина Д. Р. Модель вредоносной информации и ее распространителя в социальных сетях // Защита информации. Инсайд. 2020. № 3 (93). С. 66–72.

Работа представлена доцентом кафедры ЗСС, кандидатом технических наук А. А.Чечулиным.

УДК 004.056.53
ГРНТИ 20.19.27

К-БЛОЧНАЯ ПЕРЕКРЕСТНАЯ ПРОВЕРКА В ЗАДАЧАХ МАШИННОГО ОБУЧЕНИЯ

Л. А. Виткова, Д. Р. Голузина

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

Сегодня широкое распространение получили алгоритмы машинного обучения. Они используются в бизнес-процессах, для повышения эффективности и точности, в научной сфере, для обработки больших объемов данных и изменения подхода к существующим задачам, а также просто для развлечения. Поскольку использование алгоритмов машинного обучения позволяет быстрее и эффективнее обрабатывать большие объемы текста, они могут быть хорошим инструментом для решения задач информационной безопасности. В данной статье рассматривается способ повышения качества моделей машинного обучения в задаче обработки тестовых сообщений из социальной сети, с помощью k-блочной перекрестной проверки.

нейронные сети, обработка текста, машинное обучение, кросс-валидация.

В настоящее время большую роль в жизни общества играют социальные сети. Любые важные события, происходящие в обществе, находят в них отражение. А иногда получается и наоборот, когда события инициируются и подогреваются средствами социальных сетей [1]. Основным инструментом воздействия на массы являются посты в сообществах и на страницах.

Поскольку данное воздействие может нести угрозу, и являться инструментом манипуляции общественным мнением и даже действиями, остро

стоит вопрос своевременного контроля и выявления потенциально вредоносных постов в социальных сетях [2, 3]

В более ранних работах [3, 4] были рассмотрены различные алгоритмы машинного обучения, для решения задачи классификации текста постов, и выявления, содержится ли в них призыв к действиям. Также были произведены попытки улучшить предсказательную способность моделей, за счет изменения порога принятия решения, изменения способа представления данных на входе модели, и изменения структуры самой модели. Результаты работ представлены в таблице 1.

ТАБЛИЦА 1. Результаты предыдущих работ

	Первое значение	**После улучшения**
Логистическая регрессия	0,316	0,376
Байесовский классификатор	0,383	0,383
Нейронная сеть	0,184	0,396
Рекуррентная нейронная сеть	0	0,514

Оценка модели осуществлялась следующим образом:

На вход уже обученной модели подавались тестовые данные (те, что не участвовали в обучении). На основе предсказаний модели были получены матрицы ошибок, где по вертикали указан истинный класс, а по горизонтали тот, что предсказала модель. Таким образом можно было понять, в скольких случаях модель ошиблась, и ошибки какого рода встречаются чаще. Пример матрицы приведен на рис. 1.

Рис. 1. Пример матрицы ошибок

Общая оценка модели оценивалась при помощи *F*-меры. Для этого сначала были подсчитаны полнота и точность, при помощи формул (1), (2)

$$Percision = \frac{TP}{TP+FP} \quad (1)$$

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

где *TN* – количество верно классифицированных объектов класса 0,
FN – количество неверно классифицированных объектов класса 1,
FP – количество неверно классифицированных объектов класса 0,
TP – количество верно классифицированных объектов класса 1.

Затем рассчитывалась сама *F*-мера по формуле (3).

$$F = \frac{2*Percision*Recall}{Percision+Recal}. \quad (3)$$

В результате можно сделать вывод, что нейронные сети (обычные и рекуррентные) хорошо подходят для рассматриваемой задачи, особенно после более тонкой настройки. Но поскольку количество правильных предсказаний было хоть и выше случайного угадывания, но нем не менее не сильно высоким, остается открытым вопрос – каким образом еще можно повысить качество моделей.

Одним из возможных способов решения может быть использование кросс-проверка или кросс-валидация [6, 7].

Кросс-валидация, также называемая скользящим контролем позволяет оценивать модель, при помощи эмуляции тестовой выборки, которая не используется для обучения.

Существуют следующие виды кросс-проверки:

В случае обычной k-блочной проверки весь набор данных, доступный для обучения модели, разбивается на k блоков, одинакового размера. Из k блоков один «откладывается» для валидации не используется в обучении. Остальные k-1 блоки используются для обучения модели, а затем проверка осуществляется на отложенном блоке. Такая процедура повторяется k раз, при этом каждый из блоков будет использован в качестве валидации один раз. Итоговые k результатов усредняются, и образуют одну оценку.

Если k равно количеству элементов в наборе данных, то это называется кросс-проверкой по отдельным элементам. Такой способ хорошо подходит для небольших объемов исходных или разнородных данных. Но нужно учитывать сильно возрастающее время на обучение.

При валидации последовательным случайным сэмплированием набор данных переразбивается на блоки, не обязательно одинаковой длины, случайным образом каждый раз перед новым циклом обучения. Преимущество в том, что пропорции тренировочного и валидационного набора не зависят от числа блоков [8]. А недостатком является то, что отдельно выбранное наблюдение может ни разу не войти в валидационную выборку.

На рис. 2 представлено графическое изображение алгоритма кросс-проверки.

Для эксперимента была выбрана обычная k-блочная проверка.

В таблице 2 приведены оценки для разных моделей обучения, до и после использования кросс-проверки.

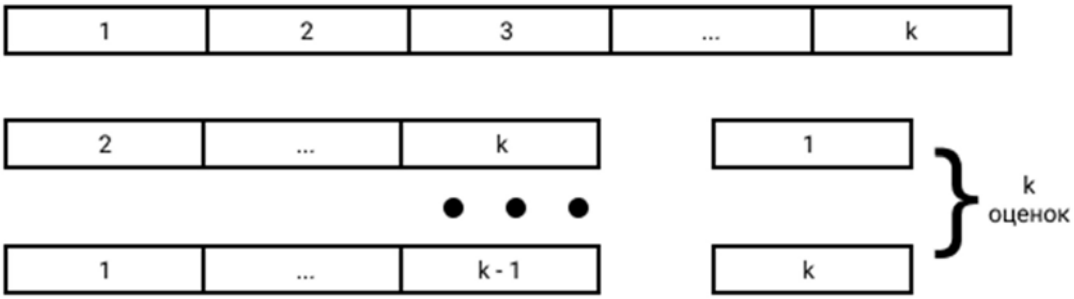


Рис. 2. Схематичное изображение алгоритма кросс-проверки

ТАБЛИЦА 2. Сравнение результатов до и после применения кросс-проверки

	После улучшения	**При применении k-блочной проверки**
Логистическая регрессия	0,376	0,516
Байесовский классификатор	0,383	0,466
Нейронная сеть	0,396	0,647
Рекуррентная нейронная сеть	0,514	0,770

Помимо повышения качества моделей кросс-проверка также может помочь решить проблему переобучения. Суть этой проблемы заключается в следующем: когда тестовая и валидационная выборки зафиксированы на протяжении всего обучения, после большого количества циклов обучения модель «запоминает» правильные ответы, вместо того, чтобы обобщать обучающие данные. Из-за этого ошибка на тестовой выборке стремится к нулю, а на валидационной начинает расти. Графически это представлено на рис. 3.

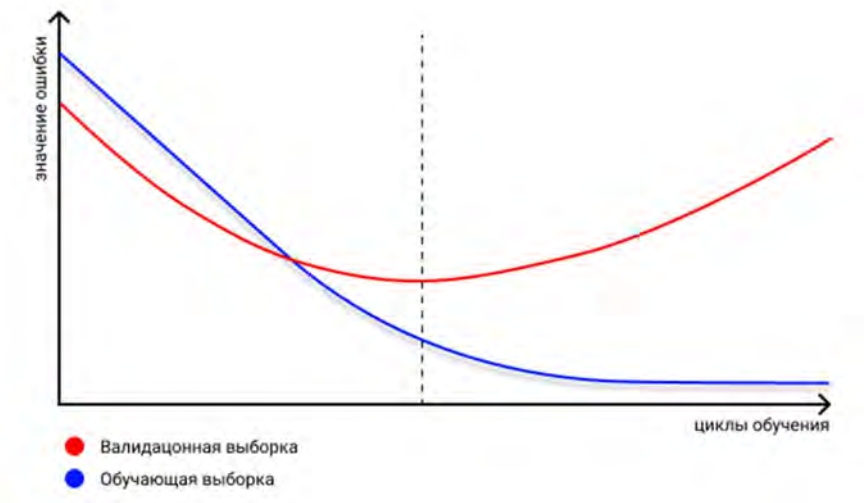


Рис. 3. Переобучение модели

Для предотвращения переобучения необходимо анализировать значения ошибок и выбирать подходящее количество циклов обучения. Использование кросс-проверки позволяет минимизировать воздействие эффекта переобучения, за счет постоянной смены валидационной выборки.

Список используемых источников

1. Денисов Е. И., Андреянов Я. В., Виткова Л. А., Сахаров Д. В. Информационное воздействие социальных сетей // Сборник трудов конференции Региональная информатика "РИ-2018" – 2018. С. 569–570

2. Виткова Л. А., Проноза А. А., Сахаров Д. В., Чечулин А. А. Проблемы безопасности информационной сферы в условиях информационного противоборства // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международна научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 191–195.

3. Саенко И. Б., Чечулин А. А., Виткова Л. А. Концепция интеллектуальных систем аналитической обработки цифрового сетевого контента с целью обнаружения нежелательной информации // Методы и технические средства обеспечения безопасности информации. 2018. № 27. С. 6–7.

4. Виткова Л. А., Сахаров Д. В., Голузина Д. Р. Разработка модели вредоносной информации и ее распространителя в социальных сетях // Защита информации. Инсайд. 2020. № 3. С. 66–72.

5. Голузина Д. Р., Виткова Л. А., Ахрамеева К. А. Методы искусственного интеллекта и анализа распространения информации в ходе инцидентов и кризисов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международна научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. С. 422–426.

6. Луис П. К. Построение систем машинного обучения на языке Python. М. : ДМК Пресс, 2019. 320 с.

7. Чио К. Машинное обучение и безопасность. М.: ДМК Пресс, 2020. 504 с.

8. Жерон О. Прикладное машинное обучение с помощью Scikit-Learn, Keras и TensorFlow. 2-е изд. М. : Вильямс, 2020. 1040 с.

Статья представлена доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Чечулиным.

УДК 004.056
ГРНТИ 81.93.29

КЛАССИФИКАЦИЯ БОТОВ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ И ИХ ПОВЕДЕНИЕ

Л. А. Виткова[1,2], В. А. Коптелова[1]

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

В статье поднимается вопрос электронного мошенничества в современном информационном сообществе. Предметом исследования является наиболее распространенный инструмент мошенников – специальные автоматизированные программы, известные как «боты». Исследование включает в себя рассмотрение последствий использования таких программ. Основной целью является классификация вышеупомянутых ботов с точки зрения информационной безопасности.

автоматизированная программа, боты, электронная коммерция, мошенничество, интеллектуальные боты, торговые боты, боты быстрых покупок, рекламные боты, чат-боты, поведение ботов.

В настоящее время электронная коммерция получила распространение во всем мире [1, 2]. В связи с этим возрастает и количество вредоносных услуг, цель которых – увеличение продаж. Недобросовестные участники рынка повышают рейтинг своих товаров и услуг, оптимизируя результаты поиска, используя поддельные посещения, покупки и т. д. [3].

По некоторым оценкам [4], на ботов приходится 51,8 % всего интернет-трафика и только 48,2 % исходит от людей. В поисковых системах или специализированных сервисах, существуют автоматизированные программы, которые анализируют веб-ресурсы на предмет привлекательности для покупателей. Другие же программы могут быть сосредоточены на таких действиях, как кража контента с сайта посредством веб-скрапинга, мошенничество с формами, с кредитными картами и т. д. Некоторые из последствий таких действий заключаются в том, что они могут искажать информацию аналитики веб-сайта, позволять конкурентам красть информацию, совершать рекламное мошенничество, а также могут влиять на пользовательский интерфейс сайта, замедляя его работу.

Рассмотрим некоторые из видов ботов, которые чаще всего встречаются в данной сфере.

Интеллектуальные боты

Миллионы компаний, в том числе и малый бизнес, используют сеть Интернет для электронной торговли. Многие порталы по всему миру, такие как eBay, Aliexpress, Ozon, Wildberries, являются популярными примерами веб-сайтов электронной коммерции. Один из способов удержать существующих клиентов и убедить новых покупателей купить продукт компании – это предлагать потенциальным покупателям предложения с помощью «интеллектуального бота». Используя онлайн-отслеживание поведения потребителей или получая информацию от них, интеллектуальные боты предоставляют потребителям наиболее «интересные» продукты. Используя интеллектуальные приемы и методы, такие боты пытаются привлечь внимание пользователя к определенному продукту или услуге. Внедрение интеллектуальных ботов увеличивает продажи интернет-магазинов, а также лояльность их потребителей [5].

Торговые боты

Торговый бот – это программный инструмент для сравнения цен в Интернете, который способен самостоятельно автоматически отслеживать данные о товарах [6] во многих различных интернет-магазинах, чтобы найти наиболее доступные цены для клиентов. Как правило, эти торговые боты ранжируют товары по цене и позволяют покупателям напрямую переходить на веб-сайт интернет-магазина, чтобы купить предпочтительный товар. Торговые боты могут быть веб-сайтами, плагинами, браузерами и так далее. Кроме того, некоторые сервисы находят товары только в сети Интернет, в то время как другие ищут дополнительно в каталогах, рассылаемых по почте, или в магазинах, работающих в режиме офлайн.

Боты быстрых покупок

Боты для быстрых покупок (их еще называют шопинг-боты, rush-боты (в переводе с англ. – боты спешки), гринч-боты) – это программы, которые за считанные секунды скупают популярные товары и товары со скидкой в интернет-магазинах, опережая реальных покупателей [7]. Rush-боты придерживаются определенной тактики – быстрая атака в начале процесса. Такие автоматизированные программы применяются с целью ускорения процесса оформления заказа при покупке товаров или услуг в сети Интернет. Они значительно упрощают процесс покупки лимитированных или редких товаров. Такие товары достаточно сложно купить без применения rush-бота, так как они быстро заканчиваются. А затем зачастую эти уникальные вещи попадают на вторичный рынок, где перепродаются перекупщиками ради прибыли гораздо дороже начальной стоимости.

В работе [8] сказано, что процесс покупки начинается с заполнения платежного профиля покупателя и переходит к этапу формирования цели покупки. Это может быть выполнено разными способами, но преимущественно указываются ключевые слова или URL-ссылки. После настройки бота процесс оформления заказов и покупки товаров становится автоматизированным. В сравнении с человеком, боты способны совершать оформления заказов за доли секунды. Однако при работе с rush-ботами в процессе могут потребоваться сервера, благодаря которым можно запустить ботов, ускорить их и улучшить соединение с сайтом, и прокси для замены IP-адреса, что позволит быть пользователю несколькими покупателями в один момент. Также такие автоматизированные программы используются для спекуляций на биржах.

Copyright ransomware

Существует ещё один тип ботов, которые называются copyright ransomware (*ransom* – выкуп и *software* – программное обеспечение) – тип зловредного программного обеспечения, предназначен для вымогательства) и переводятся с английского буквально как «программы-вымогатели авторского права». Сайты электронной коммерции могут быть наполнены огромным количеством изображений продуктов и видео-контента. Боты подобного рода тщательно сканируют все изображения и видео на сайте в поисках нарушений авторских прав в средствах массовой информации. Если они обнаруживают что-либо, компания, стоящая за ботом, связывается с владельцем веб-сайта, выдает приказ о прекращении действий и требует компенсации. Это может быть использовано как в целях поиска распространения и дальнейшей блокировки авторского контента, который был использован без ведома автора, так и с целью спекуляции.

Боты-кликеры

Ещё в 2014 году служба интернет-рекламы компании Mercedes-Benz отметила, что менее 50 % рекламы были просмотрены людьми [9]. Такой вид сетевого мошенничества представляет собой не что иное, как обманные клики на рекламную ссылку людьми или ботами, не заинтересованными в рекламном объявлении [10]. В исследовании [11], целью было сравнить соотношение количества кликов по рекламе, инициированных людьми, к кликам, созданным с помощью компьютера. Авторы отметили распространенность спам-ботов, рассылающих спам в огромном количестве, и запрограммированных на одновременное добавление рекламных ссылок. Так называемые, бот-фермы, системы, имитирующие функционирование многих устройств с отдельными каналами подключения к сети Интернет [12], часто используются в онлайн-магазинах приложений, таких как Google Play, для манипуляций с целью повышения положительных оценок и отзывов.

Чат-боты

Чат-бот – это программа-собеседник, имитирующая человеческое общение при помощи текста или голоса [13]. При использовании такого бота происходит диалог с пользователем, в процессе которого бот отвечает на вопросы, выполняет какие-либо задачи или просто поддерживает диалог для разговора. Если бот не понимает команду, фразу или предложение человека, он может перенаправить клиента на другой канал, такой как электронная почта или чат с оператором. Чат-бот может высвечиваться на сайте в виде ассистента покупателя. Он предлагает помощь в интернет-магазине, предоставляет дополнительную информацию о товарах и упрощает процесс принятия решений, помогая найти товар, который удовлетворяет требованиям покупателя и различным ограничениям.

Несмотря на огромное количество существующих чат-ботов, их всех можно разделить на две большие категории в зависимости от технологии, используемой для ведения интеллектуального диалога: программы с обработкой текстов на естественных языках (*Natural Language Processing,* NLP) и программы, основанные на формированием рассуждений на основе конкретных случаев (*Cased-Based Reasoning*) [14]. Указанные инструменты помогают увеличить посещаемость самого сайта, и продажи [15]. Данный тип автоматизированных программ широко распространён на сегодняшний день и будет рассмотрен авторами в других исследованиях более подробно.

Анализ поведения ботов

Можно сказать, что у разных типов ботов есть общий набор свойств. В статье [16] авторами было кратко описано обычно наблюдаемое поведение ботов, которое может распространяться на автоматизированные программы не только в сфере электронной коммерции:

- в первую очередь боты существуют, прямо или косвенно, для получения экономической выгоды;
- в какой-либо степени имитируют действия человека, использующего компьютер;
- повторяет такие действия несколько раз;
- инициирует активность;
- выполняет минимальное количество необходимых действий для выполнения своей задачи.

Как правило, боты выполняют простые и структурно повторяющиеся задачи с гораздо большей скоростью, чем это мог бы выполнить один человек. Для ботов также не имеет значения, где, на какой платформе, операционной системе или на каком устройстве будут происходить действия. В связи с плотным вхождением в повседневную жизнь смартфонов, все

больше создаётся ботов для мобильных телефонов и приложений, и все меньше – для ПК.

Стоит отметить, что целиком обезопасить любой сайт от действий «плохих ботов» не удастся. Можно лишь ограничить возможности их действий. Но необходимо помнить, что боты могут быть и полезны и останавливать целиком их не нужно. К примеру, правильно спроектированная система аутентификации с ролями доступа является одной из основополагающей в решении проблемы безопасности. Также в современных реалиях многие злоумышленники уже не пользуются только одним или несколькими ботами, а запускают целые сети ботов, называемые ботнетами, проблема которых актуальна на сегодняшний день не только в сфере коммерции, но и во многих других.

Работа выполнена при финансовой поддержке Гранта РНФ (проект РНФ № 18-71-10094) в СПИИРАН.

Список используемых источников

1. Vitkova L., Kotenko I., Kolomeets M., Tushkanova O., Chechulin A. Hybrid Approach for Bots Detection in Social Networks Based on Topological, Textual and Statistical Features // 4nd International Scientific Conference “Intelligent information technologies for industry” (IITI’19), December 2-7, 2019, Ostrava-Prague, Czech Republic. Advances in Intelligent Systems and Computing, Springer. 2020. vol. 1156. pp. 412–421.

2. Kolomeets M., Tushkanova O., Levshun D., Chechulin A. Camouflaged bot detectionusing the friend list. In 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). pp. 253–259. IEEE, 2021.

3. Котенко И. В., Хинензон А. В. Анализ алгоритмов обнаружения аномального поведения в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 644–648.

4. Максимов А. Интернет-2020: цифры и тренды на 2021 // ОмПОО. Омский портал открытого образования, 2021. URL: https://openedu55.ru/mod/forum/discuss.php?d=475 (дата обращения: 19.03.2021)

5. Егорова Е. А. Интеллектуальные виртуальные агенты // Управление организационно-экономическими системами. 2021. С. 54–58.

6. Горшков М. А., Сыромятников В. Н. Торговые роботы // Новое слово в науке: перспективы развития. Чебоксары: Центр научного сотрудничества "Интерактив плюс", 2016. №. 1-2. С. 227–230.

7. Жукова К., Юзбекова И. Помощники спекулянтов: как гринч-боты скупают дефицитные товары // Forbes. Технологии. URL: https://www.forbes.ru/tehnologii/416151-pomoshchniki-spekulyantov-kak-grinch-boty-skupayut-deficitnye-tovary (дата обращения: 19.03.2021).

8. Все, что нужно знать о сникер-ботах // МЦ — независимый интернет-журнал о моде и культуре. URL: https://mcmag.ru/sniker-boty-dlya-pokupki-krossovok/ (дата обращения: 24.02.2021).

9. Концаренко Ф. Financial Times: Рекламную кампанию Mercedes просматривают боты, а не люди // vc.ru — крупнейшая в рунете площадка для предпринимателей нового поколения. 2014. URL: https://vc.ru/flood/3936-mercedes-ad (дата обращения 27.02.2021).

10. Игнатенко М. В. Кликфорд-методы, признаки, защита // Новая наука: Стратегии и векторы развития. 2015. №. 6-3. С. 33–35.

11. Neal A., Kouwenhoven S., Sa O. Quantifying online advertising fraud: Ad-click bots vs humans // Tech. Rep. Oxford Bio Chronometrics, 2015.

12. Россинская Е. Р. Экспертная профилактика в условиях цифровизации судебно-экспертной деятельности // Вестник экономической безопасности. 2020. №. 2.

13. Ураев Д. А. Классификация и методы создания чат-бот приложений // International scientific review. 2019. № LXIV.

14. Иванова Е. Г. Интеллектуальные диалоговые интерфейсы в системах электронной коммерции // Известия ЮФУ. Технические науки. 2007. № 2.

15. Кушков Е. А. Инструменты увеличения конверсии сайта (на примере квизов, чат-ботов) // Российский экономический интернет-журнал. 2019. №. 2. С. 51–51.

16. Bressler L. A., Bressler M. S. Beware the evil bots: e-commerce thieves and spreaders of «fake news» // 182962 – Journal of Technology Research. 2019.

Статья представлена доцентом кафедры ЗСС СПбГУТ кандидатом технических наук, доцентом А. А. Чечулиным.

УДК 004.72, 621.391
ГРНТИ 49.33.29

МОДЕЛЬНАЯ СЕТЬ ДЛЯ ИССЛЕДОВАНИЯ МНОГОАДРЕСНОЙ ПЕРЕДАЧИ НА ОСНОВЕ МЕТОДОВ СЕТЕВОГО КОДИРОВАНИЯ

С. С. Владимиров, А. И. Фомин

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

Работа представляет структуру модельной лабораторной сети для исследования многоадресной передачи методами сетевого кодирования в сетях передачи данных на основе протоколов TCP/IP. Разработана структурная схема модельной сети и предложены варианты ее реализации на основе программных и аппаратных платформ. С учетом особенностей проведения исследований выполнен выбор программно-аппаратной платформы оборудования стенда. Рассмотрены принципы реализации программного обеспечения оконечных и маршрутизирующих узлов сети, предназначенного для проведения исследований. Представлены направления дальнейшего развития стенда и функций модельной сети.

модельная сеть, сетевое кодирование, многоадресная передача, сети TCP/IP.

Предложенная в 2000 году технология сетевого кодирования [1, 2] предназначена для ускорения многоадресной передачи пакетов данных от различных источников [1, 2, 3]. Этот принцип кодирования базируется на

вычислении линейных комбинаций передаваемых пакетов в маршрутизирующих узлах сети при помощи операции сложения по модулю 2. Затем эти маршрутизаторы передают не исходные пакеты данных, а вычисленные линейные комбинации [1, 2, 3].

Исследования технологии сетевого кодирования ведутся в различных направлениях. Предлагаются различные алгоритмы помехоустойчивого кодирования, предназначенные для повышения защиты от ошибок в системах с сетевым кодированием [4, 5, 6, 7, 8, 9]. Рассматриваются сценарии применения сетевого кодирования в различных сферах деятельности [10, 11, 12]. Важным направлением в сетевом кодировании является разработка сетевых протоколов, использующих данный принцип [13, 14, 15, 16].

Необходимым инструментом изучения и тестирования сетевых протоколов является модельная сеть, которая позволяет протестировать протоколы на модели, максимально приближенной к реальной сети, либо являющейся участком реальной сети передачи данных [17, 18].

В статье предлагается структура модельной лабораторной сети для исследования многоадресной передачи методами сетевого кодирования в сетях передачи данных на основе протоколов TCP/IP. В качестве сетевой архитектуры модельной сети выбрана классическая сетевая архитектура «бабочка», традиционно применяемая при изучении принципов сетевого кодирования. Базовая архитектура сети (рис. 1) содержит два узла-источника S_1 и S_2, два узла-адресата R_1 и R_2 и шесть маршрутизирующих узлов, отмеченных буквами от A до F.

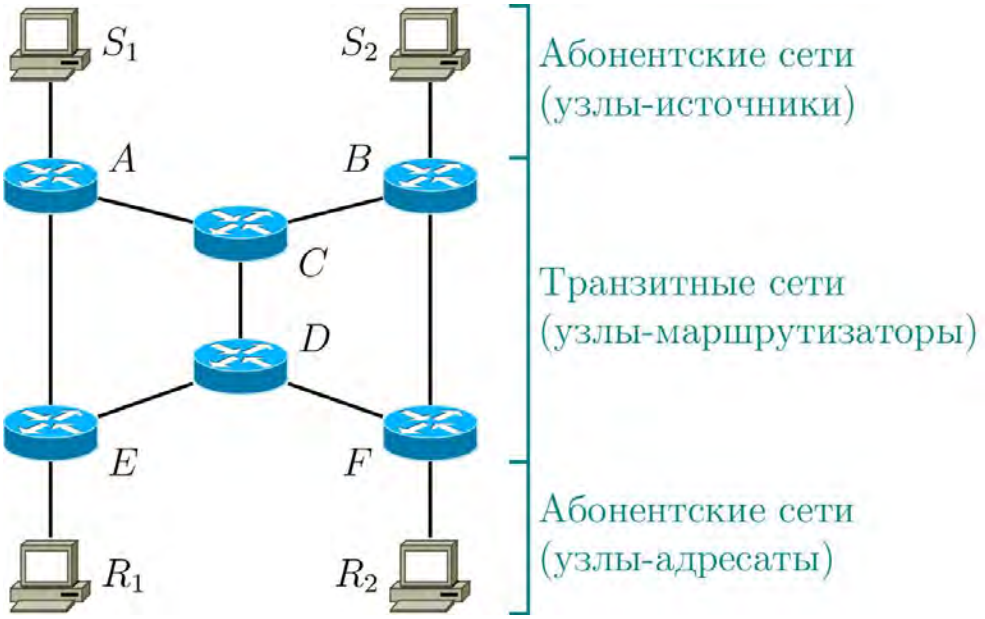


Рис. 1. Модельная сеть с архитектурой «бабочка»

Модельная сеть состоит из 11 подсетей: четыре абонентские подсети содержат узлы-источники и узлы-адресаты; семь транзитных подсетей связывают маршрутизаторы.

Маршрутизаторы, составляющие транзитную часть модельной сети, содержат по три сетевых интерфейса каждый. На маршрутизаторе C осуществляется процедура сетевого кодирования над пакетами, передаваемыми от узлов-источников S_1 и S_2.

Модельная сеть, показанная на рис. 1, может быть реализована различными методами, каждый из которых имеет свои достоинства и недостатки.

Построение модельной сети как совокупности физических устройств – маршрутизаторов и персональных компьютеров, хотя и является максимально приближенным к реальным условиям применения, требует вложения значительных ресурсов. Маршрутизаторы, имеющие 3 и более управляемых интерфейсов, стоят достаточно дорого и зачастую имеют ограничения на использование в них собственных приложений и прошивок, а реализация маршрутизаторов на основе бюджетных ПК потребует много места для их размещения.

Альтернативой является виртуальная модельная сеть на основе программного гипервизора типа 2, например VirtualBox или Qemu, и открытой сетевой операционной системы. Поскольку проектируемая модельная сеть должна содержать суммарно 10 узлов, работающих одновременно, следует использовать дистрибутивы ОС с минимальными системными требованиями. Оптимальным видится использование основанной на ядре GNU/Linux сетевой ОС OpenWrt, предназначенной для управления маршрутизаторами. Эта ОС требует для полноценной работы 64 МБ ОЗУ. Таким образом, для одновременной работы всех узлов модельной сети потребуется менее 1 ГБ оперативной памяти, что позволит запускать виртуальную модельную сеть на подавляющем большинстве современных персональных компьютеров. Важным плюсом ОС на ядре GNU/Linux, и в частности OpenWrt, является поддержка большинства существующих протоколов стека TCP/IP, что позволяет тестировать методы сетевого кодирования для различного сочетания сетевых, транспортных и управляющих протоколов. Размер виртуальной машины OpenWrt для процессорной архитектуры x86 с учетом файлов настроек гипервизора обычно не превышает 50 МБ. Соответственно, общий размер виртуальной модельной сети согласно архитектуре, приведенной на рис. 1, не будет превышать 550 МБ без учета дистрибутива гипервизора.

Важным плюсом использования виртуальной модельной сети является возможность ее развертывания на компьютерах под управлением различных операционных систем: как MS Windows, так и GNU/Linux.

Еще одним достоинством виртуальной сети является ее гибкость и расширяемость с точки зрения добавления новых узлов и усложнения сетевой архитектуры.

При развертывании виртуальной модельной сети можно дополнительно использовать сетевой програмный эмулятор GNS3, который позволяет использовать образы открытых сетевых ОС. Использование GNS3 сделает модельную сеть более наглядной и удобной для работы за счет продвинутого графического интерфейса пользователя, но потребует значительно больше оперативной памяти. Считается, что для удобной работы в GNS3 требуется более 4 ГБ оперативной памяти.

Третьим, гибридным подходом является реализация модельной сети на основе двух маршрутизаторов *X* и *Y* (рис. 2), первый из которых выполняет роль маршрутизирующих узлов *A*, *B* и *C*, а другой – узлов *C*, *D* и *F*. Абонентские и транзитные сети при этом реализуются как наложенные VPN-сети. Такой подход позволяет использовать для построения модельной сети машрутизаторы с двумя настраиваемыми интерфейсами и встроенным коммутатором на два или более порта. Транзитные сети *AC* и *BC* реализуются маршрутизацией между VPN внутри маршрутизатора *X*, а сети *DE* и *DF* – внутри маршрутизатора *Y*. Сети *AE*, *CD* и *BF* создаются как VPN-сети поверх соединения *XY*. К недостаткам такого подхода следует отнести большую сложность настройки маршрутизации пакетов и меньшую расширяемость по сравнению с виртуальной модельной сетью.

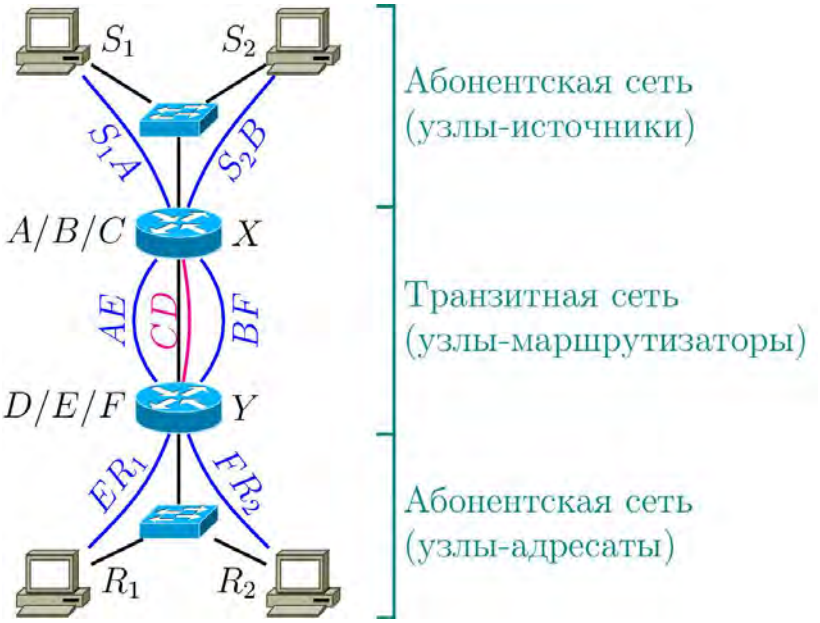


Рис. 2. Модельная сеть на основе двух маршрутизаторов и VPN-сетей

Для построения модельной сети нами был выбран подход на основе виртуальной модельной сети, как сочетающий относительную простоту реализации, низкую стоимость разработки и внедрения, а также достаточную функциональную близость к реальной сети с точки зрения работы сетевых протоколов. Для виртуализации решено использовать открытый гипервизор VirtualBox от компании Oracle. В качестве сетевой ОС выбрана OpenWrt.

Для реализации программного интерфейса виртуальной модельной сети, источников, обработчиков и приемников пакетов предполагается использовать клиент-серверные программы на языках Си и Python, предназначенные для запуска в пространстве пользователя узлов модельной сети.

В дальнейшем предполагается расширить системные возможности модельной сети, усложнив сетевую архитектуру и добавив возможность совместного тестирования нескольких маршрутов передачи пакетов с сетевым кодированием.

Список используемых источников

1. Ahlswede R., Cai N., Li S. R., Yeung R. W. Network information flow // IEEE Transactions on Information Theory. 2000. Vol. 46. Iss. 4. pp. 1204–1216.

2. Fragouli C., Soljanin E. Network Coding Fundamentals // Foundations and Trends in Networking. 2007. Vol. 2. Iss. 1. pp. 1–133.

3. Габидулин Э. М., Пилипчук Н. И., Колыбельников А. И., Уривский А. В., Владимиров С. М., Григорьев А. А. Сетевое кодирование // Труды МФТИ. 2009. Т. 1. № 2. С. 3–28.

4. Biczok G., Chen Y., Kralevska K., Overby H. Combining forward error correction and network coding in bufferless networks: A case study for optical packet switching // 2016 IEEE 17th International Conference on High Performance Switching and Routing (HPSR). Yokohama: IEEE, 2016. pp. 61–68. DOI: 10.1109/HPSR.2016.7525640.

5. Martinez-Penas U., Kschischang F.R. Reliable and Secure Multishot Network Coding using Linearized Reed-Solomon Codes // 2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton). Monticello, IL, USA: IEEE, 2018. pp. 702–709. DOI: 10.1109/ALLERTON.2018.8635644.

6. Габидулин Э. М., Пилипчук Н. И., Боссерт М. Декодирование случайных сетевых кодов // Проблемы передачи информации. 2010. Т. 46, вып. 4. С. 33–55.

7. Габидулин Э. М., Пилипчук Н. И. Ранговые подкоды в многокомпонентном сетевом кодировании // Проблемы передачи информации. 2013. Т. 49, вып. 1. С. 46–60. DOI: 10.34832/ELSV.2020.2.1.009.

8. Владимиров С. С. Коды Голда и коды максимальной длины в сетевом кодировании // Электросвязь. 2020. № 1. С. 61–66.

9. Владимиров С. С. 8-разрядные коды с прямой коррекцией ошибок в линейном сетевом кодировании // Электросвязь. 2020. № 7. С. 51–58. DOI: 10.34832/ELSV.2020.8.7.007.

10. Halloush R., Liu H., Dong L., Wu M., Radha H. Hop-by-hop Content Distribution with Network Coding in Multihop Wireless Networks // Digital Communications and Networks. 2017. Vol. 3. Iss. 1. P. 47-54.

11. Amanowicz M., Krygier J. On Applicability of Network Coding Technique for 6LoWPAN-based Sensor Networks // Sensors. 2018. Vol. 18 (6). pp. 1–20.

12. Кайсина И. А., Васильев Д. С., Абилов А. В., Мейтис Д. С., Кайсин А. Е. Применение метода сетевого кодирования в сетях БПЛА // Выставка инноваций – 2018 (осенняя сессия). Сборник материалов XXVI Республиканской выставки-сессии студенческих инновационных проектов. 2018. С. 35–40.

13. Kim M., Medard M., Barros J. Modeling network coded TCP throughput: a simple model and its validation // Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS '11). 2011. pp. 131–140.

14. Suta Z., Polgar Z., Catalin V., Varga M., Rus A., Dobrota V. Network Coding-Based Congestion Control at Network Layer: Protocol Design and Evaluation // International Journal of Computer Networks & Communications. 2011. Vol. 3. No. 1. pp. 119–138. DOI: 10.5121/ijcnc.2011.3108.

15. Santos Ribeiro Junior N., Vieira M.A., Vieira L.F., Gnawali O. CodeDrip: Data Dissemination Protocol with Network Coding for Wireless Sensor Networks // Proceedings of the 11th European Conference on Wireless Sensor Networks. – Volume 8354 (EWSN 2014). 2014, pp. 34–49. DOI: 10.1007/978-3-319-04651-8_3.

16. Li Z., Xu M., Liu T., Yu L. A Network Coding-Based Braided Multipath Routing Protocol for Wireless Sensor Networks // Wireless Communications and Mobile Computing. 2019. Vol. 2019. Art. 2757601. DOI: 10.1155/2019/2757601.

17. Киричек Р. В., Владыко А. Г., Захаров М. В., Кучерявый А. Е. Модельные сети для интернета вещей и программируемых сетей // Информационные технологии и телекоммуникации. 2015. Т. 3. № 3. С. 17–26.

18. Кучерявый А. Е., Киричек Р. В. Эволюция модельных сетей // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 58–64.

УДК 004.772
ГРНТИ 49.38.49

МЕТОДЫ И СПОСОБЫ СОЗДАНИЯ СТЕГАНОГРАФИЧЕСКИХ ВЛОЖЕНИЙ В СЕТЕВЫХ ПАКЕТАХ

В. Н. Волкогонов, Е. М. Гетьман, А. С. Салита

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

В современном мире очень остро стоит вопрос конфиденциальности информации. В отличие от криптографии, при применении стеганографии нет необходимости в лицензировании и согласовании. Также стеганография позволяет сохранить в тайне участников обмена информацией, и наоборот - отследить участников нелегального распространения данных. В данной статье описываются основные подходы и методы построения стеганографических каналов, рассматриваются библиотеки и программные утилиты для построения стеганографических каналов, а также практическая реализация в глобальной сети интернет.

стеганография, сетевая стеганография, безопасность, IPv4, канальная стеганография, сокрытие информации, защита информации, сети передачи данных.

На данный момент в нашей жизни всё большее значение играют сетевые технологии, передача информации в которых осуществляется при помощи специальных протоколов. Сетевая стеганография – это один из видов

стеганографии, в котором носителями скрытых данных выступают сетевые протоколы эталонной модели OSI. Сетевая стеганография является семейством методов по изменению данных в полях заголовка протоколов и в полях полезной нагрузки пакетов, изменению структуры передачи пакетов и гибридных методов.

Первый подход к сокрытию информации в сетевых пакетах заключается в изменении свойств передаваемых сетевых пакетов. Путем модификации определенных полей, добавлением или изменением их содержимого, становится возможным скрытно инкапсулировать определенную информацию, при этом не внося изменения в пользовательские данные, содержащиеся в пакете.

Второй подход основан на изменении структуры передачи пакетов, взаимосвязи между ними. Например, сюда можно отнести изменение порядка в последовательности пакетов, задержка при отправлении между ними, введение контролируемой потери пакетов.

Третий подход является гибридным и объединяет собой два предыдущих. Подробнее о реализации стеганографии можно прочесть в [1, 2, 3, 4]. Рассмотрим каждую группу методов сетевой стеганографии более подробно.

Как было сказано ранее, метод модификации пакетов заключается в изменении полей передаваемого пакета. Чаще всего модификации подвергаются заголовки IP и TCP протоколов, ввиду относительно большого числа полей, в том числе опциональных, т. е. используемых только при определенных условиях. Это позволяет использовать сразу несколько полей для вложения стеганограммы.

Зачастую для данного метода используется поле Identification в IPv4 пакетах (ввиду их распространенности). Данное поле занимает 16 бит и используется при фрагментации пакетов для их распознавания после фрагментации исходного пакета. Таким образом, если пакет не будет фрагментирован, это поле не будет влиять на процесс передачи информации, следовательно, данное поле можно использовать в качестве стегоконтейнера.

В качестве плюсов рассматриваемого метода можно отметить относительно неплохую пропускную способность, легкость в реализации, отсутствие влияния на пользовательские данные. Однако, при приложении определенных усилий, наблюдатель сможет выявить использование стеганографии и считать передаваемую информацию (при условии ее передачи в незашифрованном виде).

Также интерес представляет поле Options, которое является дополнительным и не влияет явным образом на процесс передачи данных. В нем можно выделить опцию Internet Timestamp размером в 32 бита; это временной штамп в миллисекундах относительно полуночи по Единому Времени.

Обращаясь к спецификации, можно заметить, что можно использовать некоторое нестандартное значение (при условии, что старший бит в данной опции будет установлен в единицу), что дает возможность вложения стеганограммы. Теоретически, возможно также использование других полей, таких как TTL и ToS.

Данный метод также может использовать поля заголовка TCP, такие как Urgent Point и Options.

Поле Urgent Point не влияет явным образом на передачу данных и анализируется приемной стороной при наличии установленного флага. Аналогично поле опций, которое по умолчанию заполнено 16 битами NOP и меткой времени, которая не учитывается приемной стороной.

Как в TCP, так и в UDP для вложения стеганограммы возможно использование поля Source port, поскольку оно так же не влияет на процесс передачи данных получателю скрытой информации. В [5, 6] описывается процесс модификации пакетов на третьем и четвертом уровнях модели OSI.

Отдельной группой можно также выделить VoIP протоколы, использующиеся для передачи голосового и видеотрафика через Интернет. Метод, модифицирующий VoIP пакеты, получил название Transcoding Steganography (TranSteg). Суть данного метода заключается в сжатии полезной нагрузки путем перекодирования; таким образом, его можно использовать в любых службах и приложениях, где возможно произведение сжатия данных. Сжатие необходимо для того, чтобы освободить некоторое количество бит для вложения стеганограммы. Однако стоит учитывать, что видео и голосовой трафик более чувствительны к потерям, а также при произведении сжатии происходит ухудшение качества передаваемых данных, что может привести к обнаружению стегановложения.

К сожалению, данный способ значительно сложнее в реализации, нежели использование IP и TCP/UDP заголовков, поскольку для успешной его реализации необходимо знать кодеки, используемые при передачи информации, их особенности и наиболее оптимальный вариант сжатия, при котором потери пользовательского трафика будут минимальны.

Еще одним способом реализации сетевой стеганографии является LACK – Lost Audio Packets Steganography, который использует в своей сути намеренную задержку в VoIP пакетах. Отправитель генерирует пакет, полезная нагрузка которого несет скрытую информацию, и затем данный пакет намеренно задерживается. Пакеты, пришедшие с чрезмерной задержкой, отбрасываются получателем; однако, если получатель знает о существовании стеганоканала, данные RTP-пакеты не отбрасываются, и из них извлекается стеганограмма.

Еще одним протоколом, позволяющим скрытно передать информацию, является SCTP (*Stream control transport protocol*). SCTP-стеганография ис-

пользует характерные особенности данного протокола, такие как мультипоточность и использование множественных интерфейсов (*multi-homing*). Методы изменения содержимого SCTP-пакетов основаны на том, что каждая часть STCP-пакета может иметь переменные параметры.

В качестве гибридного метода можно выделить метод RSTEG (*Retransmission Steganography*), который заключается в повторной отправке пакетов. Суть метода состоит в том, что отправитель посылает три пакета – исходный-стеганограмма-исходный – поскольку получатель не отправляет ACK подтверждение о получении первых двух, инициирую повторную отправку. При этом, как было указано, при повторном отправлении в первый раз исходный пакет заменяется на пакет, где полезная нагрузка заменена стеганограммой. Получатель так же не подтверждает получение пакета, инициируя повторное отправление во второй раз. Во второй раз происходит отправление исходного (оригинального) пакета, и в данном случае отправляется подтверждение получения.

К сожалению, данный метод вызывает увеличение общего числа потерянных пакетов, таким образом, делая передачу стеганограммы более явной, поскольку такой параметр, как потери, зачастую тщательно контролируется. Поэтому необходимо учитывать общий уровень потерь в сети и уровень ретрансляции пакетов для организации скрытого стеганоканала.

Существуют и другие, более специфичные способы вложения стеганограмм; например, использование более специфичных протоколов или заголовков, более сложных взаимосвязей и алгоритмов. Сетевая стеганография развивается и изменяется с появлением новых стандартов в сетях передачи данных, поэтому в данной статье были приведены лишь основные наиболее часто используемые способы.

Для реализации ранее перечисленных методов может использоваться программная библиотека Scapy. Scapy – интерактивная оболочка и программная библиотека для манипулирования сетевыми пакетами на языке программирования Python. Scapy использует библиотеку libpcap поэтому может использоваться как конструктор пакетов, так и как снифер для перехвата или анализа сетевого трафика. Scapy нужен доступ к интерфейсам, а следовательно права суперпользователя. Однако существуют и другие библиотеки, которые не требуют прав суперпользователя для генерации пакетов. Например, библиотека libnetfilter_queue, реализующая возможность модификации пакетов на уровне пользователя в ОС Linux. Данная библиотека использует подсистему ядра nfnetlink_queue. Подсистема nfnetlink_queue реализует протокол nfnetlink, который связывает уровень ядра и уровень пользователя. Сама очередь пакетов, ожидающих вердикта реализована в ядре ОС (представляет собой связанный список, содержащий пакеты и метаданные, *Linux socket buffer*). При изъятии пакета из очереди, происходит передача пакета и дополнительной информации по nfnetlink на

уровень пользователя. При принятии пользовательским ПО вердикта для сетевого пакета, происходит обратный процесс его передачи на уровень ядра, пересылка по сети или же возврат ожидающему приложению (в зависимости от направления передачи).

В доказательство всего вышесказанного был проведен небольшой эксперимент. Изначально на на виртуальном стенде, представленном на рис. Данный стенд был развернут на платформе EVE-NG в качестве эмулируемых ус-в использовались ус-ва компании Cisco. После подтверждения теоретических предположений на виртуальном стенде эксперимент был повторен уже в реальной сети. В ходе эксперимента было решено переслать пакет из AS X в AS Z. Трафик генерировлся на компьютере находящимся в AS X в Санкт-Петербурге, далее трафик шел через сеть AS Y через Хельсинки (Финляндия), где у AS X пиринг с AS Y, потом из сети AS Y трафик вернулся обратно в Санкт-Петербург и был передан сети AS Z. Трассировка маршрута представлена на рис.

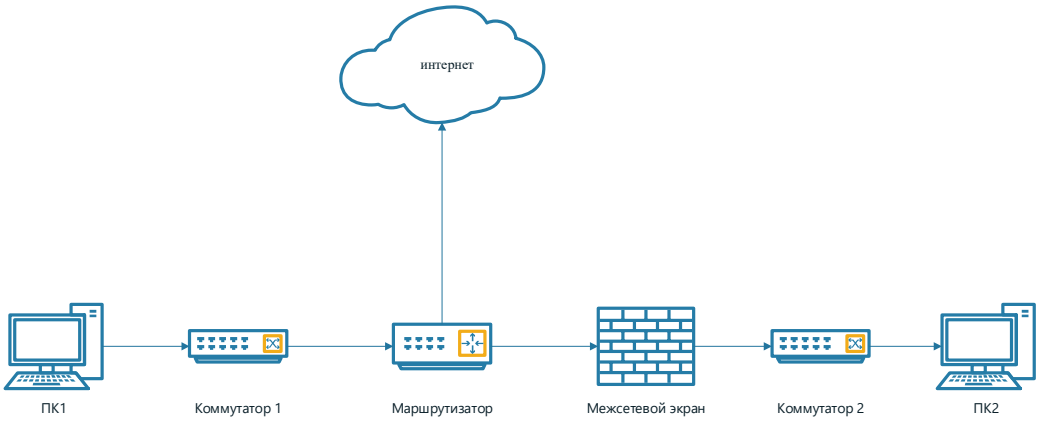


Рис. Схема виртуального стенда

Было выявлено, что поля Identification и Differentiated Services Code Point в IPv4 пригодны для создания стеганографических вложений, однако поле Identification изменяется, если на пути к принимающей стороне настроен NAT или PAT. Также в протоколах TCP и UDP в качестве стегоконтейнеров возможно использование поля source port. Для увеличения объема передаваемых данных возможно комбинировать используемые поля.

На основе полученных результатов можно сделать вывод, что стеганографические каналы имеют огромный потенциал и практически никак не отслеживаются в магистральных сетях, а их выявление в локальных сетях крайне ресурсозатратно. Отслеживание данных туннелей сильно затруднено на магистральной сети введу огромного количества пакетов в сети Интернет, а также чувствительности некоторого трафика к задержкам.

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. Часть 1. Цифровая стеганография / под общей ред. проф. В. И. Коржика. Санкт-Петербург, 2016.
2. Sharikov P. I., Krasov A.V., Gelfand A. M., Kosov N. A. Research of the possibility of hidden embedding of a digital watermark using practical methods of channel steganography // Intelligent Distributed Computing XIII. 2019. pp. 203–209.
3. Simmons G. J.: The prisoners' problem and the subliminal channel // In Chaum D. ed.: Crypto '83. Advances in Cryptography, Plenum Press (1983). pp. 51–67.
4. Костырин А. С., Красов А. В. Обзор возможностей реализации канальной стеганографии на основе протоколов сетевого и транспортного уровней модели osi // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 437–443.
5. Красов А. В., Степанов Е. И. Практическое применение сетевой стеганографии на примере протокола icmp // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 2. С. 510–513.
6. Sharikov P. I., Krasov A. V., Gelfand A. M., Kosov N. A. Research of the possibility of hidden embedding of a digital watermark using practical methods of channel steganography // Intelligent distributed computing XIII. 2019. pp. 203–209.

УДК 004.772
ГРНТИ 49.38.49

СОКРЫТИЕ ИНФОРМАЦИИ В ПРОТОКОЛАХ RTP, RTCP

В. Н. Волкогонов, Е. М. Гетьман, А. С. Салита

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

В связи с ростом популярности IP телефонии и увеличения другого медиа трафика чувствительного к задержкам возросла популярность таких протоколов как RTP, RTCP. В данной статье рассматривается возможность создания стеганографических каналов на основе протоколов RTP, RTCP, исследуются поля заголовков, которые можно использовать в качестве стегоконтейнеров.

стеганография, сетевая стеганография, безопасность, IPv4, канальная стеганография, сокрытие информации, защита информации, сети передачи данных.

Основная задача сетевой стеганографии – передача данных таким образом, чтобы сокрытые данные были невидимыми для человеческого глаза, а также для сетевых устройств (промежуточных сетевых узлов и конечного

хоста). Важно подчеркнуть, что сокрытые данные внутри стегоконтейнера (носителя) и сам факт их передачи скрыты от стороннего наблюдателя, который не знает о существовании стеганографического канала. Таким образом, происходит не только сокрытие самих данных, но и самого факта передачи секретной информации. Подробнее о реализации стеганографии можно прочесть в [1, 2, 3].

В сетевой стеганографии носителем является, как минимум один поток сетевого трафика. Обычно стеганографический канал может быть многомерным, т. е. может быть сокрыт в нескольких потоках сетевого трафика, в, так называемых, поднесущих. Такими поднесущими могут быть время передачи, поле заголовка пакета или же последовательность пакетов. Например, в [4, 5, 6] рассматривается применение сетевой стеганографии.

На сегодняшний день аудиоданные и видеоизображения распространены в сети интернет. Поэтому в данной статье рассматривается возможность использования полей заголовков протоколов RTP, RTCP в качестве стегоконтейнеров.

RTP – (англ. *Real-time Transport Protocol*) используется при передаче трафика реального времени. Протокол RTP содержит в своём заголовке данные, необходимые для восстановления аудиоданных или видеоизображения в приёмном узле, а также данные о типе кодирования информации. В заголовке данного протокола, в частности, передаются временная метка и номер пакета. Эти параметры позволяют при минимальных задержках определить порядок и момент декодирования каждого пакета, а также интерполировать потерянные пакеты. Подробнее о протоколе можно прочесть в [7].

В таблице приведена структурная схема заголовка протокола RTP.

ТАБЛИЦА. Заголовок протокола RTP

+ Биты	0-1	2	3	4-7	8	9-15	16-31
0	Ver.	P	X	CC	M	PT	Порядковый номер
32	Метка времени						
64	SSRC-идентификатор						
96, если CC > 0	[CSRC-идентификаторы]						
96 + (CC × 32), если X = 1	[Заголовок расширения – определённое профилем значение]						[Заголовок расширения – количество блоков данных по 32 бита (EHL)]
96 + (CC × 32) + 32	[Заголовок расширения — блоки данных]						
96 + (CC × 32) + X * (32 + 32 × EHL)	Данные						
если P = 1	Заполнение (*Padding data*)						L

0-1 – Ver. (два бита) в данном поле указывается версия протокола.

2 – P (один бит) если значение данного поля равно 1, то RTP-пакет дополняется пустыми байтами на конце, т. е. пакет содержит один или несколько актетов (несколько новых полей) заполненных нулями.

3 – X (один бит) в данному поле указываются расширения протокола, задействованных в пакете.

4-7 – CC (четыре бита) содержит количество CSRC-идентификаторов, следующих за постоянным заголовком.

8 – M (один бит) используется на уровне приложения и определяется профилем. Если это поле установлено, то данные пакета имеют особое значение для приложения.

9-15 – PT (7 бит) указывает формат полезной нагрузки и определяет её интерпретацию приложением.

16-63 – Порядковый номер и Метка времени (Используется для включения приемника и воспроизведения полученных образцов через соответствующие интервалы времени) – оба эти поля должны иметь случайное (не повторяющееся в сумме значение в начале установки соединения.

64-95 – SSRC-идентификатор (Идентификатор источника потока) – указывает источник синхронизации. Также можно использовать для стеганографических вложений т. к. генерируется автоматически раз за сессию.

Заголовок расширения – идентификатор профиля – Идентификатор профиля заголовка расширения.

Заголовок расширения – количество блоков – Длина заголовка расширения.

Заголовок расширения – блоки данных – Данные заголовка расширения.

Заполнение – Область заполнения пакета.

L – последний байт в пакете, определяющий длину области заполнения в байтах (используется для выравнивания в последнем пакете).

Из строения пакета видно, что для создания стеганографических каналов подходят следующие поля данного протокола: Порядковый номер и Метка времени, SSRC-идентификатор (Идентификатор источника потока) и Заполнение (*Padding data*). При этом поле Заполнение может иметь любую размерность, которая не превышает 255 бит. Данная размерность указывается в поле L. Стоит отметить, что все поля от Заголовка расширения в поле данные до поля L шифруются, что обеспечивает дополнительную защиту сокрытых данных. Поля порядковый номер и Идентификатор источника потока должны быть постоянными, если нам необходимо получить данные и отправить их приложению, однако, если у нас стоит цель организации сокрытого потока информации, то данные поля применимы для создания сте-

ганографического канала. По метке времени приложения определяют задержку пакетов и принимают решение о необходимости трансляции данных пользователю, поэтому при изменении этого поля, в большинстве случаев, данные будут отбрасываться.

Исходя из вышеперечисленной информации, можно сделать вывод, что для создания стеганографического канала, без потери передаваемых данных пригодно поле Заполнение (*Padding data*), поля Порядковый номер и Метка времени, SSRC-идентификатор (Идентификатор источника потока) ведут к потере данных при их изменении. Стоит отметить, что поля Порядковый номер и SSRC-идентификатор (Идентификатор источника потока) не меняются на протяжении установленной сессии, поэтому частое их изменение может привести к обнаружению стегоконтейниров, изменение поля метка времени также может быть обнаружено системами защиты. Начальное значение временной метки является случайным. Несколько последовательных RTP-пакетов могут иметь идентичные временные метки, если логически они генерируются одновременно (например, относятся к одному и тому же видеокадру). Однако искажение данного поля приведет к неправильной сборке данных и передачу пользователю.

Также на основе данного протокола возможна реализация такого похода как LACK. LACK (*Lost Audio Packets Steganography*) использует в своей сути намеренную задержку в VoIP пакетах. Отправитель генерирует пакет, полезная нагрузка которого несет скрытую информацию, и затем данный пакет намеренно задерживается. Пакеты, пришедшие с чрезмерной задержкой, отбрасываются получателем; однако, если получатель знает о существовании стеганоканала, данные RTP-пакеты не отбрасываются, и из них извлекается стеганограмма. Стегоанализ LACK трудно выполнить, т. к. данный метод строится на умышленной задержке пакетов. Задержка пакетов распространена в современных IP сетях, поэтому данный подход трудно обнаружить, естественно, если кол-во задержанных пакетов находится в разумных пределах.

Также рассмотрим такой протокол как RTCP. RTCP (англ. Real-Time Transport Control Protocol – протокол управления передачей в реальном времени) – протокол, используемый совместно с RTP. Протокол описан в RFC 3550. RTCP базируется на периодической передаче управляющих пакетов всем участникам сессии, используя тот же механизм рассылки, что и для пакетов данных.

Обмен RTCP основан на периодической передаче пакетов управления всем участникам сессии. Как правило, он работает с двумя типами пакетов (reports\ответов): отчет получателя Receiver Report (RR) и отчет Sender Report (SR). Определенные поля, которые включены в эти пакеты, могут использоваться для оценки состояния сети. Кроме того, все сообщения RTCP должны отправляться в составном пакете, состоящем как минимум из двух

различных типов ответов протокола RTCP. Для сеансов с небольшим количеством участников интервал между RTCP сообщений составляет 5 секунд и, кроме того, затраты на передачу RTCP сообщений не должны превышать 5 % доступной полосы пропускания сеанса. Для создания скрытых каналов могут использоваться блоки отчетов в отчетах SR и RR. Значения параметров, передаваемые в данных поля (кроме SSRC_1, который является Идентификатором источника) могут быть изменены, поэтому объем информации, которая может быть передана в каждом пакете, равна 160 битам. Естественно при использовании данного метода мы жертвуем некоторыми или всеми функциональными возможностями протокола RTCP Другие свободные/неиспользуемые поля в этих пакетах также могут использоваться аналогичным образом (SDES, APP или BYE). Итак, общая полоса пропускания для данного стеганографического метода является следующей:

$$\mathrm{RPBR_{RTCP}} = \mathrm{S_{CP}} * \mathrm{N_{RB}} * \mathrm{S_{RB}}\ [\frac{\text{бит}}{\text{пакет}}],$$

$PRBR_{RTCP}$ (*Packet Raw Bit Rate*) обозначает полосу пропускания созданного скрытого канала со стеганографией свободных/неиспользуемых полей RCTP (в битах/пакетах),

S_{CP} обозначает размер составного пакета RTCP (количество типов пакетов RTCP, т. е. разных Идентификаторов источника),

N_{RB} – количество блоков ответа внутри каждого типа пакета RTCP,

S_{RB} – это количество битов, которые могут быть скрытно отправлены в одном блоке отчета RTCP.

Также стоит отметить, что сообщения RTCP основаны на протоколах IP/UDP, поэтому дополнительно для одного пакета RTCP оба протокола могут использоваться для скрытой передачи.

Отсюда можно сделать вывод, что протоколы RTCP и RTP пригодны для создания стеганографических контейнеров, а следовательно могут использоваться для создания стеганографических каналов, однако пропускная способность таких каналов будет крайне мала, и создание стеганографических вложений может повлечь за собой искажение или потерю данных на конченом хосте. Поэтому поля данных протоколов рекомендуется использовать как одну из несущих стеганографического канала.

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. Часть 1 Цифровая стеганография / под общей ред. проф. В. И. Коржика. Санкт-Петербург, 2016.

2. Sharikov P. I., Krasov A. V., Gelfand A. M., Kosov N. A. Research of the possibility of hidden embedding of a digital watermark using practical methods of channel steganography // Intelligent Distributed Computing XIII. 2019. pp. 203–209.

3. Simmons G. J. The prisoners' problem and the subliminal channel // In Chaum D. ed.: Crypto '83. Advances in Cryptography, Plenum Press (1983). pp. 51–67.

4. Mazurczyk W., Smolarczyk M. & Szczypiorski K. Retransmission steganography and its detection // Soft Computing, 2009. No. 15 (3). pp. 505–515.

5. Костырин А. С., Красов А. В. Обзор возможностей реализации канальной стеганографии на основе протоколов сетевого и транспортного уровней модели osi // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 2. С. 437–443.

6. Красов А. В., Степанов Е. И. Практическое применение сетевой стеганографии на примере протокола icmp // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 2. С. 510–513.

7. Ушаков И. А., Красов А. В., Савинов Н. В. Организация, принципы построения и функционирования компьютерных сетей : учебник. М.: Academia, 2019. 240 с. ISBN 978-5-4468-7865-9.

УДК 004.387
ГРНТИ 50.43

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ АВТОМАТИЗАЦИИ СБОРА БЫТОВЫХ ОТХОДОВ

А. С. Мутханна, К. С. Воронина

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

В статье представлены некоторые пути решения экологической проблемы при помощи установки, во внутренней части мусорных контейнеров, датчиков контроля наполняемости бытовых отходов. Изучен опыт зарубежных стран, который показал, насколько эффективны системы управления отходам. Для эффективного контроля за наполняемостью разработана информационная система, с помощью которой диспетчер проводит мониторинг бытовых контейнеров.

автоматизация, датчики, сбор бытовых отходов, система, бизнес-процесс, облачная платформа.

Развитие цифровой экономики, приводит к тому, что она диктует области и направления технологического развития.

Одной из перспективных тенденций является Интернет Вещей (IoT). Колоссальные технологические достижения в области IoT изменили наш образ жизни и работу.

Наш мир становится умнее, и все (мобильные телефоны, автомобили, телевизоры) подключено к интернету, имеет уникальные адреса и механизмы связи. Предполагается, что к 2025 году каждая мелочь, такая как ручка, бумага, пакеты с едой и т. д. Будет управляться через IoT в направлении более «умного» мира.

В последние годы различные технологии и стандарты IoT активно разрабатывались для различных промышленных секторов и приложений, таких как умный город, интеллектуальная транспортная система, система безопасности и защиты, интеллектуальное сельское хозяйство, мониторинг окружающей среды, умная фабрика, интеллектуальное производство, здравоохранение и умный город, частью которого являются системы управления отходами

Система управления отходами включает в себя удаленные датчики, которые устанавливаются в мусорных контейнерах и специализированного программного обеспечения (ПО). Датчики контролируют и измеряют уровень наполненности мусорных контейнеров, и после передают информацию на центральный сервер. Они являются ультразвуковыми и питаются в основном за счет солнечной энергии. Это позволяет датчикам измерять уровень наполненности мусорных контейнеров в абсолютно автономном режиме.

На данный момент, аналитиками организации MarketsandMarkets, рынок систем управления отходами оценивается в $ 1,1 млрд [5].

По прогнозам можно сделать вывод, что в 2022 году рынок вырастет более, чем в два раза – до $ 2,38 млрд, при совокупном годовом коэффициенте роста (CAGR) в 16,9 % [5].

Система управления сбором бытовых отходов, в течение определенного промежутка времени обрабатывает и собирает данные о наполняемости мусорного бака. После этого, программа при помощи заложенных алгоритмов считает среднее время наполняемости. В учет берутся и динамические показатели, такие как дни недели и сезонность. Система, также производит анализ длительности нахождения мусорного бака в заполненном состоянии. Специализированное ПО, обрабатывая всю информацию, которая была получена, предоставляет подробную и качественную детализацию об уровне заполненности каждого мусорного контейнера [5].

Датчик представлен в виде маленькой коробочки, которая цепляется к внутренней стенке мусорного контейнера.

Внутри расположены несколько датчиков: датчик температуры, датчик наклона, ультразвуковой датчик, радиомодуль, который передает информацию на сервер и GPS/ГЛОНАСС [6].

При помощи датчика наклона можно в моменте зафиксировать опустошение контейнера (переворот контейнера), датчик позволяет сигнализиро-

вать о пожаре и т. д., GPS/ГЛОНАСС – определить местоположение контейнера в динамике (переезды, ротация), радиомодуль (GSM, LoraWAN) – удаленно отправлять информацию, полученную с прибора, так как он автономный» [6].

Корпус датчика сделан из ударопрочного пластика. Датчик не пропускает влагу и пыль, выдерживает перепады температур от −35 °С до +70 °С. Соответствует классу IP56.

Для моделирования и автоматизации процессов выбрана методология IDEF0 и программный продукт Microsoft Visio.

Целью моделирования является формулировка полной и всеобъемлющей модели. IDEF0 идеальный метод моделирования из-за сходства диаграмм с диаграммами IPO и добавления иерархической декомпозиции функционального моделирования. Такой подход позволяет плавно перейти от моделирования системы через теорию к обслуживанию [3].

Моделирование информационных включает в себя два этапа. На первом этапе описываются процессы, которые уже происходят и действуют в реальном времени («как есть»). Затем моделирование нового уровня задач, которые только появятся с созданием новой системы («как должно быть») [3].

В модель «как есть» входят такие блоки как:

Блок А1. Установка графика времени и участков для сбора бытовых отходов.

Блок А2. Приезд транспорта на участок по строго установленному графику.

Блок А3. Сбор бытовых отходов.

Блок А4. Выгрузка содержимого мусоровоза в месте хранения отходов.

После представления модели «как есть», рассматривается процесс, который будет выполняться после внедрения информационной системы сбора отходов на предприятии, то есть модель «как должно быть». Предлагаемая модель позволит в логической, удобной и непротиворечивой форме описать взаимоотношения между функциями управления и ответственными руководителями, предоставляет информацию о ресурсах, информационных потоках, инструкциях, нормативной информации.

Блок А1. Поступление информации о заполненном контейнере.

Блок А2. Обработка данных, полученных от датчиков.

Блок А3. Построение оптимального маршрута и выезд транспорта по необходимости.

Блок А4. Выгрузка содержимого мусоровоза в месте хранения отходов.

Таким образом, процесс вывоза бытовых отходов в модели «как должно быть» сэкономит денежные и временные ресурсы управляющей компании и государства, так как транспорт на участки, на которых располо-

жены контейнеры, будет приезжать только тогда, когда это будет необходимо, в отличии от модели «как есть», где вывоз бытовых отходов происходит по строго установленному графику, что вызывает массу неудобств.

Разработанная модель IDEF0 представляет собой отправную точку для дальнейшего выполнения задач, которые ранее было очень сложно проводить.

На рис. 1 отражены основные модули и функции информационной системы для автоматизации сбора бытовых отходов.

Построенная структура, в “Aris Express”, отражает основные возможности и модули проектируемой системы.

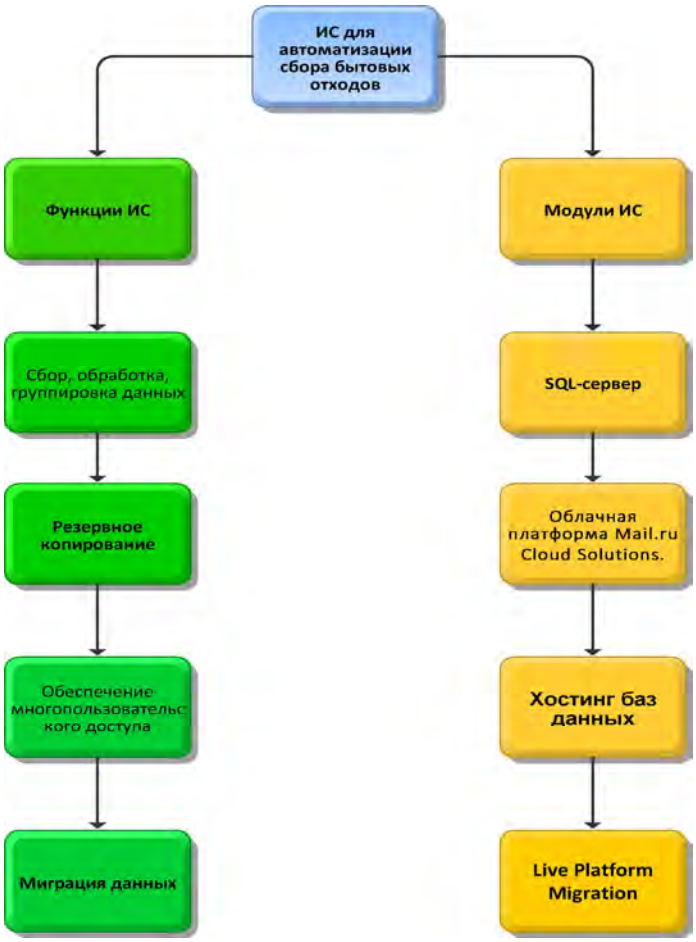


Рис. 1. Функциональная структура разрабатываемой ИС

Следующим шагом является разработка базы данных (БД), которая будет отражать все необходимые данные.

База данных может служить базой знаний для разработчиков приложений Интернета вещей и исследователей безопасности, а также способствовать повышению осведомленности о киберситуационной ситуации на предприятии и повышению общей осведомленности общественности о безопасности.

На рис. 2 представлена разработанная БД, которая включает в себя актуальные данные о контейнерах, расположенных на участках, информацию об участках и водителях [1].

База данных удовлетворяет всем требованиям, которые были поставлены, отображает необходимую информацию для пользователей, которым она предназначена. БД удобна и понятна, а обучение персонала не занимает большого количества времени.

После того как была разработана БД последним этапом является подключение к облачному хранилищу.

Облачные вычисления – это новая тенденция в мире ИТ с точки зрения экономии затрат и ускорения работы приложений. Это также называется «база данных как услуга» (DBaaS).

Облачная база данных становится самой распространенной технологией для хранения огромных данных во многих компаниями во всем мире. Это не так просто, как взять реляционную базу данных и развернуть ее на облачном сервере. Это означает добавление дополнительных узлов по мере необходимости в режиме онлайн, и увеличение производительности базы данных

Модель DBaaS предоставляет данные по запросу через интерфейс прикладного программирования (API), а модель DBaaS предоставляет системы управления базами данных по запросу. Разные источники данных требуют усилий для интеграции данных из разных моделей [2].

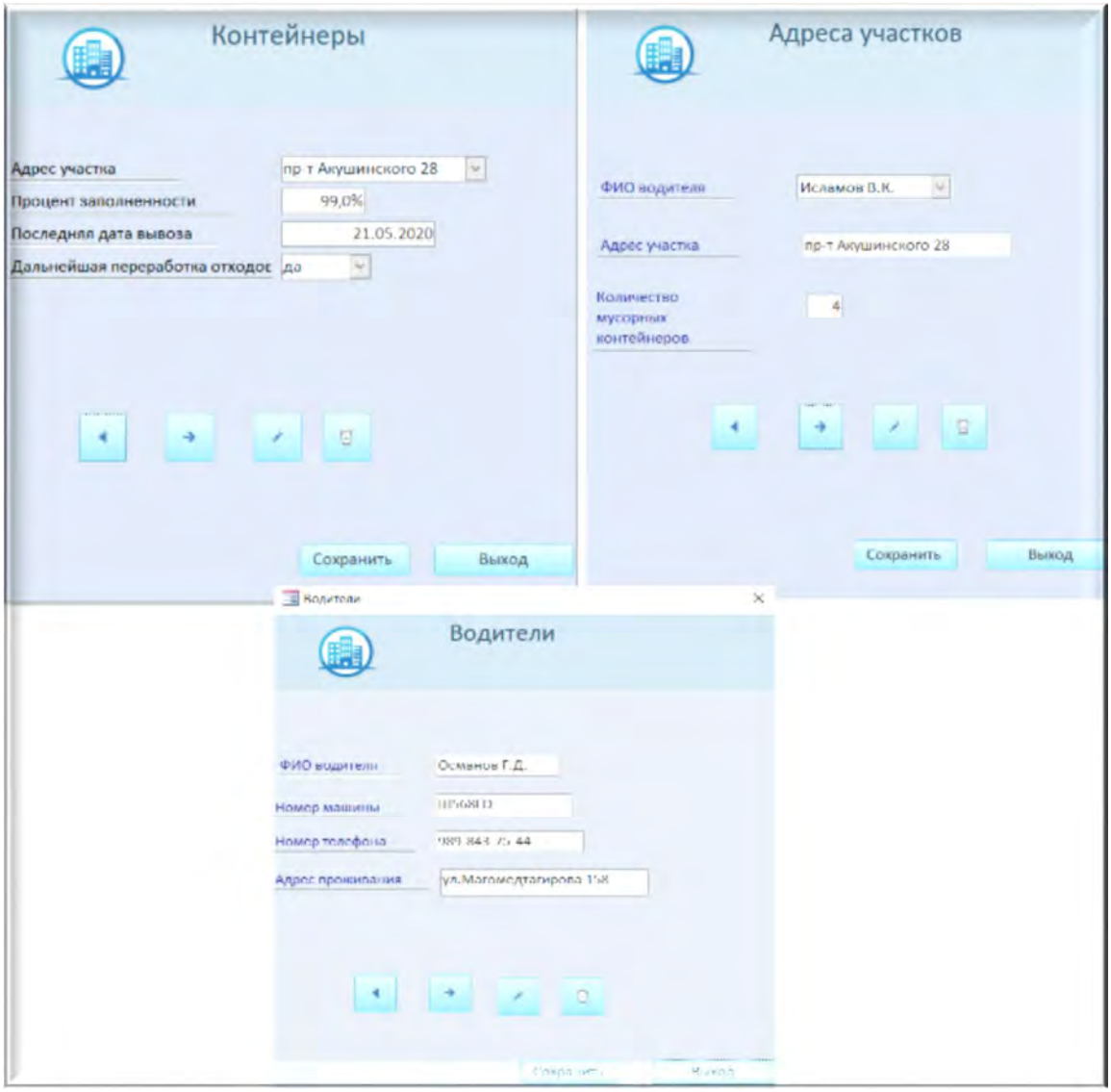


Рис. 2. База данных

Для перемещения БД в облачное хранилище можно рассмотреть платформу Mail.ru Cloud Solutions (рис. 3).

В зону ответственности входит вся IT-инфраструктура, хостинг баз данных и администрировании. Доступ к БД в онлайн-режиме из любой точки мира [4].

Виртуальные серверы в облаке можно соединяться с локальными площадками через защищенные VPN-соединения (IPsec) для создания гибридной IT-инфраструктуры.

Система обеспечивает информационную поддержку принятия решений и позволяет контролировать весь процесс сбора бытовых отходов.

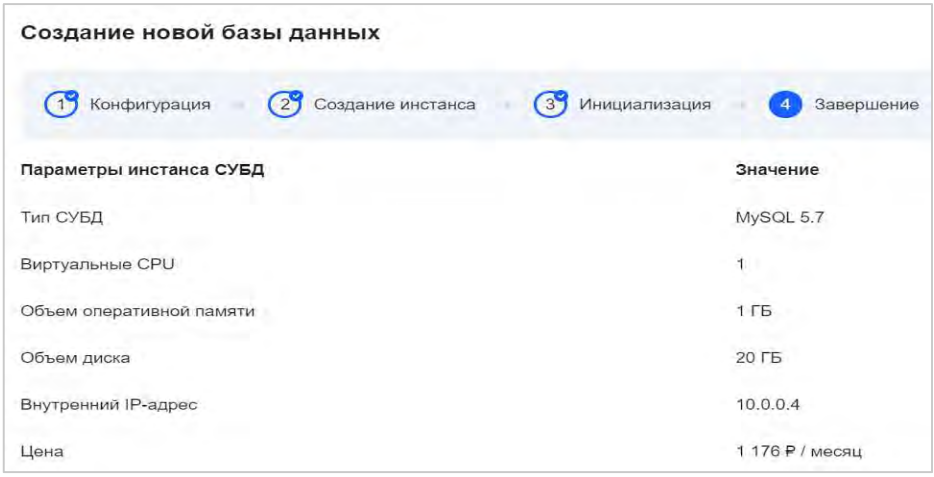


Рис. 3. Подключение БД к облачному хранилищу

Список используемых источников:

1. Баженова И. Ю. Основы проектирования приложений баз данных: учебное пособие / И. Ю. Баженова. Электрон. текстовые данные. Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. 328 с. ISBN 978-5-4487-0086-6. URL: http://www.iprbookshop.ru/67380.html (дата обращения: 28.09.2020).

2. DBaaS: базы данных в облаке. URL: https://habr.com/ru/ company/technoserv/blog/337860/ (дата обращения: 6.06.2020)

3. Методология IDEF0. URL: https://itteach.ru/bpwin/ metodologiya-idef0 (дата обращения: 15.09.2020)

4. Платформа облачных сервисов от Mail.ru Group. URL: https://mcs.mail.ru/databases/ (дата обращения: 20.09.2020)

5. Уборка мусора по-умному. URL: https://iot.ru/gorodskaya-sreda/uborka-musora-po-umnomu (дата обращения: 04.06.2020).

6. Белоусов Михаил. Сделать мусорный бак умным: как датчик Wasteout экономит деньги и делает города чище. URL: https://hightech.fm/2019/07/08/wasteout-kluev (дата обращения: 15.09.2020).

УДК 004.428
ГРНТИ 50.41.25

РАЗРАБОТКА ПЛАГИНОВ В WEB ПРИЛОЖЕНИИ LABGEN

А. О. Воронов, А. Ю. Цветков

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

2020 год показал, что учебные образовательные учреждения не могут обойтись без специализированных систем автоматизации учебного процесса. Из-за постоянного увеличения информационного потока, а также необходимости организации получения образования из любой точки мира. Автоматизированные учебные платформы чаще всего организованы по модели клиент-серверного приложения. Ввиду данной специфики необходимо на этапе разработки предусмотреть механизмы обеспечения безопасности клиент-серверного приложения для предотвращения различного рода атак.

Spring MVC, плагины, TLS, обфускация, права доступа, java.

В данной статье рассмотрена разработка клиент-серверного приложения на языке Java с применением фреймворка Spring MVC на примере программы для автоматизации учебного процесса. Расширение функциональности программы засчёт дополнительных независимых плагинов. А также механизмы обеспечения безопасности подобного рода приложений от различного рода атак.

Выбор архитектуры «клиент-сервер» для Labgen 5 обусловлен высокой доступностью, удобством пользования и несложной реализацией. А фреймворк Spring MVC позволяет без лишних действий начать реализовывать логику приложения.

Архитектура представляет из себя набор звеньев, где каждого своя роль:

– клиент (веб-браузер) – отправляют http запросы на сервер;

– сервер (tomcat) – ожидает запросы клиента, осуществляет необходимые вычисления, а также обеспечивает обмен данными с базой данных;

– база данных (MySQL) – хранилище сведений о клиентах. Позволяет сохранить данные пользователей при аварийном отключении питания.

Возможны дополнительные звенья, чаще всего они выступают посредниками между клиентами и основными серверами, у каждого из них своя функциональность и задача. В Labgen 5 есть такое звено – это сервер автоматизированного тестирования, его задача тестировать отправленные студентом работы. Хорошей практикой является организация кластеров серверов и баз данных для повышения надёжности и отказоустойчивости

системы. По сколько использование сервера и базы данных в единственных экземплярах чревато падением всего приложения в аварийной ситуации. Для лучшей работоспособности приложения кластеры необходимо использовать совместно с балансировщиком нагрузки. Тогда удастся избежать «лишних» задержек в работе системы.

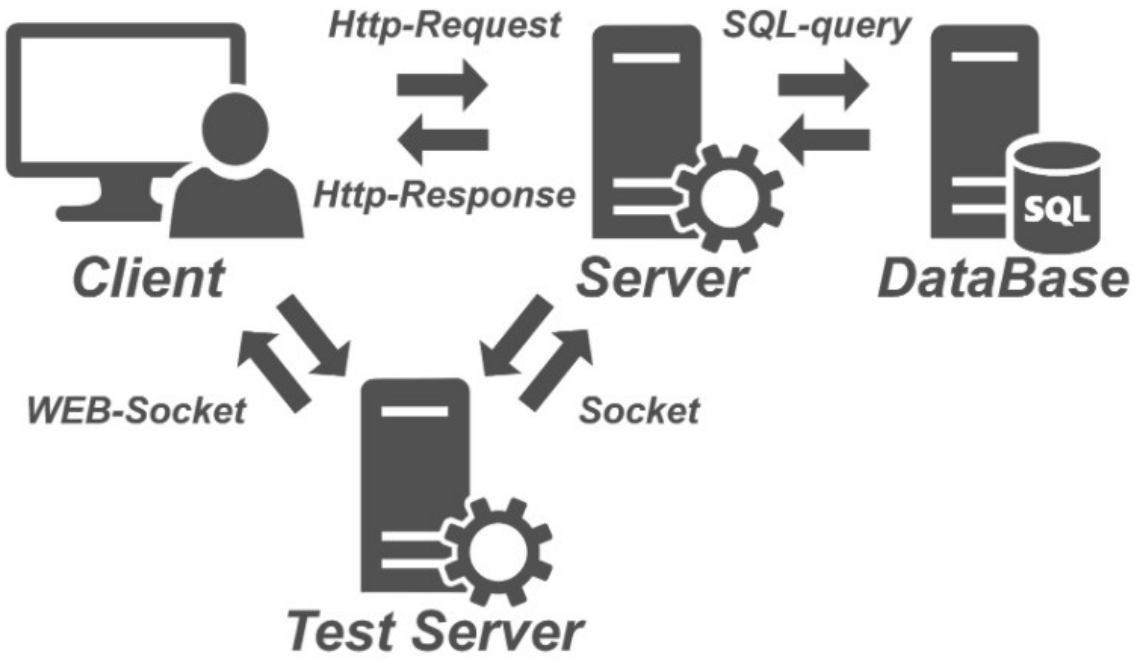


Рис. 3. Архитектура Labgen 5

Взаимодействие в системе происходит следующим образом:

Клиент обращается к серверу с помощью http-запроса, сервер его обрабатывает и запрашивает необходимые данные у базы данных с помощью SQL-запросов. С сервером тестирования клиент общается с помощью web-socket, а сервер с помощью обычных socket-ов. Их основное отличие в том, что web-socket позволяет организовать двунаправленный канал, работающий в реальном времени, то есть сервер может ответить без запроса клиента. Клиент просто прослушивает поток.

Далее рассмотрим структура сервера на Spring MVC. MVC – это шаблон проектирования model-view-controller. Он основан по принципу разделения программы на части, которые позволяют отделить графический интерфейс от бизнес логики, а бизнес логику от данных.

Под моделью, чаще всего понимается часть, содержащая в себе функциональную бизнес-логику приложения. Сама же модель ничего не знает о controllers и views.

Задача контроллера по запросу, полученному от пользователя, запросить у конкретной модели данные. Чтобы после предоставить их в представление.

После получения данных view возвращает клиенту отображение web странички соответствующей исходному запросу. Сами представления это html и css код. Также возможно применение шаблонизаторов для динамического отображения страниц, например, thymeleaf.

Элемент Dispatcher Servlet и интерфейс Handler Mapping реализованы командой Spring. Они обеспечивают передачу запросов и данных между controller, view и model.

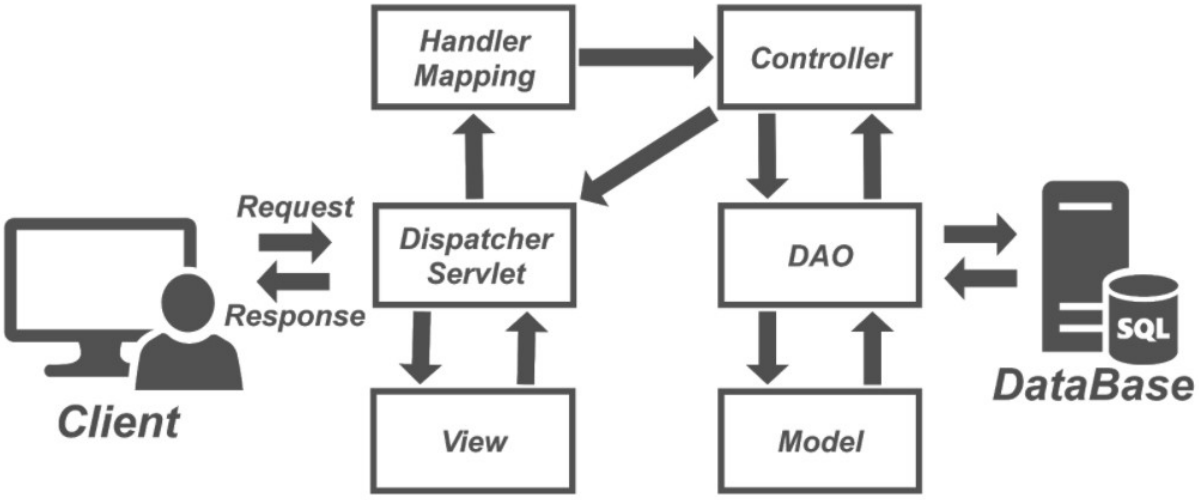


Рис. 4. Структура сервера на Spring MVC

Для обеспечения гибкости и вертикальной расширяемости используется целая система подключаемых плагинов и api для них. Сами плагины независимы и используются как организация дополнительного функционала приложения. В Labgen 5 они подключают лабораторную работу по конкретной дисциплине, а также используются для добавления тем оформления самого приложения. Модуль api позволяет разворачивать одну и ту же систему независимо для разных учебных дисциплин при различных конфигурациях, дизайне и логике.

Для успешной работы с плагинами в Labgen 5 используется Plugin Framework for Java (PF4J) [10]. Данный фреймворк позволяет превратить монолитное приложение в модульное. Для этого представлены следующие компоненты: Plugin – выступает в роли базового класса для плагинов, чтобы избежать конфликтов между разными плагинами у каждого из них свой класс загрузчик; PluginManager – данный класс позволяет управлять загрузкой, запуском и остановкой плагинов; PluginLoader – подгружает необходимый плагин, доступные плагины должны храниться в специальной директории – PluginClasspath; ExtensionPoint – используется как маркер, указывающий где в приложении может быть вызван пользовательский код.

Ввиду своей специфики, клиент-серверные системы имеют ряд уязвимостей. Которые могут навредить работоспособности приложения, а также нанести серьёзный ущерб пользователям.

Среди основных проблем информационной безопасности можно выделить следующие виды угроз:

− угроза прослушивания канала связи между клиентом и сервером;

− угроза противоправного доступа как базе данных пользователей, так и к функциональным возможностям приложения;

− внедрение и запуск вредоносного программного обеспечения на стороне сервера [6];

− реверс-инжиниринг клиентской части приложения;

В целях противодействия указанным угрозам будут использованы следующие механизмы информационной безопасности:

− TLS (англ. *transport layer security* – Протокол защиты транспортного уровня);

− механизм ограничения и разграничения прав доступа;

− безопасный загрузчик классов на стороне сервера тестирования;

− запутывание программного кода без потери функциональности (обфускация).

В современном мире информация достаточно ценный актив, именно поэтому её необходимо защищать. Недостаточная эффективность мер защиты может повлечь за собой утрату информации, её подмену или искажение в случаи несанкционированной атаки. Существует множество различных механизмов обеспечения информационной безопасности приложения, так и передаваемых данных за его пределами [4, 5, 7, 8, 9, 11].

Во избежание проблем с передачей данных хорошим и современным решением будет применение протокола TLS [1]. Он обеспечивает аутентификацию, шифрование и целостность передаваемых данных. Для организации безопасного канала связи инициализируется TLS-рукопожатие. За эту операцию клиент и сервер должны договориться о алгоритме шифрования, сгенерировать сеансовый ключ, а также проверить подлинность SSL-сертификата. В TLS версии 1.3 на ранних стадиях соединения применяется механизм цифровой подписи, что позволяет обезопасится от атак, меняющих шифронабор. А также быстрее аутентифицировать сервер.

Чтобы противостоять угрозе несанкционированного проникновения в систему был разработан механизм разграничения прав доступа. Данное решение позволяет отделить возможности студента от преподавателя.

В основе системы лежат роли, к которым привязаны права доступа к различным функциям приложения. При попытке пользователя выполнить какое-либо действие система проверит есть ли у него на это разрешение.

DPSX (*distributed permission system extended*) – распределенная система контроля доступа к различным функциям админ-панели в системе, основанная на ролевой модели контроля доступа.

В таблице представлено описание всех доступных ролей и их набора прав доступа к системе. Условно данную модель можно разделить на уровни, чем выше уровень, тем больше прав у конкретного пользователя. Данное решение позволяет легко и быстро добавить новые роли в случаи необходимости, а также достаточно эффективно с точки зрения безопасности.

ТАБЛИЦА. Набор ролей и прав доступа

Роль	Права доступа
Студент	students.view, labs.view, courses.view
Преподаватель	students.create, students.delete, groups.create, groups.delete, messages.create, messages.delete, labs.change_state
Старший преподаватель	courses.change_state, common.massive
Администратор	server.reload_dps, server.reload_crs, server.reload_plugins

Дополнительно для разграничения доступа к параллельным дисциплинам была внедрена система CRS (course role system), является логическим развитием системы DPSX.

Система CRS оперирует только лишь правами labs.* и messages.*, так как они непосредственно зависят от выбранного курса. Данное решение позволяет избежать получения доступа ко всем курсам в системе пользователям с ролью преподаватель. Не будет такого, что преподаватель сможет оценивать студентов не по своей дисциплине. Проверка доступа системой CRS происходит в несколько этапов.

Алгоритм принятия решения по правам labs.* и messages.*:

1. DPSX проверяет наличие у пользователя в целом права на действие в курсе;

2. CRS проверяет наличие соответствия администратора определенной роли по данному курсу и считывает идентификатор роли в случае успеха;

3. CRS проверяет наличие указанного права в списке прав роли администратора на данном курсе;

Для дополнительного контроля состояния системы используется логирование. Каждое произведенное успешное и неуспешное действие фиксируется в журнале. Для реализации была выбрана библиотека Log4j [2].

Labgen 5 предоставляет возможность автоматической проверки учебных работ по программированию на Java. Для проверки программ тестировочный сервис непосредственно запускает пользовательские программы. При таком устройстве пользовательская программа может получить полный доступ к системе и причинить вред серверу, поэтому необходимо реализовать механизмы защиты от таких атак.

С целью защиты сервера тестирования от повреждений вредоносным кодом был реализован безопасный загрузчик классов. Задача которого регламентировать набор допустимых к использованию студентом классов. Для каждой лабораторной работы имеется свой набор. Также установлено ограничение по времени выполнения тестируемой работы, чтобы избежать потери ресурсов сервера в случаи зависания тестируемой программы.

Для защиты данных пользователей, в случаи получения доступа к базе данных злоумышленником, пароли пользователя хранятся в захэшированном виде. Процедуру хэширования осуществляется на этапе создания аккаунта пользователя. Все пароли проходят через одностороннюю криптографическую хеш-функцию с добавлением специальной соли, после чего вернуть их в прежний вид уже не представляется возможным. (Соль представляет из себя случайную строку сгенерированную и хранящуюся на сервере.) Остаётся только атака перебором или применить радужные таблицы.

Радужная таблица – это предварительно вычисленная таблица для хэширования выходных данных криптографических хэш-функций, зачастую используется для взлома хэшей паролей [3].

Для усложнения процесса статического анализа декомпилированного программного кода приложения на java используется механизм обфускации скомпилированных классов, но это не единственно возможный вариант есть и другие методы [8]. Процесс обфускации заменяет все идентификаторы объектов на непонятные для человека случайные последовательности символов, тем самым затрудняя анализ декомпилированного кода. Но существуют и программы деобфускаторы, которые помогают злоумышленнику анализировать программный код.

Резюмируя выше изложенное можно сказать, что в современном мире существует огромное количество угроз информационной безопасности для автоматизированных систем. В качестве мер противодействия от атак в среде, где злоумышленником может являться обучающийся, внедрены следующие механизмы безопасности:

- Защита сетевого соединения при помощи протокола TLS 1.3 для защиты от прослушивания и изменения сетевых пакетов;
- Механизмы распределения прав доступа (DPSX, CRS) для предотвращения неправомерного доступа к просмотру, изменению, удалению, созданию лабораторных работ, студентов, групп студентов, курсов в системе;

● Безопасный загрузчик классов, предотвращения загрузки вредоносного ПО на сервис тестирования;

● Журналирование действий в системе;

● Применение односторонних криптографических хеш-функций к паролям пользовательских аккаунтов;

● Обфускация скомпилированного Java байт-кода для затруднения статического анализа клиентского приложения и вскрытия сетевого протокола.

Данные решения позволяют обеспечить базовый уровень безопасности [5], но при рассмотрении других возможных моделей злоумышленников, могут потребоваться модификации защиты системы.

Список используемых источников

1. СТБ 34.101.65-2014. Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS). Дата введения: 01.09.2014. Беларусь. 50 с.

2. Maven Repository: Apache Log4j. URL: https://logging.apache.org/log4j/2.x/ (дата обращения: 07.11.2020).

3. Радужная таблица. URL: https://en.wikipedia.org/wiki/Rainbow_table (дата обращения: 24.01.2021).

4. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

5. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернбородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 525–527.

6. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 321–326.

7. Хомяков И. Н., Красов А. В. Возможность скрытого вложения информации в байт-код Java // Информационные технологии моделирования и управления. 2014. № 2 (86). С. 185–191.

8. Красов А. В., Шариков П. И. Методика защиты байт-кода Java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47–50.

9. Krasov A. V., Arshinov A. S., Ushakov I. A. Embedding the hidden information into java byte code based on operands' interchanging // ARPN Journal of Engineering and Applied Sciences. 2018. Vol. 13. No. 8. pp. 2746–2752.

10. Framework PF4J. URL: https://pf4j.org/ (дата обращения: 16.02.2021).

11. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Ма-

териалы XVI Санкт-Петербургской международной конференции "Региональная информатика "РИ-2018" (Санкт-Петербург, 24-26 октября 2018 г.). СПб., 2018. С. 570–571.

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

УДК 004.056.5
ГРНТИ 49.34.01

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ VPN ТУННЕЛЕЙ ДЛЯ ОРГАНИЗАЦИИ УДАЛЕННОГО ДОСТУПА

Е. В. Гавриленко, А. Д. Докшин, М. М. Ковцур, Б. С. Мисливский

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

В настоящее время актуальны проблемы, связанные с организацией удаленных рабочих мест и получением доступа к рабочей сети через интернет. Для решения этих проблем используются протоколы для туннелирования трафика. Такие протоколы обеспечивают доступ к удаленной сети и защищают данные при передаче по открытым каналам. В статье проведен анализ популярных решений для организации туннелирования интернет-трафика, таких как IPSec, L2TP, PPTP и OpenVPN. Исследованы показатели эффективности, масштабируемости, производительности и защищенности туннелей. Рассмотрены особенности реализации VPN-шлюза на базе открытых операционных систем.

VPN, IPSec, OpenVPN, remote access, удаленный доступ, эффективность.

В ходе анализа существующих статей на данную тему [1, 2, 3, 4] выяснено, что прямое сравнение наиболее актуальных протоколов IPSec и решения OpenVPN представлено не полностью в существующих работах. В [1, 2] статьях осуществлено практическое тестирование IPSec и OpenVPN туннелей, а в [3, 4] проводится теоретическое сравнение протоколов VPN.

В таблице 1 содержится краткий обзор протоколов VPN.

ТАБЛИЦА 1. Общая таблица сравнения VPN

Название протокола	Размер overhead инкапсуляции	Алгоритмы шифрования	Совместимость
IPSec	60-80 байт	AES128-256, Blowfish и другие	Встроенная в Windows, Android и iOS. Наличие стороннего ПО для Linux и BSD
IPSec+L2TP	86-106 байт		

Название протокола	Размер overhead инкапсуляции	Алгоритмы шифрования	Совместимость
Routed IPSec (VTI)	60-80 байт		Наличие ПО для Linux и BSD, отсутствует поддержка Windows, Android, iOS
OpenVPN	~100 байт	AES128-256, Blowfish и другие	Наличие стороннего ПО для Windows, Linux, BSD, Android и iOS.

IPSec и OpenVPN могут использовать широкий набор алгоритмов шифрования, в том числе вычислительно стойкие, такие как AES и другие.

Группа протоколов IPSec отличается работой на основе соответствия политик, что не позволяет осуществлять динамическую маршрутизацию VPN-интерфейсов и передавать multicast-трафик. Эта проблема решается использованием L2TP over IPSec и Routed IPSec. OpenVPN не имеет такого недостатка, а также поддерживает большинство операционных систем и устройств.

Косвенным показателем быстродействия протокола VPN является объем накладных расходов для туннелирования трафика. Для расчета размера избыточного трафика протоколов IPSec и L2TP использовались данные из стандартов RFC 2401-2412, а также RFC 2661. Размер служебной информации OpenVPN сильно зависит от используемого режима работы VPN и выбранных алгоритмов шифрования, поэтому бралось среднее значение. Объемы заголовков к полезным данным в разных протоколах представлены на рис. 1.

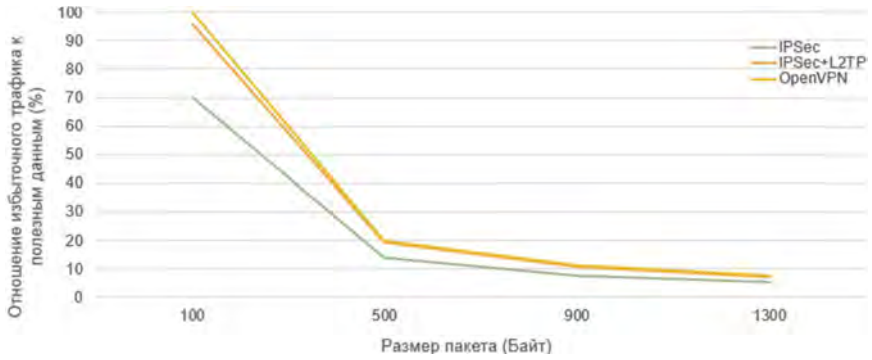


Рис. 1. Отношение накладных расходов туннелирования к полезной нагрузке

Для дальнейшего сравнения необходимо определиться с показателями эффективности VPN-туннелей. Их можно разделить на две группы: качественные и количественные. Защищенность, совместимость, возможность динамической маршрутизации VPN-туннеля и передачи multicast-сообщений представляют первую группу. Количественными же показателями выбраны: пропускная способностью туннеля, количество потребляемых им

вычислительных ресурсов, а также стабильность при работе в неустойчивом канале связи.

Тестирование проводилось в виртуальной среде с помощью программного обеспечения Oracle VM VirtualBox на компьютере с процессором Intel Xeon X3440. В качестве VPN-шлюза выбрана операционная система pfSense, так как она поддерживает все необходимые протоколы, а также имеет функционал для ограничения пропускной способности сети под названием Limiters.

На рис. 2 приведена схема тестового стенда. PC1 является удаленным клиентом, который получает доступ к PC2 через туннель с VPN-шлюзом.

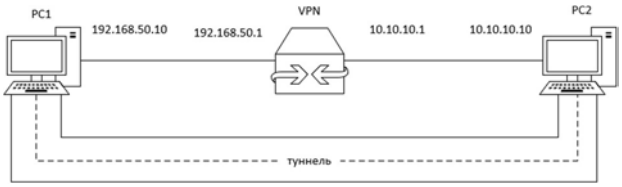


Рис. 2. Схема тестового стенда

Инструменты для тестирования – утилиты iperf, ping и sar. Все туннели тестировались с шифрованием AES 256. Для OpenVPN настроен в режиме UDP, как наиболее популярном и быстром. Виртуальной машине PC1 и VPN-шлюзу выделено по 3 потока процессора, а PC2 – два потока.

В первом тестировании замерялась максимальная пропускная способность VPN-туннеля при передаче TCP и UDP трафика от PC1 к PC2. Результаты тестирования представлены на рис. 3.

Во втором тесте проверялась стабильность пропускной способности туннеля в условиях плохого канала доступа. Для симуляции плохого канала передачи данных был задействован функционал Limiters. В нем ограничивалась пропускная способность канала между PC1 и VPN-шлюзом до 50 Мбит/с, а также задавалась 10 процентная вероятность потери пакета. Результаты второго тестирования представлены на рис. 4.

При проверке пропускной способности VPN-туннеля записывалась статистика о загрузке процессора VPN-шлюза. На рис. 5 представлены данные о максимальной загрузки процессора при использовании различных протоколов VPN.

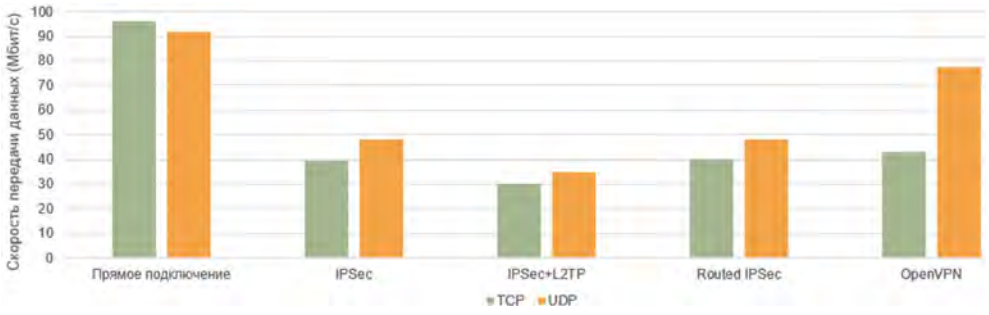


Рис. 3. Тестирование пропускной способности в режимах TCP/UDP

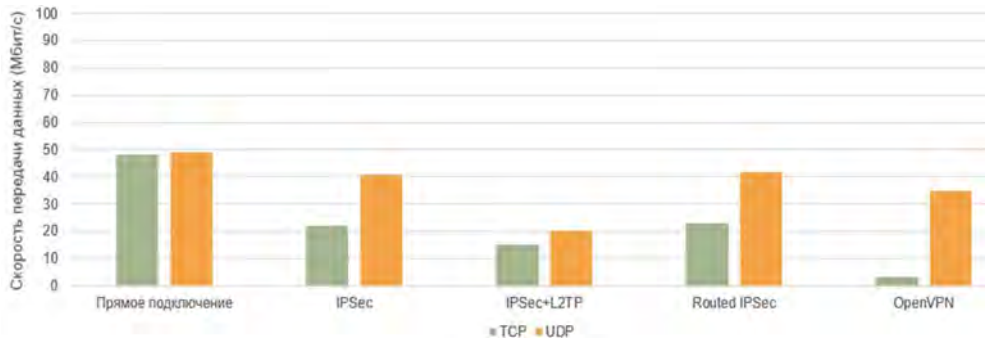


Рис. 4. Тест скорости с симуляцией плохого канала в режимах TCP/UDP

Рис. 5. Максимальная загрузка ЦП шлюза во время тестирований

По итогам тестирования выведена комплексная оценка для каждого протокола VPN. Показатель защищенности считался положительным в случае поддержки криптостойких алгоритмов. Совместимость – за наличие поддержки в большинстве операционных систем. Функциональность – за поддержку multicast-сообщений и динамической маршрутизации VPN-трафика в строке Функциональность. Показатели защищённости, совместимости и функциональности оценивались по формуле

$$f(x_i) = x_i \times k,$$

где x_i – это 1 или 0 обозначающие положительную или отрицательную оценку,

k – весовой коэффициент равный 20 при оценке защищённости и 10 в случаях оценки совместимости и функциональности

Пропускная способность оценивалась по формуле

$$f(x_i) = \frac{x_i}{y} \times k,$$

где x_i – это средняя пропускная способность туннеля,

y – пропускная способность канала без туннелирования,

k – коэффициент равный 30. Баллы за количество используемых вычислительных ресурсов считались по формуле

$$f(x_i) = \frac{(100 - i)}{100} \times k,$$

где x_i – это загрузка процессора в процентах,

k – коэффициент равный 10. Баллы, полученные за все показатели, суммировались. Результаты представлены в таблице 2.

ТАБЛИЦА 2. Комплексная оценка VPN-туннелей

	IPSEC	IPSec+L2TP	Routed IPSec	OpenVPN
Защищенность	20	20	20	20
Совместимость	10	10	0	10
Функциональность	0	10	10	10
Пропускная способность	14	10,5	14,1	19,2
Стабильность	19,5	10,8	20,1	11,7
Потребление ресурсов	5	4	4,8	2,1
Итоговая оценка	68,5	65,3	69	73

Наибольшую оценку получил OpenVPN, главными преимуществами которого являются широкая совместимость в популярных операционных системах, функциональность и пропускная способность. К недостаткам OpenVPN по итогам тестирования относятся стабильность и количество потребляемых вычислительных ресурсов.

Список используемых источников

1. Tisovský A., Baroňák I. Methodology for Benchmarking IPsec Gateways // International Journal of Computer Network and Information Security. 2012. Vol. 4. No. 9. pp. 1–9. DOI 10.5815/ijcnis.2012.09.01..

2. Hall M. Performance Analysis of OpenVPN on a Consumer Grade Router. 2008. pp. 1–15.

3. Плетеный Д. С., Аленченко В. В. Сравнение VPN – соединений для применения в защищенных корпоративных сетях // Аллея науки. 2020. Т. 2. № 5 (44). С. 979–984.

4. Arora P., Vemuganti P. R., Allani P. Comparison of VPN Protocols – IPSec, PPTP, and L2TP. 2001.

5. Коржик В. И., Ахрамеева К. А. Lecture notes on cryptography : учебное пособие; СПбГУТ. СПб., 2017. 103 с

6. Герлинг Е. Ю., Кулишкина Е. И., Гаврилов А. С., Виткова Л. А. Анализ и выявление психологических аспектов внутренних угроз на объектах связи // Известия высших учебных заведений. Технология легкой промышленности. 2018. Т. 39. № 1. С. 13–16.

7. Красов А. В., Левин М. В., Цветков А. Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 141–146.

УДК 004.056
ГРНТИ 49.33.35

АНАЛИЗ КРИТЕРИЕВ КЛАССИФИКАЦИИ ПОДХОДОВ К КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ

Д. А. Гайфулина, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В настоящее время системы киберзащиты обрабатывают огромное количество данных для аналитики безопасности и оповещении об инцидентах. При этом используются различные методы анализа событий безопасности, важное место среди которых занимает корреляция, позволяющая выявлять взаимосвязи между разнородными событиями и инцидентами. Систематизация существующих подходов к корреляции событий безопасности может осуществляться на основе различных критериев: по уровню корреляции событий, используемым методам, количеству источников информации и т.д. В данном исследовании проводится анализ критериев классификации подходов к корреляции событий безопасности. На основе проведенного анализа предлагается наиболее обширная таксономия рассмотренных подходов.

корреляция событий безопасности, корреляция предупреждений, управление безопасностью.

Чем сложнее становятся современные информационные системы, чем больше данных они обрабатывают и задач выполняют, тем сложнее становятся как способы реализации атак на подобные системы, так и способы защиты. Инструменты аналитики безопасности должны проводить мониторинг, обнаружение вторжений и анализ системных событий, которые представляют собой отдельные или совокупные сообщения, или сигналы тревоги, относящиеся к действиям в системе или сети [1]. Это может быть информация из сетевых пакетов, системных журналов и других источников данных. В рамках обеспечения безопасности должны выявляться события, несущие возможную угрозу или являющиеся частью многошаговой атаки, а также определяться их первопричины для предупреждения таких событий в будущем [2].

Процесс корреляции событий безопасности пытается определить взаимосвязь между ними, при этом связанные события могут быть объединены в мета-событие и классифицированы различным образом. Основной целью корреляции является выявление наиболее значимых событий в наборе записанных данных. В целом корреляция событий должна приводить к увеличению качества информации о событиях при уменьшении их числа [3].

Целью данного исследования определение основных критериев классификации подходов к корреляции событий безопасности. Главной задачей

исследования является анализ существующих обзоров в области анализа событий и предупреждений безопасности.

Рассмотрим существующие обзорные работы в области анализа событий безопасности, которая включает в себя: (1) корреляцию событий и предупреждений безопасности; (2) обнаружение и предупреждение сценариев атак; (3) обнаружение многошаговых и целевых атак.

В [3] методы корреляции разделяются по *уровням обработки данных*. На уровне сырых данных осуществляется отбор пакетов, вероятностный анализ пакетов, обнаружение аномальной активности, обнаружение сканирования портов, идентификация приложений и анализ полезной нагрузки пакетов. Основной целью уровня событий является сбор как можно большего количества информации, агрегирование нескольких событий путем локальной или распределенной корреляции. Уровень отчетов выполняет генерацию возможных активных контрмер и верификацию событий безопасности.

В [4] подходы к корреляции предупреждений, используемые совместными системами обнаружения вторжений, делятся на пять категорий по *методу корреляции*. Подходы на основе схожести атрибутов коррелируют предупреждения, используя сходство между их признаками. Подходы, основанные на сценариях атаки, коррелируют предупреждения на основе заранее определенных сценариев атаки, заданных экспертами или полученных на обучающих наборах данных. Таким образом, идет разделение методов по *способу извлечения знаний*. Методы предпосылок и последствий пытаются реконструировать сложные сценарии атаки, связывая отдельные шаги одной атаки. Подходы на основе нескольких источников информации объединяют различные типы информации. Подходы к фильтрации основаны на удалении из процесса корреляции событий по заранее определенным приоритетным правилам для защищаемых систем. Схожие методы выделяют в [5]. В [6] дополнительно выделяют экспертные системы и вычислительный интеллект, причем алгоритмы на основе атрибутов рассматривают с точки зрения свойств, отметок времени и статистических отношений.

Авторы [7] разделяют алгоритмы корреляции на три категории. К алгоритмам, основанным на сходстве, относят простые правила, иерархические правила и машинное обучение. Алгоритмы, основанные на знаниях, включают сценарии атак и методы предпосылок и последствий. Алгоритмы, основанные на статистике, хранят причинно-следственные связи между различными инцидентами и анализируют их частоту при обучении системы, а затем генерируют шаги атаки.

В [8] подходы к корреляции предупреждений классифицируют, помимо используемых методов, по количеству источников данных, области

применения и архитектурному дизайну системы. Так, данные могут приниматься только из одного источника данных или из нескольких. Авторы выделяют три основных области применения: системы управления сетью, ИТ-безопасность и управление процессами в производственных системах. Архитектурные решения могут быть централизованными, распределенными и иерархическими. Среди методов корреляции выделены три основные категории: методы, основанные на сходстве, последовательные и прецедентные методы, основанные на знаниях.

В [9] решения по обнаружению целевых атак подразделяются на подходы на основе хоста, на основе сети, с несколькими источниками и чисто семантические подходы, которые нельзя отнести к определенной области. В [10] выделяют четыре категории методов прогнозирования и предупреждения атак. К первой категории методов относятся дискретные модели, включающие графы атак, байесовские сети, модели Маркова и теорию игр. Вторая категория включает методы, основанные на непрерывных моделях, таких как временные ряды и серые модели. Третья категория содержит методы, основанные на машинном обучении и интеллектуальном анализе данных. Четвертая категория включает подходы, основанные на сходстве и эволюционные вычисления.

Авторы [11] рассматривают подходы к обнаружению многошаговых атак и классифицируют их на пять категорий. К подходам на основе сходства относятся прогрессивное построение путем сопоставления атрибутов или корреляции, кластеризация сценариев и обнаружение аномалий. Причинно-следственная корреляция включает себя методы предпосылок и последствий, статистический вывод или сопоставление моделей. Структурная корреляция использует модель сети, где можно спрогнозировать будущие пути атаки. Подходы на основе случая обнаруживают известные сценарии атак как ансамбль следов. Смешанные подходы используют несколько методов. В [12] проводится систематический обзор методов обнаружения и предупреждения сценариев атак. При этом выделяются три категории данных методов. Первой является анализ переходов состояний, основанный на явных сигнатурах сценария атаки, второй – корреляция событий на основе экспертных знаний, использующая правила для построения сценариев атак. К третьей категории относится корреляция событий, основанная на интеллектуальном анализе данных и машинном обучении.

В таблице представлена краткая характеристика описанных работ по критериям классификации методов корреляции, которые в каждой работе предложены.

ТАБЛИЦА. Характеристика обзорных работ

№	Авторы, год	Критерии классификации					
		Метод корреляции	Извлечение знаний	Количество источников	Уровни корреляции	Тип архитектуры	Область применения
1	Limmer&Dressler, 2008 [3]	✓	×	×	✓	×	×
2	Elshoush&Osman, 2011 [4]	✓	×	✓	×	×	×
3	Mirheidari et al., 2013 [7]	✓	✓	×	×	×	×
4	Salah et al., 2013 [8]	✓	✓	✓	✓	✓	✓
5	Yu Beng et al., 2014 [5]	✓	✓	×	×	×	×
6	Luh et al., 2017 [9]	✓	×	✓	×	×	✓
7	Husák et al., 2018 [10]	✓	✓	×	×	×	×
8	Navarro et al., 2018 [11]	✓	✓	×	×	×	×
9	Kovačević et al., 2020 [12]	✓	✓	×	×	×	×
10	Pavlov&Voloshina, 2020 [6]	✓	✓	×	×	×	×

Таким образом, можно определить следующие основные критерии классификации:

- *Количество источников данных*. Источников данных событий безопасности может быть как один, так и несколько.
- *Извлечение знаний.* По способу извлечения знаний можно выделить подходы, основанные на экспертных правилах, сигнатурных методах и обнаружении аномалий.
- *Метод корреляции.* Методы корреляции событий безопасности можно разделить на три основные категории: на основе сходства, пошаговые и смешанные. Методы на основе сходства сравнивают несколько событий на основе их атрибутов и признаков. Пошаговые методы составляют цепочки событий, восстанавливают действия атакующего и анализируют связи между несколькими событиями. Смешанные методы используют комбинированные алгоритмы.
- *Уровни корреляции событий*. Можно выделить уровни необработанных данных, событий и отчета.
- *Тип архитектуры* системы корреляции событий безопасности может быть централизованным, распределенным или иерархическим.
- *Область применения* системы корреляции событий.

Данные критерии позволят составить наиболее полную классификацию подходов к корреляции событий безопасности и охватить большую

часть исследований в научной литературе на данную тему. В рамках будущих работ планируется провести собственный систематический обзор существующих подходов к анализу событий и предупреждений безопасности, используя предложенную классификацию.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

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

2. 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. 4 (47). С. 5–27.

3. Limmer T., Dressler F. Survey of event correlation techniques for attack detection in early warning systems // University of Erlangen, Dept. of Computer Science, Technical Report, April. 2008. 37 p.

4. Elshoush H. T., Osman I. M. Alert correlation in collaborative intelligent intrusion detection systems – A survey // Applied Soft Computing. 2011. Vol. 11. No. 7. pp. 4349–4365.

5. Yu Beng, L., Ramadass, S., Manickam, S., Soo Fun, T. A survey of intrusion alert correlation and its design considerations // IETE Technical Review. 2014. Vol. 31. No. 3. pp. 233–240.

6. Pavlov A., Voloshina N. Analysis of IDS Alert Correlation Techniques for Attacker Group Recognition in Distributed Systems // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Springer, Cham. 2020. pp. 32–42.

7. Mirheidari S. A., Arshad S., Jalili R. Alert correlation algorithms: A survey and taxonomy // Cyberspace Safety and Security. Springer, Cham. 2013. pp. 183–197.

8. Salah S., Maciá-Fernández G., DíAz-Verdejo J. S. E. A model-based survey of alert correlation techniques // Computer Networks. 2013. Vol. 57. No. 5. pp. 1289–1317.

9. Luh, R., Marschalek, S., Kaiser, M., Janicke, H., Schrittwieser, S. Semantics-aware detection of targeted attacks: a survey // Journal of Computer Virology and Hacking Techniques. 2017. Vol. 13. No. 1. pp. 47–85.

10. Husák, M., Komárková, J., Bou-Harb, E., Čeleda, P. Survey of attack projection, prediction, and forecasting in cyber security // IEEE Communications Surveys & Tutorials. 2018. Vol. 21. No. 1. pp. 640–660.

11. Navarro J., Deruyver A., Parrend P. A systematic survey on multi-step attack detection // Computers & Security. 2018. Vol. 76. pp. 214–249.

12. Kovačević I., Groš S., Slovenec K. Systematic Review and Quantitative Comparison of Cyberattack Scenario Detection and Projection // Electronics. 2020. Vol. 9. No. 10. P. 1722.

УДК 621.391.823
ГРНТИ 47.05.07

АЛГОРИТМЫ ПОИСКА, ИСПОЛЬЗОВАНИЯ И УСТРАНЕНИЯ ИНДУСТРИАЛЬНЫХ РАДИОПОМЕХ

В. А. Гапоненко, А. Ю. Цветков

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

Индустриальные радиопомехи-электромагнитные возмущения, создаваемые непреднамеренно во время работы различных технических устройств, средств, приборов и аппаратов, а также, в некоторых случаях создаваемые человеком преднамеренно использующем специальные технические компоненты, или пренебрегая государственными стандартами в области борьбы с радиопомехами. Индустриальные помехи довольно сильно мешают радиоприёму, проявляя себя, например, как трески и шумы в телефонных аппаратах, устройствах вывода и вывода звука, а также, искажая сигнал на частоте, схожей с частотой помехи. В статье будут рассмотрены причины возникновения помех, влияние их на работу других устройств, способы борьбы с ними, а также техническая возможность использования помех злоумышленником в корыстных целях.

помехи индустриальные, борьба, использование помех, влияние помех, прослушивающие устройства, частота помехи, электромагнитные возмущения, шум, искажение сигнала.

Источники помех можно условно разделить на 2 типа – Устройства, которые генерируют сигналы высокой частоты и устройства, генерирующие импульсные помехи [1].

К источникам высокочастотных сигналов относятся радиопередатчики радиовещательных и телевизионных компаний, промышленные генераторы, станции сотовой связи и прочие приемники и передатчики сигналов [3].

Вторая условная группа создаёт мощные помехи различными электрическими механизмами, в которых происходит резкое изменение тока или напряжения в электроцепях в момент коммутации, особенно, если в этот момент образуются искры [5].

Уровень помех зависит также от расстояния, среды распространения, и «контура излучения» [10]. К последнему понятию можно отнести простые питающие и коммутирующие провода в том числе провода линий электропередач, которые непосредственно подключены к источнику индустриальных помех, например, трансформаторные будки, которые повсеместно распространены, создают огромные помехи. Неисправные системы автомобилей с двигателями внутреннего сгорания могут создавать спектр

излучения вплоть до 1 ГГц, а спектр помех по системе зажигания автомобилей находится в полосе частот 25–170 МГц [16].

Существует множество причин, из-за которых образуются индустриальные радиопомехи. Это нежелательное электромагнитное излучение носит зачастую непреднамеренный характер, однако, может быть усиленно умышленно, что в нашей стране запрещено на законодательном уровне [3].

Среди источников импульсных помех наиболее характерно резкое изменение напряжения в момент переключения, что и непосредственно вызывает помехи, зажигание автомобиля будет тому примером [12].

В высокочастотных источниках радиопомехи образуются из-за статических разрядов между находящимися под разным потенциалом отдельными частями устройств, а также, из-за излучения от элементов схем и компонентов [14].

Когда индустриальные радиопомехи через проводники или антенну попадают на чувствительные элементы радиоаппаратуры, они оказывают воздействие на ее нормальную работу искажением получаемой информации, либо приводят к полному сбою оборудования [14].

Чем больше радиоприборов расположено поблизости, тем выше вероятность того, что они могут глушить радиосигналы друг друга, а, следовательно, возможен сбой в работе [13].

Помимо работы на своей частоте каждый прибор излучает так называемый электромагнитный шум. И зачастую этот побочный радиошум может попадать в частотный спектр других устройств, приводя к сбоям.

Развитию радиоволнового конфликта способствуют мощность оборудования, а также разность частотных диапазонов полезного и мешающего сигналов [15].

В соответствии с государственными стандартами сущесвуют нормы, регулирующие максимально допустимое значение индустриальных радиопомех [2].

Несимметричное напряжение индустриальных радиопомех на зажимах для подключения оборудования к сети электропитания не должно превышать значений, приведенных в таблице 1 [8].

ТАБЛИЦА 1. Допустимые значения помех на сетевых зажимах

Полоса частот, МГц	Напряжение индустриальных радиопомех, дБмкВ	
	квазипиковое значение	среднее значение
От 0,15 до 0,5	79	66
От 0,5 до 30 вкл.	73	60

Квазипиковое значение напряженности поля индустриальных радиопомех на расстоянии 10 м от корпуса передвижного или переносного оборудования, или от границы объекта не должно превышать значений, приведенных в таблице 2.

ТАБЛИЦА 2. Квазипиковое значение напряжённости индустриальных радиопомех от корпуса оборудования

Полоса частот, МГц	Напряженность поля радиопомех, дБмкВ/м
От 30 до 230 вкл.	40
Св. 230 до 1 000 вкл.	47

Для ослабления радиопомех могут быть использованы некоторые способы, среди них:

- тщательное экранирование источников Индустриальных радиопомех;
- установка фильтров, помехоподавляющих конденсаторов в источники радиопомех;
- применение различных средств для снижения искрообразования;
- при возможности – вынесение радиоприемных устройств за пределы промышленной зоны.

Сужение полосы пропускания радиоприёмного и антенного устройства до необходимых пределов, так же снижает уровень воспроизводимых помех [9].

Индустриальные радиопомехи могут быть использованы злоумышленниками с целью маскировки частоты работы прослушивающих устройств под помеху, ежесекундно излучаемую источником [6]. Простейшим примером может являться эндовибратор, специально настроенный на включение под воздействием сверхвысокочастотной радиопомехи. Для его работы требуется лишь подача на него сигнала, этот сигнал может быть схож с излучаемой помехой бытового прибора, находящегося в помещении, которое злоумышленник желает прослушать. Таким образом, генерируемая частота подаваемая на средство прослушки, может быть замаскированно под обычную радиопомеху, что затрудняет поиск и выявление устройства [11].

Для быстрого и высокоточного измерения радиопомех могут быть использованы устройства из линейки ST. Например, многофункциональный поисковый прибор ST 500 «Пиранья». Среди функций устройства присутствует возможность сканирование определённого спектра радиочастот с целью поиска и локализации радиопередающих прослушивающих устройств. При помощи прибора можно не только установить частоту помехи, под которую маскируется прослушивающее устройство, но и довольно точно узнать его расположение [7]

Список используемых источников

1. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернбородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 525–527.

2. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.

3. Построение доверенной вычислительной среды: монография / А. В. Красов, А. М. Гельфанд, В. И. Коржик, И. В. Котенко, Р. Б. Петрив, Д. В. Сахаров, И. А. Ушаков, П. И. Шариков, Д. В. Юркин. СПб.: Индивидуальный предприниматель Петрив Р. Б., 2019. 108 с.

4. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 321–326.

5. Гельфанд А. М., Лансере Н. Н., Ложкина А. А., Фадеев И. И. Организация концептуальной модели критической информационной инфраструктуры // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 39–40.

6. Кушнир Д. В., Шемякин С. Н., Орлов Г. А. Представление некоторых аспектов отсеивания составных чисел для криптографических приложений // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 25–28.

7. Шемякин С. Н., Орлов Г. А., Холоденко В. Ю., Егорова А. Л. Оценка расстояния единственности... Для некоторых блочных шифров // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 34–38.

8. Волкогонов В. Н., Казанцев А. А., Катасонов А. И., Орлов Г. А. Анализ безопасности wi-fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 270–275.

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

10. Гераськина В. С., Сахаров Д. В., Пестов И. Е., Виткова Л. А. Методы и стратегии оповещения населения об угрозах возникновения кризисных ситуаций // Информационная безопасность регионов России (ИБРР-2017): материалы конференции. 2017. С. 507–509.

11. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Материалы XVI Санкт-Петербургской международной конференции "Региональная информатика "РИ-2018" (Санкт-Петербург, 24-26 октября 2018 г.). СПб., 2018. С. 570–571.

12. Sharikov P. I., Krasov A. V., Gelfand A. M., Kosov N. A. Research of the Possibility of Hidden Embedding of a Digital Watermark Using Practical Methods of Channel Steganography // Proc. Int. Symp. on Intelligent and Distributed Computing (Berlin, Germany: Springer), pp. 203–9, 2019.

13. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 2. С. 262–266.

14. Казанцев А. А., Красов А. В., Катасонов А. И., Гельфанд А. М. Создание и управление security operations center для эффективного применения в реальных условиях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 590–595.

15. Красов А. В., Волкогонов В. Н., Волостных В. А., Гельфанд А. М., Катасонов А. И. Способы коммутации пакетов в сетях Cisco // Материалы Всероссийской научно-практической конференции "Национальная безопасность России: актуальные аспекты" ГНИИ "Нацразвитие". Июль 2018. Сборник избранных статей. 2018. С. 31–35.

16. Гельфанд А. М., Пестов И. Е., Катасонов А. И., Рязанцев К. С. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2018. № 8. С. 91–97.

Статья представлена научным руководителем, заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.5
ГРНТИ 81.93.29

ИНТЕРНЕТ ВЕЩЕЙ (IoT): УГРОЗЫ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

А. М. Гельфанд, А. А. Казанцев, А. В. Красов, В. Р. Уляшева

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

Интернет вещей (IoT) используется для обеспечения связи между многочисленными устройствами. Это система, в которой объекты, встроенные в технологию датчики, взаимодействуют с другими объектами через беспроводную среду связи для обмена и передачи информации без взаимодействия с человеком. Цель данной статьи состоит в том, чтобы выдвинуть различные проблемы безопасности и конфиденциальности, с которыми сталкивается среда Интернета Вещей, а также существующие механизмы, используемые для ее защиты.

конфиденциальность, угрозы безопасности, RFID, WSN, Интернет вещей.

Интернет вещей (IoT) играет важную роль в повседневной жизни каждого человека. Это услуга, которая позволяет передавать данные от человека к объекту или от объекта к объекту. Приложения IoT используются во многих областях, таких как мониторинг окружающей среды, домашняя

автоматизация, транспорт, системы здравоохранения и т. д. Эволюция Интернета вещей одно из важнейших событий предшествующего временного промежутка. Такие технологии, к*ак* WSN и RFID-метки, развивающийся по мере увеличения масштабов Интернет технологий, создают прямую связь через Интернет. Следовательно, было совершено огромное количество атак и угроз против безопасности и конфиденциальности умных устройств. Без надлежащей защиты устройства Интернета Вещей с большей вероятностью будут использоваться в злонамеренных целях [2]. Поэтому важно понимать угрозы и решения, как для безопасности, так и для конфиденциальности.

Безопасность и конфиденциальность

Системы, основанные на IoT, управляют большим количеством информации, которая может быть использована для различных услуг, что делает парадигму IoT интересной мишенью для множества злоумышленников. Потенциальные злоумышленники могут быть заинтересованы в краже конфиденциальной информации, такой как данные о местоположении, номера кредитных карт, пароли финансовых счетов и т. д. [3].

Угрозы безопасности

Беспроводная сенсорная сеть *(Wireless Sensor Network = WSNs): WSNs* легко подвержены атакам безопасности интернета вещей из-за среды передачи [5]. Некоторые из основных угроз *WSN*:

1. Физические атаки: Изменение доступных данных в узле/датчике.
2. Репликация узла: Клонирование идентификатора узла/датчика в ту же сеть, что приводит к дублированию и неправильной маршрутизации пакетов.
3. Выборочная переадресация: Вредоносный узел выборочно пересылает пакеты или отбрасывает сообщения, не пересылая их.
4. Атака типа «червоточина»: Критическая атака, при которой происходит туннелирование пакетов от одного узла сети в другой, что приводит к нарушению маршрутизации [7].
5. Атака Сивиллы: Вид атаки в одноранговой сети, в которой жертва подключается к узлам, контролируемым злоумышленником.
6. Атака Воронки: Захват узла внутри сети и притягивание трафика с соседних узлов.
7. Атака «отказ в обслуживании» (DDoS-атака): Доведение системы до отказа, путем наводнения запросами, отправленными пользователями [8].
8. Перехват трафика: Злоумышленник перехватывает информацию во время передачи данных между двумя узлами.

Радиочастотная идентификация (*Radio Frequency Identification = RFID*):

Типы атак на технологию RFID-меток:

1. Физическое изменение данных: Злоумышленник физически получает метку, а затем модифицирует данные в ней.

2. Клонирование метки: Исходная метка заменяется новой и в нее копируется исходный идентификатор (id) [4].

3. Замена меток: Обмен метками двух разных продуктов [4].

4. Атака отказа в обслуживании: Нарушение отправки идентификатора метки считывателю в результате DDoS-атаки.

Решения безопасности для Беспроводных сенсорных сетей (*WSNs*)

Некоторые из решений, касающихся беспроводных сенсорных сетей, заключаются в следующем:

1. Общие ключи: Использование системы управления ключами, поддерживаемой IoT-устройствами с ограниченными ресурсами [6].

2. Защищенная группировка: *WSN* состоит из большого количества узлов, которые являются компактными и автономными. Сенсорные узлы необходимы для обеспечения связи между устройствами в одной группе. Для выполнения конкретной задачи важно, чтобы члены группы могли безопасно общаться друг с другом.

3. Шифрование: Использование таких методов, как коды аутентификации сообщений, схемы шифрования симметричных ключей и криптография с открытым ключом [6].

4. Безопасная агрегация данных: Использование устойчивых функций, которые обнаруживают и сообщают о поддельных сообщениях [5].

5. SPINS: Протоколы безопасности для сенсорных сетей, которые обеспечивают множество свойств, таких как аутентификация данных, свежесть данных, семантическая безопасность, низкие коммуникационные издержки и защита от воспроизведения [5].

6. TinySec: Архитектура безопасности канального уровня поддерживает два параметра безопасности: аутентифицированное шифрование, где кодируется полезная нагрузка данных; режим только аутентификации, где не применяется кодирование полезной нагрузки данных, а аутентифицируется с помощью MAC-адреса.

Физические решения безопасности для радиочастотной идентификации (RFID).

1. Удалить метку: Отключение функции метки, чтобы остановить ее отслеживание [4].

2. Клетка Фарадея: Хранение метки в клетке Фарадея для предотвращения возможности перехвата информации с целью дальнейшего клонирования.

3. Остановка метки: Использование стопорной метки для предотвращения обмена сообщениями.

Протокол безопасности RFID – программный механизм безопасности, основанный на технике секретного кода, более приветствуется пользователями, чем аппаратные механизмы, методы которых основаны на физическом коде [4]

В [1] предложен протокол хэш-блокировки, который использует meta-ID для замены реального идентификатора метки, чтобы информация не отслеживалась и не перехватывалась. Поле Meta-ID однозначно, и в него не вносятся никакие изменения. Более того, идентификатор передается обычным текстом по небезопасному каналу. Таким образом, вероятно, что протокол, может быть, уязвим перед атаками подмены имени или ретрансляции.

Угрозы конфиденциальности

1. Идентификация: Угрозы связывания идентификатора, такого как адрес или имя с конкретным устройством.

2. Локализация и отслеживание: Угроза определения и документирования местоположения человека во времени и пространстве [3].

3. Профилирование: Угроза сбора или организации информационного досье о физических лицах с целью выведения интересов путем корреляции с другими профилями и данными [7].

4. Раскрытие личной информации: Угроза передачи конфиденциальных данных через незащищенные каналы, а так же перехват злоумышленниками [3].

Решения для сохранения конфиденциальности

В ходе работы было предложено несколько подходов для решения проблем конфиденциальности:

1. Использование криптографических методов и манипулирование информацией.

2. Увеличение осведомленности о конфиденциальности: Информирование пользователей о том, что интеллектуальные устройства, такие как фитнес-браслеты, умные телевизоры, системы мониторинга здоровья и датчики умного дома могут собирать персональные данные.

3. Контроль доступа к устройствам.

4. Минимизация данных: Ограничение объема персональных данных и уменьшение срока их хранения поставщиками услуг Интернета вещей.

Заключение

Интернет вещей – это новая технология, которая добилась значительного прогресса в стандартизации технологий. В данной статье рассматриваются основные угрозы и их соответствующие решения, которые определяются путем выявления различных областей, чувствительных к атакам безопасности и конфиденциальности. Современные проблемы должны рассматриваться как расширяющаяся возможность, которая включает в себя намерения безопасности на ранней стадии разработки и успешное применение ответов, регулируемых безопасностью, на этапе производства. В качестве будущей перспективы для защиты Интернета вещей могут быть разработаны более совершенные системы безопасности, которые могут решать проблемы конфиденциальности через все границы.

Необходимы дальнейшие исследования для разработки и проектирования, соответствующих механизмов безопасности, устойчивые к различным типам атак.

Список используемых источников

1. Wang Q. et al. Low-Cost RFID: security problems and solutions // 2011 International Conference on Management and Service Science. IEEE, 2011. pp. 1–4.

2. Сахаров Д. В., Гельфанд А. М., Казанцев А. А., & Пестов И. Е. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IoT-сети // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2020. № 2. С. 86–94.

3. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернобородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. С. 525–527.

4. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. №. 1 (7). С. 19–24.

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

6. Таргонская А. И., Цветков А. Ю. Разработка защищенного веб-интерфейса для управления устройствами в сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 734–739.

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

8. Красов А. В., Ушаков И. А., Щипцов Д. И. Анализ уязвимостей релевантных решений в области обеспечения безопасности SDN-сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая

и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 611–616.

УДК 612.82:004.5
ГРНТИ 34.55.19

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ НЕЙРОГАРНИТУР: МЕТОДЫ ОБРАБОТКИ СИГНАЛА И АКТУАЛЬНОСТЬ ТЕХНОЛОГИИ

В. К. Гераськин, В. С. Елагин, Е. Е. Ермолаев, И. О. Федотов

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

В настоящее время в связи с удешевлением производства микроэлектроники и повышения точности измерительных приборов становиться проще и дешевле проводить научные эксперименты, которые ранее считались недостижимыми для лабораторий и гражданских исследователей со скромным бюджетом.

В данной статье рассматривается современный рынок нейроинтерфейсов, спектр их применения, а также будут затронуты методы анализа сигнала.

нейроинтерфейсы, электроэнцефалограмма, быстрое преобразование Фурье, мозговая активность.

Нейроинтерфейсы или же нейро-гарнитуры - точный измерительный прибор, который, получая данные из биосигналов, взятых с поверхности скальпа, преобразует их в сигнал так называемой электроэнцефалограммы (ЭЭГ).

Автоматическая расшифровка данных ЭЭГ является приоритетной задачей, стоящей перед исследователями. ЭЭГ может быть разложено на гармоники или же волны мозга. В дальнейшем же с помощью специально обученного человека или автоматических алгоритмов данные гармоники интерпретируются для той или иной цели: определение расхождения с нормалью для диагностики патологий в мозге, для интерпретации данных в научных целях в т. ч. прогнозирования того или иного критерия мозговой активности, наблюдение за активностью во время тех или иных действий.

На рынке представлены различные устройства, которые могут считывать и обрабатывать сигналы мозга, обладающими качествами, которые отличают его от его компетенции, будь то его стоимости, количества электродов, используемая технология и т. д. Основными производителями сенсоров

этого типа являются NeuroSky, Muse, Emotiv, Texas Instrument и другие (рис. 1).

Исходя из целей данной работы и анализируя каждое из устройств, доступных на рынке, серия ThinkGear-AM1 компании NeuroSky является фаворитом, несмотря на то что у него всего один электрод. У него есть необходимый набор инструментов для разработчиков для его применения и адаптации под конкретные задачи. Также важным фактором является его цена, поскольку он значительно дешевле по сравнению с аналогами [1].

Рис. 1. Носимые ЭЭГ устройства

ТАБЛИЦА. Сравнение биосенсоров ЭЭГ

Модель	Muse	EOTIV Insight	EMOTIV EPOC+	TGAM1
Компания	InteraXon	Emotiv	Emotiv	NeuroSky
Выпуск	Апрель-14	Август-15	Декабрь-09	Март-11
Сенсоры	ЭЭГ	ЭЭГ	ЭЭГ	ЭЭГ
Электроды	14	5	14	1
АЦП	16 бит	14 бит	16 бит	12 бит
Частота опроса	220-500 Гц	128 Гц	128-256 Гц	512 Гц
Входное напряжение	2 мВ	0.51 В	8.4 мВ	1 мВ
Время работы на полном заряде	5 часов	4 часа	12 часов	8 часов
Платформы	Android iOS	MacOS Windows Linux Android iOS	MacOS Windows Linux Android iOS	MacOS Windows Android iOS

Модель	Muse	EOTIV Insight	EMOTIV EPOC+	TGAM1
Интерфейс	Bluetooth 2.1	Bluetooth 4.0	Bluetooth 4.0	Bluetooth 2.1
Цена	249$	299$	799$	50$

Таким образом мы получили сравнительный анализ систем биологической обратной связи под названием нейрогарнитуры. В конечном итоге выбор пал на системы, использующие чип TGAM1. Они просты в конфигурировании и могут использоваться в небольших исследованиях, где не требуется высокая точность, так как покрывают её где-то в 90 %.

Зачастую такие чипы используются в системах для конечного потребителя, предназначенные для медитации и управлению устройств, с помощью регулируемых человеком альфа-волн [2] (рис. 2).

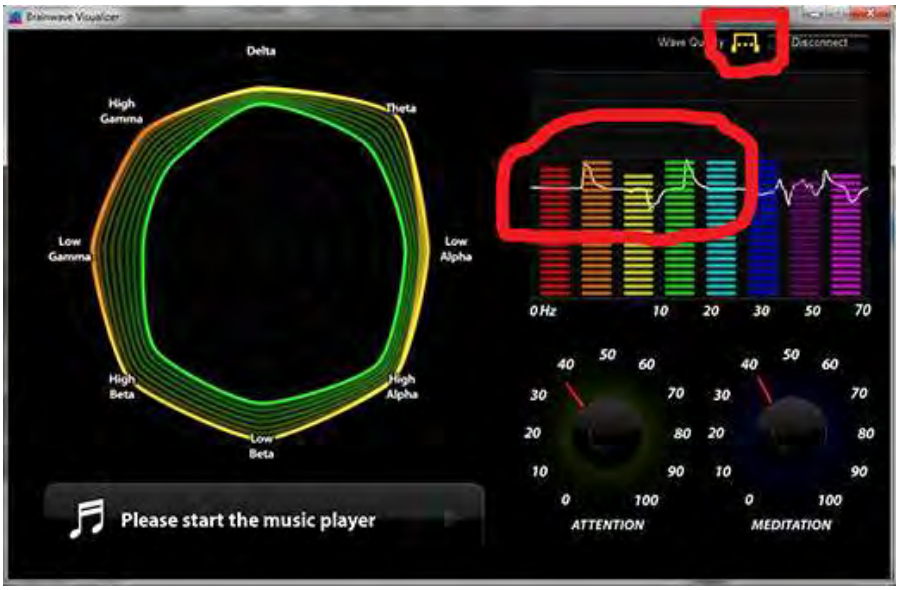


Рис. 2. Пример прикладного ПО для медитации

В ней используется БПФ (Быстрое преобразование Фурье), для анализа «Сырого сигнала».

Проведенные эксперименты более чем полностью покрыли изначальные требования (рис. 3).

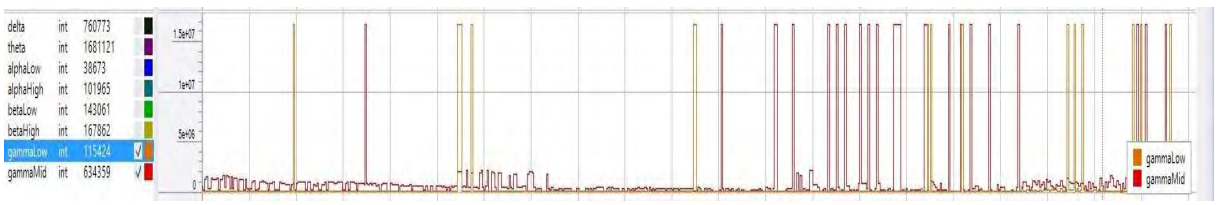


Рис 3. Исследование внимание и сосредоточенности при игре в гоночный симулятор

Дальнейшая работа предполагает сборку системы для более обширного исследования мозга, как увеличение количества каналов, так и применение более современных математических моделей для анализа сигнала, конструирование гибких шлемов [3] для удобного использования во всех местах скальпа, для гибкой возможности перенастройки датчиков, для изучения разных областей мозга. Написание прикладного программного обеспечения для шлема, так как в данный момент не существует достойных программ, которые бы распространялись по свободной лицензии.

В связи с развитием технологий, в частности машинного обучения становится возможным начать предсказывать показания мозга, в отделах, отвечающих за движение, моторику.

В современном мире, с большими темпами роста технологий нельзя обойти стороной исследование нейрокибернетики, биоинформатики, так как она позволяет получить ещё одну обратную связь на наши реакции [4].

Естественная эволюция в целом является медленной случайной последовательностью, а искусственная эволюция же напротив – создаёт вещи более узкие и в категорически меньшие сроки. Наш аналоговый «вывод» сейчас только наша мускулатура. Так в будущем, возможно, технология нейрогарнитур и многие, связанные с ними будут использованы для коррекции болезней, которые до этого считались неизлечимыми. А позже и для более глубокого взаимодействия технологий и людей, для более релевантного подбора рекомендаций для пользователей, интеграции людей с информационными системами, помощью людей с рассеянным вниманием, так и для увеличения качества обучения детей. Надеюсь, что это поможет сделать наш мир лучше.

Список используемых источников

1. Спецификация чипа TGAM1. URL: https://cdn.sparkfun.com/datasheets/Sensors/Biometric/tgam1.pdf

2. Компаниец В. С., Лызь А. Е. Возможности и перспективы применения инструментальных методов исследования пользовательского опыта. URL: https://sfedu.ru/files/upload/per/56755/7-11.pdf

3. Филипович О. В., Кошевая Д. О., Кадыков Н. Ю., Камцев В. А., Гомонюк А. Д. Применение САПР при проектировании корпуса обруча нейрогарнитуры. URL: http://www.niiatm.ru/misapr/article242

4. Aleksandra P., Leon C., Mikołaj M., Peter G., Muse Headband: Measuring Tool or a Collaborative Gadget? January 2017. URL: https://www.researchgate.net/publication/319944874_Muse_Headband_Measuring_Tool_or_a_Collaborative_Gadget

УДК 004.057.5
ГРНТИ 20.53.23

РАЗРАБОТКА ВЕБ-ИНТЕРФЕЙСА ДЛЯ СИСТЕМЫ МОНИТОРИНГА БЕСПРОВОДНЫХ СЕТЕЙ СЕМЕЙСТВА IEEE 802.11

Е. Ю. Герлинг, М. М. Ковцур, А. Э. Фёдорова

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

Веб-приложения уже давно плотно укоренились в жизни современного человека. Главным преимуществом таких приложений является возможность их использования без необходимости установки дополнительного программного обеспечения, так как вся работа происходит с помощью браузера. Среди других положительных качеств можно выделить отсутствие необходимости обновлений на рабочем месте пользователя и хранение основных файлов конфигурации на сервере, что упрощает создание резервных копий и сохранение безопасности данных. Веб-интерфейсы применяются для работы с различными онлайн-сервисами, а также для настройки и подключения к сетевым устройствам, таким как маршрутизаторы, модемы, видеокамеры. В данной статье уделено внимание особенностям реализации веб-интерфейса для встроенного устройства, обладающего крайне ограниченными ресурсами.

веб-интерфейс, беспроводные сети, система мониторинга.

Использование веб-приложений уже долгое время входит в повседневную жизнь многих людей. И с каждым годом такие приложения набирают всё большую популярность, так как для взаимодействия с ними пользователю необходимо использовать лишь браузер, который установлен по-умолчанию в большинство операционных систем. Это упрощает доступ к необходимым ресурсам, обеспечивает удобство взаимодействия через мобильное устройство, персональный компьютер или ноутбук.

В современном мире множество маршрутизаторов, коммутаторов, модемов и других маломощных сетевых устройств поддерживает управление и настройку через веб-интерфейс.

Вследствие вышеизложенного появилась необходимость создания веб-приложения для системы мониторинга беспроводной сети, осуществляющей работу на низкопроизводительном устройстве. Данная система мониторинга имеет возможность создавать дампы трафика и обнаруживать аномалии в беспроводной сети.

Устройства, обладающие ограниченными ресурсами, имеют ряд особенностей. Далее на примере одноплатного компьютера Raspberry приводятся отличительные характеристики таких устройств [1]. К ним относятся:

– ограничение в энергопотреблении;
– небольшой запас постоянной памяти;
– отсутствие возможности увеличить оперативную память;
– медленная скорость работы.

При разработке веб-интерфейса для системы мониторинга беспроводной сети, развёрнутой на таком устройстве, требуется учитывать изложенные выше особенности, а также их влияние на работу необходимых сервисов.

Для демонстрации структуры решения используется виртуальная машина с операционной системой Ubuntu Server, обладающая 1 CPU и объёмом оперативной памяти равным 1 GB. Данные параметры идентичны характеристикам одноплатного компьютера Raspberry Pi 3 Model B.

В качестве веб-сервера выбран Apache HTTP-сервер. Он представляет собой открытое программное решение, а также распространяется абсолютно бесплатно. Среди других преимуществ можно выделить тот факт, что его лицензия позволяет конечному пользователю редактировать исходный код, чтобы адаптировать Apache под собственные нужды. Следует отметить, что 2019 году web-сервер Apache вошел в тройку лидеров рейтинга самых популярных веб-серверов в рунете [2].

В отличие от веб-сервера Internet Information Services, который работает только с Windows и поставляется в комплекте с этой операционной системой, и веб-сервера Nginx, который в свою очередь осуществляет лишь некоторую поддержку Windows, Apache является кроссплатформенным решением и поддерживается на Windows, Linux, Unix и Mac OS в полной мере.

Для хранения логов и информации о пользователях выбрана база данных MySQL. Она бесплатна в большинстве случаев, а также является многопоточной, то есть поддерживает несколько одновременных запросов. База данных MySQL может быть использована для работы и с малыми, и с большими объемами данных. Так как она сочетает в себе продвинутый функционал и свободный доступ к исходному коду, MySQL обладает большими возможностями, чем, например, SQLite. Другой положительной стороной этой базы данных становится наличие в сети Интернет множества руководств по освоению системы и огромное количество всевозможных плагинов и расширений, упрощающих работу с этой системой.

База данных MySQL обладает более высокой производительностью, чем её некоммерческие конкуренты. Например, при простых операциях чтения PostgreSQL может значительно снизить работу сервера и быть медленнее, чем MySQL [3].

Для написания кода веб-интерфейса используется внутренний язык программирования PHP. Согласно Wappalyzer – приложению, которое позволяет определить используемые технологии на сайте, 82 % всех сайтов в интернете сделаны на PHP. PHP-код обычно рекомендуется использовать

в сочетании с HTML, но он с таким же успехом интегрируется и в JavaScript, WML, XML и другие языки. Положительной стороной данного языка является возможность составлять PHP-программу отдельно от разработки веб-страницы, а также следует отметить, что PHP не содержит кода, ориентированного на конкретный веб-сервер. PHP-программы не имеют проблем с зависимостью от браузеров и обладают высокой скоростью работы, что в свою очередь повышает общую производительность ресурсов [4].

На рис. 1 приведена структура вышеизложенного решения.

Рис. 1. Структура веб-интерфейса

Разработанный веб-интерфейс включает в себя страницу аутентификации с возможностью ввести логин и пароль, журнал с отображением логов, в котором пользователь сможет просматривать время обнаружения аномалий и их тип, зафиксированный системой мониторинга, а также раздел Dump, функционал которого позволяет создать дамп трафика и впоследствии его сохранить на свой персональный компьютер. Результаты работы представлены на рис. 2.

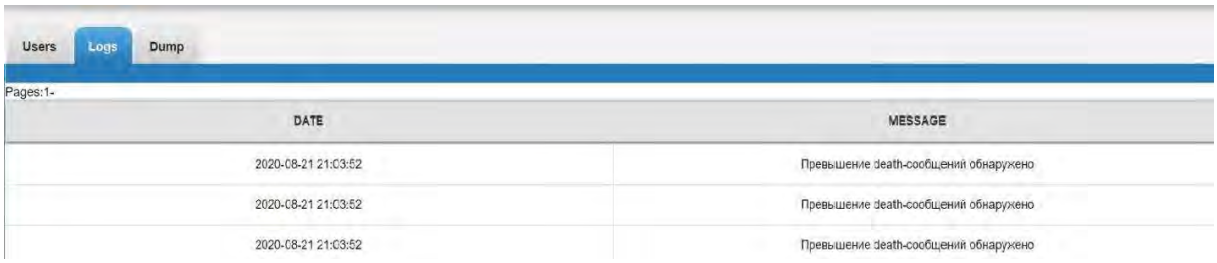


Рис. 2. Веб-интерфейс для системы мониторинга беспроводной сети

Для обеспечения безопасности полученного решения необходимо определить типы атак на веб-приложения [5]. К ним относятся:

– атаки на веб-сервер;

– атаки на базу данных;

– атаки на операционную систему.

Чтобы повысить уровень защиты веб-сервера необходимо совершать регулярные обновления Apache, отключить ненужные модули данного сервера, скрыть версию Apache и имя используемый операционной системы сервера, а также отключить список каталогов [6].

Защитить от пассивного прослушивания веб-сервер позволяют SSL-сертификаты. Сертификат SSL – это популярный тип цифрового сертификата, который привязывает информацию о владельце веб-сервера к ключу шифрования. Эти ключи используются в протоколе SSL/TLS для создания безопасной сессии между браузером и веб-сервером, на котором расположен SSL-сертификат. Центры сертификации выдают множество типов сертификатов. Сертификаты, выданные центрами сетификации, обеспечивают безопасность транзакций на веб-сайте, защиту от вредоносных программ и проверку подлинности документов и обменов электронной почтой. Существует возможность использования самоподписанных сертификатов, но она не гарантирует клиентам, что сервер является именно тем сервером, который им нужен. Преимуществом самоподписанных сертификатов является их бесплатность [7].

Для снижения рисков возникновения чрезвычайных ситуаций, связанных с атаками на базу данных MySQL, нужно настроить плагин валидации паролей (VALIDATE PASSWORD PLUGIN). При включении данного плагина будет предложено установить уровень надёжности паролей при валидации. Например, при выборе значения 2 (самый строгий уровень валидации), будут выдаваться ошибки при попытке задать пароль без цифр, букв в верхнем и нижнем регистре, а также без специальных символов. Также следует рекомендовать пользователям не использовать базу данных с правами пользователя root и обязательно настроить специальную учётную запись для взаимодействия с базой данных.

Подводя итог вышеизложенному следует отметить, что разработка веб-интерфейса для системы мониторинга беспроводной сети семейства IEEE 802.11, развёрнутой на маломощном устройстве, является трудоёмким процессом и требует учитывать различные особенности работы веб-приложения при ограниченных ресурсах и дополнительно анализировать решения, выбранные для реализации данного сервиса.

Список используемых источников

1. Габуев А. Г., Красов А. В., Ощенков Ф. Д., Тарасов Н. М. Анализ защищённости современных средств передачи информации посредством портативной лаборатории на основе микрокомпьютера Raspberry Pi // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 295–298.

2. Завражнова М. В., Родкина Э. А., Шошина А. В. Разработка базы данных и веб-интерфейса научной электронной библиотеки // Colloquium-journal. 2019. № 19-1 (43). С. 31–34.

3. Ахрамеева К. А., Ковцур М. М., Михайлова А. В. Обеспечение информационной безопасности баз данных web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 107–110.

4. Ковцур М. М., Луеке П. Э. Разработка системы учёта посещаемости студентов масштаба вуза // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 532–537.

5. Таргонская А. И., Цветков А. Ю. Разработка защищенного веб-интерфейса для управления устройствами в сети // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 734–739.

6. Жамишева Н. М., Ташенова Ж. М. Исследование и анализ защиты веб-ресурсов от атак // Актуальные научные исследования в современном мире. 2019. № 12-4 (56). С. 85–89.

7. Стригин С. А. Разработка веб-сайта с применением безопасного стека технологий // Информационная безопасность: современная теория и практика. Сборник научных трудов студентов, аспирантов и преподавателей по материалам III Межвузовской научно-практической конференции / Ответственный редактор З. В. Семенова. Омск, 2020. С. 103–111.

УДК 621.39, 530.182
ГРНТИ 49.44.31

ИСПОЛЬЗОВАНИЕ ОПТИЧЕСКИХ УСИЛИТЕЛЕЙ EDFA ДЛЯ ПОДДЕРЖАНИЯ КВАЗИСОЛИТОННОГО РЕЖИМА РАСПРОСТРАНЕНИЯ СИГНАЛОВ ПО ОДНОМОДОВЫМ ВОЛОКНАМ СО СМЕЩЕННОЙ ДИСПЕРСИЕЙ

С. Ф. Глаголев, В. С. Горсков, С. Э. Доценко

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

В работе рассмотрен метод поддержания квазисолитонного режима в одномодовых волокнах со смещенной дисперсией с помощью эрбиевых оптических усилителей (EDFA). Теоретические расчеты и моделирование показали, что существует ограничение на длину усилительного участка. Получены формулы для выбора технических решений при проектировании квазисолитонных волоконно-оптических систем связи.

одномодовое оптическое волокно со смещенной дисперсией, хроматическая дисперсия, фазовая самомодуляция, солитон, квазисолитонный режим, оптический усилитель.

С помощью нелинейного уравнения Шредингера (НУШ), для оптического волокна (ОВ) без затухания, можно описать процессы распространения оптических импульсов (далее – импульс) произвольной формы по одномодовым оптическим волокнам (ОМ ОВ) [1, 2, 3]

$$i\frac{du}{dZ}+\frac{1}{2}\cdot\frac{d^2u}{d\tau^2}+|u|^2\cdot u=0,\ u(Z,\tau)=N\cdot\frac{E_m(Z,\tau)}{|E_m(0,0)|}, \quad (1)$$

где $u(Z,\tau)$ – нормированная комплексная амплитуда напряженности электрического поля $E_m(Z,\tau)$ световой волны распространяющейся в направлении Z на оси ОМ ОВ;

$Z=z/L_D$ – нормированное расстояние вдоль ОМ ОВ;

L_D – дисперсионная длина ОВ;

$N^2=L_D/L_{NL}$, L_{NL} – нелинейная длина ОВ;

$|E_m(0,0)|$ – модуль $E_m(Z,\tau)$ на входе ОМ ОВ;

$\tau = T/T_0$ – нормированное время, отсчитываемое от середины импульса с полушириной T_0.

Решить прямую задачу нахождения спектра и формы произвольных импульсов на выходе ОМ ОВ с известными параметрами позволяет НУШ (1). Для нахождения параметров импульса на входе ОМ ОВ необходимо решить обратную задачу, это позволит определить требуемые начальные условия, для сохранения своей форму при распространении по ОМ ОВ на безгранично большие расстояния. Такой импульс может существовать и распространяться в ОМ ОВ с положительной хроматической дисперсией (ХД) и с учетом равенства $L_D = L_{NL}$, то есть при $N = 1$. За счет нелинейного эффекта фазовой самомодуляции (ФСМ) происходит полная компенсация ХД. Для этого импульс должен обладать определенной пиковой мощностью и иметь форму гиперболического секанса

$$P_{m\Phi}=\frac{|\beta_2|}{\gamma\cdot T_0^2},\ u(Z,\tau)=\mathrm{sech}(\tau)\cdot\exp(i\cdot\frac{Z}{2}). \quad (2)$$

Такой импульс называют – фундаментальный солитон. Распространение фунтаментального солитона описывается выражением (2), в котором набег фазы пропорционален расстоянию, а с увеличением расстояния пиковая мощность не меняеться.

Рассмотрим возможность поддержания близкого к солитонному режиму – квазисолитонный режим распространения секансных импульсов в реальном ОМ ОВ с потерями. Затухание приводят к уменьшению пиковой мощности импульса при распространении по ОВ (увеличение расстояние *Z)*. Пиковая мощность уменьшается и её становиться недостаточно для поддержания квазисолитонного режима, импульс расширяется и затухает.

Для компенсации затухания рассмотрим возможность применения оптических усилителей (ОУ) EDFA. В волоконно-оптической линейном тракте (ВОЛТ) ОУ EDFA устанавливаются через расстояние L_A. Идея метода управления затуханием заключается в сохранении на каждом усилительном участке (УУ) длиной L_A средней величины пиковой мощности $\overline{P_m}$ равной пиковой мощности фундаментального солитона $P_{m\Phi}$ в ОМ ОВ без затухания

$$\overline{P_m} = P_{m\Phi} = \frac{1}{L_A}\int_0^{L_A} P_m(Z)\cdot dz. \quad (3)$$

Величина пиковой мощности на входе УУ $P_m(0)$ должна значительно превышать мощность фундаментального солитона $P_{m\Phi}$. В таком случае длительность импульса вначале УУ с увеличением расстояния уменьшается за счет эффекта ФСМ, достигнув минимума, начинает увеличиваться за счет ХД до исходного состояния.

В процессе восстановления квазисолитонный импульс теряет часть своей энергии в виде рассеянного излучения. Рассеянное излучение накапливается в ВОЛТ, состоящий из нескольких УУ, до значительного уровня и искажает форму секансного импульса. Для уменьшения искажений импульсов и стоимости волоконно-оптической системы связи (ВОСС) нужно выбирать максимально возможную длину L_A в соответствии с условием (4) [1, 2, 3]

$$L_A \le L_D = \frac{T_0^2}{|\beta_2|}. \quad (4)$$

НУШ для моделирования процессов распространения секансых импульсов в ВОЛТ, состоящий из ОУ EDFA, расположенных на расстоянии L_A (рис. 1) можно использовать в следующей форме [1, 2, 3]

$$i\frac{du}{dZ} + \frac{1}{2}\cdot\frac{d^2u}{d\tau^2} + |u|^2\cdot u = -\frac{i}{2}\cdot u\cdot L_D\cdot[\alpha - g(Z)],$$
$$g(Z) = \sum_{m=1}^{N_A} g_m\cdot\delta(Z - Z_m), \quad (5)$$

где $g(Z)$ – функция дискретного усиления,

α – коэффициент затухания ОВ,

g_m – усиление ОУ.

Для упрощения анализа выполним преобразование [1, 2, 3]

$$u(Z,\tau) = \sqrt{p(Z)}\cdot v(Z,\tau), \quad (6)$$

где $p(Z)$ – функция быстро меняющаяся в пределах одного УУ,

$v(Z,\tau)$ – функция медленно меняющаяся в пределах всего ВОЛТ.

Подставим (6) в (5) и найдем, что $v(Z,\tau)$ удовлетворяет уравнению

$$i\frac{dv}{dZ}+\frac{1}{2}\cdot\frac{d^2v}{d\tau^2}+p(Z)\cdot|v|^2\cdot v=0, \qquad (7)$$

в котором $p(Z)$ удается решить обыкновенным дифференциальным уравнением (ДУ)

$$\frac{dp}{dZ}=[g(Z)-\alpha]\cdot L_D\cdot p. \qquad (8)$$

Решение ДУ (8) находиться аналитически, учитывая дискретное усиление обеспечивающее периодичность функции $p(Z)$. Функция $p(Z)$ экспоненционально убывает на каждом периоде как

$$p(Z)=p(0)\exp(-\alpha L_D Z).$$

В конце периода начальное значение функции $p(0)=p(Z_A)=1$ восстанавливается. Она описывает относительные изменения пиковой мощности импульса между двумя ОУ. Например, для ОВ с потерями $\alpha = 0{,}25$ дБ/км функция $p(Z)$ на УУ изменяется в 10 раз, если $L_A = 40$ км.

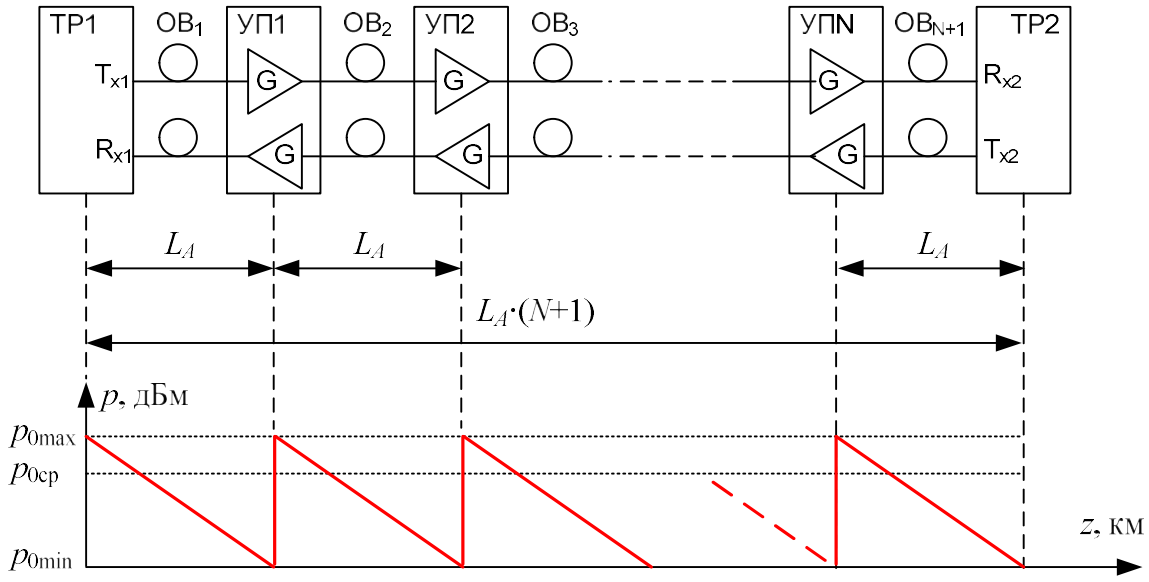


Рис. 1. Схема ВОЛТ с использованием ОУ EDFA

Резкое изменение энергии квазисолитонного оптического импульса секансной формы $p(Z)$ сопровождается изменением формы и длительности импульса и испусканием рассеянного излучения. На расстоянии $L_A \le L_D$,

сильно меняеться пиковая мощность квазисолитонного импульса, а длительность и форма меняются сравнительно мало.

В уравнении (7) заменим средним значением $\bar{p}$ функцию $p(Z)$. Введя другую переменную $u = v\sqrt{\bar{p}}$, уравнение (7) сводится к стандартному НУШ (1) для ОМ ОВ без затухания. Одним из его решений является усредненный по длине ОВ солитон.

Определим усиление G для ОУ, требуемое для компенсации затухания α на УУ, и среднее значение относительных изменений пиковой мощности $\bar{p}$ на УУ

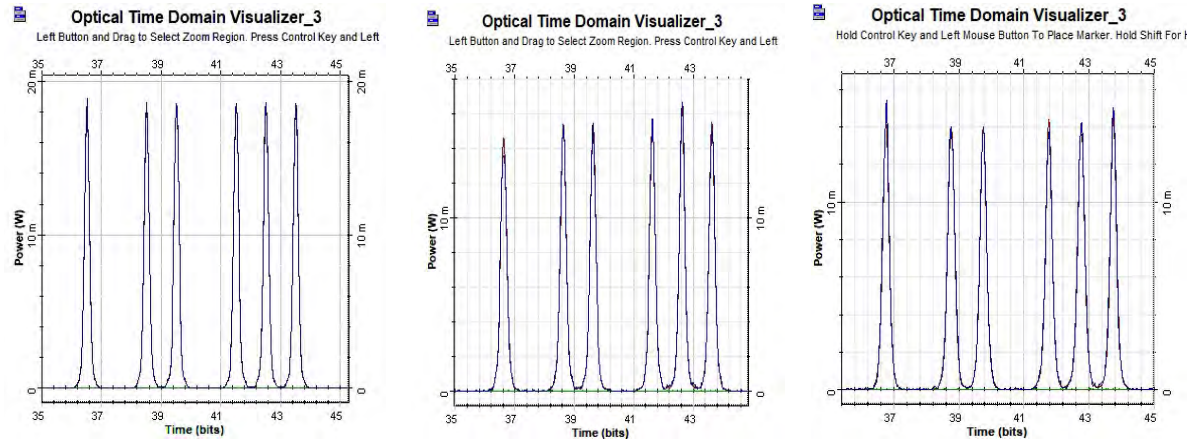
$$G = \exp(\alpha \cdot L_A),\ \bar{p} = \left(\frac{1}{\alpha \cdot L_A}\right) \cdot [1 - \exp(-\alpha \cdot L_A)] = \frac{L_{ef}}{L_A}, \quad (9)$$

где L_{ef} – эффективная длина ОМ ОВ длиной L_A, причем L_{ef} всегда меньше L_A.

Необходимую пиковую мощность для квазисолитонного режима определим с помощью уравнения

$$P_m(0) = \frac{P_{m\Phi}}{\bar{p}} = P_{m\Phi} \cdot \frac{\alpha \cdot L_A}{1 - \exp(-\alpha \cdot L_A)} = P_{m\Phi} \cdot \frac{L_A}{L_{ef}}. \quad (10)$$

Проведем расчеты параметров и моделирование ВОЛТ квазисолитонной ВОСС, использующей ОМ ОВ типа DSF со следующими параметрами: α = 0,22 дБ/км, коэффициент хроматической дисперсии D_x = 1 пс/(нм км), крутизна дисперсионной характеристики S_x = 0,085 пс/(нм^2 км), β_2 = 1,27 пс^2/км, коэффициент нелинейности γ = 2,6 1/(Вт м). Примем B = 10 Гбит/с, а длительность секансного импульса на уровне половины амплитуды t_u = 20 пс. В результате расчетов получим: T_0 = 11,34 пс, L_D = 100 км (4), $P_{m\Phi}$ = 3,8 мВт (3) и L_{ef} = 18 км (10). Выбираем L_A = 80 км, т. е. меньше L_D и рассчитаем коэффициент усиления ОУ G = 17,6 дБ (9) и $P_m(0)$ = 18 мВт (10). На рис. 2 показаны импульсы на выходе ВОЛТ, состоящего из одного УУ (80 км), 8-х УУ (640 км) и 16 УУ (1 280 км). Результаты измерений приведены в таблице.



а б в

Рис. 2. Импульсы на выходе ВОЛТ 1 УУ, 80 км (а), 4 УУ, 640 км(б), 16 УУ, 1 280 км (в)

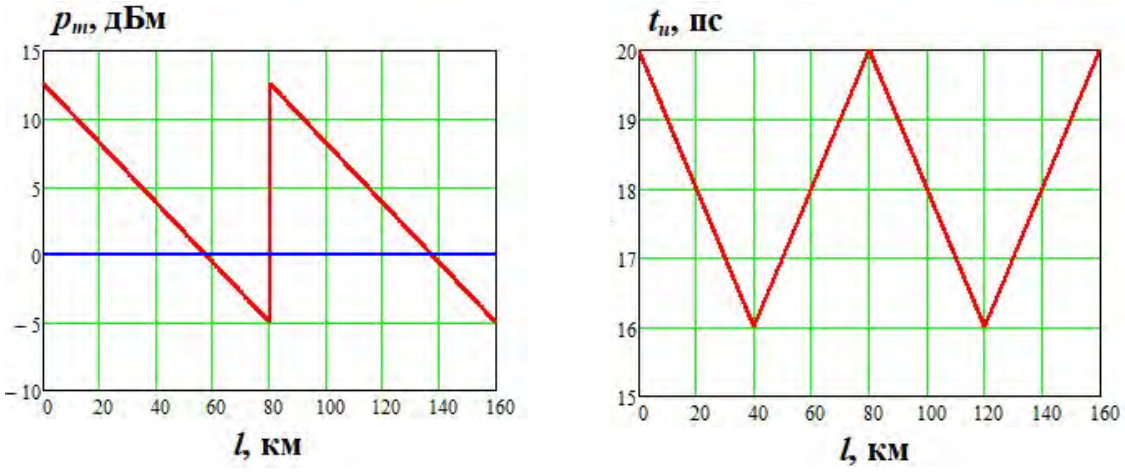
ТАБЛИЦА. Количественные результаты моделирования

Количество УУ, n	Длина ВОЛТ, L, км	Пик. мощность на входе, P_{0m} , мВт	Пик. мощность на выходе, P_{lm} , мВт	Длит. импульса t_u, пс	Кач. связи Q-фактор
1	80	18	18,5-19	19	161
4	320	18	17-18	22	77
8	640	18	15-16,2	22	51
16	1280	18	14-15	24	44

Из рис. 2 и таблицы следует, что квазисолитонный режим в протяженном ВОЛТ с ОУ EDFA практически сохраняется, что подтверждается сохранением длительности импульсов на уровне половины амплитуды и пиковой мощности. Некоторые отклонение длительности выходных импульсов и их пиковой мощности на выходе ВОЛТ длиной от 80 до 1 280 км лежат в пределах 20 % от номинальных значений. Отклонения возрастают с увеличением длины ВОЛТ и их можно объяснить неидеальностью ОУ. Отметим также, что индивидуальная подстройка отдельных ОУ позволит устранить эти отклонения.

На рис. 3 показаны результаты расчетов изменений уровня пиковой мощности и длительности импульсов от расстояния в ВОЛТ для двух первых УУ.

Таким образом, получены расчетные выражения и проведено моделирование многопролетной ВОЛТ с ОУ EDFA. Подтверждена возможность реализации квазисолитонной ВОСС с протяженностью более 1 000 км без использования регенераторов.



а б

Рис. 3. Изменение уровня пивой мощности (а)
и длительности импульсов от расстояния в ВОЛТ для двух УУ (б)

Список используемых источников

1. Андреева Е. И., Былина М. С., Глаголев С. Ф., Доценко С. Э., Чаймарданов П. А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Части 1-4 // Труды учебных заведений связи. 2018-2019. Т. 4, № 1-3. Т. 5, № 1.

2. Агравал Г. Нелинейная волоконная оптика. М.: Мир, 1996. 323 с.

3. Кившарь Ю.С., Агравал Г.П. Оптические солитоны. От волоконных световодов до фотонных кристаллов. М.: ФИЗМАТЛИТ, 2005. 648 с.

УДК 621.39, 530.182
ГРНТИ 49.44.31

ИСПОЛЬЗОВАНИЕ ВКР УСИЛИТЕЛЕЙ ДЛЯ ПОДДЕРЖАНИЯ КВАЗИСОЛИТОННОГО РЕЖИМА В ОДНОМОДОВЫХ ВОЛОКНАХ СО СМЕЩЕННОЙ ДИСПЕРСИЕЙ

С. Ф. Глаголев, В. С. Горсков, С. Э. Доценко

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

В работе рассматривается метод поддержания квазисолитонного режима в одномодовых оптических волокнах (ОВ) со смещенной дисперсией с помощью распределенных оптических усилителей (ОУ) Рамана, которые называют также усилителями вынужденного комбинационного рассеяния (ВКР). Теоретические расчеты

и моделирование проведены для усилителей с встречной и двунаправленной накачками. Показано, что использование ОУ ВКР позволяет увеличить длину усилительного участка в квазисолитонных волоконно-оптических системах связи (ВОСС) по сравнению с системами, использующими дискретные ОУ. Также показаны преимущества двунаправленной накачки. Получены формулы для выбора технических решений при проектировании квазисолитонных волоконно-оптических систем связи.

Данная работа является продолжением работы С. Ф. Глаголева, В. С. Горскова, С. Э. Доценко «Использование оптических усилителей EDFA для поддержания квазисолитонного режима распространения сигналов по одномодовым волокнам со смещенной дисперсией», приведенной в настоящем сборнике, которая посвящена квазисолитонным ВОСС, использующим для поддержания квазисолитонного режима дискретные ОУ.

одномодовое оптическое волокно со смещенной дисперсией, хроматическая дисперсия, фазовая самомодуляция, солитон, квазисолитонный режим, оптический усилитель.

ОУ ВКР с встречной накчкой

Рассмотрим схему квазисолитонной ВОСС с распределенными ВКР ОУ со встречной накачкой (рис. 1), которая содержит два оконечных транспондера (ТР1 и ТР2), *N* усилительных участков (УУ), *N*-1 усилительных пунктов (УП), содержащих источники накачки (ИН) и WDM направленные ответвители (НО).

Для усиления и поддержания формы оптических секансных импульсов в качестве активной среды используется активное ОМ ОВ. Необходимая для усиления энергия отбирается у непрерывного излучения накачки, которая вводится через НО навстречу излучению сигнала активного ОМ ОВ. Частота накачки при этом смещается вверх относительно несущей частоты сигнала на 13 ТГц.

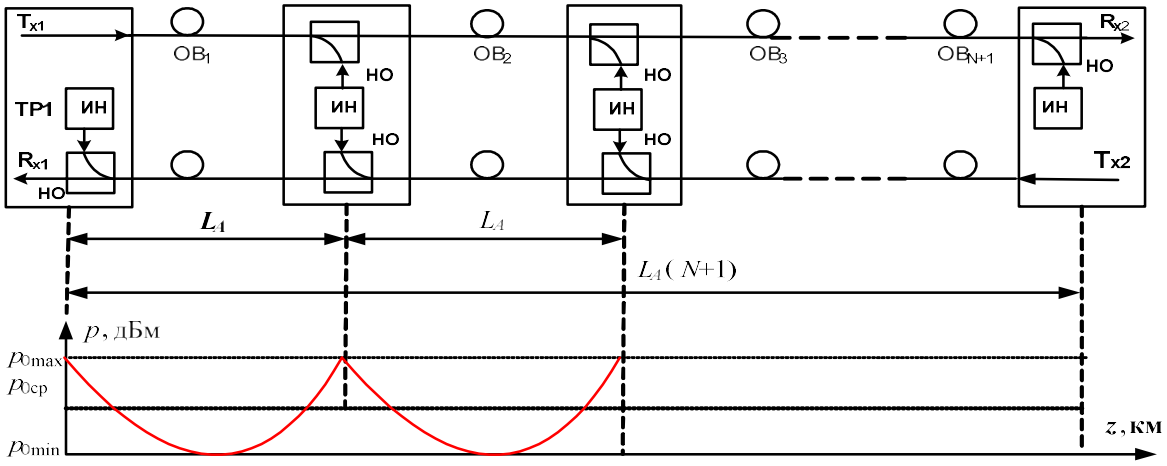


Рис. 1. Схема квазисолитонной ВОСС с ВКР ОУ и диаграммы изменения сигнала

На примере одного из УУ, запишем упрощенное уравнение (1), описывающее изменение пиковой мощности $P_m(z)$ на участке dz в ОМ ОВ, который обладает усилительной способностью $g(z)$ и коэффициентом затухания α

$$\frac{dP_m(z)}{dz} = \left[g(z) - \alpha\right] \cdot P_m(z). \quad (1)$$

Усилительная способность на УУ длиной L_A зависит от z и определяется уровнем накачки в данной точке. Максимальная усилительная способность и уровень накачки достигается в конце УУ при $z = L_A$. Из уравнения (1) видно, что при $g(z) > \alpha$, на участке dz ОМ ОВ пиковая мощность возрастает, в противоположном случае она будет уменьшаться.

Изменения уровня сигнала при распространение в многопролетной квазисолитонной ВОСС показаны на рис. 1. Уровень накачки вначале УУ минимален, затухание преобладает и уровень сигнала уменьшается. С увеличением расстояния возрастает усилительная способнасть и растет уровень накачки. Сигнал, достигнув минимума начинает возрастать до первоначального уровня в конце УУ.

Учитывая, что компенсировать потери в каждой точке ОВ нельзя, возможно компенсировать общее затухание на расстояние L_A между ОУ при условии [1, 2, 3]

$$\int_0^{L_A} g(z) \cdot dz = \alpha \cdot L_A.$$

Упрощенное выражение (2) для усилительной способности на УУ можно записать, если пренебречь истощением накачки

$$g(z) = g_0 \cdot \exp\left[-\alpha_p \cdot (L_A - z)\right], \quad (2)$$

где α_p – коэффициент затухания ОВ для накачки,

$g_0 = g(L_A)$ – максимальная усилительная способность ВКР ОУ, изменять которую можно с помощью управления мощностью накачки.

Запишем уравнение (3) для мощности накачки, которая обеспечивает необходимое значение g_0 и при которой на выходе ОУ обеспечивается такая же пиковая мощность, как и на входе $P_m(0) = P_m(L_A)$ решив уравнение (1) с учетом уравнения (3)

$$P_m(z) = P_m(0) \cdot \exp\left\{\alpha \cdot \left[L_A \cdot \left[\frac{\exp(\alpha_p \cdot z) - 1}{\exp(\alpha_p \cdot L_A) - 1}\right] - z\right]\right\} = P_m(0) \cdot p(z). \quad (3)$$

Действительно при $z = 0$ и $z = L_A$ $p(z) = 1$. На рис. 2 показаны нормализованные зависимости пиковой мощности $p(z/L_D)$ от расстояния при различных значениях длины УУ L_A = 1, 1.5 и 2 L_D и различных коэффициентах затухания $\alpha = \alpha_p$ = 0,2 и 0,25 дБ/км при оптимальном выборе g_0 для каждой L_A. Там же показано изменение $p(z/L_D)$ при отсутствии распределенного усиления $g_0 \rightarrow 0$, т. е. при использовании дискретных ОУ.

В случае использования встречной накачки, как и при использовании дискретных ОУ, пиковая мощность входных импульсов $P_m(0)$ должна быть больше или равна мощности $P_{m\Phi}$, необходимой для формирования фундаментального солитона в ОМ ОВ без потерь

$$P_m(0) = P_{m\Phi} / \overline{p}, \qquad \overline{p} = (1/L_A) \cdot \int_0^{L_A} p(z) \cdot dz,$$

где $\overline{p}$ – среднее значение нормализованной пиковой мощности излучения на УУ.

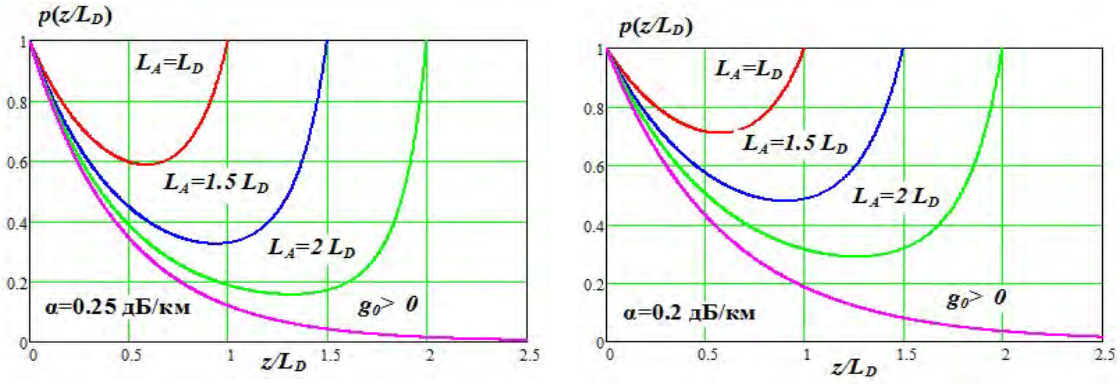


Рис. 2. Зависимость нормализованной пиковой мощности $p(z/L_D)$ от относительного расстояния в пределах одного УУ

Из рис. 2 видно, что при использовании распределенного ВКР усиления с встречной накачкой изменения пиковой мощности и длительности импульсов, а также требуемые пиковые мощности в пределах УУ меньше, а длина самого УУ больше по сравнению с использованием дискретных ОУ.

ОУ ВКР с двунаправленной накчкой

Схема квазисолитонной ВОСС с распределенными ВКР ОУ с двунаправленной накачкой показана на рис. 3, обозначения использованы как на рис. 1.

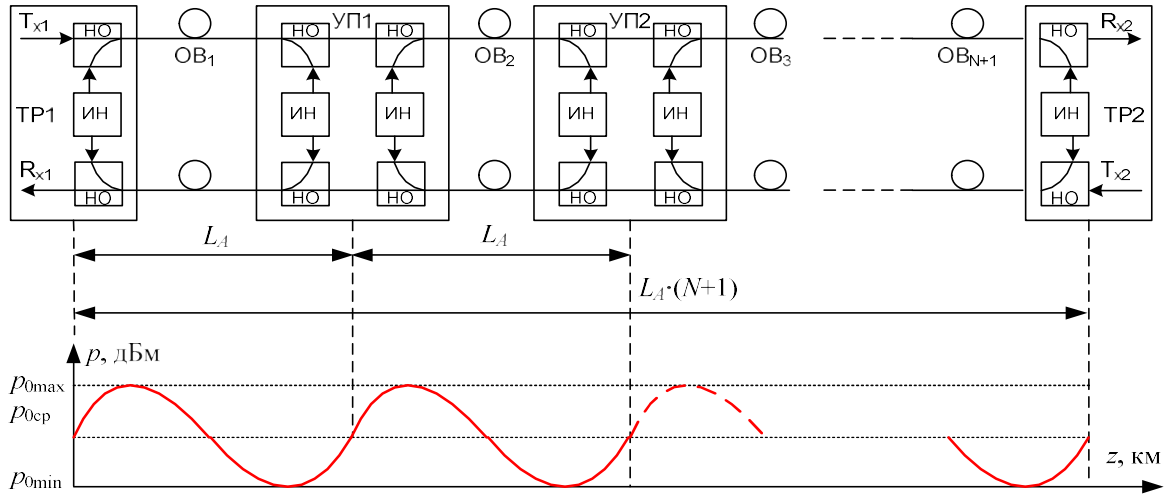


Рис. 3. Схема ВОСС с распределенными ОУ с двунаправленной накачкой

Запишем выражение (6) для усилительной способности $g(z)$ без учета истощения накачки.

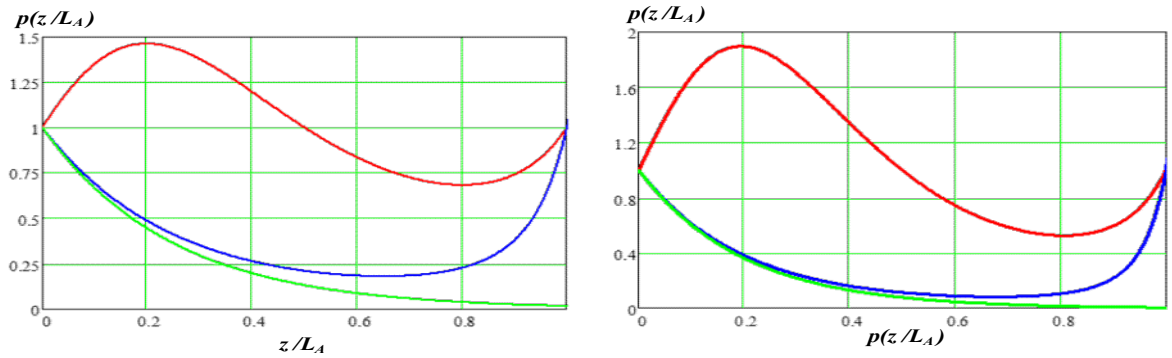
$$g(z) = g_1 \cdot \exp(-\alpha_p z) + g_2 \exp\left[-\alpha_p (L_A - z)\right], \quad (4)$$

где g_1 и g_2 связаны с мощностями попутной и встречной накачек.

Полагая, что мощности попутной и встречной накачек равны, решим уравнение (1) с учетом (4), получим уравнение (5) для определения изменения пиковой мощности секансных ОИ от расстояния

$$P_m(z) = P_m(0) \cdot \exp\left\{\alpha L_A \left(\frac{sh\left[\alpha_p (z - L_A/2)\right] + sh(\alpha_p L_A/2)}{2 \cdot sh(\alpha_p L_A/2)}\right) - \alpha z\right\} = P_m(0) \cdot p(z). \quad (5)$$

На рис. 4 показаны зависимости относительной пиковой мощности $p(z)$ вдоль ОВ при $L_A = L_D = 80$ км и $\alpha = \alpha_p = 0{,}22$ дБ/км для двунаправленной (1 кривая), встречной (2 кривая) накачек и зависимости $p(z)$ для УУ ВОСС с дискретными ОУ.



а б

Рис. 4. Зависимости нормализованной пиковой мощности $p(z/L_A)$ при $L_A = 0{,}8L_D$ (а) и $L_A = L_D$ (б) от относительного расстояния в пределах одного УУ и коэффициента затухания 0,22 дБ/км для ВОСС

ТАБЛИЦА. Сравнение различных способов поддержания квазисолитонного режима

α, дБ/км	L_A	K_α		
		Дискр. ОУ	ВКР ОУ со встречной накачкой	ВКР ОУ с двунаправленной накачкой
0,18	0,8 L_D	3,443	2,041	1,013
0,18	L_D	4,214	2,677	1,042
0,18	1,2 L_D	5,012	3,455	1,099
0,22	0,8 L_D	4,127	2,599	1,037
0,22	L_D	5,101	3,536	1,107
0.22	1,2 L_D	6,097	4,597	1,242

Для сравнения эффективности рассмотренных способов поддержания квазисолитонного режима используем величину $K_\alpha = 1/\bar{p}$. Она рассчитывалась при различных α и L_A для ОМ ОВ типа DSF с параметрами: $\beta_2 = -3.5$ пс^2/км, $\gamma = 2.5$ (Вт·км)$^{-1}$ в ВОСС со скоростью $B = 10$ Гбит/с со скважностью секансных ОИ $q = 5$. Результаты расчета представлены в таблице.

Из таблицы видно, что при использовании ВКР ОУ с двунаправленной накачкой на вход ОВ необходимо подавать солитонные ОИ с пиковой мощностью, практически равной мощности фундаментального солитона в ОВ без потерь. В таких ВОСС можно значительно увеличить длину УУ и обеспечить сохранение квазисолитонного режима на больших расстояниях.

Список используемых источников

1. Андреева Е. И., Былина М. С., Глаголев С. Ф., Доценко С. Э., Чаймарданов П. А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Части 1-4 // Труды учебных заведений связи. 2018-2019. Т. 4, № 1-3. Т. 5, № 1.

2. Агравал Г. Нелинейная волоконная оптика. М.: Мир, 1996. 323 с.

3. Кившарь Ю. С., Агравал Г. П. Оптические солитоны. От волоконных световодов до фотонных кристаллов. М.: ФИЗМАТЛИТ, 2005. 648 с.

УДК 004.416.6
ГРНТИ 50.41.25

АНАЛИЗ СПОСОБОВ ОРГАНИЗАЦИИ ХРАНЕНИЯ ЗАПИСЕЙ УЧЕБНЫХ ЗАНЯТИЙ ПРИ ПРОВЕДЕНИИ ИХ НА ОНЛАЙН-ПЛАТФОРМАХ ВИДЕОКОНФЕРЕНЦИЙ

Э. С. Голованов, Д. А. Куликов, А. А. Швидкий

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

В статье рассматриваются способы организации хранения записей учебных занятий, проводимых на онлайн-платформах видеоконференций, проводится анализ их отличий и недостатков. Также предлагается решение авторов, совершенствующее один из описываемых методов, и приводится принцип его работы.

видеоконференции в образовательных учреждениях, запись видеоконференций, хранение видеоконференций в облаке, Jibri, Nextcloud.

В ходе пандемии COVID-19 образовательные учреждения столкнулись с необходимостью проведения занятий в онлайн-формате. Как правило, решение о выборе платформы для проведения видеоконференции приходилось принимать преподавателям.

Разные платформы предоставляют различный уровень удобства и функционала, однако при использовании в учебных заведениях к ним предъявляются дополнительные требования по возможностям интеграции платформы в инфраструктуру учреждения (авторизация пользователей по внутренним учетным записям, проведение видеоконференций и хранение их записей на собственных серверах, независимых от внешних сервисов).

В таблице 1 сравниваются наиболее известные платформы для проведения видеоконференций в рамках возможностей их интеграции с инфраструктурой образовательного учреждения.

ТАБЛИЦА 1. Сравнение платформ видеоконференций

Платформа	Достоинства	Недостатки
Google Meet	Доступна запись видеоконференций	Закрытый исходный код
Zoom		Проприетарное ПО

Платформа	Достоинства	Недостатки
BigBlueButton	Открытый исходный код Свободное ПО Возможность загружать презентации напрямую в сервис	Низкая производительность Низкая масштабируемость Сложность разработки под свои нужды Запись и сохранение конференции только на тот сервер, к которому она привязана Зависимость от стороннего ПО
Jitsi Meet	Открытый исходный код Свободное ПО Высокая масштабируемость	Интеграция только с облачным хранилищем Dropbox Запуск презентаций только с рабочего места модератора

Наибольшую популярность у преподавателей получили сервисы Google Meet и Zoom, однако эти платформы используются на условиях проприетарной лицензии с ограничениями бесплатной версии, а также не предоставляют ПО и исходный код для разработки и развертывания на собственных серверах, что делает невозможной полноценную интеграцию с инфраструктурой образовательного учреждения.

Менее известные сервисы BigBlueButton и Jitsi Meet позволяют провести интеграцию с собственной инфраструктурой, но в то же время они имеют ограниченные возможности по записи видеоконференций. Так, в BigBlueButton запись видеоконференции осуществляется тем же сервером, на котором была запущена конференция [1] (негативно влияет на производительность), и ее сохранение возможно только локально на тот же сервер (менее надежно, чем облачное хранилище). В свою очередь, Jitsi Meet имеет реализацию записи видеоконференции только в проприетарное облачное хранилище Dropbox, которое невозможно использовать на собственном сервере.

Рассматривая применимость BigBlueButton и Jitsi Meet в качестве онлайн-платформ для проведения учебных занятий, следует отметить, что последний лучше подходит для такой цели, так как BigBlueButton имеет проблемы с производительностью, масштабированием и виртуализацией. В них входят серьезные ограничения как на количество участников одной конференции (до 100 человек), так и на количество одновременных конференций, запущенных на одном сервере в зависимости от числа участников [2], что делает эту платформу неприменимой для крупных образовательных учреждений.

Jitsi Meet, в свою очередь, при соответствующей конфигурации и балансировке нагрузки позволяет организовывать конференции на неограниченное число участников [3].

Рассмотрим методы записи видеоконференций, доступные при использовании Jitsi Meet (табл. 2).

ТАБЛИЦА 2. Сравнение способов записи видеоконференций в Jitsi Meet

Способ записи видеоконференции	Достоинства	Недостатки
Захват экрана	Нет необходимости в инфраструктуре, осуществляющей запись	От модератора конференции требуются определенные навыки и наличие специализированного ПО Затруднено распространение записи
Перехват медиаданных и служебной информации	Наименьшая нагрузка на сервер записи Наибольшая простота использования как для модератора конференции, так и для администратора	Наибольшие сложность и время реализации
Захват виртуального экрана	Для модератора видеоконференции упрощается инициирование записи	Отсутствуют средства привязки записанного файла к учетной записи модератора Отсутствует сортировка записанных файлов по учетным записям

Захват экрана с помощью специальных программ не требует доработки серверной части Jitsi Meet, однако является наиболее сложным и неудобным в эксплуатации для пользователя.

С точки зрения производительности самый эффективный вариант – программа-демон, работающая на сервере и записывающая конференцию путем «перехвата» медиаданных и служебной информации (история сообщений, привязка учетных записей пользователей к отправляемым ими сообщениям и медиаданным). Главным недостатком такого способа следует отметить необходимость разработки описанной программы и сложность ее реализации, требующую наличие опытного разработчика и большие временные затраты.

В Jitsi Meet доступен также гибридный метод – программа-демон Jibri (*JItsi BRoadcasting Infrastructure*), аналогично предыдущему способу работающая на сервере, но записывающая видеоконференцию путем захвата изображения с виртуального экрана, что позволяет получить запись конференции в таком виде, в котором ее наблюдали пользователи. Программа имеет и недостаток – записанные файлы могут сохраняться либо локально на сервере без сортировки и привязки к учетным записям пользователей, либо в облачное хранилище Dropbox, что приводит к зависимости от внешнего сервиса.

Рассмотрим возможные варианты усовершенствования последнего из описанных методов с целью внедрения возможности сохранения записей в облачное хранилище на собственном сервере.

Вместе с файлом записи видеоконференции Jibri также сохраняет файл с информацией об этой конференции. Составление скриптов, осуществляющих сбор и обработку таких данных, позволит автоматизировать процесс сохранения записи: информация о модераторе конференции будет использована скриптом для авторизации в облачном хранилище с помощью учетной записи модератора и загрузки в него нужного файла. Однако для этого Jibri вместе с информацией о конференции потребуется получить учетные данные модератора, осуществление чего скомпрометирует безопасность его облачной учетной записи.

Более предпочтительным, безопасным и удобным решением является разработка модуля интеграции облачного хранилища с веб-интерфейсом Jitsi Meet. Такой модуль позволит модератору самостоятельно авторизоваться в облачном хранилище через пользовательский интерфейс видеоконференции при помощи протокола OAuth, что предоставит Jibri необходимые права доступа к облачному аккаунту модератора для автоматической загрузки файла.

С учетом проведенного анализа способов записи видеоконференций и требований к онлайн-платформам по возможностям их интеграции в инфраструктуру образовательных учреждений, авторами сформулировано следующее решение. Исходя из сравнения, проведенного в таблице 1, платформа Jitsi Meet представляется наиболее перспективной для использования в учебных заведениях благодаря высокой масштабируемости и наличию открытого исходного кода. Анализируя сведенные в таблицу 2 особенности методов записи видеоконференций на этой платформе и описанные ранее варианты усовершенствования одного из них, как наиболее компромиссный предлагается использовать метод захвата виртуального экрана при помощи Jibri с внедренным в Jitsi Meet модулем интеграции облачного хранилища.

Архитектура и принцип работы предлагаемого метода представлены на рис. Для реализации такой системы в инфраструктуру образовательного учреждения необходимо внедрить:

- Сервер Jitsi Meet, позволяющий организовывать проведение видеоконференций;
- Сервер Jibri, необходимый для записи видеоконференций;
- Сервер Nextcloud – облачное хранилище с поддержкой стандарта OAuth [4], в которое будет производиться сохранение записей видеоконференций.

Рис. Принцип работы модуля интеграции NextCloud с веб-интерфейсом Jitsi Meet

Обеспечение взаимодействия описанных функциональных элементов осуществляется путем разработки модуля для Jitsi Meet. Этот модуль добавляет в веб-интерфейс форму авторизации в облачном хранилище Nextcloud. С ее помощью модератор конференции может авторизоваться напрямую в NextCloud и предоставить Jitsi Meet токен доступа (*access token* [5]) OAuth к своей учетной записи. Запросив этот токен у Jitsi Meet, Jibri при окончании записи видеоконференции получит возможность загрузить файл напрямую в облачный аккаунт модератора без необходимости передачи данных учетной записи пользователя третьим лицам.

Список используемых источников

1. BigBlueButton : Recording. URL: https://docs.bigbluebutton.org/dev/recording.html (дата обращения 29.03. 2021)

2. BigBlueButton : FAQ. URL: https://docs.bigbluebutton.org/support/faq.html#how-many-simultaneous-users-can-bigbluebutton-support (дата обращения 29.03. 2021)

3. How many Users and Conferences can Jitsi support on AWS?. URL: https://meetrix.io/blog/webrtc/jitsi/how-many-users-does-jitsi-support.html#how-many-concurrent-meetings-and-concurrent-users-can-jitsi-handle (дата обращения 29.03. 2021)

4. OAuth2 – Nextcloud latest Administration Manual latest documentation. URL: https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/oauth2.html (дата обращения 29.03. 2021)

5. Access Tokens – OAuth 2.0 Simplified. URL: https://www.oauth.com/oauth2-servers/access-tokens/ (дата обращения 29.03. 2021)

Статья представлена директором НИИ ТС СПбГУТ, кандидатом технических наук, доцентом А. Г. Владыко.

УДК 535.8
ГРНТИ 49.33

ДОМАШНИЕ СЕТИ. РАЗВИТИЕ ТЕХНОЛОГИИ HOMEPNA

Е. Е. Головкова, Ю. Д. Теребенина, Б. К. Резников

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

Сейчас для каждого из нас персональный компьютер стал незаменимым домашним инструментом, который мы используем для развлечений, образования и работы. Интернет уже давно является средством получения информации, поэтому возникает потребность увеличение скорости передачи цифровых данных в пределах одной квартиры или же офиса. В таком случае развертывание локальной сети окажется невыгодным из-за особых сложностей технического характера. Решением этой проблемы стала технология домашней сети HomePNA (HomePhonelineAlliance), который базируется на использовании существующей телефонной линии и обеспечивает простую, высокоскоростную и недорогую домашнюю сеть.

HomePNA, сети доступа, электросвязь.

История появления технологии HomePNA началась с идеи создания дешевого способа передачи данных по уже существующей инфраструктуре, точнее по телефонной проводке или коаксиальному кабелю. В 1996 году телекоммуникационные компании AT&T, 2Wire, Motorola, CopperGate, ScientificAtlanta и другие, объединились с целью создания альянса HomePNA. Их задача состояла в том, чтобы продвигать подобные домашние сети и создание спецификации стандартов, а их стандартизацией занимается международный союз электросвязи ITU (*InternationTelecommunicationUnion*) [1].

Для того чтобы технология организации домашних сетей имели популярность среди потребителей, у нее должна быть низкая стоимость, что позволит продвинуть ее на массовый рынок, и легкая установка. Имеются также некоторые особенности связанные с поддержанием высокой скорости передачи данных и возможностью сети быть увеличенной, с большим ростом пользователей.

Главное преимущество технологии HomePNA является не восприимчивость к помехам, которые возникают в телефонной линии. Частотный диапазон подобран таким образом, чтобы избежать воздействия различных источников помех, которые имеются в доме. Одновременное использование одной телефонной линии для передачи сетевого трафика и телефонных служб возможно при частотном разделении, когда каждая служба выделяет свой частотный спектр, который не пересекается со спектрами других служб.

Путем использования частотно-избирательных фильтров устройства могут обмениваться информацией между собой и при этом не оказывать влияния на устройства, работающие в другом частотном диапазоне. Получается, что в одной паре телефонных проводов организуется несколько частотно-разделенных каналов.

Еще одним преимуществом технологии HomePNA является использование нестандартных и случайных топологий проводки. Заранее мы не можем узнать структуру телефонной проводки каждой квартиры или дома, а она может меняться даже из-за простых действий, например, подключение телефонного или факсимильного аппарата, которые в свою очередь создают новое ответвление телефонной проводки внутри квартиры.

Развитие технологии домашних сетей HomePNA происходило поэтапно и со временем появлялись все новые спецификации.

HomePNA 1.0

Спецификация HomePNA 1.0 была разработана в 1998 году, она подразумевает использование топологии «звезда» и метода доступа к предающей среде CSMA/CD. Спецификация определяется некоторыми правилами функционирования локальной сети:

– среда передачи данных – телефонная проводка;

– топология «звезда» (необходимо применение коммутатора);

– максимальная скорость передачи данных – 1 Мбит/с;

– для доступа к передающей среде, применяется метод множественного доступа с контролем несущей и обнаружения коллизий (CSMA/CD);

– частотный диапазон 4,5 – 9,5 МГц используется для передачи данных;

– кодировка одиночного битового импульса PMM (PulsePositionModulation), которая позволяет подстраиваться под условия среды;

– поддерживает работу 32 устройств;

– максимальный диаметр сети 150 м.

Данная спецификация стала первой, но не была широко распространена, так как использование коммутатора для соединения компьютера с сетью, делало сеть дорогой и сложной [2].

HomePNA2.0

Компания Epigramв 1999 году разработала спецификацию HomePNA2.0, которая имела весомых отличий от первой версии:

– топология «шина»;

– среда передачи данных – телефонная проводка или коаксиальный кабель;

– максимальная скорость передачи данных – 10 Мбит/с;

– сервис качества QoS (*QualityofService*);

– технология кодирования QAM (*QuadratureAmplitudeModulation*), позволяющая добиться увеличения длины сегментов сети;

– частотный диапазон 4–21 МГц;

– поддерживает работу 32 устройств;

– максимальный диаметр сети 350 м, в зависимости от типа кабеля может достигать до 1 000 м.

Стандарт HomePNA2.0 на практике показал свою гибкость и функциональность.

HomePNA3.0

Появление стандарта HomePNA3.0 в 2005 году было ожидаемым потому, что по сравнению с другими спецификациями, скорость передачи данных выросла в разы и имели следующие особенности:

– среда передачи данных –телефонная проводка или коаксиальный кабель;

– максимальная скорость передачи данных – 128 Мбит/с;

– технология кодирования QAM (*QuadratureAmplitudeModulation*);

– применяется сервис качества QoS (*QualityofService*);

– частотный диапазон 4–36 МГц используется для передачи данных;

– поддерживает работу 32 устройств;

– максимальный диаметр сети 350 м.

HomePNA 3.1

В 2007 году была представлена последняя и наиболее перспективная спецификация HomePNA 3.1, ее достоинство в высокой скорости передачи данных и подключения большего количества устройств, по сравнению с предыдущими версиями. Основные характеристики представлены ниже:

– среда передачи - телефонная проводка или коаксиальный кабель, применяемый для цифрового сигнала;

– скорость передачи данных – 320 Мбит/с;

– технология кодирования QAM (*QuadratureAmplitudeModulation*);

– сервис качества QoS (*QualityofService*);

– для передачи данных используется диапазон 4–65 МГц;

– обратная совместимость с оборудованием предыдущих стандартов;

– автоматическая адаптация скорости и схемы применения частотных каналов в зависимости от зашумленности канала;

– низкая стоимость оборудования.

Технологию HomePNA по праву можно считать удачным решением, для дома и офиса. При своей дешевизне и малой трудоемкости при прокладке сети, технология оказывается спасением для компаний, которые арендуют офисы в старых знаниях, или для подключения к сети Интернет жилого сектора. Все особенности этой локальной сети позволяет ей сохранять довольно прочные позиции на рынке.

Список используемых источников

1. HomePNA. URL: http://www.homepna.org/
2. HomePNA: сеть передачи данных в каждой квартире. XDSLlastmiletехнологии. URL: http://www.xdsl.ru/articles/homepna1.htm.

Статья представлена заведующим базовой кафедрой ССС СПбГУТ, доктором технических наук, доцентом В. В. Котовым.

УДК 004.056.53
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ СПОСОБА НЕБЕЗОПАСНОГО ВЫЗОВА API ЯДРА В ОС WINDOWS

Н. В. Гололобов[1], **К. Е. Израилов**[1,2]

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

Одной из популярных операционных систем в современном мире является Windows. В основе ее функционирования лежит разделение пространства выполнения на доступные для работы пользовательских программ и работы ядра системы. В статье рассмотрен один из механизмов проведения атаки на операционную систему путем обхода механизмов безопасности при проверке вызовов из пользовательских приложений функций ядра. Приводится гипотетический пример ассемблерного кода вызова функции выделения виртуальной памяти NtAllocateVirtualMemory, а также предлагается общий порядок действий для обхода защиты такого рода. В интересах противодействия данному виду атак предлагаются основные моменты соответствующего подхода.

режим ядра, системные вызовы, API ядра, безопасность системы.

Введение

Современные операционные системы используют явное разделение режимов пользователя и ядра. Такой подход обеспечивает безопасность

на уровне системы [1], изолируя потенциального нарушителя от пространства ядра. Для выполнения кода данного пространства процессор переходит в режим ядра, что позволяет выполнять операции ввода-вывода к периферийным устройствам, изменять настройки памяти – параметры защиты и настройки виртуальной памяти. Таким образом, код, работающий в режиме ядра, имеет доступ ко всем системным ресурсам.

В ОС Windows интерфейс API ядра обернут в пользовательские функции, которые могу контролировать передаваемые параметры. В общем случае вызов к этому API разделяется на несколько последовательных этапов: в пространстве пользователя – вызов Win32 API, проверка и подготовка параметров, проверка прав доступа для вызова; в пространстве ядра – вызов API ядра (включающее собственное API – используемое для внутренних «доверенных» вызовов) и непосредственное выполнение запроса (см. рис. 1).

Рис. 1. Схема вызова API ядра

Во время проверки прав доступа также совершается сторонний вызов к API ядра, но такой вызов считается доверенным за счет неконтролируемости кода API «Win32». Тем не менее гипотетически можно предположить возможность вызова собственного API ядра напрямую – без проверки параметров и прав доступа (2-й и 3-й этапы). Такой вызов, очевидно, будет небезопасным и исследованию этой возможности посвящена данная статья.

Разработка способа вызова собственного API ядра

Собственное API ядра вызывается из динамических библиотек, которые используются исключительно в пространстве ядра. К таким библиотекам относится ntdll.dll. В сущности, выполнение запроса при корректных параметрах и правах происходит посредством определенного системного вызова, который выполняется в пространстве ядра. Контекст работы при вызове не проверяется, что приводит к непосредственному исполнению кода. Номера системных вызовов в разных версиях ОС Windows могут отличаться, что необходимо учитывать при совершении вызова. Номер системного вызова для выделения виртуальной памяти (функция NtAllocateVirtualMemory) равен 24 для ОС Windows 10 версии 1904 (рис. 2),

а сам вызов происходит непосредственно инструкцией syscall(). API ядра, как правило, недокументировано производителем, но на практике, набор параметров для API «Win32» и собственного API совпадает.

```
00007ffc`0325faa0 cc              int     3
0:004> x ntdll!NtAllocateVirtualMemory
00007ffc`0325c360 ntdll!NtAllocateVirtualMemory (NtAllocateVirtualMemory)
0:004> u 00007ffc`0325c360
ntdll!NtAllocateVirtualMemory:
00007ffc`0325c360 4c8bd1          mov     r10,rcx
00007ffc`0325c363 b818000000      mov     eax,18h
00007ffc`0325c368 f604250803fe7f01 test    byte ptr [SharedUserData+0x308 (00000000`7ffe0308)],1
00007ffc`0325c370 7503            jne     ntdll!NtAllocateVirtualMemory+0x15 (00007ffc`0325c375)
00007ffc`0325c372 0f05            syscall
00007ffc`0325c374 c3              ret
00007ffc`0325c375 cd2e            int     2Eh
00007ffc`0325c377 c3              ret
```


```
00007ffc`0325faa0 cc              int     3
0:004> x ntdll!NtAllocateVirtualMemory
00007ffc`0325c360 ntdll!NtAllocateVirtualMemory (NtAllocateVirtualMemory)
0:004> u 00007ffc`0325c360
ntdll!NtAllocateVirtualMemory:
00007ffc`0325c360 4c8bd1          mov     r10,rcx
00007ffc`0325c363 b818000000      mov     eax,18h
00007ffc`0325c368 f604250803fe7f01 test    byte ptr [SharedUserData+0x308 (00000000`7ffe0308)],1
00007ffc`0325c370 7503            jne     ntdll!NtAllocateVirtualMemory+0x15 (00007ffc`0325c375)
00007ffc`0325c372 0f05            syscall
00007ffc`0325c374 c3              ret
00007ffc`0325c375 cd2e            int     2Eh
00007ffc`0325c377 c3              ret
```


Рис. 2. Ассемблерный код вызова функции NtAllocateVirtualMemory

Непосредственный вызов API ядра из пользовательского кода можно осуществить с использованием ассемблерной вставки или вызова функции через указатель, который установлен на буфер с бинарным кодом системного вызова. Таким образом для вызова API ядра следует выполнить следующие действия:

Посредством отладки приложения Windows (например, «Блокнот») обнаружить динамическую библиотеку, в которой находится реализация интересующего API ядра.

Посредством декомпиляции [2-6] обнаружить номер системного вызова, который происходит при исполнении функции API ядра.

Аналогично декомпилированному коду реализовать вызов в пользовательском коде.

Вызвать реализацию из пользовательского кода.

Подход к защите от несанкционированных вызовов собственного API ядра

Сформулируем основные моменты подхода, направленного на защиту от несанкционированного доступа собственного API ядра.

При обеспечении защиты от несанкционированного вызова собственного API необходимо учитывать, что количество обращений к ядру может

достигать десятков тысяч в минуту и контроль каждого обращения значительно снизит производительность системы. Защитный механизм должен функционировать на уровне ядра ОС и предоставлять простой интерфейс для совершения запросов о легитимности того или иного системного вызова.

Под приведенные выше критерии подходит драйверная архитектура. В ее основе лежит принцип протокольного обращения, что значительно снижает время обработки запроса за счет стандартизации. Также в целях повышения производительности предлагается разделение доверенных и не доверенных приложений.

К доверенным могут относиться предустановленные приложения, а также приложения, подписанные производителем, по аналогии с подписями драйверов. Контроль за группой доверенных приложений не будет производится. Считается, что таких приложений большинство.

К не доверенным приложениям должны относиться все приложения, не имеющие подписи, а также проявляющие подозрительную активность (по оценке ПО «Защитник Windows» [7]). Считается, что контроль за такими приложениями несущественно повлияет на производительность и конечный пользователь не заметит разницы.

К предложенному походу должны предъявляться самые высокие требования по обеспечению безопасности, драйвер должен быть подписан УЦ производителя операционной системы – в данном случае Microsoft.

Заключение

Разделение пространств на пользовательское и ядра системы реализовано во многих операционных системах. Данный подход обеспечивает безопасность функционирования системы на обоих уровнях. Использование API при создании ПО нежелательно ввиду человеческого фактора. Ошибка, допущенная разработчиком, может привести к отказу системы в обслуживании или появлению других потенциальных уязвимостей [8]. Наиболее же опасным случаем может считаться злонамеренное использования таких вызовов [9]. Такая возможность была теоретически продемонстрирована в данной статье.

В будущих научных работах планируется провести исследования по внедрению вредоносного кода, использующего API ядра [10], в приложения Windows, а также по разработке методов защиты от атак данного вида [11].

Список используемых источников

1. Буйневич М. В., Васильева И. Н., Воробьев Т. М., Гниденко И. Г., Егорова И. В., Еникеева Л.А и др. Защита информации в компьютерных системах: монография. СПб.: СПбГЭУ, 2017. 163 с.

2. Израилов К. Е. Применение генетических алгоритмов для декомпиляции машинного кода // Защита информации. Инсайд. 2020. № 3 (93). С. 24–30.

3. Буйневич М. В., Израилов К. Е., Покусов В. В., Тайлаков В. А., Федулина И. Н. Интеллектуальный метод алгоритмизации машинного кода в интересах поиска в нем уязвимостей // Защита информации. Инсайд. 2020. № 5 (95). С. 57–63.

4. Буйневич М. В., Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 1. Функциональная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 1. С. 115–130.

5. Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 2. Информационная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 86–104.

6. Израилов К. Е., Покусов В. В. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 3. Модульно-алгоритмическая архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 4. С. 104–121.

7. Хэй Р. Тестируем фильтр SmartScreen и возможности обнаружения Защитника Windows // Windows IT Pro/ RE. 2017. № 1. С. 26.

8. Олексюк Д. Уязвимости в драйверах режима ядра для Windows // RSDN Magazine. 2009. № 1. С. 13–30.

9. Израилов К. Е., Гололобов Н. В., Краскин Г. А. Метод анализа вредоносного программного обеспечения на базе Fuzzy Hash // Информатизация и связь. 2019. № 2. С. 36–44.

10. Рыжков С. Е. Доступ к Crypto Api ядра ОС Linux из пространства пользователя // Молодежный научно-технический вестник. 2017. № 7. С. 50.

11. Баранов А. Руткиты режима ядра: алгоритмы работы и защита // Системный администратор. 2007. № 1 (50). С. 74–78.

УДК 004.056.53
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ АЛГОРИТМА ДЛЯ ПОИСКА ИНСАЙДЕРОВ ВО ВНУТРЕННЕЙ СЕТИ

Н. А. Голубов, Н. А. Косов

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

В данной статье будет рассмотрены понятие инсайдера и их разновидности, существующие методы для поимки, а также алгоритм по их поиску во внутренней сети. Данная проблема актуальна, так как инсайдеры на сегодняшний день представляют серьезнейшую опасность для организаций всех уровней, вне зависимости от рода деятельности. Вследствие собственных знаний и легального доступа к информационным системам, они благополучно обходят физические и электронные средства контроля для достижения собственной корыстной цели. Вмешательство данных лиц трудно обнаружить во время совершения атаки, а на устранение огромного ущерба потребуется

большое количество времени и денежных средств. Ущерб может быть не только репутационным и финансовым, действия внутренних нарушителей также способны нанести вред здоровью и жизни людей.

инсайдер, DLP-системы, honey-pot, UEBA-системы.

Опасность со стороны лиц, действующих против собственных нанимателей, а также коллег, появилась с тех самых пор, когда возникли наемные сотрудники. Прежде подобных людей называли предателями либо «двойными агентами», в настоящее время используется термин «инсайдер».

«Инсайдер» – сотрудник организации, имеющий доступ к информации, закрытой для широкой публики. Он может использовать имеющиеся сведения для причинения вреда бизнесу или для извлечения прибыли.

Инсайдеры – это вторая по значимости угроза для организаций после внешних атак, которые еще называют хакерскими атаками. Согласно докладу фирмы Secure Automatic Technologies, 99 % европейских организаций как минимум три раза за историю собственного существования сталкивались с финансовыми утратами, случившимися из-за инсайдерской деятельности. В отчете американской ассоциации Insider Threat 2019 сообщается, что на сегодняшний день 61 % банкротств в США происходят по вине инсайдеров, при этом угроза становится особенно острой во время заключения крупных контрактов [1].

Рассмотрим выделяемые разновидности инсайдеров [2]:

- «Халатный» инсайдер.

Это наиболее часто встречающийся вид внутреннего нарушителя. Как правило, это пользователь рядового состава, выполняющий простую работу. Нарушения данного типа инсайдеров в отношении конфиденциальной информации немотивированы, не имеют конкретной цели, замысла, корысти. Зачастую они даже не обладают способностью заработать на собственных действиях, однако вред от разглашения данных может быть катастрофическим.

- «Манипулируемый» инсайдер.

Данный тип становится нарушителем из-за социальной инженерии. Типичный сценарий такого инцидента выглядит так. В офисе раздается звонок от начальника существующего отдела, который очень решительно представляется, предельно правдоподобно описывает проблему, связанную с невозможностью доставки почты в сеть филиала. И просит прислать ему определенную информацию на электронную почту. Сотрудник даже не сомневается, что звонящий вовсе не тот, кем он представился. И в считанные минуты запрашиваемая информация, представляющая собой строго секретную информацию, отправляется по указанному адресу.

- «Обиженный» инсайдер.

Исходя из названия, этот тип работника действует из личной обиды на работодателя. Его задача – нанести наибольший ущерб. Для этого он может сфальсифицировать или уничтожить важные документы. Зачастую, похищенную информацию такой человек передает прессе или теневым структурам.

- «Нелояльный» инсайдер.

К данному типу нарушителей относят сотрудников, решивших сменить место работы или открыть собственное дело. При увольнении с работы они забирают те данные, которые могут. В последнее время нередки стали случаи похищения информации из высокотехнологичных фирм Европы или Америки, работниками из развивающихся стран.

- «Подрабатывающие» инсайдеры.

Сюда включаются люди, вступивших на стезю инсайдерства из-за различных обстоятельств. Сюда относятся лица, решившие подзаработать на пару тысяч, которых им недостает на покупку автомобиля. Нередки случаи инсайдеров поневоле – из-за угроз или шантажа, у них не остается выбора, кроме как выполнение указов третьих лиц. Непосредственно по этой причине «подрабатывающие» имеют все шансы совершать наиболее разнообразные действия при невозможности выполнения задачи. В зависимости от обстоятельств, они могут прекратить попытки и начать изображать производственную деятельность, а трудных ситуациях пойти на взлом, подкуп коллег, ради получения доступа к данным любыми методами.

- «Внедренные» инсайдеры.

В текущее время к подобным способам добычи информации прибегают не только в целях правительственного шпионажа, но и промышленного. Угроза от этого типа нарушителя заключается в том, что в случае технических ограничений на передачу данных за пределы корпоративной информационной сети «работодатели» имеют все шансы предоставить ему необходимые устройства или программное обеспечение для обхода системы безопасности. А сам шпион сделает все, чтобы получить информацию.

Существует большое количество методов и средств защиты информации, созданных для выявления инсайдерских угроз [3].

DLP-системы (*data leak protection* – предотвращение утечек информации) контролируют потоки информации, с целью выявления передачи конфиденциальных данных. Данные системы используются для мониторинга и предотвращения попыток несанкционнировай передачи данных за границы корпоративной сети. Так же DLP-системы способны отслеживать операции работников, записывать и анализировать их общение посредством электронной почты, социальных сетей и чатов. Главная задача DLP – обеспечение соблюдения политики конфиденциальности компании. Применение DLP особенно важно для компаний, в которых потенциальная утечка может нанести серьезный репутационный или же финансовый ущерб.

Следующее средство защиты от инсайдерской угрозы – Honey-pot. Honey-pot представляет собой приманку для привлечения внимания атакующего и сбора информации о нападающем. Они могут быть замаскированы под важные файлы, ссылки, учетные данные пользователей или почтовые сообщения. Любое обращение к приманке, можно расценивать в качестве инсайдерской атаки.

UEBA (User and Entity Behavior Analytics – поведенческий анализ пользователей и сущностей) – технология выявления киберугроз, основанная на анализе поведения пользователей, а также устройств, приложений и иных объектов в информационной системе. UEBA-системы собирают и анализируют информацию из различных источников (логи серверов, рабочих станций; данные брандмауэров, антивирисусов; почтовые переписки пользователей). С помощью машинного обучения и статистического анализа формируются шаблоны нормального поведения пользователей. Если действие сотрудника отклоняется от данного шаблона, система уведомит об этом специалиста по безопасности [4].

Существуют разные инструменты для борьбы с инсайдерами, однако ни одно из них не является универсальным. Для решения проблемы инсайдерских атака, необходим комплекс данных технических средств. Кроме выявления инсайдерских атак, существует и другое направление – их прогнозирование, основанное на поиске людей, склонных к совершению инсайдерской атаки.

Алгоритм для поиска инсайдеров выглядит следующим образом (рис.).

В данном алгоритме на первом шаге идентифицируется тот пользователь информационной системы, работа которого исследуется. Если пользователей несколько, то они анализируются независимо друг от друга. Затем для выбранного пользователя строится множество допустимых для него функциональных обязанностей. Работа любого пользователя представляет из себя последовательность обращений к хранилищу данных. Для каждого обращения проводится проверка на соответствие функциональным обязанностям. Отличие честного пользователя от инсайдера заключается в том, соответствует ли его действия функциональным обязанностям, или нет.

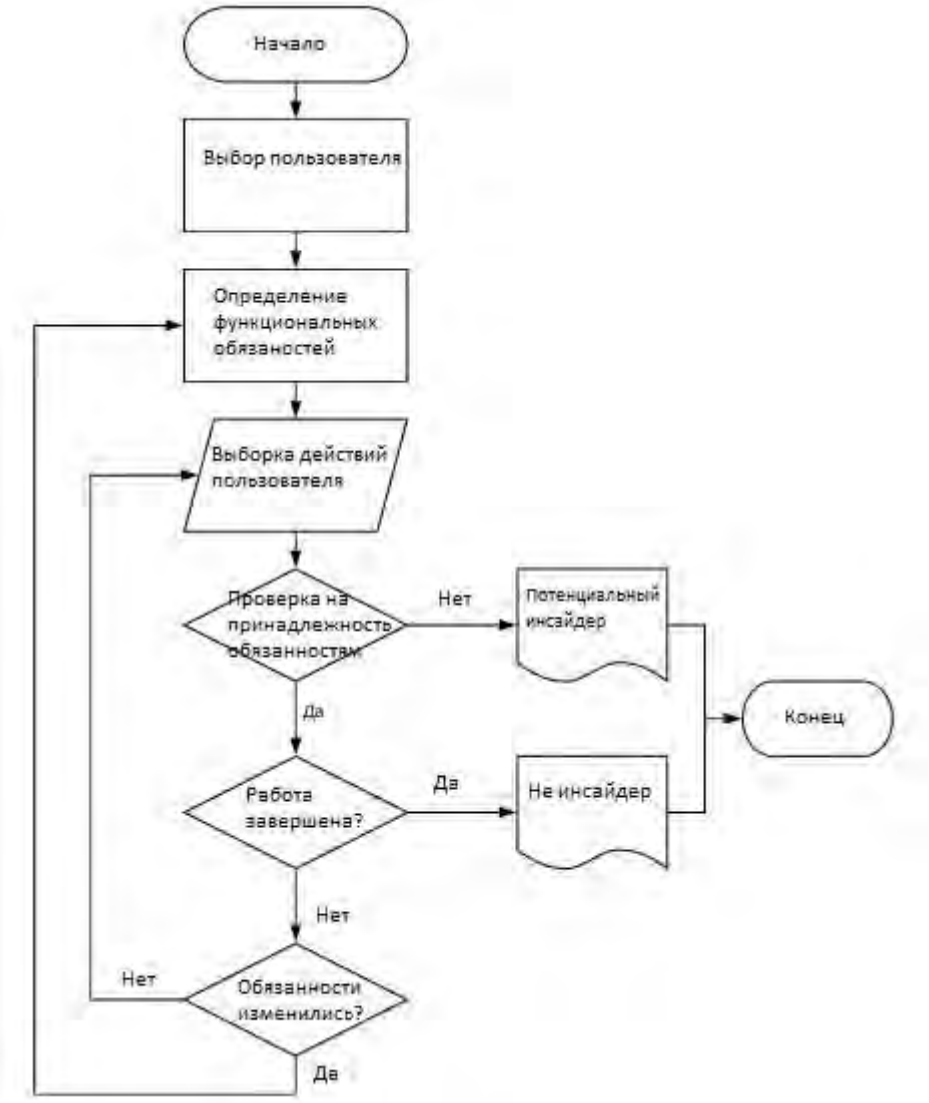


Рис. Алгоритм для поиска инсайдеров

Список используемых источников

1. Как распознать инсайдера и не дать ему навредить? URL: https://falcongaze.com/ru/pressroom/publications/articles/kak-raspoznat-insajdera.html (дата обращения 20.02.2021).

2. Кто такой “инсайдер” и какие они бывают // Энциклопедия “Касперского”. URL: https://encyclopedia.kaspersky.ru/knowledge/recognizing-different-types-of-insiders/ (дата обращения 20.02.2021).

3. Веденев В. С., Бычков И. В. Система выявления инсайдеров // Математические структуры и моделирование. 2014. № 4 (32). С. 236–239.

4. Что такое User and Entity Behavior Analytics (UEBA) // Энциклопедия “Касперского”. URL: https://encyclopedia.kaspersky.ru/glossary/ueba/ (дата обращения 20.02.2021).

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

УДК 003.26.09
ГРНТИ 81.96

РАЗРАБОТКА ПОДХОДОВ К СОЗДАНИЮ СИСТЕМЫ ТАЙНОГО ДИСТАНЦИОННОГО ГОЛОСОВАНИЯ В ДИССЕРТАЦИОННОМ СОВЕТЕ ВУЗА

А. В. Горлина, В. А. Яковлев

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

Предлагается подход по созданию системы тайного дистанционно голосования членами диссертационного совета с сохранением конфиденциальности и анонимности их голоса, что является актуальным в период пандемии. Определены состав системы голосования, ее параметры и алгоритм функционирования. В основе системы голосования предлагается использовать криптографическую систему гомоморфного шифрования Пэйе.

система голосования, тайное дистанционное голосование, шифрование Пэей.

Голосование но присуждению ученых степеней кандидатов и докторов наук по требованиям ВАК должно быть тайным [1].

В основу разработки подхода к созданию системы тайного электронного дистанционного голосования в диссертационном совете Университета взята криптографическая система гомоморфного шифрования Пэйе [2]. Она в наибольшей степени подходит к решению этой задачи, так как голосование в диссовете не масштабное и не требуется много пересылок между участниками процесса голосования.

В состав системы электронного голосования диссертационного совета (ДС) входят:

– члены диссертационного совета – физические лица, имеющее право голоса в диссовете. Решение члена диссертационного совета – положительный или отрицательный результат по присуждению ученой степени.

– соискатель ученой степени, получает положительный результат, если за присуждение степени проголосовало 2/3 членов диссовета, принявших участие в голосовании.

– сервер обработки зашифрованных бюллетеней (сервер голосования) – выполняет функцию обработки криптограмм, полученных от членов диссовета и хранит зашифрованные голоса.

– сервер университета выполняет функции идентификации членов ДС, рассылку открытых ключей и взаимодействие с компьютером ДС;

– счетная комиссия – определяет, что член диссертационного совета принял участие в голосовании, осуществляет подсчет голосов и объявляет результаты выборов.

Предполагается, что защите диссертации осуществляется публично в режиме видеоконференции с использованием платформ для видеоконференций Zoom или Google meet. Также в этой среде решаются вопросы открытого голосования.

Предлагаемая система относится только к процедуре тайного голосования. Мы рассматриваем подход, при котором часть членов диссовета (председатель, секретарь, несколько членов диссовета, соискатель степени) присутствуют на защите очно, а другие члены участвуют в заседании дистанционно.

Система электронного голосования на основе криптосхемы Пэйе представлена на рис. и функционирует следующим образом:

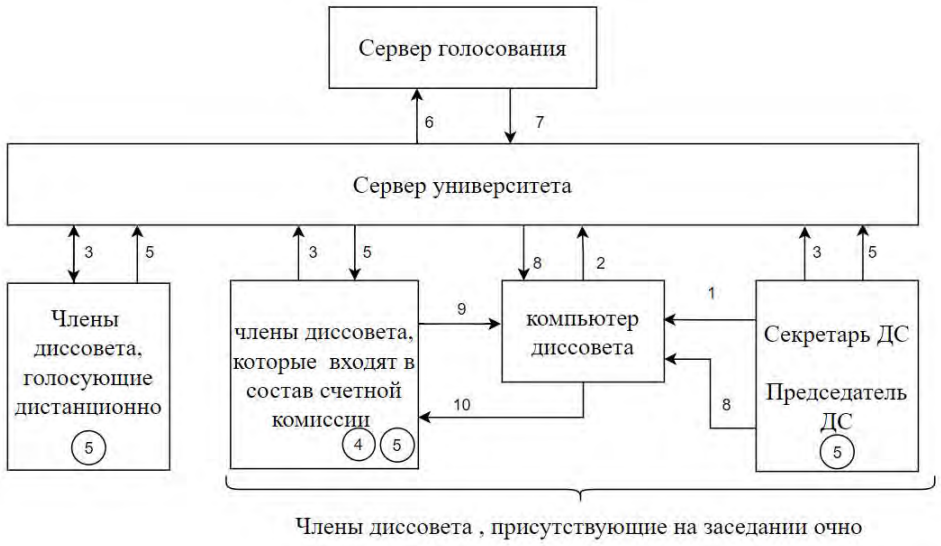


Рис. Гомоморфная система электронного голосования на основе схемы Пэйе

1. Секретарь ДС запускает на компьютере ДС программу генерации открытого и закрытого ключа согласно алгоритму Пэйе.

2. Открытый ключ отправляется на сервер университета, закрытый хранится в памяти компьютера и может быть активирован, только членами счетной комиссии по их номерам, после процедуры избрания счетной комиссии.

3. Все члены ДС, участвующие в голосовании удаленно или очно, проходят процедуру идентификации в личном кабинете и после ее прохождения получают открытый ключ для голосования.

4. Открытым голосованием избирается счетная комиссия из членов диссовета, присутствующих на заседании ДС очно.

5. Члены диссертационного совета голосуют и зашифровывают свои бюллетени открытым ключом.

6. Члены ДС отправляют свои зашифрованные бюллетени (криптограммы) на сервер университета, который их пересылает на сервер голосования (выделенный ресурс сервера университета или, как вариант, сервер аутсортинга). (Бюллетень может быть принят только 1 раз, член ДС получает уведомление, о приеме бюллетеня).

7. Сервер голосования перемножает все криптограммы и отправляет обратно криптограмму-произведение на сервер университета.

8. Председатель счетной комиссии загружает криптограмму-произведение в компьютер ДС.

9. Члены счетной комиссии вводят свои номера и активируют закрытый ключ. Счетная комиссия расшифровывает криптограмму-произведение, получает сумму голосов, поданных ЗА и НЕТ, оформляет протокол счетной комиссии.

10. Председатель счетной комиссии объявляет в режиме видеоконференции результаты голосования, которые открытым голосованием утверждаются членами ДС.

Рассмотрим пример построения и функционирования системы электронного голосования на основе схемы Пэйе. Пусть количество членов ДС 31 человек, обозначим их $(A1, A2, \dots, A31)$ – , возможны 3 решения члена ДС ($Nc = 3$):

– присутствие на защите и заполнение бюллетеня – идентифицируется *числом* $B1$*:* $32^0 = 1$,

– голос «ЗА» присуждение ученой степени – идентифицируется числом $B2$: $32^1 = 32$,

– голос «НЕТ» присуждению ученой степени $B3$ идентифицируется числом $32^2 = 1024$.

Число 32 в данном случае является основанием системы счисления, в которой представляется сумма голосов членов ДС. При таком выборе основания системы счисления нет переноса из младшего разряда в старший при суммировании голосов, даже если все члены ДС проголосуют одинаковым образом. Максимально возможная сумма голосов всех членов ДС $T_{max} = 31 + 31 \cdot 1024 = 31\,775$.

В таблице показаны заполненные бюллетени от членов ДС (колонки 1-5) и зашифрованные бюллетени (колонка 6).

Генерация ключей производится программой, которую запускает секретарь диссовета. Программа реализует следующий алгоритм: (для простоты изложения размерность чисел уменьшена в примерно в 100 раз).

ТАБЛИЦА. Таблица из заполненных бюллетеней членовДС

Члены ДС	Решения членов ДС			Голос члена ДС-число – m	Зашифрованное значение голоса
	B1 (32^0)	B2 (32^1)	B3 (32^2)		
1	2	3	4	5	6
A1	v	v		$m = 32^0 + 32^1 = 33$	1375817496
A2	v	v		$m = 32^0 + 32^1 = 33$	1953742920
A3	v	v		$m = 32^0 + 32^1 = 33$	3671807970
A4	v		v	$m = 32^0 + 32^2 = 1025$	1667544822
,,,				…	…
A29	v		v	$m = 32^0 + 32^2 = 1025$	241382535
A30	v	v		$m = 32^0 + 32^1 = 33$	4847812779
A31	v	v		$m = 32^0 + 32^1 = 33$	3318512662
Итог	31	26	4	$\sum_{i=1}^{31} m_i = 4959$	

Выбираются два простых чисел p, q такие, что наибольший общий делитель $gcd(pq, (p-1)(q-1)) = 1$ вычисляются: $n = pq$. .$(n \geq T_{ma} + 1)$ и наименьшее общее кратное $\lambda = lcm(p-1)(q-1)$.

Пусть $p = 293,\ \ q = 433,\ n = pq = 126869;\ \ \ n^2 = 16095743161,$ $\lambda = 31536.$

Случайно генерируется число g $\in Z^*_{n^2},\ g = 6497955158$ и проверяется условие

$$gcd(\frac{g^{\lambda} mod(n^2-1)}{n}, n) = 1.$$

Вычисляем $\mu = \left[L\left(g^{\lambda}\ mod\ n^2\right)\right]^{-1}\ mod\ n$, где $\mathrm{L(u)} = \frac{u-1}{n}$ – наибольшее целое число, удовлетворяющее выражению $u - 1 \geq \mathrm{L(u)} \cdot n$.

$$\mu\ = \left[L\left(g^{\lambda}\ mod\ n^2\right)\right]^{-1}\ mod\ n = 53022.$$

Тогда $(n, g) = (126869, 6497955158) -$ открытый ключ

$$(\mu, \lambda) = (53022,\ \ 31536) -$$ закрытый ключ

Шифрование голоса m_i i-м членом ДС выполняется по формуле

$$E(m_i) = g^{m_i} * r_i^n\ mod\ n^2 =\ 6497955158^{mi} \times r_i^{126869} mod\ 16095743161,$$

где r_i – случайное число.

Зашифрованные значения голосов членов ДС представлены в таблице (последний столбец).

Сервер голосов в конце голосования получает не более чем 31 криптограмму (по числу членов ДС, присутствовавших на защите). Сервер голосов перемножает криптограммы и отправляет в счетную комиссию криптограмму – произведение:

$$T = \prod_{i=1}^{Nv} c_i \; mod \; n^2 = (8934407892 * 182720171 * 15841170776 * \ldots * 9362461590 * 12644107668 * 5108299233) \; mod \; 16095743161 = = 7689477671.$$

Счетная комиссия выполняет дешифрование криптограммы-произведения и согласно гомоморфному и свойству криптосистемы Пэйе вычисляет:

$$D(T) = \sum_{i=1}^{Nv} m_i \; mod \; n = L\left(T^{\lambda} mod \; n^2\right) * \mu \; mod \; n = 4959.$$

Для получения конечного результата необходимо преобразовать получившееся число в 32-ичную системе счисления [3].

$$4959_{10} = 4 * 32^2 + 26 * 32^1 + 31 * 32^0.$$

Анализируя данное представление числа, соответствующего сумме голосов в поданных бюллетенях, можно сделать вывод о том, что в голосовании принял участие 31 член ДС, за присуждение ученой степени подано голосов 26, против 4, недействительных голосов нет.

В представленной системе голосования выполняются следующие требования:

− тайна голосования обеспечивается за счет шифрования бюллетеня членом ДС;

− анонимность голоса члена ДС обеспечивается тем, что результатом расшифрования является сумма всех голосов ДС и невозможно определить, какой выбор сделал член ДС;

− оповещение о приеме бюллетеня обеспечивается отправкой сообщения сервером в личный кабинет члену ДС;

− исключается повторное голосование членом ДС путем блокировки доступа к серверу, после приема криптограммы от него.

Список используемых источников

1. О порядке присуждения ученых степеней: Постановление Правительства РФ от 24.09.2013 N 842 (ред. от 01.10.2018, с изм. от 26.05.2020).

2. Paillier P. Public key cryptosystems based on composite degree residue classes // In Proc. EUROCRYPT 1999, pp. 223–238.

3. Коржик В. И., Яковлев В. А. Основы криптографии: учебное пособие. СПб.: ИЦ Интермедиа, 2016.

УДК 519.876.5:519.6:004.357
ГРНТИ 49.03.03

О МНОГОКАНАЛЬНОЙ АУДИОСТЕГОСИСТЕМЕ НА ОСНОВЕ МАРКИРОВАНИЯ ЦИФРОВЫХ АУДИОСИГНАЛОВ

М. В. Гофман, А. А. Корниенко

Петербургский государственный университет путей сообщения Императора Александра I

Разрабатывается многоканальная аудиостегосистема на основе маркирования цифровых аудиосигналов, ориентированная на устойчивую передачу данных в условиях воздушного аудиоканала. Эта система позволяет выполнять внедрение элементов маркера в произвольные частотные составляющие цифрового аудиосигнала с учетом обеспечения слуховой транспарентности маркера и возможности слепого приёма. Разрабатываемая аудиостегосистема обеспечивает достаточную степень устойчивости при передаче маркированного аудиосигнала через воздушный аудиоканал даже при малых силах внедрения элементов маркера. Особое внимание уделяется разработке метода определения наличия маркера в аудиосигнале, принятом из воздушного аудиоканала. Решение о наличии маркера в аудиосигнале выносится по пороговому принципу на основании величины пик-фактора эксцесса целевой случайной величины. В качестве значений этой величины используются значения корреляционной функции между искомым маркером и цифровой последовательностью, извлеченной из записанного акустическими микрофонами аудиосигнала.

стеганография, маркирование аудиосигналов, скрытая передача данных.

Актуальность задачи маркирования аудиосигналов

Методы цифрового маркирования появились и получили широкое применение как средство скрытой передачи и защиты информации, подтверждения и защиты авторских прав. Поэтому традиционные методы цифрового маркирования аудиосигналов ориентированы на решение задач, связанных со слышимостью маркера и проблемами, которые создаёт нарушитель путём преднамеренных воздействий и преобразований на маркиро-

ванные аудиосигналы с целью извлечь маркер из аудиосигнала или разрушить маркер, при этом с минимальными потерями для качества аудиоинформации.

Методы цифрового маркирования аудиосигналов, ориентированные на передачу через воздушный аудиоканал, описаны в статьях [1, 2]. В них для передачи используется весь слышимый диапазон, что обычно повышает устойчивость маркера. Однако, из-за того, что маркер внедряется путём полной замены фаз, то такой способ внедрения может оказывать значительное влияние на слышимость маркера. Кроме этого, так как внедрение выполняется во все коэффициенты преобразования, то это не позволяет использовать, например, их номера в качестве возможного ключа, который был бы известен только авторизованному приёмнику, и применялся им для выделения частей маркера только из тех коэффициентов, индексы которых составляют ключ.

Длительное время в системах связи используется ортогональное частотно-разделённое мультиплексирование или OFDM (от англ. orthogonal frequency division multiplexing). В работе [3] предлагается методика и система цифрового маркирования аудиосигналов, названная авторами системой «Dolphin», которая использует OFDM, и позволяет выполнять передачу информации маркированными аудиосигналами через воздушный аудиоканал. Система Dolphin выполняет внедрение маркера в диапазон частот от 8 до 20 кГц. В системе Dolphin используется адаптивный метод маркирования, основанный на анализе распределения энергии в маркируемом аудиосигнале перед выбором метода модуляции аудиосигнала для каждого информационного пакета. В этой системе используется один из двух методов, либо амплитудная манипуляция ASK (от англ. *amplitude shift keying*), либо так называемый метод усреднённой энергии спектральной плотности EDK (от англ. *average energy spectrum density keying*). Приёмник определяет использованный передатчиком метод модуляции, опираясь на сведения, извлекаемые из преамбулы пакета. Так как диапазон частот меньших 8 кГц не используется для внедрения маркера, то систему Dolphin нельзя отнести к тем, которые используют весь слышимый диапазон частот. Вследствие того, что внедрение выполняется по результатам энергетического анализа аудиосигнала, при этом сам исходный аудиосигнал обычно не известен получателю, то это затрудняет использование ключей, опираясь на которые авторизованный приёмник точно бы знал, какие части аудиосигнала будут содержать скрытую информацию.

В работе [4] предлагается методика цифрового маркирования аудиосигналов, которая также ориентирована на связь через воздушный аудиоканал. Её особенностью является то, что она предполагает передачу маркированных аудиосигналов между смарт-устройствами, обычно смартфонами. При передаче используется диапазон частот от 19,5 до 22 кГц. В качестве

переносчиков используются чирп-сигналы (от англ. *chirp signal*), ещё их называют линейно-частотно-модулированные сигналы или ЛЧМ-сигналы. Из-за того, что передача ведётся только в области высоких частот, близкой к ультразвуковому и отчасти ультразвуковому диапазону частот, то предъявляются особые требования к микрофонам и динамикам. По утверждениям авторов, эта методика позволяет выполнять передачу на расстояния до 25 м.

В работе [5] предлагается система цифрового маркирования аудиосигналов, ориентированная на организацию связи на малых расстояниях до 10–15 см. Передача ведётся в частотном диапазоне от 6 до 7 кГц. При этом окружающий шум используется в качестве скрывающего сигнала. Если уровень окружающего шума падает ниже определённого уровня, то передача прекращается в целях безопасности.

Постановка задачи и путь её решения

Таким образом, среди нерешённых задач остается следующая – допустимость внедрения в произвольные частотные составляющие при сохранении возможности слепого приема маркированных аудиосигналов. В этой работе разрабатывается многоканальная аудиостегосистема на основе маркирования цифровых аудиосигналов по методу, разработка которого была начата в работах [6, 7]. Разрабатываемая модель ориентирована на обеспечение достаточной устойчивости маркирования при передаче маркированного аудиосигнала через воздушный аудиоканал. Особенностью разрабатываемой модели является возможность внедрения маркера в требуемые частотные составляющие маркируемого аудиосигнала, а также отсутствие необходимости приёмнику знать аудиосигнал, который был подвергнут маркированию. Таким образом появляется возможность реализации слепого приёма. В выполненной авторами работе разработке подвергается та часть модели, с помощью которой выполняется детектирование наличия маркера в сигнале, принятом из акустического канала. Практическая работоспособность этого блока модели была подтверждена результатами натурных экспериментов передачи маркированных аудиосигналов через воздушный акустический канал в условиях значительного постороннего акустического шума.

Результаты натурных экспериментов

В качестве аппаратных средств использовалась доступная и недорогая аппаратура: четыре динамика Edifier R1280DB, микрофон AKG Lyra. Натурные эксперименты показали, что, когда отношение среднего значения амплитуд отсчетов принятого цифрового маркированного аудиосигнала к среднему значению амплитуд отсчетов переданного цифрового маркированного аудиосигнала превышает -12 дБ, можно ожидать, что вероятность

ложного детектирования наличия маркера будет меньше 10^{-6}, а вероятность восстановления информации при отсутствии ошибки детектирования наличия маркера была меньше 10^{-3}. Натурные эксперименты показали, что разработанный метод обеспечивает вероятность удачной передачи информации маркированными аудиосигналами не меньше $1 - 10^{-9}$.

Заключение

Результаты имитационного моделирования и натурных экспериментов показали, что разрабатываемая модель аудиостегосистемы позволяет осуществлять скрытую передачу информации в слышимом диапазоне частот. Особенностью процесса детектирования является то, что в нём используются пик-факторы эксцессов целевой случайной величины, значения которой вычисляются на основе значений отсчетов записываемого микрофоном аудиосигнала.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ; Соглашение № 7/2020).

Список используемых источников

1. Yun H. S., Cho K., Kim N. S. Acoustic data transmission based on modulated complex lapped transform // IEEE Signal Processing Letters. 2010. Vol. 17. No. 1. pp. 67–70.

2. Cho K., Baek S., Moon H. G., Kim N. S. Multi-microphone approach for reliable acoustic data transmission // 2016 IEEE International Conference on Consumer Electronics (ICCE). IEEE. 2016. pp. 557–560.

3. Wang Q., Ren K., Zhou M., Lei T., Koutsonikolas D., Su L. Messages behind the sound: real-time hidden acoustic signal capture with smartphones // Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, New York City, New York, USA. 2016. pp. 29–41.

4. Nandakumar R., Chintalapudi K. K., Padmanabhan V., Venkatesan R. Dhwani: secure peer-to-peer acoustic NFC // ACM SIGCOMM Computer Communication Review. 2013. Vol. 43. No. 4. pp. 63–74.

5. Lee H., Kim T. H., Choi J. W., Choi S. Chirp signal-based aerial acoustic communication for smart devices // 2015 IEEE Conference on Computer Communications (INFOCOM). IEEE. 2015. pp. 2407–2415.

6. Гофман М. В. Методика скрытой передачи данных при связи через воздушный аудиоканал // Труды СПИИРАН. 2017. Вып. 2. С. 97–122.

7. Гофман М. В., Корниенко А. А., Мирончиков Е. Т., Никитин А. Б. Цифровое маркирование аудиосигналов для робастной скрытой акустической связи через воздушный аудиоканал // Труды СПИИРАН. 2017. Вып. 6. С. 185–215.

УДК 004.942
ГРНТИ 49.33.01

ОБЗОР МОДЕЛИ АВТОРЕГРЕССИИ И ПРОИНТЕГРИРОВАННОГО СКОЛЬЗЯЩЕГО СРЕДНЕГО ARIMA ДЛЯ ПРОГНОЗИРОВАНИЯ СЕТЕВОГО ТРАФИКА

А. А. Гребенщикова, В. С. Елагин

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

Прогнозирование сетевого трафика представляет значимый интерес в таких областях, как: отслеживание перегрузок в сети, контроль потоков данных и сетевое управление. Тщательно подобранная модель трафика способна выявить и предсказать важнейшие характеристики сетевого трафика: кратковременные и долговременные процессы, а также самоподобность трафика на больших временных масштабах. Наиболее популярной моделью прогнозирования являются модели авторегрессии и проинтегрированного скользящего среднего (ARIMA). Модель ARIMA является важным классом параметрических моделей, который позволяет описывать нестационарные ряды. Современные исследования показывают, что использование обычной модели ARIMA дает большую частоту ошибок по сравнению с комбинированной моделью ARIMA с другими методиками. Поэтому крайне важно разобрать не только функционирующий состав такой модели, но также и рассмотреть возможные комбинации для более удачного прогноза сетевого трафика.

прогнозирование трафика, модели трафика данных, модели ARIMA, модели GARCH, самоподобность, мультифрактальность.

Точность модели для прогнозирования сетевого трафика характеризуется определением таких основных характеристик, как зависимости в кратковременной и долгосрочной перспективе, самоподобность на больших временных масштабах и мультифрактальность на малых. Модель ARIMA/GARCH является нелинейной моделью временных рядов, которая объединяет линейную модель авторегрессии и проинтегрированного скользящего среднего и обощённую модель авторегрессионной условной гетерраскодичности GARCH [1].

Модели ARIMA

Согласно [2], модели авторегрессии и проинтегрированного скользящего среднего (ARIMA) – это важный класс параметрических моделей, который позволяет описывать нестационарные ряды. Краткая запись модели описывается, как.

$$\varphi(B)(1-B)^{d}\beta_t = \theta(B)a_t, \quad (1)$$

где β_t – временной ряд для анализа;

α_t – белый шум;

B – оператор сдвига назад ($B\beta_t = \beta_{t-1}$);

φ() и θ() – полиномы степени p и q;

d – порядок взятия последовательной разности ($\Delta\beta_t = \beta_{t-1} - \beta_t = (1 - B)^d \beta_t$ …).

При попытке разобраться в структуре ARIMA, важно сразу уточнить, что основной составляющей модели является недетерминированный ряд, рассматривающийся при анализе реализацией стохастического процесса [3].

Стохастический процесс – модель, описывающая вероятностную структуру последовательности наблюдений. Важным классом такого наблюдения является стационарный процесс, для описания которого успешно используются автокорреляционные функции. Также, стоит отметить частные случаи стохастических стационарных процессов при моделировании временных рядов: авторегрессия, скользящие средние и смешанные процессы между этими двумя составляющими. При рассмотрении сетевого трафика, подразумевается наличие нестационарных характеристик, поэтому из стационарных процессов выводится новый класс нестационарных – модели авторегрессии и проинтегрированного скользящего среднего.

При построении моделей с определённым количеством неизвестных параметров очень важно учитывать такой фактор, как экономия. Данный аспект определяет использование интеративных подходов и осторожности при выборе параметров.

Интеративный подход

Модели ARIMA (p, q) представляют особый класс нестационарных моделей, которые считаются однородными и находятся в статистическом равновесии. Модель ARIMA определяется уравнением (1) и, согласно [3], такая модель является обобщённой, т. к. включает в себя в качестве частных случаев следующие модели: авторегрессионные, скользящего среднего, смешанные модели авторегрессии-скользящего среднего и интеграция всех трёх соответственно.

Эффективная итеративная процедура построения моделей для описания зависимости наблюдаемых временных рядов состоит из трёх этапов:

1. Идентификация. Подразумевает использование уже имеющихся данных о временном ряде, чтобы подобрать соответствующий и оптимальный класс моделей для последующей оценки.

2. Оценка. Подразумевает выявление сопутствующих параметров для построения модели.

3. Диагностика. Подразумевает проверку модели на соответствие имеющимся данным, чтобы выявить несоответствия и определить оптимальные пути улучшения модели.

Структура ARIMA

Авторегрессионная модель AR (p) – выражает текущее значение процесса как конечную линейную совокупность предыдущих значений процесса и импульса белого шума:

$$\varphi(B)\tilde{\beta}_t = a_t, \quad (2)$$

где $\beta_t = \beta_t - \mu$ – уровень временного ряда в момент времени t (зависимая переменная) с учётом разности значения процесса относительно параметра уровня μ;

$\varphi(B) = 1 - \varphi_1 B - \varphi_2 B^2 - \ldots - \varphi_p B^p$ – оператор авторегрессии порядка ρ.

Модель скользящего среднего MA (q) дает прогноз значений функции β_t на основе линейной комбинации ограниченного числа q остатков, в то время как авторегрессионные модели AR (p) дают прогноз значения β_t на основании линейной функции аппроксимации ограниченного числа p прошлых значений β_t:

$$\tilde{\beta}_t = \theta(B)a_t, \quad (3)$$

где $\theta(B) = 1 - \theta_1 B - \theta_2 B^2 - \ldots - \theta_p B^p$ – оператор скользящего среднего порядка q.

Авторегрессионную модель и модель со скользящим средним можно объединить. Модель авторегрессии и скользящего среднего ARMA (p,q), где p – порядок авторегрессионной части модели, q – порядок части скользящего среднего, записывается как:

$$\varphi(B)\tilde{\beta}_t = \theta(B)a_t.$$

Данная модель позволяет составлять прогноз, зависящий как от текущего и прошлого значений зависимой переменной, так и от текущих и прошлых значений величины случайного возмущения [4].

Модели GARCH

Экспоненциальный спад автокорреляционной функции моделей ARIMA дает им возможность фиксировать только характеристики зависимостей в краткосрочной перспективе времени [5]. Однако в [6] уже было

продемонстрировано, что данные о трафике описываются также и высокой степенью зависимостей на больших временных масштабах.

Согласно [2], модель GARCH происходит от модели авторегрессионной условной гетероскедастичности ARCH и предполагает, что:

$$\alpha_t = \sigma_t e_t,$$

где e_t – последовательность независимых и одинаково распределённых случайных величин со средней равной нулю и дисперсией равной единице.

Модель GARCH(s, r) записывается, как:

$$\sigma_t{}^2 = \alpha_0 + \sum_{i=1}^{s} \alpha_i \alpha_{t-i}{}^2 + \sum_{j=1}^{r} \beta_j \sigma_{t-j}{}^2,$$

где $\alpha_0 > 0$, $\alpha_i \geq 0$, $i = 1, \ldots, s-1$, $\alpha_s > 0$, $\beta_j \geq 0$, $j = 1, \ldots, r-1$, $\beta_r > 0$.

Согласно [6], с помощью ARIMA/GARCH можно провести такую оценку параметров, что посредством адаптивной схемы прогнозирования можно успешно фиксировать как нестационарные характеристики, так и изменяющийся рост трафика.

Адаптивная схема прогнозирования

Пошаговая оценка параметров модели ARIMA (p, d, q) / GARCH (s, r) продемонстрирована на рис.

Некоторые из этих этапов описываются, как [6]:

1. Необходимо установить параметр d, обозначающий порядок разности, как это делается при интеративном подходе (с помощью АКФ).

2. Для получения стационарного ряда исследуется характер поведения выборочных АКФ и частных АКФ (ЧАКФ), т.е. выдвигаются гипотезы о значениях параметров p (порядок авторегрессии) и q (порядок скользящего среднего). Таким образом, определяется параметр скользящей средней порядка q (3) и порядок p параметра авторегрессии (2).

Рис. Процесс оценки параметров модели ARIMA/GARCH

3. Необходимо определить параметры второй части модели: s и r. Для этого полученные параметры p и q приравниваются к нулю, чтобы оперировать с моделью ARIMA (0, *d*, 0) / GARCH (*s*, *r*) было удобнее.

Параметры нелинейной модели ARIMA/GARCH фиксируют статистические характеристики трафика и способны подробно описать данные в выбранном временном промежутке. Изучение их влияния на производительность сети может быть полезно для оценки трафика и последующего управления сетью. Таким образом, оценка параметров нелинейной модели ARIMA/GARCH отличается от классических моделей прогнозирования повышенной точностью в изучении поведения трафика и способностью фиксировать условную дисперсию.

Стоит отметить, что определение порядка параметров модели GARCH (*s*, *r*) можно инициализировать с помощью АКФ и ЧАКФ, как это описывалось при установлении порядка разности *d*. А когда необходимо оценить параметры модели, для этих целей используется метод максимального правдоподобия (ММП).

Заключение

Точная модель предсказания трафика должна иметь возможность фиксировать значимые характеристики: например, зависимости в краткосрочной и долгосрочной перспективе, самоподобие на больших временных масштабах и высокий уровень мультифрактальности на малых масштабах времени. По этим причинам вводятся модели временных рядов для моделирования и предсказания сетевого трафика. Основная цель внедрения и предложения модели ARIMA в специализированной литературе — возможность прогнозирования. Не смотря на достоинства такой модели, была выявлена невозможность ARIMA качественно уловить специфичные характеристики сетевого трафика, как “всплески”. Согласно [1], внедрение модели GARCH обусловлено наличием у последней изменяющейся во времени дисперсии, в отличие от ARIMA с достаточно постоянной дисперсионной составляющей.

Список используемых источников

1. Rutka G. Network Traffic Prediction using ARIMA and Neural Networks Models // Electronics And Electrical Engineering. 2008. № 4.

2. Крюков Ю. А., Чернягин Д. В. ARIMA – модель прогнозирования значений трафика // Информационные технологии и вычислительные системы. 2011. № 2. С. 41–49.

3. Box G. E. P., Jenkins J. M. Time series analysis: Forecasting and control, Holden-Day, San Francisco, CA, 1976.

4. Трегуб А. В., Трегуб И. В. Методика построения модели ARIMA для прогнозирования динамики временных рядов // Вестник Московского государственного университета леса – Лесной вестник. 2011. № 5. С. 179–183.

5. Shu Y. Traffic prediction using FARIMA models // ICC. 1999, vol. 2. pp. 891–895.

6. Zhou B. Network traffic modeling and prediction with ARIMA/GARCH // Proceeding of the third international working conference: performance modelling and evaluation of heterogeneous networks (HETNETs'05), Ilkly, UK, July 2005.

УДК 336.743
ГРНТИ 49.03.05

ОБЗОР ФИЛЬТРОВ-ПРОТОТИПОВ, ПРИМЕНЯЕМЫХ В ТЕХНОЛОГИЯХ ПЕРЕДАЧИ ДАННЫХ НА МНОГИХ НЕСУЩИХ

И. В. Гришин, С. Н. Михеева, К. А. Подгорная

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

Активный рост мобильного интернет-трафика, наблюдаемый в последние годы, приводит к необходимости совершенствования и развития технологий радиодоступа. Метод ортогонального частотного мультиплексирования OFDM стал одним из наиболее используемых в широкополосной беспроводной связи. Это было обусловлено такими достоинствами метода как: высокая помехоустойчивость к частотно-селективным замираниям и аддитивным помехам, а также простота формирования и обработки сигналов. В то же время технология OFDM обладает рядом недостатков, таких как чувствительность к частотным сдвигам и медленным ослаблением спектра сигналов вне выделенной под передачу полосы частот, что приводит к внеполосным излучениям. В связи с этим технология OFDM была модернизирована до технологии F-OFDM (filtered OFDM), что подразумевает фильтрацию внеполосных излучений. В докладе производится сравнительный анализ фильтров-прототипов, применяемых в данной технологии.

OFDM, F-OFDM, RC, SRRC, фильтр Эрмита.

Технология ортогонального частотного мультиплексирования OFDM позволяет максимально эффективно использовать отводимую под передачу полосу частот. Разбиение отводимого под передачу диапазона частот на множество узкополосных подканалов позволяет добиться минимизации амплитудно-частотных и фазо-частотных искажений в каждом подканале. Также в значительной степени снижается влияние аддитивных помех, поскольку в каждый подканал проходит только часть их спектральных составляющих. Вышеперечисленные факторы позволяют обеспечить приближающуюся к пропускной способности скорость передачи данных в каждом подканале. Сигнал OFDM получается путём объединения сигналов, передаваемых в подканалах. Центральные частоты подканалов, соответствующие

частотам поднесущих гармонических колебаний, обеспечивают ортогональность данных поднесущих. Эффективность использования спектра может быть увеличена за счет перекрытия подканалов. Выигрыш по ширине полосы частот в случае перекрывающихся подканалов может достигать двух раз. Для борьбы с межсимвольной интерференцией к символам OFDM добавляется циклический префикс (ЦП), представляющий копию конечной части передаваемого символа заданной длины, что упрощает процедуру обнаружения начала символов в принимаемом OFDM сигнале, но снижает скорость передачи данных и нарушает ортогональность поднесущих. Данные характеристики классических сигналов с OFDM являются результатом использования огибающей символов прямоугольной формы, которая имеет наихудшие характеристики по спектральной эффективности, если рассматривать со стороны скорости спада внеполосных излучений.

Вышеперечисленные недостатки технологии OFDM, могут быть значительно уменьшены в случае применения фильтров-прототипов на передающей и приёмной сторонах (filtered OFDM, f-OFDM), при этом сохраняя преимущества данной технологии [1]. Блок-схема оборудования представлена на рис. 1.

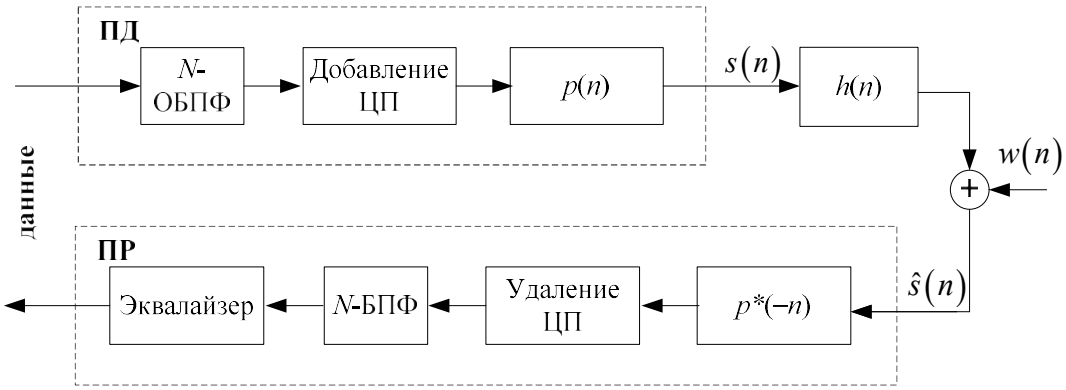


Рис. 1. Блок-схема системы связи f-OFDM

Так как у импульсов прямоугольной формы значительная часть энергии 9,5 % приходится на боковые лепестки спектра (рис. 2) [2], то с целью предотвращения взаимного влияния между различными станциями разнос по частоте для данных станций должен быть весьма велик. В статье рассматриваются фильтры-прототипы, позволяющие сформировать такие сигналы, у которых энергия сосредоточена в заданной полосе частот, отведенной под передачу, и не рассеивается вне её пределов.

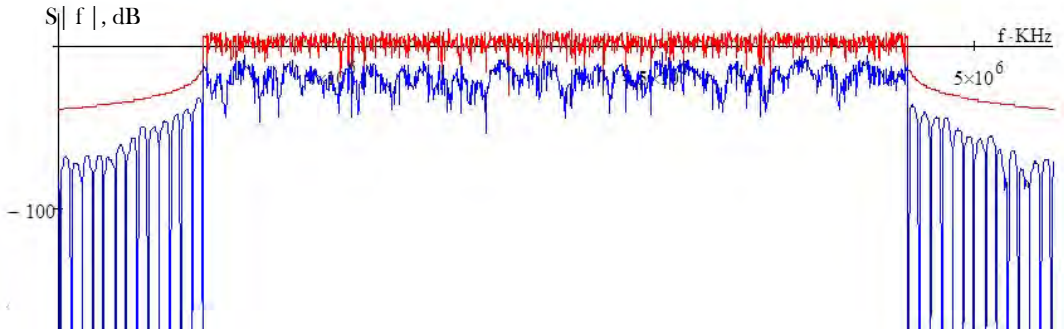


Рис. 2. Спектры сигналов OFDM с ЦП (красный) и без ЦП (синий)

Оконные функции имеют спектры с лепестками. У прямоугольного спектра сигнала ширина лепестков равна единице, у других оконных функций она может быть больше единицы. Оконные функции применяются для повышения локализации сигнала в частотной и временной областях таким образом, чтобы можно было исключить применение циклического префикса или значительно уменьшить его длину. Основным достоинством применения оконных функций и фильтра Найквиста можно указать возможность сужения полосы сигнала вплоть до теоретического предела 1 бит/с на 1 Гц полосы с полным подавлением боковых лепестков. Для этого в работе были рассмотрены оконные функции приподнятого косинуса, корня приподнятого косинуса и фильтр Эрмита.

Оконная функция приподнятого косинуса RC

Одним из фильтров относящихся к типу фильтров Найквиста является фильтр с характеристикой в виде приподнятого косинуса (*raised cosine*, RC), импульсная характеристика которого может быть описана выражением:

$$p(t,\beta) = \operatorname{sinc}\left(\frac{t}{T}\right)\frac{\cos\left(\frac{\pi\beta t}{T}\right)}{1-\left(\frac{2\pi\beta t}{T}\right)^2},$$

и представлена на рис. 3. Как видно из рисунка, сумма последовательных импульсов сигнала после фильтрации равна нулю в моменты выборки сигнала, и поэтому они не искажают предыдущие или последующие импульсы в соответствующие моменты выборки.

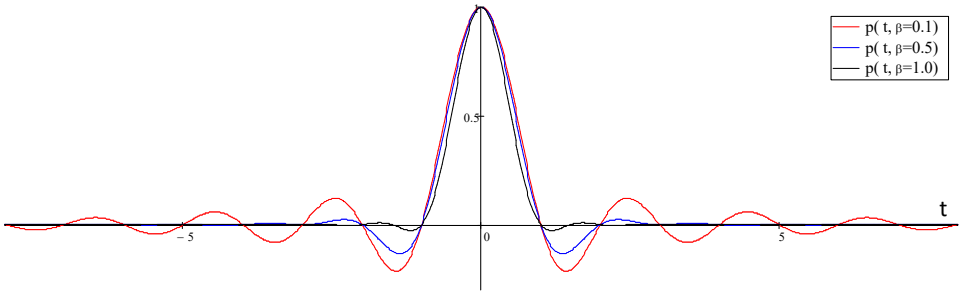


Рис. 3. Импульсная характеристика фильтра RC
с разными коэффициентами сглаживания

Передаточная функция фильтра приподнятого косинуса получается через преобразование Фурье импульсной характеристики $H_{RC}(f,\beta) \Leftrightarrow p(t,\beta)$. Выражение, описывающее амплитудно-частотную характеристику фильтра, имеет вид:

$$\left|H_{RC}(f,\beta)\right| = \begin{cases} 1, \ |f| < \dfrac{1-\beta}{2T_s} \\ 0.5\left(1+\cos\left(\dfrac{\pi T_s}{\beta}\left(|f| - \dfrac{1-\beta}{2T_s}\right)\right)\right), \ |f| \in \left(\dfrac{1-\beta}{2T_s}, \dfrac{1+\beta}{2T_s}\right) \\ 0, f > \dfrac{1+\beta}{2T_s} \end{cases}.$$

Графики спектров импульсов на выходе RC фильтра-прототипа, представлены на рис. 4, из которого видно, что увеличения значения коэффициента сглаживания β приводит к увеличению ширины основного лепестка (в 1,5 для β = 0,5 и в 2 раза для β = 1), и резкому снижению уровня боковых лепестков (более чем на 70 дБ для β > 0,1).

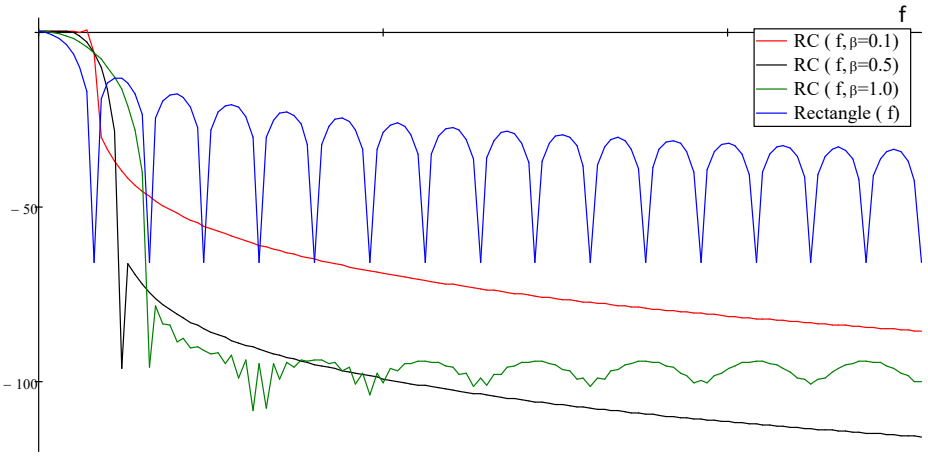


Рис. 4. Нормированные спектры прямоугольной оконной функции
и функции RC для трех значений β

В результате передача дискретного сигнала происходит без межсимвольной интерференции.

Оконная функция корня приподнятого косинуса SRRC

При последующем уменьшении отводимой под передачу полосы частот существуют исключения, при которых намеренно допускается межсимвольная интерференция в канале передачи. В этом случае применяется фильтр-прототип корня приподнятого косинуса, импульсная характеристика (рис. 5) которого описывается выражением:

$$p(t,\beta)=\begin{cases}\frac{1}{T}\left(1+\beta\left(\frac{4}{\pi}-1\right)\right), & t=0\\ \frac{1}{T\sqrt{2}}\left(1+\frac{2}{\pi}\right)\sin\left(\frac{\pi}{4\beta}\right)+\left(1-\frac{2}{\pi}\right)\cos\left(\frac{\pi}{4\beta}\right), & t=\pm\frac{T}{4\beta}\\ \left(\sin\left(\frac{\pi t}{T}(1-\beta)\right)+4\beta\frac{t}{T}\cos\left(\frac{\pi t}{T}(1+\beta)\right)\right)\left(\pi t\left(1-\left(\frac{2\beta t}{T}\right)^2\right)\right)^{-1}, & \text{otherwise}\end{cases}$$

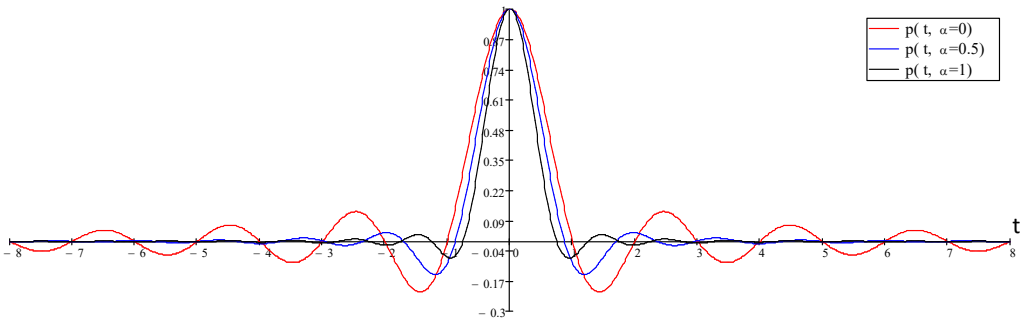


Рис. 5. Импульсная характеристика фильтра корня приподнятого косинуса с различными коэффициентами сглаживания

Передаточная функция фильтра может быть получена путем извлечения корня из передаточной функции RC фильра: $H_{SRRC}(f,\beta)=\sqrt{H_{RC}(f,\beta)}$.

Графики спектров импульсов на выходе SRRC фильтра-прототипа, представлены на рис. 6, из которого видно, что увеличения значения коэффициента сглаживания β приводит к аналогичному для RC фильтра-прототипа увеличению ширины основного лепестка, и резкому снижению уровня боковых лепестков (более чем на 60 дБ для β > 0,5).

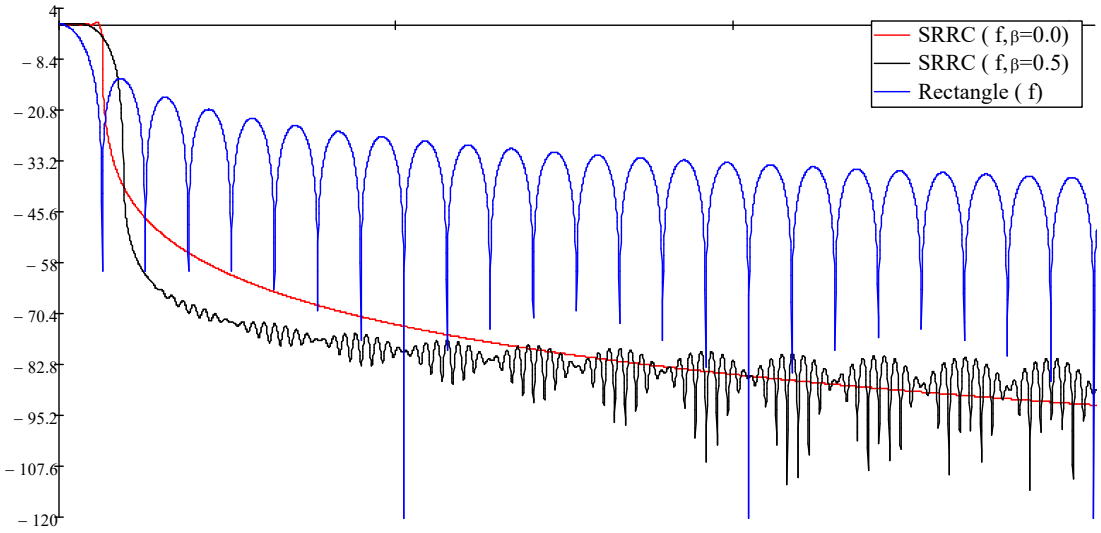


Рис. 6. Нормированные спектры прямоугольной оконной функции и функции SRRC для трех значений β

Оконная функция Эрмита

Фильтр Эрмита получается из линейных комбинаций функций Эрмита-Гаусса. Путем деформации фильтра Гаусса функциями Эрмита высокого порядка обеспечивается переход через ноль, который удовлетворяет критерию Найквиста [3]. Импульсная характеристика фильтра (рис. 7) имеет вид:

$$p(t)=\sum_{k=0}^{N}\alpha_{4k}\varphi_{4k,\infty,\infty}(t)$$

где $\varphi_n(t)=H_n\left(\sqrt{2\pi}t\right)\cdot e^{-\pi t^2}$ и $H_n(t)=(-1)^n e^{t^2}\cdot\dfrac{d^n}{dt^n}e^{-t^2}$.

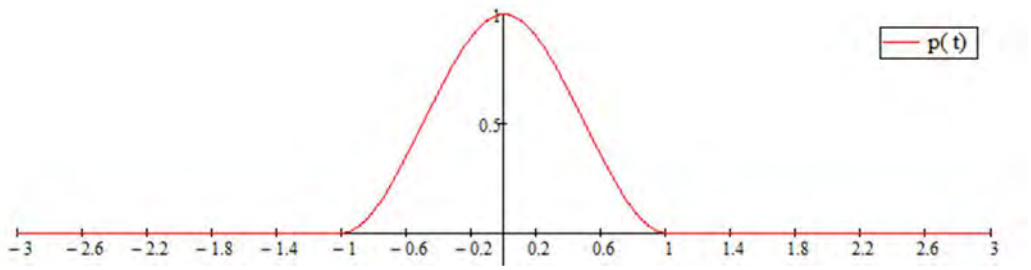


Рис. 7. Импульсная характеристика фильтра Эрмита

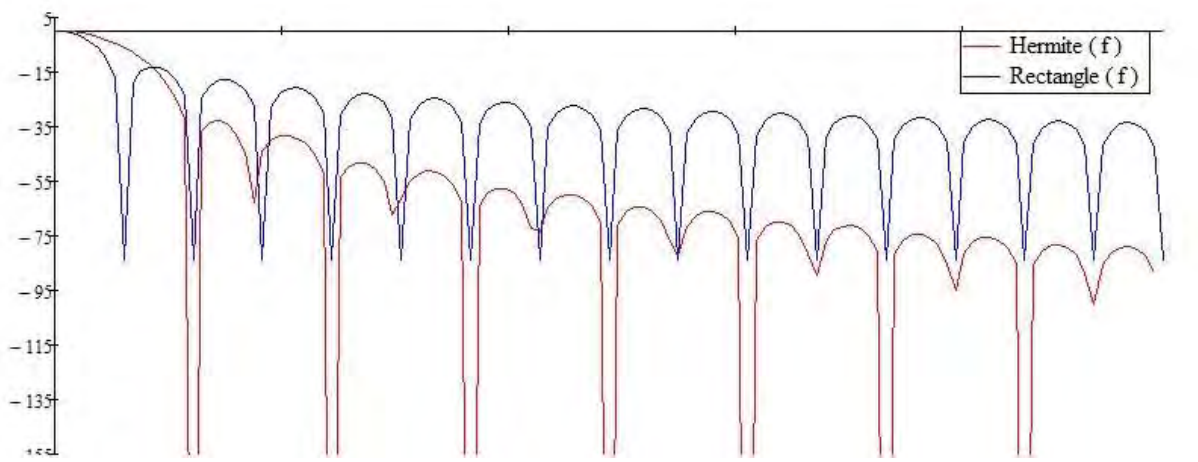


Рис. 8. Нормированный спектр фильтра Эрмита

На рис. 8 представлены графики импульсов на выходе фильтра Эрмита, где можно увидеть увеличение ширины основного лепестка вдвое по сравнению со спектром прямоугольного импульса, а также снижение уровня боковых лепестков (на 40 дб).

Рассмотренные фильтры-прототипы позволяют эффективно подавить внеполосное излучение и тем самым повысить эффективность использования частотного ресурса. Также применение фильтров позволяет формировать сигналы, хорошо локализованные в частотной и временной областях, что позволяет эффективно бороться с межсимвольной и межканальной интерференциями, оказывающими в ряде случаев серьёзное влияние на сигналы OFDM.

Список используемых источников

1. Abdoli J., Jia M., Ma J. Filtered OFDM: A new waveform for future wireless systems // 2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). IEEE, 2015. pp. 66–70.

2. Zhang, X., Jia, M., Chen, L., Ma, J., & Qiu, J. Filtered-OFDM – Enabler for Flexible Waveform in The 5th Generation Cellular Networks // Accepted to IEEE Globecom, San Diego, CA, Dec. 2015. pp. 1–6.

3. Штыков В. В., Балакин Д. А. Построение ортогонального банка фильтров на основе преобразований эрмита для обработки сигналов // Журнал радиоэлектроники. 2014. № 9. 8 с.

УДК 004
ГРНТИ 49.33.29

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ BLOCKCHAIN

В. Д. Гулевич, В. С. Елагин, А. В. Лошакова, А. В. Помогалова

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

Целью данной работы является разработка информационной системы электронного голосования на основе технологии Blockchain, которая автоматизирует процесс проведения процедур голосования, а также обеспечит прозрачность, доступность, анонимность и невозможность фальсификации голосов. Актуальность разработанной системы заключается в возможности проведения процедуры голосования, дистанционно с использованием компьютера или телефона, что значительно сэкономит время участников голосований, а также уменьшит контакты с другими людьми, что является особо значимым во время карантинных мер. Результатом работы является разработанная децентрализованная информационная система на базе платформы Ethereum, в рамках которой пользователи могут выражать свое мнение при помощи голосования по интересующим их темам. В работе рассматриваются особенности реализации информационной системы, разработанные функциональные возможности и вопросы, касающиеся безопасности проведения процедуры голосования с использованием разработанной системы.

блокчейн, система голосования, смарт-контракт, умный контракт, защищенная система голосования, Ethereum.

В современном мире большое количество внимания уделяется процедурам голосования. Они проводятся по различным направлениям: начиная от бытовых вопросов, заканчивая общегосударственными проблемами [1].

Но существующие системы голосования имеют множество недостатков, которые вызывают недоверие у общества. Помимо этого, они слабо защищены от атак, что ставит под сомнение подлинность результатов голосования. Так, например, при традиционной форме голосования важную роль играет человеческий фактор, который отражается в принятии человеком ошибочных решений и действий преднамеренного и непреднамеренного характера [2]. Из этого следуют различные негативные обстоятельства:

– ошибки в подсчете голосов от утомления или недомогания [2];

– необходимость большого количество времени для определения результатов голосования и занесения их в соответствующие протоколы [2];

– фальсификация и порча бюллетеней [3];

– заведомо неправильный подсчет голосов [3];

– замена действительных бюллетеней [3].

Для повышения уровня доверия участников голосований и повышения вероятности исключения ошибок и фальсификации применяются бумажно-электронные и электронные системы голосования. Бумажно-электронная система представляет собой заполнение в ручном режиме бюллетеней и подсчет их в электронном виде [2]. Такой способ не исключает способ выбора варианта голосования ручкой в бумажном бюллетене, что не может полностью исключить подмену голосов. В случае электронной системы голосования, которая включает в себя различные виды голосования, которые обеспечивают подачу и подсчет голосов [4], выделяются следующие достоинства:

– отсутствие затрат на подготовку бумажных бюллетеней;
– отсутствие вмешательства в процесс подсчета голосов.

Одной из разновидностью системы электронного голосования является дистанционное голосование, которое осуществляется средствами технологии Blockchain. Такой подход не требует наличия избирателя на избирательном участке [5]. Blockchain – это распределенная база данных, в которой отсутствует общий сервер хранения данных. Такая база хранит в себе постоянно растущий список упорядоченных записей, которые называются блоками. База защищена от подделки. Каждый блок содержит метку времени и хэш предыдущего блока. Для записи нового блока необходимо последовательное считывание информации о старых блоках [6]. Для того, чтобы новый блок был принят другими пользователями сети, он должен удовлетворять определенным требованиям, которые варьируются от выбранного протокола и алгоритма консенсуса [5].

С целью предотвращения фальсификации информации каждая транзакция внутри блока подписывается электронной цифровой подписью. Электронно-цифровая подпись образована преобразованием информации с использованием криптографического алгоритма. Она основывается на использовании блочного шифрования и хеш-функции [6].

Разработанная система для электронного голосования на основе технологии Blockchain обеспечивает прозрачность, доступность, невозможность подделки голосов и внесений корректировок. Она предназначена для проведения голосований в рамках университета.

Идея использования данной технологии заключается в обеспечении возможности для каждого студента проголосовать строго единожды и всегда иметь возможность отследить свой голос в единой системе. Также проголосовавший может в режиме реального времени просматривать статистику голосования и следить за ходом выборов.

Информационная система имеет три группы пользователей: гость (посетитель без личного кабинета), пользователь и администратор. Каждая группа имеет свой набор прав:

– гость может просматривать список всех голосований и их результатов;

– пользователь имеет право просматривать все голосования и их результаты, а также принимать участие в них;

– администратор просматривает все голосования и их результаты, а также создает новые и удаляет предыдущие, не являющиеся больше актуальными.

Для разработки смарт-контракта, включающего в себя алгоритм проведения голосования использован язык Solidity. После разработки и тестирования смарт-контракт устанавливается в блокчейн-сеть. Для установки и дальнейшего функционирования в рамках разработки проекта была использована платформа Ethereum.

Для упрощения пользования системой также была разработана вебстраница, архитектура связи которой со смарт-контрактом представлена на рис. 1.

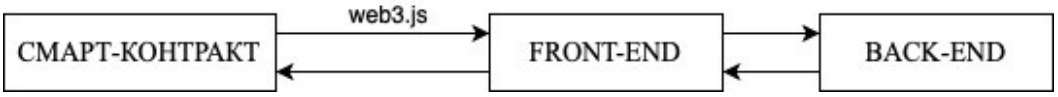


Рис. 1. Структура работы информационной системы

Для взаимодействия с графическим интерфейсом пользователя применяется библиотека web3.js.

К основным возможностям разрабатываемой системы голосования относятся:

- Регистрация. После прохождения регистрации у пользователя создается кошелек, на который будут приходить токены для голосования.
- Создание голосования. Администратор создаёт опрос с тремя выбранными кандидатами.
- Процесс голосования. Для передачи голоса пользователя необходимо отправить на кошелек выбранного варианта токен. Суммарное количество токенов на кошельке кандидатов обозначает результат голосования.
- Защита от двойного голосования. Прежде чем транзакции будут добавлены в блокчейн, они проверяются на предмет того, поступали ли уже токены на данный кошелек от этого пользователя, в рамках проводимого голосования.
- Подсчет голосов. Как только все пользователи, имеющие доступ к голосованию, сделали свой выбор или как только закончилось время

для голосования, система суммирует все токены, которые скопились на кошельках кандидатов, и объявляет победителя.

На рис. 2 представлен алгоритм регистрации выбора пользователя в системе электронного голосования.

Разработанная система функционирует согласно требованиям, определенным перед разработкой. Как итог можно заключить, что для дальнейшего развития данного проекта необходимо внести некоторые усовершенствования. В частности, модифицировать смарт-контракт и переработать его в формат контракта-фабрики, чтобы каждое новое голосование представляло из себя новый полноценный смарт-контракт, изготавливаемый системой автоматически по шаблону. Также авторы работы рассматривают возможность перехода на альтернативную блокчейн-платформу или разработку собственного блокчейн-решения с целью оптимизации скорости работы масштабирования системы.

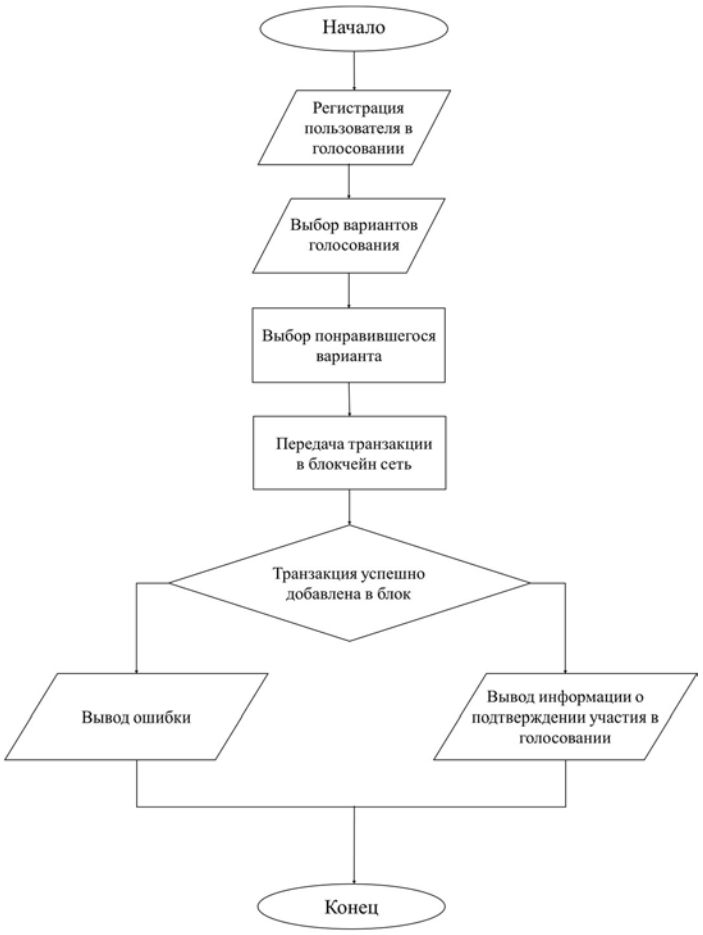


Рис. 2. Алгоритм регистрации голоса

Список используемых источников

1. Пескова О. Ю., Половко И. Ю., Фатеева С. В. Обзор подходов к организации электронного голосования // Известия Южного федерального университета. Технические науки. 2014. №. 2 (151). С. 237–247.

2. Богдан Ю. И., Веселая О. О. Анализ существующих систем голосования // Восточно-Европейский журнал передовых технологий. 2011. № 1 (2). С. 33–37.

3. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 27.10.2020). УК РФ Статья 142.1. Фальсификация итогов голосования

4. How E-voting Works. URL: https://people.howstuffworks.com/e-voting.htm#pt4 (дата обращения: 14.03.21).

5. Олейник М. Н., Мартыненко Д. В. Система онлайн-голосования на основе технологии blockchain // StudNet. 2020. Т. 3. № 8.

6. Фаррахов И. Г., Якупов И. М. Система онлайн-голосования на базе технологии blockchain // Наука и образование: сохраняя прошлое, создаём будущее. Сборник статей XXXII Международной научно-практической конференции. Пенза, 2021. С. 43–46.

УДК 004.056
ГРНТИ 49.33.35

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ KUBERNETES

Г. О. Гурбатов, А. Д. Паничев, И. А. Ушаков

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

Технологии контейнеризации значительно упростили работу с приложениями, а также позволили более эффективно использовать вычислительные ресурсы, посредством запуска набора только необходимых библиотек в контейнере. Появились удобные системы развертывания и управления контейнерами такие как Kubernetes. Но вместе с удобством и скоростью работы с новыми технологиями появились и новые уязвимости, которые необходимо устранить средствами безопасности для обеспечения сохранности данных и корректной работы.

Kubernetes, Docker, контейнеры, кластер, безопасность, атака, шифрование.

В связи с ростом популярности контейнеризации из-за удобства использования и экономии ресурсов, возник спрос на системы управления контейнерными нагрузками. Впервые проект Kubernetes был начат Google и теперь поддерживается многими компаниями, среди которых Microsoft, RedHat, IBM и Docker.

Kubernetes представляет собой систему с открытым исходным кодом для автоматизации развертывания, масштабирования и управления контейнерными приложениями. Он группирует контейнеры, составляющие приложение, в логические блоки для упрощения управления и обнаружения. Как и любая другая популярная платформа или инфраструктура для разработки и развертывания приложения она подвержена опасности хакерских атак и другого несанкционированного доступа.

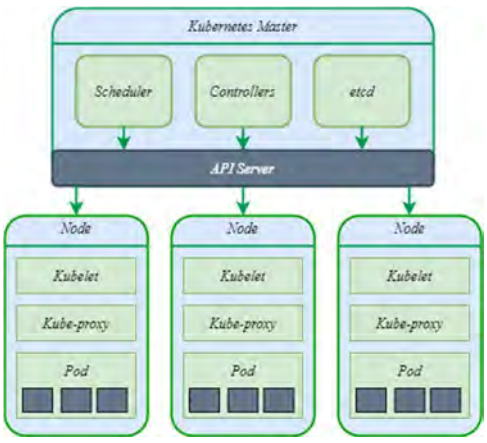


Рис. 1. Архитектура кластера Kubernetes

Архитектура Kubernetes состоит из множества компонентов на каждый из которых, может быть совершена атака. На рис. 1 (см. выше) показана структура основных компонентов кластера Kubernetes.

- Узлы кластера:

1) Worker Nodes – узлы кластера, образующие основную рабочую плоскость (data plane) кластера. На них запускаются контейнеры пользовательских приложений, а также системные компоненты, предназначенные для запуска на каждом узле (агенты, прокси серверы и другие).

2) Master Nodes – узлы кластера, образующие плоскость управления (control plane). Они содержат все основные системные компоненты Kubernetes, занимаются планированием развертывания конфигурации и управляют рабочими узлами.

- Pods – элементарные единицы развертывания состоящая из одного или нескольких контейнеров с общими ресурсами хранения, сети и спецификацией для запуска контейнеров [1].
- System Components – внутренние системные компоненты для управления кластером Kubernetes (сервер API, Kubelet и т. д.).

Атаки могут проводиться на любой из данных компонентов в целях получения несанкционированного доступа к внутренним ресурсам кластера. На основе анализа известных инцидентов можно выделить основные уязвимости, которые чаще всего используются в процессе реализации атаки:

- Уязвимости самой системы Kubernetes, ошибки в построении кластера, отсутствие связности с внутренними компонентами безопасности позволяют скомпрометированным контейнерам устанавливать несанкционированные соединения друг с другом и запускать атаку.
- Плохо реализованная система сетевой безопасности, использование незащищенных протоколов, отсутствие грамотно настроенных правил фильтрации сетевого трафика, ключей шифрования и сертификатов безопасности.
- Отсутствие безопасных механизмов аутентификации и авторизации, логической и физической изоляции компонентов и узлов кластера.
- Особенности технологий контейнеризации, уязвимости наиболее часто используемой контейнерной платформы Docker.
- Развертывание взаимосвязанных приложений в разных облачных или физических системах и отсутствие безопасного уровня изоляции, провоцирующее чрезмерное увеличение трафика между кластерами позволяет реализовать DDoS-атаки.
- Локальные уязвимости хостовой операционной системы, недостатки реализации отдельных библиотек и других отдельных компонентов.

• Уязвимости развертываемых приложений, отсутствие ограничения ресурсов для контейнеров, использование недостоверных образов способствуют компрометации контейнеров, запуску вредоносного программного обеспечения и утере данных.

Обеспечение безопасности Kubernetes условно можно представить двумя практическими подходами. Первый подход – это настройка опций безопасности (*security hardening*) и использование лучших практик (*security best practices*) на всех ключевых элементах Kubernetes. Второй подход – применение сторонних утилит с открытым исходным кодом и коммерческих решений для обеспечения мониторинга, контроля и управления уровнем безопасности. Для обеспечения высокого уровня безопасности необходимо использовать комплексный подход на всех слоях инфраструктуры, которые изображены на рис. 2.

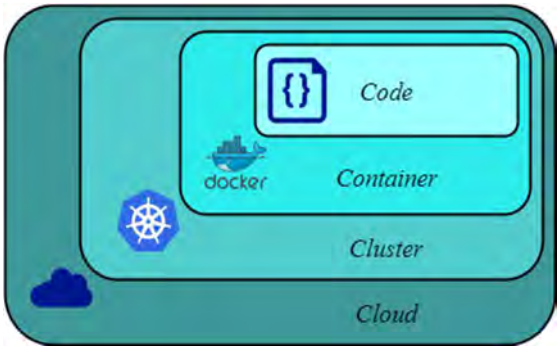


Рис. 2. Слои инфраструктуры

Исходя из вышеперечисленных угроз и уязвимостей можно привести ряд рекомендаций по увеличению уровня безопасности кластера Kubernetes и развертываемых приложений, на основе средств, поддерживаемых платформой:

• Необходимо выбрать механизм аутентификации для серверов API, который соответствует общим шаблонам доступа при установке кластера. Для больших кластеров может быть целесообразно интегрировать существующий сервер OIDC (OpenID *Connect*) или LDAP (*Lightweight Directory Access Protocol*), который позволит разделить пользователей на группы [2].

• После аутентификации каждый вызов API должен пройти проверку авторизации. Kubernetes предоставляет интегрированный компонент управления доступом на основе ролей – RBAC (*role-based access control*), который сопоставляет входящего пользователя или группу с набором разрешений, объединенных в роли. Эти разрешения объединяют операции (получение, создание, удаление) с ресурсами (подами, службами, узлами) и могут относиться к пространству имен или кластеру.

• Использование шифрования TLS (*transport layer security*) обеспечивает защищенную передачу данных, идентификацию клиента и сервера, защищает от сниффинга трафика. В целях обеспечения высокого уровня безопасности требуется включить использование TLS на всех поддерживающих его компонентах кластера.

• Контроль доступа к Kubelet необходимо реализовать посредством авторизации и аутентификации. Данный компонент предоставляет широкий

доступ к узлам и контейнерам через HTTPS, и по умолчанию разрешает неаутентифицированный доступ.

- Использование квоты ограничивает количество ресурсов, предоставляемых пространству имен. Квота чаще всего используется для ограничения объема центрального процессора, памяти или постоянного диска, который может использовать пространство имен, но также может контролировать количество модулей, служб или томов, существующих в каждом пространстве имен [3].
- Необходимо сконфигурировать контейнеры приложений на работу под пользователем без root – привилегий, во избежание несанкционированного доступа к ресурсам хоста [4].
- Network Policy – сетевая политика для пространства имен (*namespace*) позволяет владельцам приложений ограничивать доступ в свое пространство имен из приложений другого пространства имен. Диапазоны квот и ограничений можно использовать для управления возможностью запрашивать порты узлов или службы с балансировкой нагрузки, которые контролируют видимость приложения вне кластера
- Обеспечение дополнительных средств защиты, которые управляют сетевыми правилами для каждого подключаемого модуля или среды, например: межсетевые экраны для каждого узла, физическое разделение узлов кластера или расширенная сетевая политика [5].
- Контроль доступа узлов к развертыванию. По умолчанию нет ограничений на то, какие узлы могут запускать под. Kubernetes предлагает богатый набор политик для управления размещением контейнеров на узлах. Плагин допуска бета-версии PodNodeSelector может использоваться для принудительного использования контейнеров в пространстве имен по умолчанию или для требования определенного селектора узла.
- Частая смена учетных данных усложнит работу для злоумышленника. Необходимо установить короткие сроки жизни сертификатов и токенов, и автоматизировать их ротацию.
- Обеспечение безопасности etcd. Данный компонент является критически важным в обеспечении безопасности платформы так как он хранит сведения о состоянии кластера Kubernetes, токены и сертификаты. Хорошей практикой будет обеспечение отдельного уровня безопасности для etcd, а также шифрование резервных копий с помощью проверенного программного обеспечения и по возможности полное шифрование диска. Kubernetes поддерживает шифрование в состоянии покоя. Это функция зашифрует секретные ресурсы в etcd, не позволяя сторонам, получающим доступ к вашим резервным копиям etcd, просматривать содержимое.
- Систематический анализ файлов конфигурации. Исключение хранения конфиденциальных данных, ключей и паролей в открытом виде, исполь-

зование шифрования для их представления в конфигурации. Данная процедура должна проводиться регулярно для поддержания актуальности и корректности конфигураций, а также для исключения подложенных файлов.

Для обеспечения высокого уровня безопасности кластера Kubernetes и данных с которыми он работает, необходимо учитывать возможные уязвимости на всех уровнях архитектуры. Платформа Kubernetes поддерживает множество механизмов защиты внутри кластера, а также интегрируется с внешними системами безопасности. Комплексный подход позволяет исключить несанкционированный доступ и потерю данных.

Список используемых источников

1. The Kubernetes Authors, “Kubernetes security". URL: https://kubernetes.io/docs/concepts/security/overview/

2. Rice Liz & Hausenblas Michael Kubernetes security. O'Reilly Media, Inc. ISBN: 9781492039068

3. Ibryam B., Huß R. Kubernetes Patterns: Reusable Elements for Designing Cloud-native Applications. O'Reilly Media, 2019.

4. Mouat A. Docker Security: Using Containers Safely in Production. O'Reilly Media, 2015.

5. Kotenko I., Doynikova E., Security assessment of computer networks based on attack graphs and security events // Lecture Notes in Computer Science. 2014. 8407 LNCS. pp. 462–471. DOI: 10.1007/978-3-642-55032-4_47.

УДК 535.015
ГРНТИ 49.46.33

ДИСТАНЦИОННЫЙ ВОЛОКОННО-ОПТИЧЕСКИЙ ДАТЧИК ДЛЯ КОНТРОЛЯ РАДИОАКТИВНОГО ИЗЛУЧЕНИЯ РАЗЛИЧНОЙ МОЩНОСТИ

В. В. Давыдов, Д. С. Дмитриева

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

Обоснована необходимость улучшения метрологических характеристик и функциональных возможностей волоконно-оптических датчиков для проведения измерений на больших расстояниях (более 10 км). Предложен новый способ построения линии связи с волоконно-оптическим датчиком для контроля экспозиционной дозы радиоактивного излучения в большом диапазоне её изменения (несколько порядков) в дистанционном режиме. Определены функциональные возможности датчика, разработана схема его подключения и пределы измерения. Представлены результаты экспериментальных исследований.

волоконно-оптический датчик, радиоактивное излучение, оптическое волокно, лазерное излучение, экспозиционная доза облучения, радиационно-наведенные потери.

Развитие научно-технического прогресса привело к появлению большого числа объектов, как научных, так и промышленных, на которых используются радиоактивные материалы [1, 2]. Увеличилось число случаев утечки радиоактивных материалов (попадание их в воду и почву, в атмосферы и т. д.), а также выходов радиоактивного излучения (в основном γ – излучения) за пределы защитной зоны (через защитные экраны и перекрытия) [2].

Возникшие под влиянием γ-излучения потери в оптическом волокне превышают стандартные потери в несколько сотен раз, что делает его непригодным для передачи информации (стандартные потери для оптического волокна при рабочей длине волны λ = 1 550 нм и диапазоне температур эксплуатации от 213 до 338 К составляют от 0,26 до 0,38 дБ/км.). Даже если источником облучения является единичный источник, зона сильного облучения вокруг него может составлять порядка 100–150 м. Это приводит к сильному искажению или полной утере передаваемой информации на расстоянии более 200 км, так как уровень сигнала становится слишком низким и теряется в уровне шумов. Так как некоторые линии связи обладают большой протяженностью, то и исключить возможность возникновения γ-излучения в зоне прокладки волоконно-оптических линий связи нельзя.

К данной проблеме добавляется тот факт, что восстановление параметров ВОЛС после облучения занимает продолжительное время, в течение которого использование их для передачи информации затруднительно. Восстановление может занять большое количество времени, из-за чего приходится выводить линию, подвергшуюся влиянию γ-излучения, из эксплуатации и заменять поврежденный участок. Однако, так как волокно имеет свойство не накапливать радиацию в своей структуре, то после прекращения воздействия точное определение поврежденного участка так же становится затруднительным.

Постоянному контролю радиационной обстановки, как в атмосфере, так и на территории различных объектов уделяется большое внимание. Одной из актуальных задач является дистанционный контроль (на расстояниях 10 и более км) в автоматическом режиме в ситуации, когда экспозиционная доза облучения D_R может изменяться на несколько порядков за короткий промежуток времени. После прекращения действия дозы облучения прибор через некоторое время проводить измерения в штатном режиме. Одним из перспективных направлений для таких измерений является использование волоконно-оптических датчиков. Разработанные в настоящее время волоконно-оптические датчики на основе измерения изменения поляризации лазерного излучения под действием γ – излучения позволяют регистрировать

очень слабые изменения D_R, которые вызывают падение мощности лазерного излучения на 0,05 дБ. При больших значениях D_R лазерное излучение в них полностью затухает и датчик прекращает работу на долгое время. Естественная релаксация оптического волокна даже при наличии слабого лазерного излучения занимает время порядка 10^6 с и более [3]. Поэтому разработка новых моделей волоконно-оптических датчиков крайне актуальна.

Проведенные нами ранее исследования магистральных ВОЛС [3] позволили разработать новый метод восстановления работоспособности оптической линии связи в условиях воздействия γ – излучения при длительной её эксплуатации. Поэтому предлагается к ВОЛС с сердцевиной из чистого кварца подключить оптический датчик (оптическое волокно длинной 100 м с сердцевиной $SiO_2 – GeO_2$ с различной степенью легирования). На рис. в качестве примера представлена исследования радиационно-наведенных потерь α_s от изменения D_R для различного процента легирования оптического волокна.

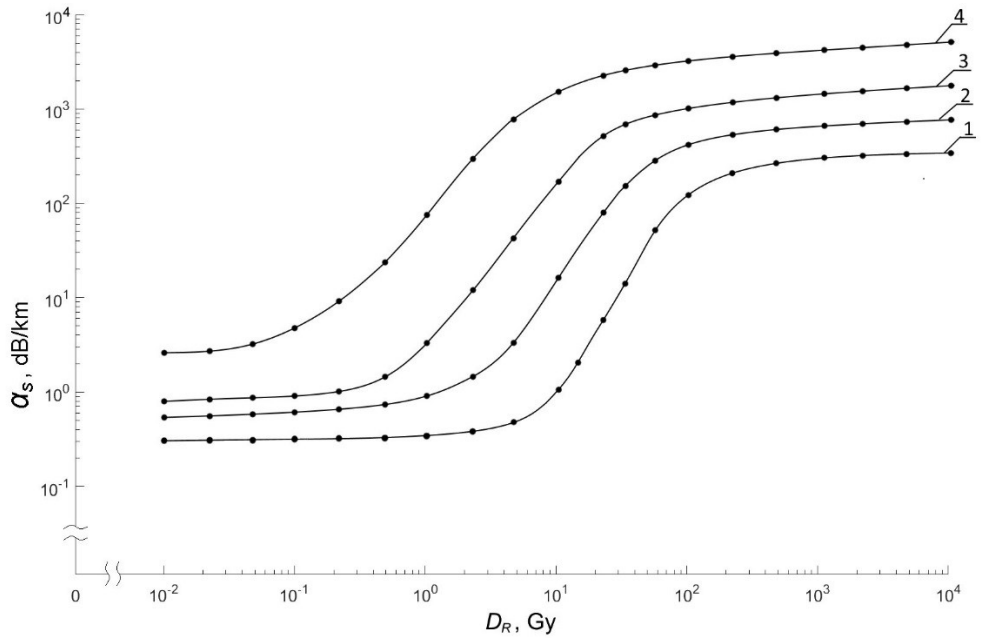


Рис. Зависимость α_s одномодового волокна на длине волны $\lambda = 1550$ нм от дозы облучения D_R с сердцевиной $SiO_2 – GeO_2$ находящийся при T = 294.2 К. Графикам 1, 2, 3 и 4 соответствует легирование в %: 1,5; 4,0; 10,0 и 20,0

Анализ полученных на рис. результатов показал, что увеличение процента легирования повышает чувствительность данного волокна к экспозиционной дозе γ – излучения. Это позволяет регистрировать изменения небольших значений D_R, которые при воздействии на оптическое волокно уменьшают мощность лазерного излучения на выходе ВОЛС на 0,2 дБ.

Полученные экспериментальные результаты показали надежную работу разработанного датчика по контролю экспозиционной дозы облучения с 0,1 до 1 000 Гр в дистанционном режиме с возможностью восстановления

режима работы с использованием дополнительного лазерного излучения с $\lambda = 1\ 310$ нм, как в ранее разработанных магистральных ВОЛС [3]. В оптических датчиках с измерениями, основанными на поляризации применить разработанный нами метод сложно, так как высока вероятность выхода из строя используемых в них фотоприемников с повышенной чувствительностью.

Список используемых источников

1. Davydov R., Antonov V., Angelina M. Parameter Control System for a Nuclear Power Plant Based on Fiber-Optic Sensors and Communication Lines // Proceedings of the 2019 IEEE International Conference on Electrical Engineering and Photonics, EExPolytech 2019, 8906791, 2019.

2. Davydov R., Antonov V., Makeev S., Batov Y., Dudkin V., Myazin N. New high-speed system for controlling the parameters of a nuclear reactor in a nuclear power plant // E3S Web of Conferences. 2019. Vol. 140. pp. 02001.

3. Dmitrieva D., Pilipova V., Andreeva E., Dudkin V., Davydov V. Method for determination of negative influence to γ – radiation on fiber optic information transmission systems // Proceedings of ITNT 2020 – 6th IEEE International Conference on Information Technology and Nanotechnology. 2020. 9253348.

Статья представлена заведующим кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной.

УДК 654.739
ГРНТИ 49.33.29

ВОЛОКОННО-ОПТИЧЕСКИЙ ИМИТАТОР АВАРИЙНОЙ СИТУАЦИИ ДЛЯ ПРОВЕРКИ РАБОТЫ СИСТЕМ КОНТРОЛЯ КОРАБЕЛЬНЫХ АТОМНЫХ ЭНЕРГЕТИЧЕСКИХ УСТАНОВОК

В. В. Давыдов, В. М. Пилипова

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

Обоснована необходимость тестирования аппаратуры контроля работы атомных энергетических установок. Предложено использовать для этих целей оптическое волокно и импульсное лазерное излучение. Установлено, что оптическое волокно более устойчиво к радиационному излучению чем другие системы связи. Разработана конструкция волоконно-оптическом имитатора аварийной ситуации. Проведен расчет его характеристик. Проведено их экспериментальное исследование. Установлено, что при

задержке оптического сигнала на 98,6 мкс, потери составляют – 26 дБ при неравномерности АЧХ ± 2 дБ. Это позволяет проводить тестирование всего комплекта аппаратуры, в которой используются оптические сигналы, применяемой для контроля атомной энергетической установки.

атомные энергетические установки, система контроля, волоконно-оптический имитатор, лазерное излучение, время задержки.

Для подвижных морских объектов (корабли, плавучие атомные электростанции и т. д.) разрабатываются новые конструкции ядерных реакторов, а также модернизируются действующие. Для контроля ядерных энергетических установок необходимо надежное оборудование. Одним из главных условий безопасной эксплуатации атомных энергетических установок (АЭУ) является чёткая работа систем охлаждения [1]. Для охлаждения в АЭУ морского базирования используется «тяжелая» вода, расход которой и её параметры контролируются ЯМР измерителями проточного типа [1, 2].

При аварийной ситуации в атомном реакторе происходит резкое повышение уровня ионизирующего излучения, действующего на «тяжелую» воду системы охлаждения реактора. Экспериментально установлено, что в этом случае происходит сдвиг во времени момента появления сигнала ЯМР в системе его регистрации и изменение его вида. Этот сдвиг будет носить однократный характер. Измерив, этот однократный сдвиг (временной интервал) между регистрируемыми сигналами ЯМР и сравнив его с тем, который определялся ранее, и, используя ранее полученные данные о таких событиях, можно гораздо быстрее принять решение в сложившейся аварийной ситуации. Кроме того, используя полученное значение временного интервала и другие результаты измерений можно более достоверно определить возможные причины случившегося изменения и смоделировать возможные сценарии развития аварийной ситуации.

Чтобы поддерживать систему измерения временного интервала в рабочем состоянии, необходимо проводить её регулярную проверку и тестирование. С учетом того, что для передачи ЯМР сигналов в системах контроля АЭУ применяется ВОЛС, то более логично для имитации аварийной ситуации работы АЭУ разработать устройство на основе оптического волокна и лазерного излучения.

В данной работе волоконно-оптический имитатор разработан на основе пассивной волоконно-оптической линии задержки с включением в конструкцию на входе оптического изолятора для исключения обратных отраженных сигналов. Для имитации аварийной ситуации было разработано три имитатора на разные времена задержки τз (49, 75 и 98,6 мкс) оптического сигнала. Это связано с тем, что ранее было экспериментально установлено, что временной сдвиг момента появления сигнала ЯМР в системе регистрации при повышении уровня ионизирующего излучения составляет от 45 до

130 мкс (в зависимости от величины экспозиционный дозы облучения). Для них было рассчитано затухание оптического сигнала (максимальное значение, которого составило 26 дБ с учетом системного запаса по затуханию на участке регенерации в 2 дБ). На рис. 1 и на рис. 2 в качестве примера представлены измеренное время задержки τз одних из имитаторов. Верхний сигнал получен без включения имитатора, нижний – с имитатором.

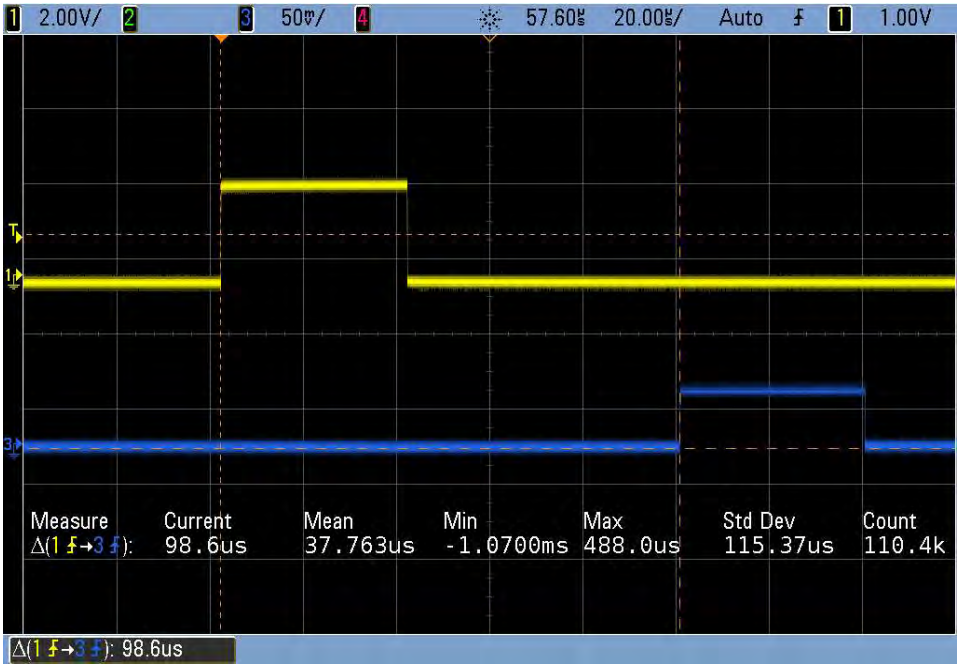


Рис. 1. Временное прохождение сигнала через имитатор с задержкой на 98.6 мкс. Цена деления по горизонтали 20 мкс

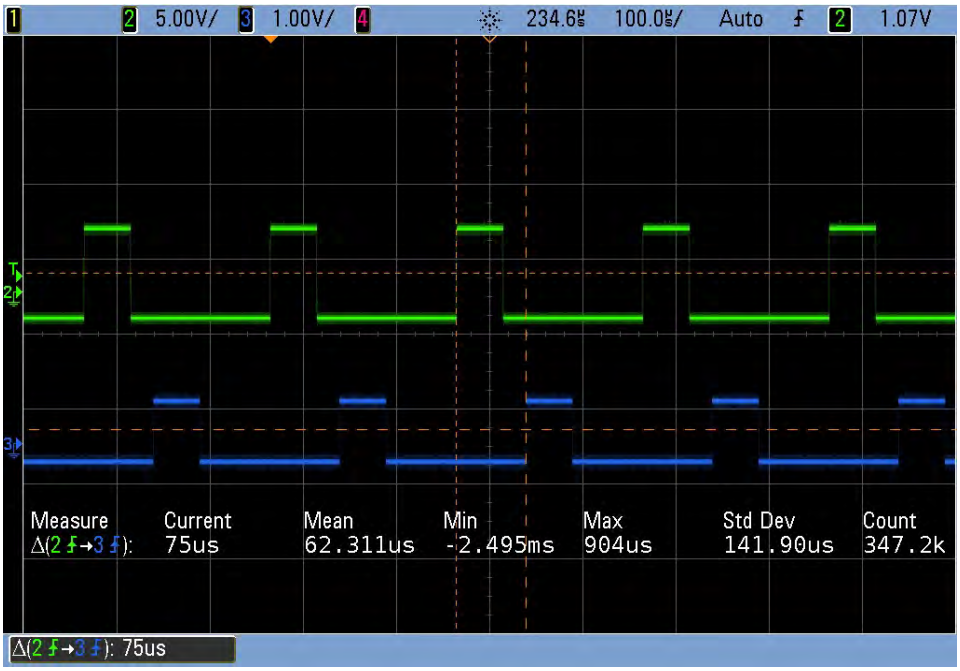


Рис. 2. Временное прохождение сигнала через имитатор с задержкой на 75 мкс. Цена деления по горизонтали 100 мкс

Анализ полученных сигналов показывает уменьшение мощности. Поэтому при включении волоконо – оптического имитатора в волоконо – оптическую систему передачи сигналов ЯМР для тестирования систем контроля АЭУ передаваемые сигналы необходимо будет усиливать, чтобы обеспечить необходимую точность при измерениях во время тестирования. Измеренные динамические характеристики волоконо – оптических имитаторов показали, что три конструкции приборов имеет динамический диапазон не хуже 56 дБ. Поэтому данное усиление реализовать достаточно просто.

Проведенные исследования параметров волоконно-оптических имитаторов показали, что их также можно успешно применять для проверки аппаратуры в радиолокационных станциях, так как коэффициент шума разработанного имитатора в диапазоне частот от 2 до 18 ГГц изменяется на 7 дБ (максимальное значение 27 дБ). Это показывает широкие функциональные возможности прибора.

Список используемых источников

1. Климов Д. А., Гулевич А. В., Каграманян В. С. и др. Вызовы и стимулы развития натриевых быстрых реакторов в современных условиях // Атомная энергия. 2018. Т. 125. Вып. 3. С. 131–135.

2. Davydov V. V., Myazin N. S., Kiryukhin A. V. Nuclear-Magnetic Flowmeter-Relaxometers for Monitoring Coolant and Feedwater Flow and Status in Npp Atomic Energy. 2020. 127 (5). pp. 274–279.

УДК 004.054
ГРНТИ 50.43.19

СРАВНИТЕЛЬНАЯ ОЦЕНКА СИСТЕМ МОНИТОРИНГА КОМПОНЕНТОВ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ

А. А. Дедухова, А. А. Швидкий

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

В статье рассмотрены наиболее популярные многофункциональные системы мониторинга компонентов облачных инфраструктур, а также произведена их сравнительная оценка по определенным критериям. Данные системы в настоящий момент представляют функциональные возможности и производительность на высоком уровне, а также доказали важность и удобство подхода к мониторингу со стороны единых систем мониторинга.

система мониторинга, облачные технологии, серверы, графический интерфейс.

Мониторинг компонентов облачной инфраструктуры – это процесс сбора и анализа данных о текущей производительности систем хранения компонентов. Для этого используются специальные утилиты, функциональность которых несколько отличается друг от друга. Некоторые программы для Windows или Linux предназначены только для контроля свободной памяти и загрузки CPU сервера, а другие подходят для расширенного мониторинга корпоративных систем хранения данных.

Основная задача мониторинга – контроль производительности, наличия свободной памяти и функциональности серверов в режиме реального времени. Так же он позволяет накапливать исторические данные, и с помощью дальнейшего анализа выявлять аномалии в работе сервисов [4]. Самое главное – это обнаружение проблемы до того, как на себе ее ощутят пользователи.

Существует несколько подходов к мониторингу:

1. Просмотр состояния устройства напрямую.
2. Получение уведомлений на почту от различных систем.
3. Единая система мониторинга.

Наиболее верным решением, выбирая подход к мониторингу, будет остановиться на единой системе мониторинга. Их существует достаточное количество, пользующиеся большим спросом из них: Grafana, Zabbix, Nagios.

Nagios – это инструмент непрерывного мониторинга с открытым исходным кодом, который контролирует сеть, приложения и серверы. Он может находить и устранять проблемы, обнаруженные в инфраструктуре, и останавливать будущие проблемы, прежде чем они затронут конечных пользователей [3].

Данная система предлагает следующие функции, которые делают его доступным для большой группы пользователей:

− контроль серверов баз данных, такие как SQL Server, Oracle, Mysql, Postgres;

− предоставление информации о приложениях (Apache, Postfix, LDAP, Citrix);

− возможность работы на любой операционной системе;

− для настройки хоста, происходит опрос всех систем.

Nagios обладает большим количеством преимуществ для пользователей:

− отсутствие периодического тестирования;

− обнаружение сбоев работы в долях секунд;

− снижение стоимости обслуживания без ущерба для производительности;

− своевременность уведомлений о контроле и поломках.

Nagios имеет и недостатки:

− отсутствие возможности конфигурирования через web-интерфейс. Все дополнительные изменения выполняются с последующим полным перезапуском сервера Nagios;

− наличие большого интервала между проверками и замерами параметров;

− RRD (Циклическая база данных) усредняет данные, поэтому невозможно сказать, каково было точное значение параметров в определенный промежуток времени;

− нет встроенных средств визуализации (кроме карты сети);

− сложность масштабирования без использования плагинов от сторонних производителей;

− каждый плагин запускается отдельно.

Каждая из этих проблем имеет техническое решение с помощью расширяемой архитектуры, но требует дополнительных трудозатрат при установке и конфигурировании, а итоговое решение будет сложно поддерживать из-за большого применения нестандартных решений.

Zabbix – это свободная многофункциональная система мониторинга с web-интерфейсом, которая в случае большой нагрузки и наблюдением за большим количеством хостов позволяет распределить части многофункциональной системы на несколько раздельных машин [2].

Система состоит из четырёх основных компонентов:

- Сервер мониторинга, который отвечает за сбор и обработку данных от всех агентов.
- Прокси сервер, отвечающий за сбор, обработку и последующее отправление данных на центральный сервер.
- Web-интерфейс для мониторинга.
- Агент, собирающий данные на физическом сервере.

Для работы необходимо настроить одну из нескольких вариантов баз данных: MySQL; Oracle; PostgreSQL; SQLite; IBM DB2; TimescaleDB.

Поддерживаемые операционные системы: OpenBSD, Linux, FreeBSD, NetBSD, AIX, Power8, HP-UX, Solaris, Mac OS X, ОС Windows, начиная с 2000.

Среди основных особенностей можно выделить:

− управление производится через web-интерфейс, конфигурации хранятся в базе;

− единая точка доступа для пользователей;

− вариации разграничения доступа к данным и конфигурации;

− минимальный интервал между снятием замеров – 1 секунда;

− происходит сбор и анализ на стороне сервера количественных характеристик работы;

− время хранения данных зависит только от дискового пространства;

− развитые возможности анализа собранных данных.

При этом данная система обладает рядом недостатков:

− хранение всех данных истории в одной базе, что неэффективно и ограничивает масштабируемость;

− нет обеспечения отказоустойчивости.

Grafana – это платформа с открытым исходным кодом для визуализации, мониторинга и анализа данных. Она позволяет пользователям создавать информационные панели данных, каждая из которых отображает определенные показатели в течение установленного периода времени. Каждая информационная панель данных универсальна, поэтому ее можно настроить для конкретного проекта или с учетом любых потребностей разработки.

Платформа поддерживает десятки различных форматов отображения данных – таблицы, графики, распределения, диаграммы. Можно выстроить простые и понятные графики для данных любой сложности.

Она сама ничего не хранит и не собирает, а является лишь универсальным клиентом для систем хранения метрик. Например, с помощью нее можно брать данные как в традиционную базу PostgreSQL, так и в специализированные аналитические системы Prometheus или Influx.

Grafana можно подключать к любому хранилищу статистических данных. Она может использовать разные СУБД и системы сбора статистики и умеет работать с любой популярной системой хранения данных [1].

Grafana обладает следующими особенностями:

− масштабирование графиков;

− сортировка значений таблиц;

− смена вида графиков;

− выделения, подсвечивания;

− выведения нескольких графиков на одну информационную панель.

Можно выделить и недостатки:

− нет собственной базы данных для хранения метрик.

− нет поддержки сбора данных.

− нет возможности управления тревогами и отслеживания событий.

На основе информации о различных системах, можно сделать сравнение (табл.) их функциональных характеристик.

ТАБЛИЦА. Сравнительная характеристика функциональных особенностей программ мониторинга

	Grafana	Zabbix	Nagios
Визуализация	Да	Да	Да
Собственная реализация источника данных	Нет	Да	Да
Генерация событий	Да	Да	Да

Хранение данных визуализации	Нет	Да	Да
Отчеты SLA	Да	Да	Через плагин
Конфигурирование через web-интерфейс	Да	Да	нет
Возможность внешних оповещений	Да	Да	Через плагин
Количество поддерживаемых источников	>30	4	2
Возможность создания распределенной системы мониторинга	Нет необходимости	Да	Нет
Динамический выбор объектов мониторинга	Да	Нет	Нет
Встроенная система загрузки шаблонов	Да	Нет	Нет

Качественный мониторинг компонентов облачных инфраструктур невозможен без многофункциональной системы. Nagios, Zabbix и Grafana являются хорошими инструментами для мониторинга: Nagios – классическая программа, доказавшая свою эффективность; Zabbix – инструмент с большим выбором шаблонов оборудования; но для применения в облачной инфраструктуре больше всего подходит Grafana, т. к. Grafana – это идеальный вариант для мониторинга компонентов облачных инфраструктур, наглядность графиков, полнота картинки, гибкость настройки, сортировка значений таблиц и возможность вывода нескольких графиков на одну информационную панель.

Список используемых источников

1. Grafana Labs. 2020. URL: https://grafana.com/grafana/ (дата обращения: 26.03.2021).

2. Zabbix. 2020. URL: https://www.zabbix.com/ru (дата обращения: 26.03.2021).

3. Nagois. 2020. URL: https://www.nagios.org/ (дата обращения: 26.03.2021).

4. Швидкий А. А., Спиркина А. В., Савельева А. А., Тарлыков А. В. Evaluation of the impact the hyper-converged infrastructure storage subsystem synchronization on the overall performance // 12th International congress on ultra modern telecommunications and control systems and workshops (ICUMT), 2020. pp. 248–252.

Статья представлена научным руководителем, директором НИИ ТС СПбГУТ, кандидатом технических наук, доцентом А. Г. Владыко.

УДК 004.056.5
ГРНТИ 81.93.29

ФОРМАЛЬНОЕ ОПИСАНИЕ ОСОБЕННОСТЕЙ МОДЕЛИ НАРУШИТЕЛЯ И КРИТИЧНОСТЬ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ НА БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ

В. А. Десницкий[1,2], **И. Б. Паращук**[2]

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

Рассматривается подход к формальному описанию модели нарушителя в интересах анализа защищенности беспроводных сенсорных сетей от атакующих воздействий. Данный подход опирается на классификационные признаки нарушителя, способного применять многошаговые атакующие воздействия, как физического, так и программно-информационного характера. При этом использование классификационных признаков нарушителя позволяет конкретизировать показатели критичности атакующих воздействий на сети такого класса.

беспроводная сенсорная сеть, атакующие воздействия, защищенность, модель, критичность, нарушитель, признак, показатель.

Беспроводные сенсорные сети (БСС) завоевывают все большую популярность, поскольку объединяют в себе достоинства сетей Интернета вещей и традиционных сетей встроенных устройств [1]. Эти информационно-телекоммуникационные инфраструктуры, объединяющие множества встроенных устройств, датчиков и сенсоров, являются, вместе с тем, самоорганизующимися системами. Они состоят из беспроводных встроенных электронных устройств (одноплатные компьютеры, программно-аппаратные сенсоры, датчики, исполнительные элементы, отдельные микросхемы и др.) и физических объектов, связанных не только коммуникационными соединениями, но и семантическими связями. Самоорганизация БСС подчинена иерархии и взаимосвязи потребностей в обработке, хранении, отображении и защите разнородных данных.

Важное место в вопросах планирования применения и в рамках эксплуатации БСС занимают проблемы защиты устройств, программного обеспечения и критически важных данных, циркулирующих в сетях такого класса. Это связано как к общей тенденцией все более активного применения БСС в различных сферах деятельности (включая промышленный Интернет ве-

щей – IIoT), так и с последствиями этого – неизбежным потенциальным возрастанием числа угроз и уязвимостей, а также количества и разнообразия атакующих воздействий на такие сети [2].

Именно поэтому актуальной остается задача анализа защищенности программно-аппаратного обеспечения БСС и выработки рекомендаций по повышению их безопасности. Одним из обязательных этапов исследований при разработке научно-методического инструментария анализа защищенности программно-аппаратного обеспечения БСС, является этап построения моделей, в частности, модели нарушителя, а также вопросы категоризации и классификации атакующих воздействий, которые могут влиять на функционирование сети. При этом анализ нарушителя и моделирование его поведения должны осуществляться с учетом всего многообразия признаков, позволяющих достоверно его классифицировать, с учетом особенностей его поведения и его итоговых целей. Более того, необходим детальный анализ и классификация особенностей модели нарушителя с точки зрения его ресурсных возможностей и различного вида ограничений и допущений (например, время атаки, уровень компетентности нарушителя и др.), определяющих его деятельность.

Иными словами, путем анализа и синтеза отдельных классификационных признаков и индивидуальных одиночных моделей построена обобщенная модель нарушителя. При этом данная модель нарушителя ориентирована на задачи оценивания защищенности БСС, может учитывать как особенности протоколов взаимодействия элементов БСС, так и особенности современных многоэтапных атакующих воздействий на сети такого класса.

В модели предусмотрены приоритеты – предложено ограничиться функциями обнаружения и защиты не против всех, а только против наиболее распространенных и критически опасных атакующих воздействий. Это связано с объективными фактами – существующими ограничениями на программно-аппаратные и энергетические ресурсы БСС, ориентированные на обеспечение информационной безопасности таких инфотелекоммуникационных сетей. С этой целью модель нарушителя предполагает учет только наиболее актуальных для БСС и наиболее опасных атакующих воздействий из всего множества (широкого диапазона) допустимых атак.

Обобщенная модель нарушителя является традиционной аналитической моделью и имеет комплексный, комбинированный характер, включающий отдельные классификационных признаки и индивидуальные особенности элементов БСС, а также может быть адаптирована с учетом условий и характера применения сетей такого класса.

В рамках формального описания модели нарушителя безопасности БСС определен ряд характерных черт (отличительных признаков, классификаторов) и особенностей:

итоговая цель нарушителя, которая отражает его намерения по негативному изменению свойств конфиденциальности, целостности и доступности данных, циркулирующих в рамках инфраструктуры БСС, по негативному изменению свойств отдельных элементов, датчиков (сенсоров), а также по негативному изменению предоставляемых БСС сервисов;

− вид атак нарушителя – пассивные атаки или активные [3];

− вид нарушителя с точки зрения БСС – внутренний (негативно настроенный инсайдер) или внешний нарушитель [3, 4];

− какие каналы и тракты использует нарушитель для атаки – атака по прямому или непрямому каналу доступа к элементу или устройству БСС;

− степень возможностей и уровень компетенции нарушителя;

− количество элементов (узлов) БСС, используемых нарушителем для реализации конкретной многоэтапной атаки;

− масштабность последствий и воздействий атаки;

− вид подсистем БСС, против которых направлено атакующее воздействие – на ключевые подсистемы БСС – например, адресацию, маршрутизацию и т. д., или на подсистемы защиты информации в БСС – например, подсистемы криптографии, управления ключами, идентификации вторжений и др. [4];

− вид негативных воздействий нарушителя на БСС с точки зрения уровней открытой эталонной сетевой модели [3].

Таким образом, в рамках формального описания модели нарушителя каждая конкретная атака может быть отнесена к одной или нескольким категориям. Это, в свою очередь, может обуславливать величину риска информационной безопасности, а также характер средств защиты, которые целесообразно применять против рассматриваемого вида нарушителей.

При этом для каждой конкретной БСС возможно выявить перечень опасных именно для нее атак, а также определить их критичность, используя дополнительно вводимые (экспертным путем) правила и известные методы верификации.

Например, нет смысла оценивать защищенность БСС от нарушителей, способных выполнять атаки исключительно дистанционно, из сети Интернет, когда наша конкретная БСС не имеет выхода во внешнюю глобальную сеть, а к ней и к ее элементам не может быть реализован удаленный физический доступ извне.

Предложенное в разработанной модели нарушителя трансформирование однородной номенклатуры возможных классов атак на БСС к номенклатуре, каталогизированной по характерным чертам (отличительным признакам нарушителя), делает реальной и рациональной возможность сократить множество анализируемых видов атак до некоторого небольшого набора наиболее критичных видов атакующих воздействий и анализировать защищенность лишь от них.

Кроме критичности атакующих воздействий для конкретной сенсорной сети на основе сепарации характерных черт (отличительных признаков) нарушителя, также могут быть сформулированы показатели и критерии оценивания таких атак с учетом их принадлежности к тем или иным видам нарушителей.

К числу таких показателей, например, могут быть отнесены:

− величина потребляемых нарушителем вычислительных (аппаратных и программных) и финансовых ресурсов на осуществление атаки;

− время реализации атакующих воздействий;

− количество виртуальных хостов и прокси-серверов, задействованных в ходе реализации атаки;

− показатели сложности реализации атаки, включающие, например, число внешних или внутренних (по отношению к БСС) физических устройств, задействованных нарушителем в процессе атаки и др.

Состав такой системы показателей и их отличающиеся для каждого конкретного случая количественные значения, в сущности, характеризуют конкретную разновидность атак на БСС, позволяют объективно оценить их критичность.

Вместе с тем, критичность конкретной атаки обязательно определяется в контексте условий функционирования, а также целей применения и функционирования БСС. Критичность атаки может выражаться в количестве (проценте) утерянной или искаженной информации; в существенном возрастании времени отклика устройств БСС (сенсоров); в сокращении времени безаварийной работы автономного элемента (узла) сети; в возрастании количества ошибок (снижении достоверности и точности) данных, собираемых и агрегируемых с датчиков (сенсоров) сети и др.

Достоинствами предлагаемого подхода к формулировке модели нарушителя и показателей критичности атакующих воздействий являются возможность повысить безопасность информационных ресурсов, хранимых и обрабатываемых в современных БСС (за счет контроля этих текущих показателей в режиме, близком к реальному времени), а также, в конечном итоге, возможность повысить качество принимаемых решений по управлению защитой информационных ресурсов сетей такого класса.

Работа выполнена при финансовой поддержке РФФИ (проект 19-07-00953) в СПИИРАН.

Список используемых источников

1. Ghildiyal S., Gupta A., Vaqur M., Semwal A. Analysis of wireless sensor networks: security, attacks and challenges // IJRET: International Journal of Research in Engineering and Technology. Vol. 03. Issue 03. 2014. pp. 160–164.

2. Десницкий В. А., Паращук И. Б. Обобщенный алгоритм анализа защищенности беспроводных сенсорных сетей от атакующих воздействий // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2020. Т. 1. С. 394–398.

3. Khan M. A., Khan M. A Review on Security Attacks and Solution in Wireless Sensor Networks // American Journal of Computer Science and Information Technology. Vol. 7. No. 1:31. 2019. pp. 6–10.

4. Pathan A-S. K., Hong C. S. Security Attacks and Challenges in Wireless Sensor Networks // Encyclopedia on Ad Hoc and Ubiquitous Computing. 2009. pp. 397–425.

УДК 621.3:004.71
ГРНТИ 49.13.15

ИСПОЛЬЗОВАНИЕ ПРИНЦИПОВ АНТЕННЫХ РЕШЕТОК В ОПТИЧЕСКОЙ ОБРАБОТКЕ СИГНАЛОВ

В. В. Дмитриева, Б. К. Резников

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

В статье описываются принципы работы антенных решеток, рассматриваются возможности их использования в оптической обработке сигналов. Примером такого использования является возможность определения угла прихода радиосигнала на антенную решетку с использованием возможностей преобразования Фурье в оптическом процессоре.

антенные решетки, оптические процессоры, дифракционные решетки.

Принципы функционирования антенных решеток

Антенной решеткой называют массив антенн (приемных или передающих), располагающихся в пространстве в определенном порядке. Основная цель создания антенных решеток состоит в возможности регулирования ее диаграммы направленности и повышении точности приема и коэффициента направленного действия.

Оптическая обработка сигнала, оптический процессор

Одной из наиболее сложно реализуемых функций в цифровом процессоре является преобразование Фурье. В оптическом процессоре данное преобразование выполняется достаточно изящно – при помощи линзы. Простой оптические фурье-процессор осуществляет преобразование Фурье двумерного сигнала за время прохождения света через оптическую систему. Здесь в полной мере реализуется обработка сигналов многоканальных систем с

использованием разделения каналов в пространстве (*Spatial Division Multiplexing*, SDM).

Простейший оптический фурье-процессор (рис. 2) имеет в своем составе элемент ввода информации в оптическую систему (пространственный модулятор света), линзу, совершающую преобразование Фурье и элемент вывода информации из оптической системы (регистрирующее устройство). При этом скорость обработки информации в таком процессоре почти полностью зависит от скоростей ввода и вывода информации из оптической системы [1, 2].

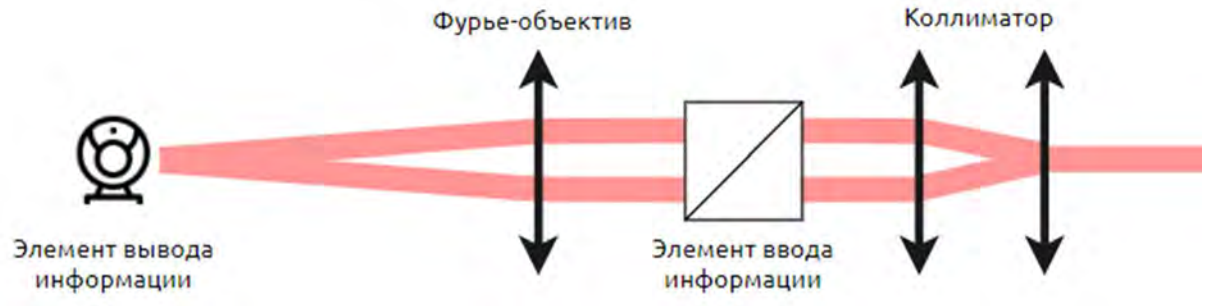


Рис. 2. Схема оптического фурье-процессора

В качестве элемента ввода информации (пространственного модулятора) в самом простейшем случае может использоваться жидкокристаллическая матрица, а также различные оптические вещества, в которых под воздействием внешнего сигнала может возникать девиация его показателя преломления. Примером может служить акустооптический модулятор, в звукопроводе которого под воздействием акустической волны создается периодическое изменение показателя преломления, и формируется фазовая дифракционная решетка. Размеры такого модулятора могут быть различными и зависят от потребностей при проектировании оптической системы. В случае обработки многоканального сигнала элемент ввода информации может быть представлен в виде массива таких модуляторов – многоканального акустооптического модулятора. В этой связи в таком модуляторе будет создаваться двумерная дифракционная решетка, параметры которой зависят от частот и разностей фаз между каналами модулятора. Картина дифракции такой решетки показана на рис. 3.

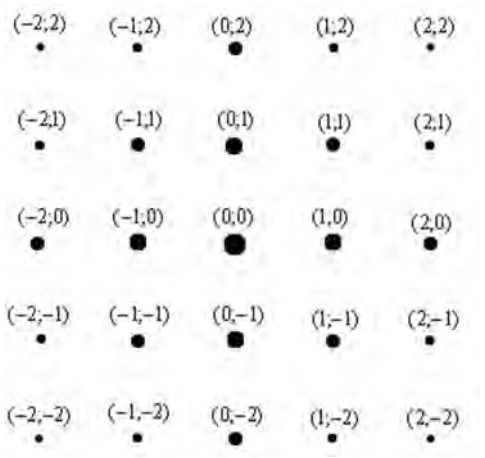


Рис. 3. Картина дифракции двумерной плоской дифракционной решетки

В качестве источника акустической волны могут быть использованы сигналы элементов линейной антенной решетки (рис. 4). При этом разность

фаз принятых радиоволн будет перенесена на акустические волны в каналах модулятора, а также на результат картины дифракции, возникающей при прохождении световой волны через многоканальный акустооптический модулятор. Результатом наличия разности фаз в получаемой дифракционной решетке станет угловое отклонение оси Y в картине дифракции. При этом величина отклонения будет полностью зависеть от разности фаз между каналами.

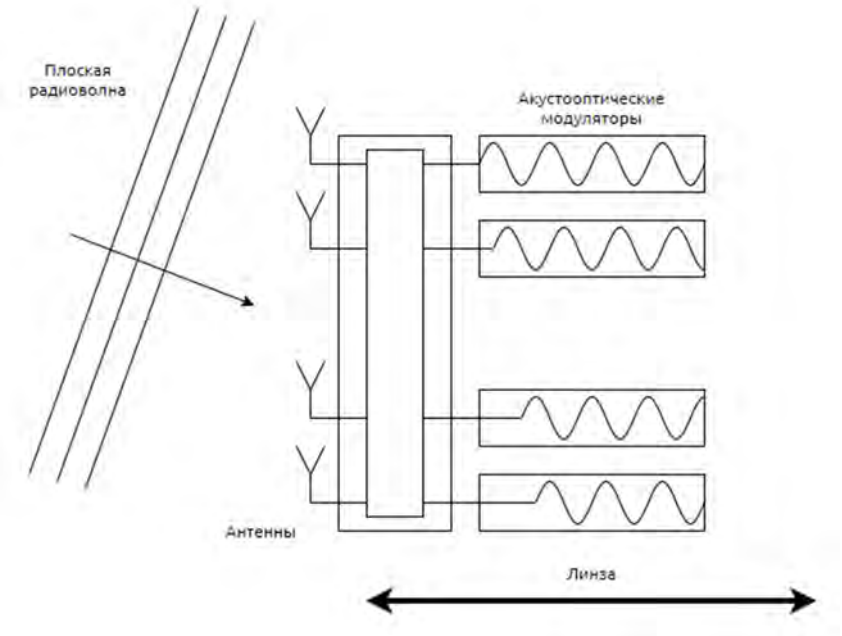


Рис. 4. Обработка сигналов с линейной антенной решетки

Наличие разности фаз может быть вызвано причиной прихода на антенную решетку, элементы которой являются источником волны, подаваемой на многооканальный акустооптический модулятор, плоской радиоволны под углом. Отсюда следует вывод, что при помощи данной оптической системы возможно определять угол прихода плоской радиоволны на линейную антенную решетку.

Лабораторный модуль

В условиях эксперимента было проведено моделирование поведения акустооптического модулятора при помощи жидкокристаллической матрицы. На жидкокристаллической матрице воспроизводилось поведение 25-канального акустооптического модулятора. Каналы модулятора были расположены слева направо. На рис. 5 показаны изображения, подаваемые на жидкокристаллическую матрицу. В каналах модулируемого акустооптического модулятора наблюдается разность фаз между каналами. Более темные части изображений соответствуют низкому значению показателя преломления.

а) б) в)

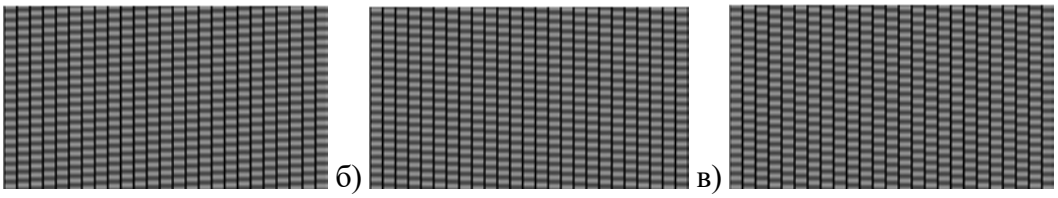


Рис. 5. Изображения, подаваемые на жидкокристаллическую матрицу, имитирующие поведение многоканального акустооптического модулятора

После прохождения световой волны через пространственный модулятор и фурье-объектив на регистрирующем устройстве наблюдались следующие картины (рис. 6).

а) б) в)

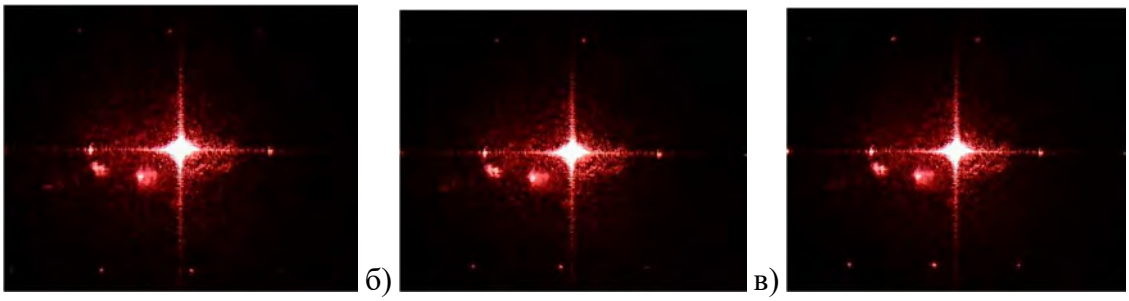


Рис. 6. Изображения, получаемые на регистрирующем устройстве

Анализ изображений показал, что, во-первых, присутствует отклонение оси Y от нормали, а также что величина отклонения однозначно определяется разностью фаз в соседних каналах.

Определение угла прихода сигнала может быть полезно при создании систем наведения антенных устройств в целях более качественного приема сигнала, а использование оптических методов обработки информации позволит повысить скорость данных процессов.

Список используемых источников

1. Хансен Р. С. Фазированные антенные решетки. 2-е изд-е. М.: Техносфера, 2012. 560 с.

2. Рогов С. А. Оптические методы и устройства информации. Спецвопросы квантовой электроники: учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2004. 78 с.

Статья представлена заведующим базовой кафедрой ССС СПбГУТ, доктором технических наук, доцентом В. В. Котовым.

УДК 654.739
ГРНТИ 49.33.29

ПОДХОДЫ К МОДЕЛИРОВАНИЮ РЕСУРСОВ SDN

Ю. С. Дмитриева, В. С. Елагин

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

Концепция SDN позволяет конфигурировать сеть как единую систему, независящую от производителя оборудования. Что достигается путем создания унифицированного интерфейса между уровнем управления и уровнем передачи данных.

программно-конфигурируемая сеть (SDN), протокол OpenFlow, контроллер SDN-сети, коммутатор SDN-сети.

В архитектуре компьютерных сетей, основанных на стандартных технологиях средства управления сетью и передачи трафика, используют единую системную логику, реализованную на базе единых сетевых устройств и наборов средств по обеспечению требуемого качества обслуживания (QoS), не соответствует скорости внедрения новых приложений и новых услуг; сеть ограничена для исследований и практически любых изменений. Она не обеспечивает необходимые минимальные задержки передачи пакетов, проприетарные (т. е. закрытые) протоколы взаимодействия устройств требуют значительных временных затрат, а нарастающая сложность сетевых устройств приводит к необходимости решения задач, которые связаны с внедрением новых протоколов и технологий, существенно увеличивает стоимость и время разработки. Новые технологии расширяют возможности старых протоколов, но при этом заметно усложняют управление сетью [1, 2, 3, 4, 5, 6, 7].

Для устранения вышеперечисленных проблем был предложен переход к виртуализации сети – программно-конфигурируемым сетям SDN (*Software-Defined Networking*), главной идеей которых является введение единого центра управления, принимающего решения по обработке сетевого трафика, и передача функций управления от сетевого коммутатора к сетевой операционной системе централизованного контроллера. Фрагмент архитектуры SDN-сети представлен на рис. 1.

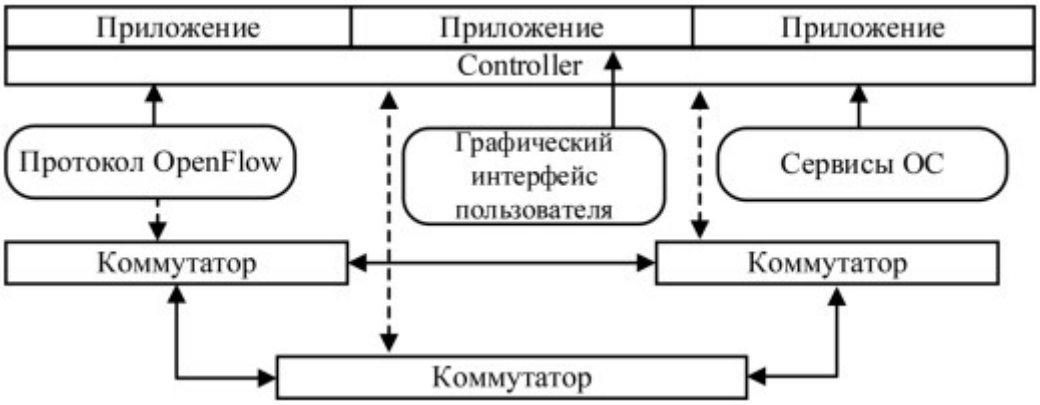


Рис. 1. Фрагмент архитектуры SDN-сети

SDN – это концепция создания и организации архитектуры компьютерных сетей, в основе которой лежит перенос функций управления (коммутаторов и маршрутизаторов) в отдельные программные приложения, функционирующие на отдельном сервере. Контроллер управляет коммутатором с помощью открытого протокола OpenFlow.

Потери пакетов и задержки, возникающие на различных этапах взаимодействия сетевых элементов – это показатели качества функционирования сети SDN. Решение задачи расчета необходимого объема сетевого ресурса путем разработки моделей функционирования соответствующего оборудования, вычисления и исследования его, основных вероятностно-временных характеристик.

В статье рассматривается модель функциональных блоков SDN-сети, разработанная на основе теории массового обслуживания и позволяющая находить основные вероятностно-временные характеристики процессов взаимодействия контроллера SDN и коммутаторов.

Методология исследования

На рис. 2 представлена модель функциональных блоков SDN-сети в виде сети массового обслуживания (СеМО). Узлами сети являются многоканальные СМО с неограниченным ожиданием. Коммутатор и контроллер представлены соответственно трехфазной и двухфазной СеМО, где поток заявок определяется входящим потоком Пуассона и экспоненциальным временем обслуживания на всех фазах.

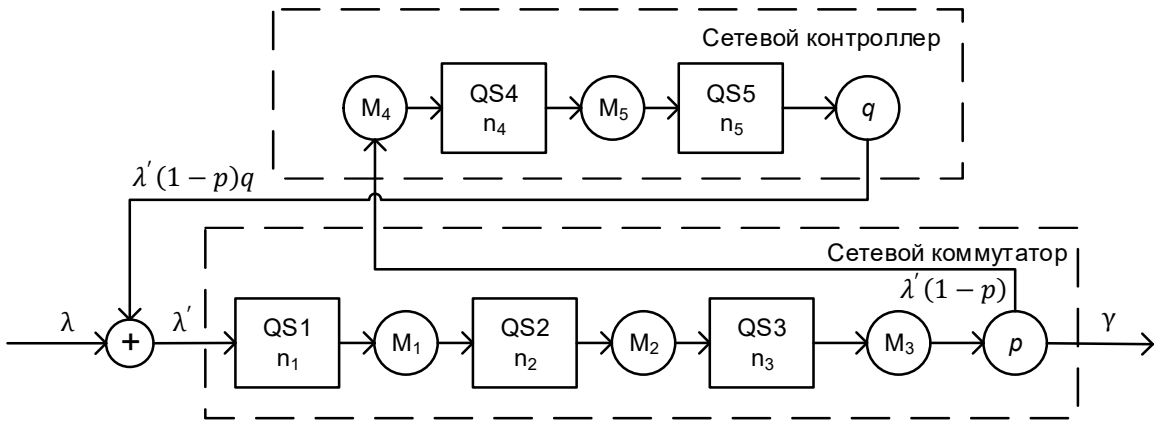


Рис. 2. Модель функциональных блоков SDN-сети

На вход коммутатора с интенсивностью λ поступает поток заявок-пакетов. Обслуженная заявка с вероятностью p покидает сеть, а с вероятностью (1 − p) (вероятность того, что информации о пакете нет в таблице потоков) переходит в узел-контроллер. Заявка, обслуженная в узле-контроллере, с вероятностью q возвращается на вход коммутатора и после повторного обслуживания в этом узле покидает сеть.

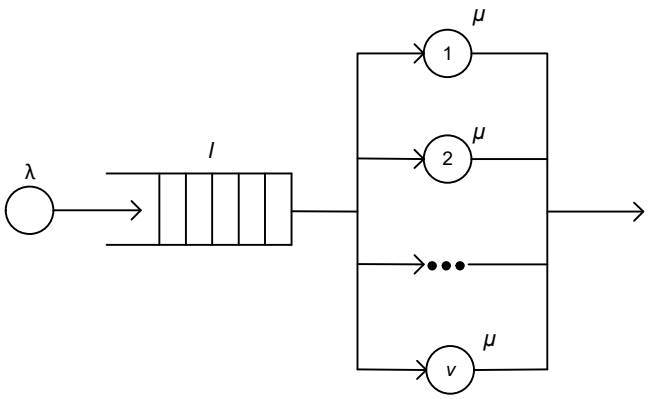


Рис. 3. Структурная схема СМО типа M/M/v/l

Потоки заявок определяются потоком Пуассона, а время обслуживания экспоненциально распределено на всех фазах. Процессы, протекающие в СеМО – марковские случайные с дискретными состояниями и непрерывным временем. Потоки заявок и их обслуживание стационарно. Для стационарной работы, анализируемой многофазной СеМО должны совместно выполняться следующие условия [8]:

$$u_1 = \frac{\lambda(1+q-pq)}{n_1 M_1} < 1;\ u_2 = \frac{\lambda(1+q-p\ )}{n_2 M_2} < 1;$$

$$u_3 = \frac{\lambda(1+q-pq)}{n_3 M_3} < 1;\ u_4 = \frac{\lambda(1+q-p\ )}{n_4 M_4} < 1;$$

$$u_5 = \frac{\lambda(1+q-pq)}{n_5 M_5} < 1.$$

Проанализируем многофазную СеМО как последовательность v-узловых СМО с l-местным буфером (см. рис. 3).

Среднее время пребывания пакета-заявки в СМО1, в соответствии с формулами Эрланга, будет равно:

$$\overline{t_1} = (p_1 + \overline{r_1})\lambda'^{-1} = \frac{1}{V_1} + \frac{p_1^{n_1+1} P_{0_1}}{n_1 n_1!(1-U_1)^2 \lambda'},$$

где $p_1 = \frac{\lambda'}{V_1}$;

$$P_{0_1} = \left[1 + \frac{p_1}{1!} + \frac{p_2}{2!} + \cdots + \frac{p_1^{l_1}}{l_1!} + \frac{p_1^{l_1+1}}{l_1 + l!(1-U_1)}\right]^{-1}.$$

Аналогично рассчитываем величины $\overline{t_2}$ и $\overline{t_3}$ для СМО2 и СМО3, при $\lambda_2 = \lambda'$ и l_2, V_2, l_3, V_3.

Аналогично рассчитываем величину $\overline{t_5}$ для СМО5.

Считаем, что $P_i\left(1/\lambda', l, lV_1,\ lV_2,\ L_3V_3\right)$ – вероятность потери пакета на *i*-й фазе обслуживания. Тогда, используя результат, полученный в [9, 10], вычисляем:

$$P_{i+1}\left(1/\lambda', l, lV_1, l_2V_2, l_3V_3\right) = \iint_{U,V} V_1^2\, e^{-l_1V(U+V)} \times P_i(1/\lambda' + V + U; l-1; V_2, V_3)\mathrm{dudv},$$

где U и V – это промежутки времени между соседними моментами поступающих пакетов полученного потока. К выражению для вычисления вероятности потери пакета применяем преобразование Лапласа и рассчитываем вероятностно-временные характеристики объема сетевого ресурса.

Показатели качества передающей части коммутатора оцениваем следующими параметрами:

– время пребывания пакетов в системе

$$V = \frac{N}{v\mu(1-p_0)} = \frac{\sum_{k=0}^{l+v} k p_k}{v\mu(1-p_0)},$$

– время ожидания пакетов в очереди

$$W = \frac{N_0}{v\mu(1-p_0)} = \frac{\sum_{k=v+1}^{l+v}(k-v)p_k}{v\mu(1-p_0)},$$

– время обслуживания

$$T_{\text{об.}} = V - W = \frac{\sum_{k=1}^{l+v} k p_k}{v\mu(1-p_0)} - \frac{\sum_{k=1}^{l+v}(k-v)p_k}{v\mu(1-p_0)} = \frac{1}{v\mu} + \frac{(v-1)\sum_{k=v}^{m+n} p_k + \sum_{k=2}^{v-1}(k-1)p_k}{v\mu(1-p_0)}.$$

Заключение

Разработана и исследована математическая модель фрагмента архитектуры сети-SDN, представленная в виде многофазной СеМО с потерями, состоящая из последовательно соединенных узлов типа M | M | v | l. На основе преобразований Лапласа и формул Эрланга для стационарного режима работы предложен метод расчета параметров фрагмента SDN-сети, получены выражения для вычисления параметров, позволяющие определить средние доли потерь пакетов на каждой из фаз их обработки коммутатором. В работе был сделаны допущения, которые позволили рассматривать трехфазный коммутатор как однофазный с тремя независимыми потоками.

Используя предложенную модель программно-конфигурируемой сети, сетевые администраторы и планировщики могут формализовать функционирование элементов фрагмента сети, прогнозировать вероятные изменения производительности, которые возникают в результате изменения трафика. Результаты исследования могут быть использованы при проектировании и эксплуатации компьютерных сетей, реализующих концепцию SDN.

Список используемых источников

1. Architecture SDN. Open Networking Foundation. URL: https://www.opennetworking.org (дата обращения: 17.02.2021).

2. Software-Defined Networking: The New Norm for Networks. Open Networking Foundation. URL: https://www.opennetworking.org/images/ stories/downloads/sdn-resources/whitepapers/ wp-sdn-newnorm.pdf (дата обращения: 17.02.2020).

3. OpenFlow Switch Specification, Version 1.3.0 (WireProtocol 0x04). Open Networking Foundation. URL: https://www.opennetworking.org/ images/stories/downloads/sdn-resources/ onfspecifications/openflow/openflow-specv1.3.0.pdf (дата обращения 17.02.2021).

4. Openflow Tutorial. URL: https://www.openflow. org/wk/index.php/OpenFlow_Tutorial (дата обращения 20.02.2021).

5. OpenFlow Switch Specification (Series). URL: https://www.opennetworking.org/sdn-resources/ onfspecifications/openflow (дата обращения: 20.02.2021).

6. Гольдштейн Б. С., Елагин В. С., Зарубин А. А., Селиванов А. Е. Программно-Конфигурируемые Сети SDN. Протокол OpenFlow. Учебное пособие. СПб.: СПбГУТ, 2018. 48 с.

7. Елагин В. С. Динамическое управление нагрузкой в программно-конфигурируемых сетях // Труды учебных заведений связи. 2017. Т. 3 № 3. С. 60–67.

8. Мочалов В. П., Линец Г. И., Палканов И. С. Аналитическая модель сегмента архитектуры программно-конфигурируемых сетей // Инфокоммуникационные технологии. 2020. Т. 18. № 2. С. 149–159.

9. Пугачев В. С. Введение в теории вероятностей. М.: Наука, 1968. 368 с.

10. Вентцель Е. С., Овчаров Л. А. Теория случайных процессов и ее инженерные приложения. М.: Издательский центр «Академия», 2003. 440 с.

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ СОВРЕМЕННЫХ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОКОММУНИКАЦИЙ ОТ СЕТЕВЫХ АТАК

Я. А. Домбровский, В. А. Малофеев, И. Б. Паращук

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

Проведен сравнительный анализ современных программных средств защиты инфокоммуникаций от сетевых атак. Полученные в ходе исследования данные могут помочь при оценивании потенциальной эффективности применения тех или иных средств обнаружения вредоносных воздействий с учетом достоинств и недостатков рассмотренных программных средств. Результаты анализа позволят повысить обоснованность принятия решений при выборе систем обнаружения атак в интересах обеспечения защиты данных в инфокоммуникационной сети или системе.

инфокоммуникационная сеть, система, обнаружение, сетевая атака, воздействие, блокирование, угроза, ресурс.

Защита и обеспечение безопасности инфокоммуникационных сетей и систем была и остается приоритетной задачей для специалистов. Их задача заключается в наиболее эффективной нейтрализации угроз, которые могут нарушить конфиденциальность, целостность и доступность данных, циркулирующих, обрабатываемых и хранящихся в рамках инфокоммуникационных сетей и систем.

Угрозы безопасности данных инфокоммуникационных сетей и систем – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, используемой сетью (системой), а также условиями обработки и хранения данных.

Одной из самых опасных угроз являются сетевые атаки – злоумышленные действия (мероприятия, процедуры), целью которого является захват контроля над удаленной локальной инфокоммуникационной сетью или системой.

Кроме того, сетевые атаки нацелены на отказ в обслуживании либо дестабилизацию сети, а также получение личных идентификационных данных пользователей, являющихся абонентами (пользователями) этой удаленной локальной инфокоммуникационной сети или системы.

Иными словами, сетевая атака – информационное разрушающее воздействие на распределенную IT-инфраструктуру, вычислительную инфокоммуникационную сеть или систему, осуществляемое программно по каналам связи. Это направленные действия на удаленные сервера для создания затруднений в работе или для утери данных.

Важнейшим этапом противодействия сетевым атакам является этап их выявления и классификации, предназначенный для выяснения (идентификации) их происхождения, характера воздействия и степени опасности.

При этом принято различать сетевые атаки на инфокоммуникационные сети или системы: атаки типа mailbombing, переполнение буфера, атаки с использованием специализированных вредоносных программ (вирусов, снифферов, троянских коней, почтовых червей и т. д.), сетевая разведка, IP-спуфинг, man-in-the-middle, атаки типа «инъекция» (PHP-инъекция, SQL-инъекция, межсайтовый скриптинг или XSS-атака, XPath-инъекция), атака типа «отказ в обслуживании» (DoS- и DDoS-атаки), а также «фишинг»-атаки.

Сниффер-атаки – анализаторы трафика, программы или устройства для оценки и перехвата своего или чужого сетевого трафика. IP-спуфинг – тип атаки, при которой один человек или программа (IP-адрес) успешно маскируется под другую, путем фальсификации данных и позволяет получить незаконные преимущества.

Сетевая атака man-in-the-middle или атака «человек посередине» – вид атаки, при которой злоумышленник перехватывает и подменяет сообщения, которыми обмениваются пользователи, причем ни один из них не догадывается о присутствии нарушителя в канале [1, 2].

При этом, в рамках комплексной защиты информации от актуальных угроз, наиболее вредоносными принято считать сетевые атаки типа «захват» (системы, данных, управления, информации), типа «срыв» (нарушение, деградация, отрицание, уничтожение) и типа «манипуляция» (внешней информацией, датчиками, беспроводными сенсорами и подмена системной информации) [3, 4].

Существует несколько ключевых направлений обеспечения безопасности инфокоммуникаций от сетевых атак. Это реализация устойчивости к сетевым атакам, аутентификация данных, контроль доступа, а также реализация приватности пользователя.

Защита от сетевых атак должна выполняться следующими методами: псевдослучайная смена сетевых адресов; блокирование соединения; блокирование хоста сети; блокировка трафика от сетевого хоста (целиком, или на основе некоторых критериев); снижение интенсивности трафика; внесение изменений в трафик (например, удаление атакующих последовательностей); передача данных другим системам, а также комбинацией вышеперечисленных методов.

Базовым инструментом обнаружения сетевых атак являются программы и программные комплексы, способные выявлять (идентифицировать) и блокировать воздействия такого типа. Причем обнаружение атак – динамический процесс определения и реагирования на любую подозрительную деятельность, направленную на сетевые или вычислительные ресурсы инфокоммуникаций.

Результативность данного процесса зависит от методов анализа входной сетевой информации. Например, методы обнаружения хакерских атак используют результаты анализа контролируемых пространств (сетевой трафик или журналы регистраций). Этот метод основан на статистике и на наборе правил экспертных систем. В дополнение к этим подходам, зачастую используются нейронные сети, позволяющие анализировать информацию и оценить, насколько согласуются полученные данные с характеристиками атак, которые нейронная сеть может распознавать.

Проведем сравнительный анализ современных программных средств защиты инфокоммуникаций от сетевых атак. Рассмотрим популярные и зарегистрированные в реестре ФСТЭК России программные комплексы и системы обнаружения атак, такие как:

- система обнаружения атак «ФОРПОСТ»;
- система обнаружения вторжений Dallas Lock;
- система ViPNet HIDS; система Security Capsule SIEM;
- система Kaspersky Anti Targeted Attack;
- система обнаружения вторжений «Кречет».

Система обнаружения сетевых атак «ФОРПОСТ» предназначена для автоматического выявления воздействий на контролируемую инфокоммуникационную сеть или систему, которые могут быть классифицированы как сетевые атаки или вторжения, а также для блокировки развития выявленных сетевых атак. Достоинствами этой системы является ее способность обнаруживать и предотвращать развитие сетевых атак, нацеленных на серверы телематических служб (FTP, Web, электронная почта, СУБД пр.) и рабочие станции, размещенные в контролируемых сегментах инфокоммуникационной сети или системы.

Программа осуществляет анализ сетевого трафика со второго по седьмой уровень сетевой модели стека протоколов OSI/ISO, обработку сетевого трафик на скоростях порядка 10 Гбит/с, а также оповещение об обнаруженных атаках и новых сообщениях в системных журналах. В системе обнаружения сетевых атак «ФОРПОСТ» имеется подсистема собственной безопасности, которая позволяет шифровать передаваемую между компонентами программы информацию с использованием отечественных средств, а также проводить контроль целостности собственных ресурсов и ресурсов защищаемой инфокоммуникационной сети или системы [5].

Система обнаружения вторжений Dallas Lock предназначена для противодействия сетевым атакам различной степени сложности путем реализации ряда функций: сигнатурный и эвристический анализ попыток нарушения защиты; обнаружение вторжений по результатам анализа служебной информации протоколов сетевого уровня; определение аномалий в действиях пользователя сети; динамические настройки реагирования на попытки нарушений, а также дискреционный и мандатный контроль доступа к объектам и устройствам инфокоммуникационной сети [6].

Программно-аппаратный комплекс ViPNet HIDS предназначен для обнаружения вторжений в инфокоммуникационные сети или системы. Это реализуется на основе динамического анализа сетевого трафика стека протоколов TCP/IP.

При этом анализ осуществляется для протоколов всех семи уровней модели взаимодействия открытых систем. Важным достоинством таких систем является их способность собирать данные и выявлять признаки вторжений непосредственно на серверах (хостах) защищаемой инфокоммуникационной сети или системы, причем, для этого не требуется дополнительной вычислительной мощности и расширенной функциональности сетевых устройств [7].

Система Security Capsule SIEM предназначена для мониторинга и управления событиями безопасности инфокоммуникационных сетей или систем и позволяет контролировать состояние информационной безопасности, управлять информацией об угрозах, оценивать эффективность применяемых средств защиты, а также полноту и корректность настроек средств и механизмов защиты. Помимо этого, система способна восстанавливать работоспособность после сбоев и отказов [8].

Система Kaspersky Anti Targeted Attack позволяет обнаруживать многоступенчатые сетевые атаки и блокировать их за счет уникальной платформы противодействия комплексным угрозам на уровне сети. Обладает средствами наглядной визуализации, опирается на прозрачность инфраструктуры инфокоммуникационных сетей или систем.

Эта система позволяет автоматизировать процессы сбора и хранения информации и «цифровых улик». Система способна готовить данные для оперативного расследования и реагирования, автоматизировать задачи расследования инцидентов и, как следствие, позволяет оптимально расходовать ресурсы служб безопасности инфокоммуникаций [9].

Система обнаружения вторжений «Кречет» – программный инструмент, реализующий в инфокоммуникационной сети или системе функции автоматизированного обнаружения и блокирования действий, нацеленных на несанкционированный доступ к данным, негативных воздействий на информацию в целях ее добычи, модификации (изменения) и блокирования доступа к ней.

Данное программное средство встраивается в существующую сетевую инфраструктуру и анализирует копию сетевого трафика, проходящего через пограничное устройство инфокоммуникационной сети [10].

Таким образом, проведен сравнительный анализ современных программных средств защиты инфокоммуникаций от сетевых атак. Полученные в ходе исследования данные могут дать реальную возможность осуществить оценивание потенциальной эффективности применения тех или иных средств обнаружения вредоносных воздействий с учетом достоинств и недостатков рассмотренных программных средств.

Помимо этого, результаты анализа, по мнению авторов, позволят повысить обоснованность принятия решений при выборе систем обнаружения атак в интересах обеспечения защиты данных в инфокоммуникационной сети или системе.

Список используемых источников

1. Бокова О. И. Оптимальное управление безопасностью территориальных сегментов информационно-телекоммуникационных систем: монография. Воронеж: Воронежский институт МВД России, 2006. 153 с.

2. Miller D., Harris S., Harper A., VanDyke S. Security Information and Event Management (SIEM) Implementation. London, McGraw-Hill. 2010. 464 p.

3. Паращук И. Б., Чернявский А. В., Шестаков Е. О. Эффективность комплексной защиты информации в системах хранения данных и электронных библиотеках: модели и методы оценивания. // Информационная безопасность регионов России (ИБРР-2019) XI-я Санкт-Петербургская Межрегиональная конференция. Санкт-Петербург, 23-25 октября 2019 г., Материалы конференции, СПб., СПОИСУ, 2019. С. 248–250.

4. Авраменко В. С., Бобрешов-Шишов Д. И., Беденков В. Н., Маликов А. В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция. Т. 3. СПб.: СПбГУТ, 2017. С. 13–18.

5. Система обнаружения атак «Форпост» версия 3.0 // Акционерное общество «Российские наукоемкие технологии» (АО «РНТ»). URL: https://www.rnt.ru/ru/production/detail.php?ID=689 (дата обращения: 15.12.2020).

6. Обнаружение и предотвращение вторжений // ООО «Конфидент». URL: https://dallaslock.ru/resheniya/obnaruzhenie-i-predotvraschenie-vtorzhenii/ (дата обращения: 16.12.2020).

7. ViPNet IDS // Компания «ИнфоТеКС». URL: https://infotecs.ru/product/setevye-komponenty/vipnet-ids/ (дата обращения 16.12.2020).

8. Система мониторинга и корреляции событий информационной безопасности Security Capsule SIEM// Инновационные технологии в бизнесе. URL: https://www.itb.spb.ru/ products/Security_Capsule_SIEM/ (дата обращения: 16.12.2020).

9. Kaspersky Anti Targeted Attack. Комплексная защита от сложных угроз и целевых атак] // ОАО «Лаборатория Касперского». URL: https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform (дата обращения: 17.12.2020).

10. Система обнаружения вторжений «Кречет» // НПП «Гамма». URL: https://nppgamma.ru/catalog/setevaya_bezopasnost/krechet/ (дата обращения: 17.12.2020).

УДК 004.043
ГРНТИ 81.93.29

АНАЛИЗ СОСТЯЗАТЕЛЬНЫХ АТАК НА КОМПОНЕНТЫ МАШИННОГО ОБУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Е. А. Донсков, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В настоящее время при решении задач обнаружения вторжений все чаще применяется машинное обучение. Несмотря на большую эффективность, модели (компоненты) машинного обучения подвержены состязательным атакам - атакам злоумышленников, направленным на то, чтобы ввести компоненты машинного обучения в заблуждение. В данном исследовании проводится анализ существующих состязательных атак на системы обнаружения вторжений и способов противодействия им.

машинное обучение, состязательная атака, система обнаружения вторжений.

Введение

В последние годы машинное обучение стало необходимым инструментом для решения различных задач. Такие системы получили большое распространение в критически важных областях, среди которых медицина, банковские системы, системы противодействия спаму, автоматизированные процессы управления транспортными средствами, системы обнаружения вторжений в корпоративных инфраструктурах. Критический характер таких систем требует тщательной проработки вопросов информационной безопасности [1, 2]. Злоумышленник при нахождении уязвимости может получить доступ к конфиденциальной информации, а также значительно изменить алгоритмы машинного обучения. Поэтому необходимо обеспечивать безопасность систем, использующих машинное обучение, и иметь защиту от так называемых состязательных атак, направленных на модели машинного обучения. В работе рассматриваются состязательные атаки, которые могут быть нацелены на компоненты машинного обучения систем обнаружения вторжений, производится их категоризация, и предлагаются возможные варианты защиты.

Состязательная атака

Состязательная атака – это атака, направленная на модели машинного обучения для достижения смещения расчетов и, соответственно, некорректной работы этих алгоритмов.

На данный момент выделяются следующие типы состязательных атак: (1) уклонения; (2) отравления; (3) на основе решения уравнений; (4) с поиском пути; (5) вычисляющие оптимальный входной вектор признаков; (6) использующие свойство переносимости.

Атаки уклонения взаимодействуют с моделью машинного обучения, передавая такой сформированный набор данных, что модель неверно обучается и затем неверно функционирует [3]. Атаки данного типа не требуют доступа к обучающим данным и манипулирования ими, они выполняются при обучении и тестировании моделей машинного обучения.

Атаки отравления направлены на передачу модели машинного обучения нестандартных данных, которые находятся за пределами обычного набора данных, для внесения значительных изменений в обучение нейронной сети. Атаки отравления выполняются в момент обучения и требуют знаний об обучающих выборках целевой модели [4, 5].

Атаки на основе решения уравнений применимы к облачным провайдерам, которые предоставляют машинное обучение как услугу через API, а также для таких моделей, как многослойный персептрон, двоичная логистическая регрессия и многоклассовая логистическая регрессия, где они представлены в виде уравнений с известными и неизвестными переменными [6]. Цель состоит в том, чтобы использовать данные для поиска неизвестных переменных, которые обычно являются параметрами, используемыми для обучения моделей. Предполагается, что эти атаки предоставят злоумышленнику информацию о модели и ее архитектуре.

Атаки с поиском пути нацелены на алгоритмы машинного обучения, использующие бинарные деревья, многозначные деревья и деревья регрессии. В этих атаках значение каждой входной функции варьируется до тех пор, пока не будут выполнены условия в каждом узле, чтобы достигнуть необходимую вершину [6].

Атаки, вычисляющие оптимальный входной вектор признаков, близкий к целевому вектору признаков, осуществляются с использованием взвешенной вероятностной оценки, которая указывает правильное значение [7]. Это используется для создания злоумышленником модели, крайне близкой к целевой модели машинного обучения.

Атаки, использующие свойство переносимости, выполняются при отсутствии у злоумышленника полноценной информации о внутреннем устройстве целевой модели машинного обучения и при наличии API, которое передает ответ на переданный набор данных [8, 9].

Предлагаемые способы защиты

В качестве основных способов защиты от состязательных атак выделяются: обучение на наборах данных состязательных атак, манипуляции

с маскировкой градиента модели машинного обучения, технология дистилляции, методика отклонения при отрицательном воздействии, технология MagNet, обнаружение состязательных атак. Подробное описание способов защиты представлено в таблице.

ТАБЛИЦА. Способы защиты

Способ защиты	Описание
Обучение на наборах данных состязательных атак	Способ предполагает добавление наборов данных, используемых в состязательных атаках, в наборы обучающих данных [10, 11]. Основная идея данного способа заключается в создании устойчивого к атакам классификатора.
Манипуляции с маскировкой градиента модели машинного обучения	Различают два подхода к маскировке градиента: скрытие градиента и сглаживание градиента. Однако манипуляции с маскировкой в качестве средства защиты не полноценны, так как не останавливают злоумышленника, а лишь задерживают его в процессе анализа моделей и проведения атак [12].
Технология дистилляции	В работах [13, 14] предлагается использовать дистилляцию в качестве меры защиты от состязательных атак. Создавая с помощью одной из моделей образцы состязательных атак и передавая их во вторую модель, специалисты по информационной безопасности обучали целевую модель и формировали устойчивость к подобному виду атак.
Технология MagNet	Использование технологии MagNet позволяет подвергнуть дополнительной проверке и обработке входные данные. В тех случаях, когда совершается атака, и передаются состязательные экземпляры данных, сеть MagNet проверяет статистическим путем отклонения от стандартных значений и в зависимости от результата проверки либо классифицирует эти данные как состязательную атаку и отбрасывает их, либо проводит небольшие корректировки и передает данные дальше по конвейеру [15].
Обнаружение состязательных атак	К основной защищаемой модели машинного обучения добавляется еще один компонент для классификации входных данных и выявления состязательных атак. Добавленный компонент может быть представлен как в виде статистических функций, созданных специалистом, так и в виде другой машинной модели, специально обученной на подготовленных примерах состязательных атак [16, 17].

В сфере информационной безопасности также крайне актуальна проблема состязательных атак на компоненты машинного обучения. Каждый из приведенных способов защиты применим к большинству подобных систем, но среди работ выделяются частные случаи.

Вэйлинь Сюй и соавторы рассматривают в статье [18] аспекты атаки и защиты от вредоносных PDF. Отмечено, что классификаторы PDFrate и Hidost, предназначенные для выявления вредоносного файла формата PDF, значительно хуже отслеживают образцы, которые предварительно были мо-

дифицированы механизмами, создающими программные мутации. В качестве способов защиты предлагается учитывать модифицированные образцы в процессе обучения модели машинного обучения, более тщательно скрывать информацию и использовать в алгоритмах устойчивые к атакам функции.

Чинавле Дипак со своей командой предложили метод, который позволяет автоматически переобучать классификатор после обнаружения модифицированных образцов с помощью псевдометок и меры взаимного согласования на ансамблевой модели. Данный метод оказался крайне эффективным в задаче обнаружения спама [19].

Андерсон Хайрам [20] использовал большое количество функций (2350) для создания пространства переменных переносимых исполняемых (PE) файлов. Созданное пространство переменных использовалось моделью машинного обучения для преобразования исходного файла в модифицированный образец. Для защиты модели машинного обучения от этого типа атак предлагается также создавать модифицированные вредоносные образцы, а затем передавать их в обучающую выборку.

Заключение

В рамках исследования был проведен сравнительный анализ основных видов и типов состязательных атак на компоненты машинного обучения. Также были рассмотрены основные способы защиты от этих атак. В качестве основных результатов исследования можно заключить, что существующие способы защиты от атак не являются абсолютно эффективными и требуют доработки и совершенствования. Возможные подходы и инструменты, которые могут быть использованы для усовершенствования способов защиты, будут рассмотрены в дальнейших исследованиях авторов работы.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7-10 August 2006. pp. 339–344.

2. 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. С. 68–75.

3. Blockeel H., Kersting K., Nijssen S., Železný F. Evasion Attacks against Machine Learning at Test Time // ECML PKDD 2013. Lecture Notes in Computer Science. Vol. 8190. Springer, Berlin, Heidelberg.

4. Mozaffari-Kermani M., Sur-Kolay S., Raghunathan A., Jha N.K. Systematic poisoning attacks on and defenses for machine learning in healthcare // IEEE Journal of Biomedical and Health Informatics. Vol. 19. No. 6, Nov. 2015. pp. 1893–1905.

5. Huang L., Joseph A. D., Nelson B., Rubinstein B., Tygar J. D. Adversarial machine learning // Proceedings of the 4th ACM workshop on Security and artificial intelligence (AISec'11). Association for Computing Machinery, New York, NY, USA. pp. 43–58.

6. Tramer F., Zhang F., Juels A., Reiter M. K., Ristenpart T. Stealing machine learning models via prediction APIs // Proceedings of 25th Usenix Security Symposium, Austin, Texas. 2016. pp. 601–618.

7. Frekrikson M., Jha S., Ristenpart T. Model inversion attacks that exploit confidence information and Basic Countermeasures // Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15), Colorado, USA. 2015. pp. 1322–1333.

8. Tramer F., Papernot N., Goodfellow I., Boneh D., McDaniel P. The Space of Transferable Adversarial Examples. URL: https://www.researchgate.net/publication/316035255_The_Space_of_Transferable_Adversarial_Examples.

9. Papernot N., McDaniel P., Goodfellow I. Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples. URL: https://www.researchgate.net/publication/303490367_Transferability_in_Machine_Learning_from_Phenomena_to_Black-Box_Attacks_using_Adversarial_Samples.

10. Tramer F., Kurakin A., Papernot N., Boneh D., McDaniel P. Ensemble adversarial training: Attacks and defenses // Proceedings of the International Conference on Learning Representations. 2018. pp. 1–20.

11. Miyato T., Maeda S.I., Koyama M., Ishii S. Virtual adversarial training: a regularization method for supervised and semi-supervised learning // IEEE transactions on pattern analysis and machine intelligence. Vol. 41. No. 8. 2018. pp. 1979–1993.

12. Papernot N., McDaniel P., Sinha A., Wellman M. Towards the Science of Security and Privacy in Machine Learning. URL: https://www.researchgate.net/publication/310122918_Towards_the_Science_of_Security_and_Privacy_in_Machine_Learning.

13. Papernot N., McDaniel P., Wu X., Jha S., Swami A. Distillation as a defense to adversarial perturbations against deep neural networks // IEEE Symp. on Security and Privacy. 2016. pp. 582–597.

14. Soll M., Hinz T., Magg S., Wermter S. Evaluating Defensive Distillation for Defending Text Processing Neural Networks Against Adversarial Examples // International Conference on Artificial Neural Networks. 2019. pp. 685–696.

15. Meng D., Chen H. Magnet: a two-pronged defense against adversarial examples // ACM SIGSAC Conference on Computer and Communications Security. ACM. 2017. pp. 135–147.

16. Gu S., Zhu T., Yao Y., Wang W. Detecting Adversarial Examples in Deep Neural Networks using Normalizing Filters // Proceedings of the 11th International Conference on Agents and Artificial Intelligence. Vol. 2: ICAART, 2019, Prague, Czech Republic. pp. 164–173.

17. Akhtar Z., Monteiro J., Falk T. Adversarial Examples Detection Using No-Reference Image Quality Features. // IEEE International Carnahan Conference on Security Technolog, 2018. pp. 1–5.

18. Xu W., Qi Y., Evans D. Automatically Evading Classifiers: A Case Study on PDF Malware Classifiers. // Network and Distributed System Security Symposium 2016 (NDSS), San Diego. 2016. pp. 1–15.

19. Deepak C., Pranam K., Tim O., Tim F. Ensembles in adversarial classification for spam // Proceedings of the 18th ACM conference on Information and knowledge management (CIKM '09). Association for Computing Machinery, New York, NY, USA, 2015–2018.

20. Anderson, H. Evading Machine Learning Malware Detection // Black Hat. 2017. pp. 1–9.

УДК 004.732
ГРНТИ 49.43.29

АНАЛИЗ ВЛИЯНИЯ ТЕХНОЛОГИИ РАНДОМИЗАЦИИ MAC-АДРЕСОВ МОБИЛЬНЫХ УСТРОЙСТВ НА МОНИТОРИНГ И АНАЛИЗ ПАССАЖИРОПОТОКА

Р. А. Дунайцев, Н. А. Лебедева

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

В последние годы технология Wi-Fi, помимо традиционного использования для беспроводного доступа в глобальную сеть Интернет, получила еще одну область применения в виде Wi-Fi аналитики и гиперлокального таргетинга в сфере маркетинга и рекламы. Чтобы обезопасить пользователей от слежки за ними, производители мобильных операционных систем разработали технологию рандомизации MAC-адресов. В статье описывается принцип работы данной технологии, а также дается оценка возможности использования собираемых MAC-адресов для мониторинга и анализа пассажиропотока.

MAC-адрес, рандомизация, смартфон, Wi-Fi.

Сегодня сети Wi-Fi и точки доступа (ТД) окружают нас повсюду: в кафе и ресторанах, в торговых центрах и транспорте. Как результат, многие пользователи предпочитают держать Wi-Fi постоянно включенным, чтобы смартфон сам подключался к знакомой сети, как только он оказывается в зоне ее покрытия. Для обнаружения сетей Wi-Fi, находящихся поблизости, обычно рассылаются широковещательные кадры Probe Request с использованием MAC-адреса смартфона, который является уникальным для каждого устройства. Это означает, что перехват подобных кадров позволит отследить пользователя, даже если он не подключался ни к одной ТД. MAC-адреса не привязаны к персональным данным, но компании могут почерпнуть из них информацию о покупательских привычках и маршрутах передвижения пользователя, чтобы на основании этого затем показывать таргетированную рекламу магазинов, аптек, салонов красоты и т. д. Также собранные таким методом MAC-адреса могут быть использованы для замера трафика и проходимости [1]. Например, центр организации дорожного движения Москвы в 2020 году провел тендер на разработку системы мониторинга пассажиропотока [2]. Система предусматривает размещение на остановках общественного транспорта снифферов, которые будут собирать MAC-адреса мобильных устройств пользователей (смартфонов, план-

шетов и т. п.) и отслеживать по ним движение пешеходов и пассажиров. Такая система может позволить детально проследить маршрут каждого пользователя по городу и собрать данные для анализа пассажиропотока.

Чтобы защитить пользователей от сбора и анализа MAC-адресов смартфонов сторонними организациями, производители мобильных операционных систем (ОС) внедрили рандомизацию MAC-адресов [3]. В этом случае при отправке широковещательных (*broadcast*) и одноадресных (*unicast*) кадров Probe Request вместо реального MAC-адреса устройством производится подстановка некоего случайного MAC-адреса. Такой MAC-адрес назначается одноразово для проведения сканирования и время его жизни составляет от нескольких секунд до нескольких минут. Далее MAC-адрес заменяется на новый случайный и больше повторно не используется. Таким образом устройства могут генерировать широковещательные запросы без раскрытия своего реального MAC-адреса. В ОС Android, начиная с версии 6.0, используется рандомизация для активного сканирования, если драйвер и оборудование позволяют это сделать [4].

Теоретически такая автоматическая смена MAC-адресов должна была затруднить отслеживание смартфона сторонними организациями, но, как оказалось, данная мера защиты бесполезна в связи с рядом уязвимостей и ошибок в реализации. Например, когда смартфон обнаруживает знакомую сеть (т. е. известный SSID), то при подключении к ней использует свой настоящий MAC-адрес, что позволяет снифферам получить информацию о реальных MAC-адресах мобильных устройств. Поэтому, начиная с ОС Android версии 9.0, для каждого известного SSID смартфон генерирует и хранит случайный MAC-адрес. Тем самым даже при подключении к ТД реальный MAC-адрес устройства не раскрывается [5].

Чтобы проверить, насколько эффективно технология рандомизации MAC-адресов мобильных устройств работает на практике, была проведена серия экспериментов. Для исследования были выбраны три смартфона на базе ОС Android, а именно: Xiaomi Redmi 6 под управлением Android 9 (последнее обновление системы безопасности от 01.05.2020), Xiaomi Redmi Note 7 под управлением Android 10 (последнее обновление системы безопасности от 01.10.2020) и Samsung Galaxy A30 под управлением Android 10 (последнее обновление системы безопасности от 01.01.2021). По идее, в каждом смартфоне из этого списка должна использоваться рандомизация MAC-адресов как и при поиске ТД, так и при подключении к ней. Для сбора трафика была использована программа Acrylic Wi-Fi Professional и внешний Wi-Fi адаптер D-Link Wireless G DWA-110, работающий в диапазоне 2,4 ГГц и настроенный так, чтобы мониторить один канал. В данном случае был выбран канал 11, на котором работала ТД, к которой и подключались исследуемые смартфоны. Для просмотра и анализа собранных кадров была использована программа Wireshark.

Сначала был собран трафик в режиме поиска ТД. Для каждого смартфона время сбора трафика составляло 5 минут. Смартфоном Xiaomi Redmi 6 за это время было отправлено 25 кадров Probe Request (рис. 1). Все они имеют рандомизированные MAC-адреса, старшие три байта которых принадлежат компании MediaTek, а младшие три байта представляют собой случайную комбинацию. Также можно заметить, что кадры Probe Request чаще всего посылаются попарно с одинаковым MAC-адресом.

No.	Time	Source	Destination	Protocol	Length	Info
211	11.184873	MediaTek_66:cb:f8	Broadcast	802.11	81	Probe Request, SN=1563, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
212	11.184873	MediaTek_66:cb:f8	Broadcast	802.11	81	Probe Request, SN=1564, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
823	54.612082	MediaTek_15:4e:e4	Broadcast	802.11	81	Probe Request, SN=1175, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
824	54.612082	MediaTek_15:4e:e4	Broadcast	802.11	81	Probe Request, SN=1176, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
827	54.705504	MediaTek_15:4e:e4	Broadcast	802.11	81	Probe Request, SN=1178, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
841	55.627487	MediaTek_2d:60:e4	Broadcast	802.11	81	Probe Request, SN=1611, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
955	65.656355	MediaTek_b4:28:0b	Broadcast	802.11	81	Probe Request, SN=551, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
956	65.656355	MediaTek_b4:28:0b	Broadcast	802.11	81	Probe Request, SN=552, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1051	74.622686	MediaTek_51:6d:ed	Broadcast	802.11	81	Probe Request, SN=1760, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1052	74.622686	MediaTek_51:6d:ed	Broadcast	802.11	81	Probe Request, SN=1761, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1259	94.633883	MediaTek_0a:d3:2f	Broadcast	802.11	81	Probe Request, SN=1840, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1260	94.633883	MediaTek_0a:d3:2f	Broadcast	802.11	81	Probe Request, SN=1841, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

Рис. 1. Кадры Probe Request смартфона Xiaomi Redmi 6 в режиме поиска ТД

Схожую картину можно наблюдать и при просмотре кадров Probe Request смартфона Xiaomi Redmi Note 7 (рис. 2). За 5 минут было собрано 35 кадров и все они имеют рандомизированные MAC-адреса, старшие три байта которых принадлежат компании Google, а младшие три байта представляют собой случайную комбинацию. При этом кадры Probe Request также посылаются попарно, но с небольшой задержкой.

No.	Time	Source	Destination	Protocol	Length	Info
162	11.122993	Google_fe:64:c4	Broadcast	802.11	179	Probe Request, SN=230, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
165	11.138612	Google_fe:64:c4	Broadcast	802.11	179	Probe Request, SN=231, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
434	31.102694	Google_4b:4b:0a	Broadcast	802.11	179	Probe Request, SN=306, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
438	31.133889	Google_4b:4b:0a	Broadcast	802.11	179	Probe Request, SN=307, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
695	51.129181	Google_1a:0c:ce	Broadcast	802.11	179	Probe Request, SN=382, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
698	51.144797	Google_1a:0c:ce	Broadcast	802.11	179	Probe Request, SN=383, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
929	71.124454	Google_b2:9c:53	Broadcast	802.11	179	Probe Request, SN=458, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
932	71.140070	Google_b2:9c:53	Broadcast	802.11	179	Probe Request, SN=459, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1212	91.119632	Google_6d:de:f1	Broadcast	802.11	179	Probe Request, SN=534, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1216	91.134974	Google_6d:de:f1	Broadcast	802.11	179	Probe Request, SN=535, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

Рис. 2. Кадры Probe Request смартфона Xiaomi Redmi Note 7 в режиме поиска ТД

Смартфоном Samsung Galaxy A30 за 5 минут было отправлено 13 кадров Probe Request и все они имеют рандомизированные MAC-адреса, представляющие собою полностью случайную комбинацию (рис. 3).

No.	Time	Source	Destination	Protocol	Length	Info
79	29.149351	c6:cf:cf:36:2b:37	Broadcast	802.11	133	Probe Request, SN=2861, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
81	29.180594	c6:cf:cf:36:2b:37	Broadcast	802.11	133	Probe Request, SN=2862, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
129	44.864385	52:b4:26:de:18:ee	Broadcast	802.11	133	Probe Request, SN=803, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
210	81.246403	da:ea:56:1f:d6:21	Broadcast	802.11	133	Probe Request, SN=2507, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
300	120.422091	92:95:9d:35:00:2f	Broadcast	802.11	133	Probe Request, SN=59, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
386	158.741153	0a:10:4b:17:59:e6	Broadcast	802.11	133	Probe Request, SN=3424, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
424	172.238000	86:fb:ee:2b:9e:3d	Broadcast	802.11	133	Probe Request, SN=238, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
452	185.203644	62:83:63:30:58:cc	Broadcast	802.11	133	Probe Request, SN=768, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
479	197.759567	d2:c0:2c:b8:f0:78	Broadcast	802.11	133	Probe Request, SN=2532, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
589	239.727795	c6:72:28:db:ed:35	Broadcast	802.11	133	Probe Request, SN=2937, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
591	239.759077	c6:72:28:db:ed:35	Broadcast	802.11	133	Probe Request, SN=2938, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
673	276.531591	be:7e:07:04:b0:2d	Broadcast	802.11	133	Probe Request, SN=3927, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
696	289.419167	d2:f9:f3:79:25:3a	Broadcast	802.11	133	Probe Request, SN=4036, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

Рис. 3. Кадры Probe Request смартфона Samsung Galaxy A30 в режиме поиска ТД

Теперь рассмотрим ситуацию с подключением смартфонов к ТД. Время сбора трафика также составляло по 5 минут для каждого устройства.

Как выяснилось, смартфон Xiaomi Redmi 6 при подключении к ТД использует свой реальный MAC-адрес. Поэтому в дальнейшем исследовании он рассматриваться не будет.

Смартфон Xiaomi Redmi Note 7 изначально подключается к ТД со своим реальным MAC-адресом, однако в настройках для каждой сети Wi-Fi можно задать параметры конфиденциальности, которые позволят использовать случайный MAC-адрес (рис. 4). После выбора данного пункта происходит переподключение к ТД.

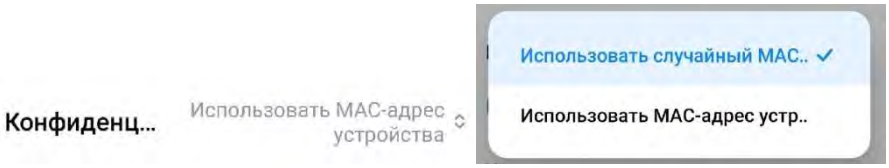


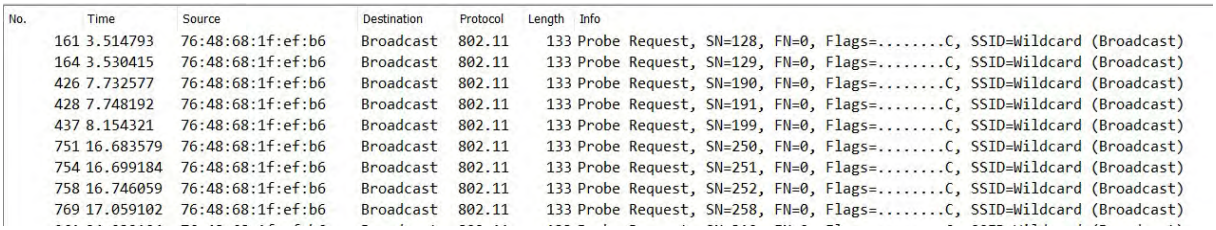
Рис. 4. Настройки конфиденциальности смартфона Xiaomi Redmi Note 7

За время исследования смартфон Xiaomi Redmi Note 7 отправил 35 кадров Probe Request с одинаковым рандомизированным MAC-адресом, с которым он подключился к данной ТД (рис. 5). Использованный MAC-адрес является локально администрируемым и его первые три байта не принадлежат ни одной компании.

При подключении смартфона Samsung Galaxy A30 к сети Wi-Fi можно сразу указать нужные параметры конфиденциальности. Также следует отметить, что по умолчанию выбран вариант использования рандомизированного MAC-адреса. В итоге за 5 минут было собрано 70 кадров Probe Request с одинаковым рандомизированным MAC-адресом, с которым смартфон подключился к данной ТД (рис. 6). Использованный MAC-адрес также является локально администрируемым и его первые три байта не принадлежат ни одной компании.

No.	Time	Source	Destination	Protocol	Length	Info
42	1.718349	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=425, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
191	11.747251	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=480, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
402	21.796511	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=538, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
718	31.778258	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=612, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
884	41.791796	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=671, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1074	51.836307	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=730, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1078	51.898784	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=731, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1277	61.818323	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=791, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1397	71.815970	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=837, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1574	81.844833	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=887, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1577	81.876075	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=888, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1784	91.857494	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=951, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
1790	91.873079	16:7d:92:b0:33:62	Broadcast	802.11	139	Probe Request, SN=953, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

Рис. 5. Кадры Probe Request смартфона Xiaomi Redmi Note 7 при подключении к ТД



No.	Time	Source	Destination	Protocol	Length	Info
161	3.514793	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=128, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
164	3.530415	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=129, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
426	7.732577	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=190, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
428	7.748192	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=191, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
437	8.154321	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=199, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
751	16.683579	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=250, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
754	16.699184	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=251, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
758	16.746059	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=252, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
769	17.059102	76:48:68:1f:ef:b6	Broadcast	802.11	133	Probe Request, SN=258, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

Рис. 6. Кадры Probe Request смартфона Samsung Galaxy A30 при подключении к ТД

Таким образом, несмотря на разработку и внедрение технологии рандомизации MAC-адресов, достаточно большое количество смартфонов на базе ОС Android либо не поддерживает ее, или поддерживает не в полной мере. Как показало исследование, не все смартфоны на базе ОС Android версии 9 используют рандомизированный MAC-адрес при подключении к ТД. Среди смартфонов на базе ОС Android версии 10 хоть и присутствует функция рандомизации в полном объеме, но не на всех устройствах она работает по умолчанию. Можно предположить, что далеко не все пользователи знают о данной уязвимости, и, соответственно, могут не включать функцию рандомизации при подключении к ТД, таким образом раскрывая реальный MAC-адрес своего мобильного устройства. Однако нельзя исключать возможность использования рандомизации MAC-адресов при подключении к ТД по умолчанию в одном из следующих обновлений ОС Android. На основании вышеизложенного хочется вернуться к упомянутой в начале статьи системе мониторинга пассажиропотока центра организации дорожного движения Москвы. Сейчас от этого проекта могут отказаться как раз в связи с последними обновлениями ОС Android и iOS [6]. Иными словами, использование MAC-адресов смартфонов для показа таргетированной рекламы и/или отслеживания пассажиропотока в обозримом будущем может оказаться крайне проблематичным.

Список используемых источников

1. Дунайцев Р. А., Шабанова А. А. Использование технологии Wi-Fi в маркетинге // Информационные технологии и телекоммуникации. 2019. Том 7. № 4. С. 37–42.

2. В сложной оперативной остановке. Пассажиров Москвы будут мониторить по смартфонам. URL: https://www.kommersant.ru/doc/4539137 (дата обращения: 31.03.2021).

3. К чему приведет ограничение на сбор MAC-адресов в наружной рекламе: оценка индустрии. URL: https://adindex.ru/publication/opinion/media/2019/11/10/276919.phtml (дата обращения: 31.03.2021).

4. MAC address randomization in WiFi probe requests. URL: https://macaddress.io/faq/mac-address-randomization-in-wifi-probe-requests (дата обращения: 31.03.2021).

5. Конфиденциальность: рандомизация MAC. URL: https://source.android.com/ devices/tech/connect/wifi-mac-randomization?hl=ru (дата обращения: 31.03.2021).

6. СМИ узнали о планах мэрии Москвы закрыть проект по сбору данных пешеходов. URL: https://www.rbc.ru/society/14/01/2021/5fffceaf9a79471d2da44e9e (дата обращения: 31.03.2021).

УДК 621.396.9
ГРНТИ 47.49.31

ОБЗОР ТЕХНОЛОГИЙ ВНУТРЕННЕГО ПОЗИЦИОНИРОВАНИЯ

Р. А. Дунайцев, Д. А. Лобач

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

Системы позиционирования и навигации играют важную роль в жизни современного общества, проникая во все сферы науки и техники. В последние годы технологии позиционирования внутри помещений, известные также как локальное или внутреннее позиционирование, быстро развиваются и являются одной из актуальных тем для научных исследований. В данной статье рассматриваются основные системы внутреннего позиционирования, сравнивается точность определения координат объекта, преимущества и недостатки, а также описывается влияние преград на распространение сигнала внутри помещения.

внутреннее позиционирование, позиционирование внутри помещений, indoor positioning, Bluetooth, RFID, Wi-Fi.

В современном мире системы спутниковой навигации, такие как американская система глобального позиционирования (*Global Positioning System*, GPS) и отечественная глобальная навигационная спутниковая система (ГЛОНАСС), имеют самое широкое распространение и используются практически во всех мобильных устройствах. Этому в немалой степени поспособствовало решение Федеральной комиссии по связи США (*Federal Communication Commission*, FCC), принятое в 1999 году, согласно которому все мобильные телефоны были обязаны поддерживать функцию определения местоположения абонента при обращении к экстренным службам в рамках системы E-911 (*Enhanced* 911). К сожалению, системы спутниковой навигации имеют существенные ограничения в применении, связанные с необходимостью нахождения объекта на открытом пространстве и наличия в прямой видимости спутников, поскольку из-за помех многолучевого распространения сигнала точность определения координат объекта падает. В результате внутри зданий и помещений подобные системы оказываются малопригодны. В настоящее время наиболее перспективными технологиями для позиционирования внутри помещений, также известного как локальное или внутреннее позиционирование, являются Wi-Fi, Bluetooth и RFID. Однако возможные области их применения ограничены радиусом работы и обеспечиваемой точностью позиционирования. Таким образом, целью данной статьи является рассмотрение основных систем внутреннего

позиционирования (*indoor positioning system*, IPS), сравнение точности определения координат объекта, а также их преимуществ и недостатков.

В настоящее время технология Wi-Fi используется практически повсеместно и имеет широкое применение во многих сферах жизни. Благодаря тому, что любая точка доступа (ТД) регулярно отправляет широковещательные кадры-маяки (*beacon frames*), можно получить необходимые данные для определения местоположения мобильного устройства. Использование этой технологии не требует предварительной настройки самого мобильного устройства, что позволяет применять ее в любой сети Wi-Fi, где ТД регистрируют данные об уровне принятого сигнала. Точность позиционирования варьируется от 15 сантиметров до нескольких десятков метров в зависимости от расстояния до ТД [1]. В результате Wi-Fi позиционирование обладает рядом преимуществ:

− низкая себестоимость,

− не требуется установка дополнительного оборудования, так как необходимая инфраструктура в виде ТД имеется практически в каждом здании.

В сфере беспроводных персональных сетей (*Wireless Personal Area Network*, WPAN) технология Bluetooth была разработана для того, чтобы избавиться от проводов в непосредственной близости от терминала (компьютера, ноутбука, планшета или смартфона). Таким образом, радиус действия Bluetooth достаточно мал и обычно составляет около 10 метров [2]. Однако для внутреннего позиционирования все большую популярность набирают Bluetooth-маячки, которые работают на базе технологии Bluetooth с низким энергопотреблением (*Bluetooth Low Energy*, BLE).

На рынке существует два основных стандарта для Bluetooth-маячков:

1) iBeacon (компания Apple, Inc.), впервые представленный на всемирной конференции для разработчиков на платформах Apple в 2013 году. Для отображения нужной информации мобильное устройство получает универсальные уникальные идентификаторы (*Universally Unique Identifier*, UUID) Bluetooth-маячков. Чтобы устройство могло найти нужный маячок, дополнительно задаются значения 16-битных идентификаторов Major и Minor (см. рис.). Например, сетевые магазины могут записывать общую информацию в Major, а идентификаторы отдельных магазинов – в Minor.

2) Eddystone (компания Google LLC), выпущенный в качестве альтернативы стандарту iBeacon в 2015 году. Eddystone обеспечивает аналогичную функциональность с iBeacon, но является более гибким и имеет открытый исходный код, доступный на сайте GitHub [3].

К преимуществам Bluetooth позиционирования можно отнести следующее:

− высокая безопасность,

− низкая стоимость,

− низкое энергопотребление,
− небольшой размер Bluetooth-маячков.

Рис. Принцип работы Bluetooth-маячков в технологии iBeacon

Системы позиционирования на основе технологии радиочастотной идентификации (*Radio Frequency Identification*, RFID) используют радиочастотные сигналы для бесконтактного обмена данными с целью идентификации и определения координат объекта. Любая система, использующая RFID, состоит из считывающего устройства и одной или нескольких RFID-меток (также известных как транспондеры) [4]. В зависимости от типа питания RFID-метки делятся на активные и пассивные. Активные метки снабжены собственным источником питания и не зависят от энергии считывающего устройства, благодаря чему читаются на большем расстоянии. Пассивные метки собственного источника питания не имеют, а их работа обеспечивается за счет электрического тока, индуцированного в антенне электромагнитным сигналом от считывающего устройства. В результате системы позиционирования с использованием активных RFID-меток обеспечивают дальность работы от 20 до 80 метров и точность до 3 метров. Системы позиционирования с использованием пассивных RFID-меток обеспечивают гораздо меньшую дальность работы, но имеют низкую стоимость и больший жизненный цикл. Основные параметры описанных систем приведены в таблице 1 [5, 6].

ТАБЛИЦА 1. Сравнение характеристик технологий внутреннего позиционирования

Технология	Точность, м	Дистанция, м	Стоимость	Примечание
Wi-Fi	0,5–10	до 100	низкая	Требуется не менее трех ТД
Bluetooth LE	0,5–4	до 30	низкая	Требуется периодическая замена батареек

Технология	Точность, м	Дистанция, м	Стоимость	Примечание
Активные RFID	0,5–3	до 80	высокая	Требуется периодическая замена батареек
Пассивные RFID	0,1–0,5	до 1	низкая	Требуются мощные считыватели

Согласно [7], для оценки потери мощности сигналов радиосистем, работающих внутри помещений в диапазоне от 300 МГц до 450 ГГц, следует использовать следующую формулу:

$$L = 20\log_{10} f + N * \log_{10} d + L_f(n) - 28,$$

где f – частота в МГц;

d – расстояние в метрах между источником и приемником;

N – дистанционный коэффициент потерь мощности;

$L_f(n)$ – коэффициент потерь при прохождении сигнала через препятствия;

n – количество препятствий между приемником и передатчиком.

Для оценки коэффициента потерь при прохождении сигнала Wi-Fi через различные материалы была проведена серия экспериментов. Результаты представлены в таблице 2.

ТАБЛИЦА 2. Затухание сигнала при прохождении через различные материалы

Материал	Толщина материала, мм	Ослабление сигнала в диапазоне 2,4 ГГц, дБ	Ослабление сигнала в диапазоне 5 ГГц, дБ
Фанера	20	2,0 ± 0,2	2,2 ± 0,3
Стеклопластик	8	0,1 ± 0,1	0,2 ± 0,2
Стекло	4	0,5 ± 0,1	1,5 ± 0,2
Линолеум	5	0,1 ± 0,1	0,3 ± 0,1
Бетон	36	9,5 ± 0,3	11,0 ± 0,4
Кирпич	65	6,5 ± 0,5	10,0 ± 0,6

Список используемых источников

1. Ocana M., Bergasa L., Sotelo M., Flores R. Indoor robot navigation using a POMDP based on WiFi and ultrasound observations // IEEE/RSJ International Conference on Intelligent Robots and Systems, Edmonton, Canada. 2005. pp. 2592–2597.

2. Samama N. Indoor Positioning: Technologies and Performance. Wiley-IEEE Press, 2019. 368 p.

3. Eddystone. URL: https://github.com/google/eddystone (дата обращения: 30.03.2021).

4. Guo X., Ansari N., Hu F., Shao Y., Elikplim N., Li L. A Survey on Fusion-Based Indoor Positioning // IEEE Communications Surveys & Tutorials. 2019. Vol. 22. No. 1. pp. 566–594.

5. Брагин Д. С., Поспелова И. В., Черепанова И. В., Серебрякова В. Н. Радиочастотные технологии локального позиционирования в здравоохранении // Известия вузов России. Радиоэлектроника. 2020. Т. 23. № 3. С. 62–79.

6. Коновалов Е. В. Обзор алгоритмов и систем определения координат объекта // Научный взгляд в будущее. 2016. Т. 4. № 4. С. 30–36.

7. ITU-R P.1238-10 Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 450 GHz. Geneva: ITU-R Recommendations, 2019. 28 p.

УДК 535.8
ГРНТИ 29.31.27

ОБЗОР ТЕХНОЛОГИИ ПРОСТРАНСТВЕННОЙ МОДУЛЯЦИИ СВЕТА

А. С. Дюбов, Б. К. Резников, Г. Ю. Самойлов

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

Несмотря на то, что пространственная модуляция стала частью нашей жизни в уже не близкой второй половине прошлого века, мы до сих пор ее используем. Более того, технологии, основанные на пространственной модуляции, если и имеют аналоги, то превосходят их по показателям. На сегодняшний день с пространственной модуляцией света мы пересекаемся каждый день – многие устройства, которыми мы имеем дело каждый день используют ее в качестве своей основы.

пространственные модуляторы, LCD, DMD, LCoS.

Для начала нужно вспомнить, что такое модуляция света. Модуляция света – изменение одного или нескольких параметров оптического сигнала: интенсивности, частоты, фазы, поляризации, направления, частоты распределения мод и т. д. в зависимости от управляющего сигнала. Модуляция света может быть прямой или внешней. В первом случае, необходимое оптическое излучение формируется посредством воздействия либо на накачку, либо на параметры оптического резонатора (оптическую длину, добротность или величину обратной связи) источника излучения, последнее также называется внутренней модуляцией. Во втором, происходит изменение оптического сигнала в модуляторе по закону управляющего сигнала (модулирующего сигнала).

Говоря о пространственной модуляции, можно выделить два способа ее достижения – формирования изображения на модуляторе света электрическим и оптическим способом. За это отвечают электрически адресованный пространственный модулятор (EASLM) и оптически адресованный пространственный модулятор (OASLM).

В этой статье речь пойдет об электрически адресованных модуляторах.

EASLM (*Electrically-addressed spatial light modulator*) похож на обычный электронный дисплей, за исключением размера – модулятор обычно имеет рабочую площадь около 2 см^2.

Примером EASLM является Микросхема DMD основанная на технологии цифрового микро зеркального устройства или DMD (рис. 1). Микросхема DMD состоит из нескольких сотен тысяч подобных микроскопических зеркал, расположенных в виде прямоугольной матрицы, которая соответствует пикселям отображаемого изображения.

Зеркала можно поворачивать по отдельности на ± 10–12 °. При повороте зеркала происходит включение или выключение пикселя – в включенном состоянии свет от лампы проектора отражается в линзу, делая пиксель на экране ярким, в выключенном состоянии свет направляется в другое место (обычно на радиатор), в результате чего пиксель кажется темным [1].

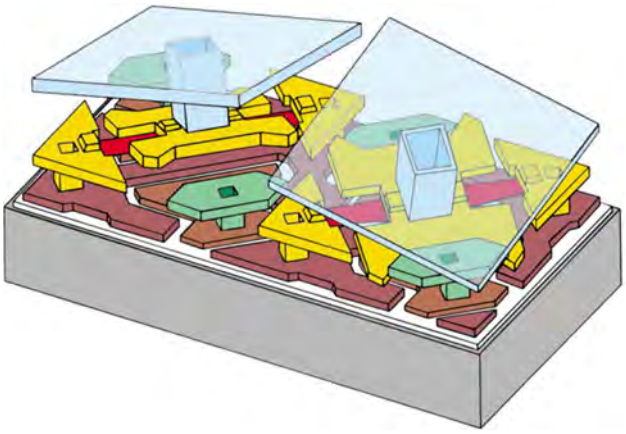


Рис. 1. Цифровое
микро зеркальное устройство

Эти микросхемы служат основой для технологии цифровой обработки света. Технология цифровой обработки или DLP (*Digital Light Processing*) использует микроскопические зеркала, которые позволяют включать и выключать соответствующий им пиксель. Различные оттенки серого достигаются быстрым включением и выключением пикселя.

Формировать цветное изображение на выходе позволяют две технологии – одночиповая и трехчиповая DLP. В проекторе с одним чипом DLP для создания цвета используется цветовой круг, расположенный перед между белой лампой и DLP чипом либо три разных источника с базовым набором цветов. В проекторе с тремя чипами DLP каждый из основных цветов, полученных разделением света лампы призмой, подается на свой DLP чип и рекомбинируется и подается на линзу [2].

Трехчиповые системы используются в проекторах для домашних кинотеатров более высокого класса, в проекторах для больших помещений

и в проекционных системах DLP Cinema, используемых в цифровых кинотеатрах.

Множество других пространственных модуляторов построены на основе жидких кристаллов. Жидкие кристаллы – это фазовое состояние, в которое переходят некоторые вещества при определённых условиях (температура, давление, концентрация в растворе). Жидкие кристаллы одновременно обладают текучестью жидкости и анизотропией кристаллов. На основе способности ЖК изменять ориентацию молекул под воздействием электрических полей была создана ЖК-ячейка, которая представляет собой две оптически прозрачные подложки, склеенные между собой с заданным зазором, заполненным жидким кристаллом (рис. 2). Благодаря выравнивающему слою, прилегающие к нему молекулы укладываются в заданном направлении. Таким образом, с помощью двух выравнивающих слоев задается исходное направление ЖК, что будет соответствовать исходной поляризации света, то есть интенсивности света. На электроды, нанесенной на поляризаторы пленке ITO, подается напряжение, что приводит к изменению направления ЖК. Из-за этого меняется интенсивность проходящего света, так как изменение направления ЖК изменяет направление поляризации света [3, 4].

Рис. 2. Устройство ЖК-ячейки

На ЖК-ячейках построены такие технологии, как ЖК-дисплей и LCD-проектор [2, 3]. Они представлены на рис. 3.

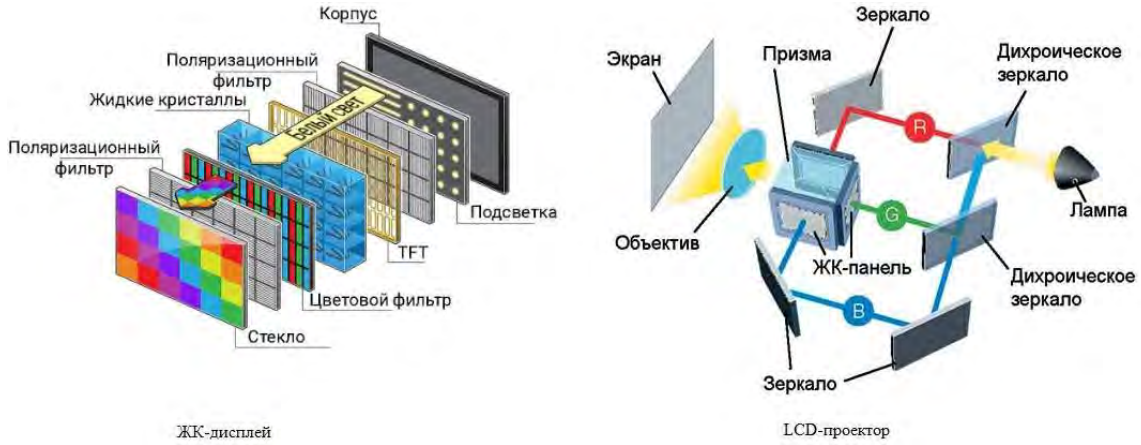


Рис. 3. Устройство ЖК-дисплея и LCD-проектора

Также, на основе жидких кристаллов построена ячейка LCoS (*Liquid Crystal on Silicon*). Она является некой комбинацией технологии DMD и

ЖК-ячейки, то есть ячейка LCoS отражает приходящее оптическое излучение, но в отличии от DMD управление интенсивностью осуществляется за счет жидких кристаллов [4].

Из рис. 4 видно устройство LCoS ячейки – на полупроводниковой подложке расположен отражающий слой, поверх которого находится жидкокристаллическая матрица и поляризатор. Под воздействием электрических сигналов жидкие кристаллы либо закрывают отражающую поверхность, либо открываются, позволяя свету от внешнего направленного источника отражаться от зеркальной подложки кристалла.

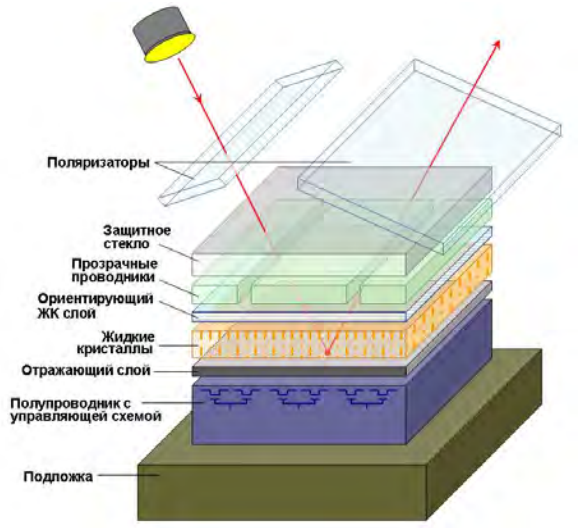


Рис. 4. Устройство LCoS-ячейки

Из этих ячеек, создаются LCoS чипы, которые используется в проекторах. Как и в LCD-проекторах, в LCoS-проекторах (рис. 5) сегодня используются в основном трехчиповые схемы на основе монохромных LCoS-матриц. Для формирования цветного изображения обычно используются три чипа LCoS, призма, дихроичные зеркала и светофильтры красного, синего и зелёного цветов. Помимо трехчипового существуют одночиповые решения, но одночиповые LCoS-проекторы не получили широкого распространения из-за ряда недостатков: перегрев матрицы, потери светового потока, сложное производство, невысокое качество цветопередачи.

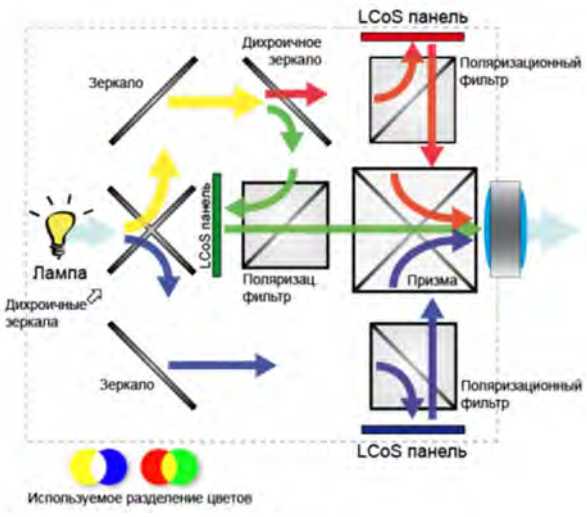


Рис. 5. Устройство LCoS-проектора

Список используемых источников

1. Larry J. Hornbeck. Multi-level digital micromirror device. Пат. US5083857A США; заявитель и патентообладатель Texas instrumental inc. – № US07/546,465; заявл. 29.06.1990; опубл. 28.01.98.

2. Evan Powell. The Great Technology War: LCD vs. DLP. URL: https://www.projectorcentral.com/lcd_dlp_update7.htm?page=Rainbow-Artifacts (дата обращения: 23.02.2021).

3. Мухин И. А. Современные плоскопараллельные отображающие устройства // BROADCASTING Телевидение и радиовещание. 2004. № 1 (37). С. 43–47.

4. Kristina M. Johnson, Douglas J. McKnight, Ian Underwood. Smart spatial light modulators using liquid crystals on silicon // IEEE journal of quantum electronics. 1993. Vol. 29. N. 2. pp. 699–714.

УДК 681.7
ГРНТИ 23.31

ЛАБОРАТОРНАЯ УСТАНОВКА ПО ИССЛЕДОВАНИЮ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ НА ОСНОВЕ РЕШЕТОК БРЭГГА

А. С. Дюбов, В. А. Хричков

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

Волоконно-оптические датчики на основе решеток Брэгга могут служить для измерения давления, деформации, температуры и других физических параметров. Для демонстрации и изучения работы измерительных систем и датчиков на основе волоконных брэгговских решеток разработана лабораторная установка. Для определения спектров отражения и пропускания волоконной брэгговской решетки в лабораторной установке используется перестраиваемый по длине волны узкополосный лазер. Реализованы конструкции датчиков давления, температуры и деформации.

волоконная брэгговская решетка, волоконно-оптический датчик, измерение температуры, измерение деформации, волоконно-оптическая измерительная система, лабораторная установка.

Современные волоконно-оптические датчики позволяют измерять всевозможные физические характеристики, например, температуру, давление, деформацию, расстояние и положение в пространстве, ускорение, магнитное поле, электрический ток, уровень жидкости, концентрацию газов и т. д. Во многих сферах применения волоконно-оптические датчики обладают рядом преимуществ по сравнению с их электрическими аналогами. Изучение и разработка оптических измерительных систем является важной и актуальной задачей [1, 2].

Разработанная лабораторная установка представляет собой законченное решение для проведения лабораторных и исследовательских работ по изучению измерительных систем и волоконно-оптических датчиков физических параметров таких как: температура, давление, изгибные деформации. В состав оборудования установки входят: волоконно-оптические датчики на основе решеток Брэгга, измерительный блок и персональный компьютер с программным обеспечением.

Волоконная брэгговская решетка (ВБР) представляет собой участок оптического волокна, у которого показатель преломления сердцевины периодически изменяется в продольном направлении. При прохождении оптического излучения по брэгговской решетке происходит его частичное отражение в определенном спектральном диапазоне. Спектральный диапазон отражения и пропускания ВБР зависит от периода изменения показателя преломления сердцевины. Механические воздействия на ВБР приводят к ее растягиванию или сжатию и изменению периода решетки, и соответственно, изменяется спектр пропускания и отражения.

Работа лабораторной установки (как и многих измерительных систем с волоконно-оптическими датчиками на основе решеток Брэгга) основана на регистрации спектров пропускания и отражения ВБР. Волоконно-оптический датчик на основе решетки Брэгга представляет собой механическую систему с закрепленной волоконной брэгговской решеткой. Механическая система преобразует изменение физических параметров (температуры, давления, механических напряжений) в удлинения или сжатия волоконной бреэгговской решетки.

Измерительный блок содержит источник оптического излучения и два фотоприемных измерительных модуля для регистрации отраженного и проходящего через ВБР излучения. Структурно-функциональная схема лабораторной установки приведена на рис. 1.

В качестве источника сигнала для лабораторной установки выбран узкополосный лазер с перестраиваемой длиной волны. Схема управления измерительного блока имеет возможность точно устанавливать и поддерживать значения длины волны изучения источника. Схема управления обрабатывает измеренные значения оптических сигналов, отображает режим работы и показания на двухстрочном символьном ЖК экране. Измерительный блок регистрирует и передает в компьютер данные о центральной длине волны отражения ВБР, размещенной в датчике. Персональный компьютер с программным обеспечением служит для удобства сбора, отображения и хранения результатов измерительных экспериментов.

Сигнал источника с выхода измерительного блока поступает на датчик (волоконную брэгговскую решетку). Решетка Брэгга отражает оптический сигнал в узком диапазоне длин волн. Отраженный сигнал поступает обратно на выход измерительного блока. Оптический циркулятор разделяет сигнал источника и отраженный от брэгговской решетки. Отраженный сигнал поступает на первый фотодиод измерителя. При несовпадении длины волны источника и спектра отражения решетки большая часть сигнала поступает на вход измерительного блока. Второй фотодиод измерителя регистрирует уровень сигнала, прошедшего через датчик. Последовательно перестраивая узкополосный источник по длине волны, выполняется сканирование.

Настраивая длину волны лазерного источника на максимальное отражение можно отслеживать сжатия или растяжения брэгговской решетки.

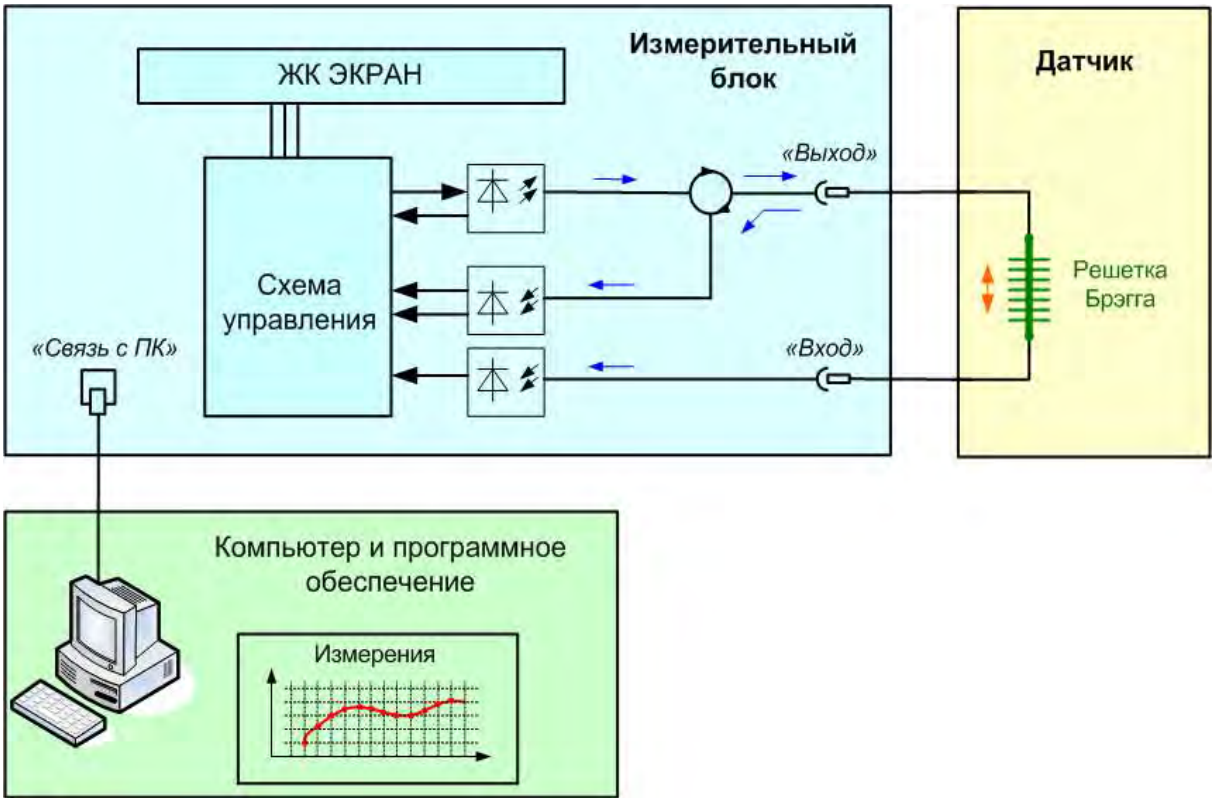


Рис. 1. Схема лабораторной установки

На рис. 2 приведена трехмерная модель печатной платы с расположенными на ней электронными компонентами измерительного блока.

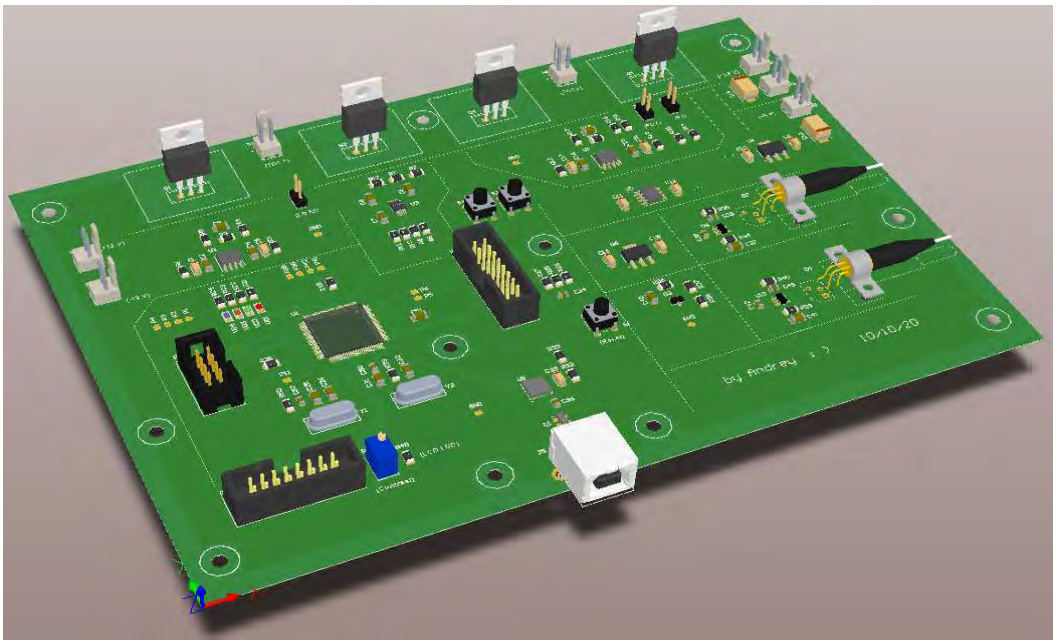


Рис. 2. Модель печатной платы блока управления

На печатной плате размешен микроконтроллер управления, два измерительных фотодиода, элементы цепей питания и управления перестраиваемым лазерным источником, разъемы для подключения клавиатуры, экрана и связи с компьютером по интерфейсу USB. Управление лабораторной установкой осуществляется программой микроконтроллера, реализующей алгоритмы измерения токов фотодиодов и управления длиной волны лазера.

В качестве примеров волоконно-оптических датчиков на рис. 3 и 4 приведены датчики температуры и деформации.

Волоконно-оптический датчик температуры лабораторной установки построен на эффекте температурного расширения алюминиевой пластины. Конструкция датчика представляет собой две алюминиевые пластины между которыми закреплена волоконная решетка Брэгга (рис. 3). Одна из пластин подвергается нагреву и охлаждению. В лабораторной установке изменение температуры осуществляется при помощи термоэлектрического элемента Пельтье. Элемент Пельтье – это термоэлектрический преобразователь, управляемый током. Управляя величиной и направлением тока элемента Пельтье можно охлаждать или нагревать алюминиевую пластину. Например, при охлаждении пластины происходит ее сжатие, а закрепленная на ней одним концом брэгговская решетка растягивается. Таким образом изменение температуры преобразуется в регистрируемое смещение спектра отражения и пропускания брэгговской решетки.

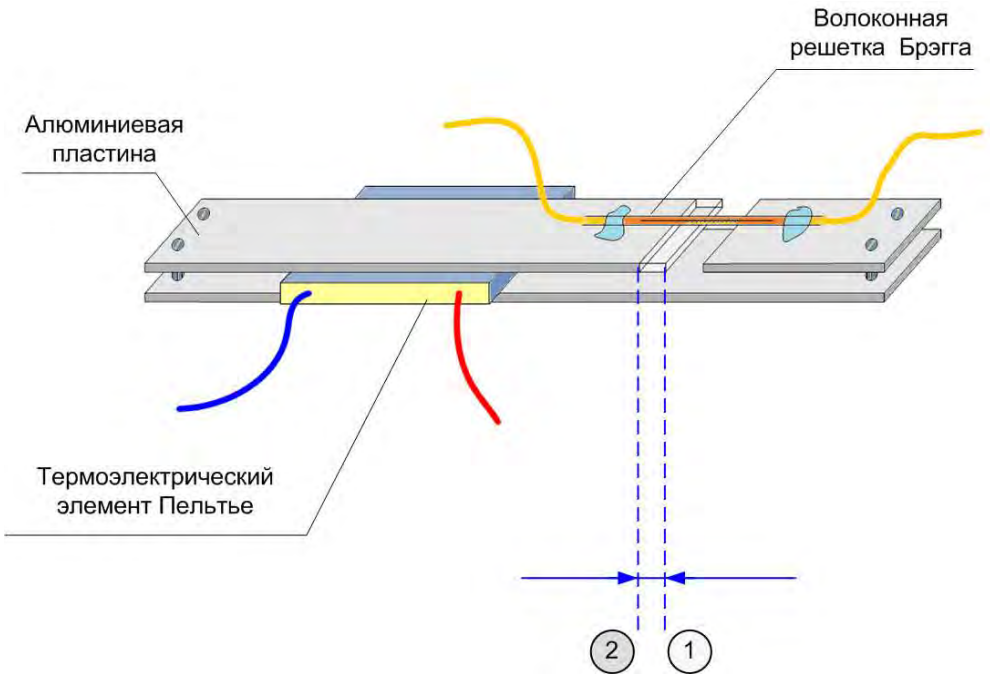


Рис. 3. Волоконно-оптический датчик температуры

Датчик деформации (рис. 4) лабораторной установки представляет собой двухслойный элемент – «балку с защемленным концом». Первый (ниж-

ний) слой – это тонкая стальная полоса обеспечивающая упругость и минимальные продольные сжатия и удлинения. Второй верхний слой – толстая полоса плотной резины. На поверхности второго слоя закреплена волоконная брэгговская решетка. При поперечном изгибе происходит значительное растяжение или сжатие второго (верхнего) слоя и, соответственно, брегговской решетки. Таким образом изгибная деформация преобразуется в регистрируемое смещение спектра отражения и пропускания брэгговской решетки.

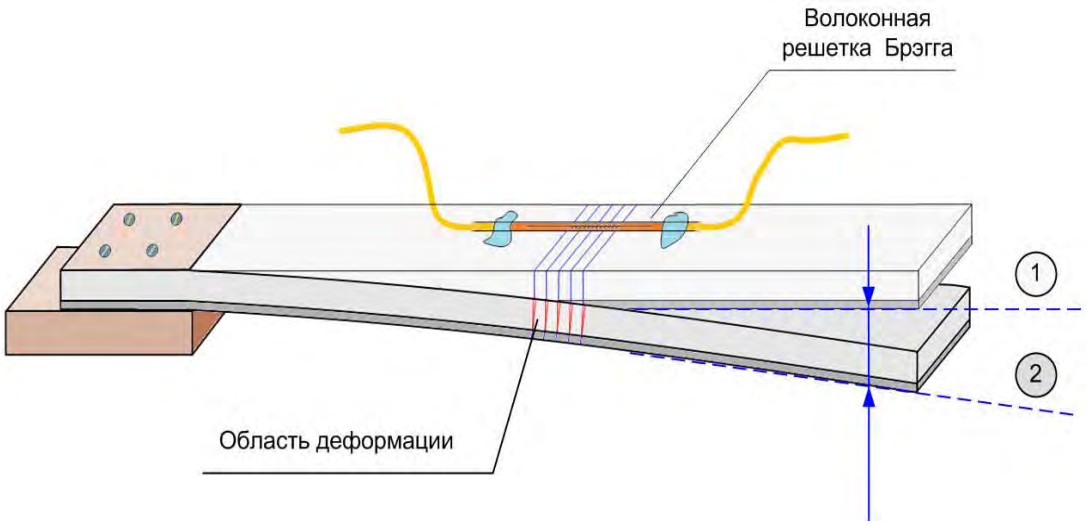


Рис. 4. Волоконно-оптический датчик деформации

Лабораторные работы затрагивают теоретические вопросы работы датчиков на основе ВБР. Помимо возможностей наглядной демонстрации, лабораторные работы могут включать исследовательские задания.

Список используемых источников

1. Отокси Т., Окамото К., Оцу М., Нисихара Х., Кюма К., Хататэ К. Волоконно-оптические датчики / под ред. Т. Окоси. Перевод с япон. Г. Н. Горбунова. Ленинград. : Энергоатомиздат. Ленинградское отделение, 1991. 256 с.

2. Волоконно-оптические датчики. Вводный курс для инженеров и научных работников / под. ред. Э. Удда. М.: Техносфера, 2008. 520 с.

ГРНТИ 49.33.29
УДК 004.77

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ БЛОКЧЕЙН-ПЛАТФОРМЫ TON ДЛЯ ПКС

В. С. Елагин, Е. Е. Ермолаев, А. В. Помогалова, И. О. Федотов

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

Современные ПКС и их контроллеры предлагают гибкий выбор для конфигурации сети, управления и настройки правил конфигурации. SDN – это новая, простая в управлении, гибкая и экономически эффективная сетевая архитектура, обеспечивающая высокую пропускную способность и динамичность, что принципиально важно для современных приложений.

Целью данной работы является создание тестового стенда с элементом сети blockchain TON и её пробный запуск в программно-конфигурируемой сети с программным контроллером. Все программные системы распространяются по лицензии открытого программного обеспечения.

Результатом работы является имитационная инфокоммуникационная система, построенная на технологиях: Telegram Open Network и Open Network Operating System в качестве контроллера ПКС. Имитация нод кластера SDN будут является симулированные хосты, созданные с помощью mininet.

блокчейн, программно-конфигурируемые сети, ONOS, Telegram Open Network, моделирование, симуляция сетей.

Сейчас мы поговорим про отдельные составляющие системы:

В качестве программного коммутатора выступает Open-switch – технология, которая была внедрена в ядро Linux в версии 2.6.2. Обеспечивает абстракцию аппаратных устройств платформ сетевых коммутаторов в среде ОС Linux. Он использует стандартное программное обеспечение с открытым исходным кодом. Работа на уровне ядра, поддержка существующих возможностей Linux по работе в качестве моста и что самое важное - поддерживает Openflow [4] для управления логикой коммутации.

ONOS (*Open Network Operation System*) [1] или, по-другому, открытая сетевая операционная система. Это многоуровневый программный комплекс, выстроенный в собственную ОС, в основе которого лежит контроллер ПКС. Разрабатывается сообществом открытого программного обеспечения и поддерживается Linux Foundation. Содержит в себе структуру, позволяющую использовать его в суровых эксплуатационных условиях. Например, ONOS содержится в составе популярного комплекса программ для провайдеров виртуализации и больших отказоустойчивых ЦОД OpenStack [3].

TON (*Telegram Open Network*) [2]: Открытая сеть телеграм. Можно подумать о TON как об огромном распределенном суперкомпьютере или, скорее, как об огромном «суперсервере», предназначенном для размещения и предоставления разнообразных услуг. Позиционируется, не просто как блокчейн платформа, а как целая огромная система, предназначенная для сайтов p2p, собственных доменных серверов, распределенных приложений и хранилищ, и обмена валютой (Gram).

В качестве сетевого эмулятора, который создаёт сеть виртуальных конечных хостов, коммутаторов, контроллеров и ссылок будет использоваться mininet [5]. Он позволяет создавать требуемую топологию сети, провести комплексное тестирование топологии, без необходимости подключения физической сети, так же удобен для дальнейших исследований в данной области из-за встроенного API, работающего с языком программирования Python, которой позволяет создавать сложные топологии сети и их конфигурацию из небольшого скрипта.

Рис. 1. Топология сети

Отметим основные пункты создания стенда:

Характеристики сервера:

- OS: Ubuntu 18.04,
- CPU: AMD Threadripper 1920X,
- RAM: 64 Гб DDR3.

Выбрана минимально необходимая топология для работы системы (рис. 1).

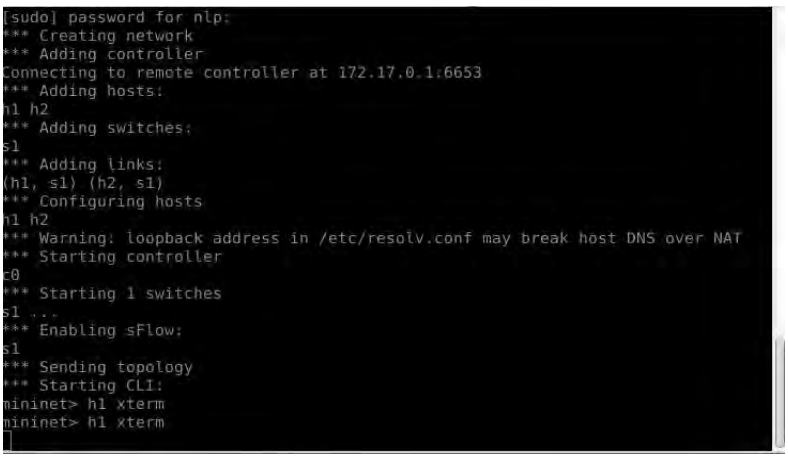


Рис. 2. Создание виртуальных хостов

Топология сделана с NAT функцией, для доступа к внешней сети Ethernet, для подключения к тестовой сети TON, с помощью конфигурации легковесного клиента (рис. 2).

Ton Blockchain был скомпилирован с функциональностью легкого клиента (рис. 3, 4).

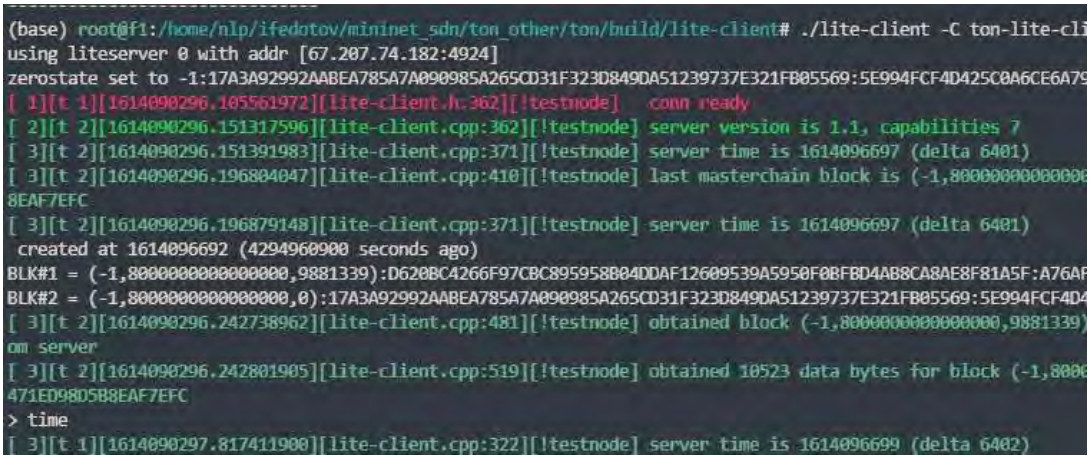


Рис. 3. Успешное соединение клиента с тестовой сетью

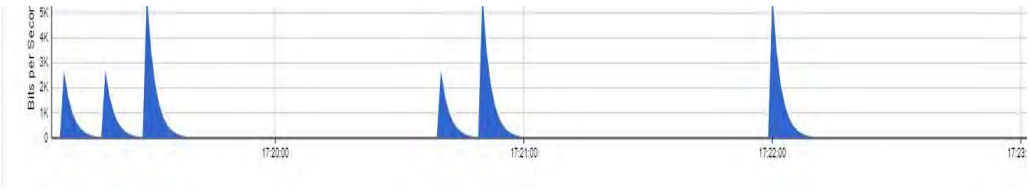


Рис. 4. Исходящий трафик в графическом интерфейсе ONOS

При сборке из исходников TON было встречено немало проблем, но, к счастью, он ещё поддерживается сторонними разработчиками в добровольном порядке и многие несостыковки были решены.

Таким образом был получен тестовый стенд, который предполагался в начале работы. Было произведено тестовое подключение к blockchain сети.

В дальнейшем планируется расширить систему, протестировать производительность при масштабировании и использовании на физическом оборудовании [6]. Так же будет проверена возможность расширения blockchain системы до полной, включающий в себя распределенные хранилища, p2p сайты, для независимого тестирования внутри симуляционной сети. Также планируется использовать данную структуру данных для построения стендов для обучения.

Список используемых источников

1. Open Network Operating System (ONOS) Wiki. URL: https://wiki.onosproject.org/
2. Telegram Open Network. Dr. Nikolai Durov. March 2, 2019

3. ONOS – A new carrier-grade SDN network operating system designed for high availability, performance, scale-out. URL: https://onosproject.org/

4. Braun W., Menth M. Software-defined networking using OpenFlow: Protocols, applications and architectural design choices // Future Internet. 2014. Vol. 6. No. 2. pp. 302–336.

5. Mininet – Instant Virtual Network Wiki. URL: https://github.com/mininet/mininet/wiki/_pages

6. Koponen T., Casado M., Gude M. Onix: A Distributed Control Platform for Large-scale Production Networks. URL: http://yuba.stanford.edu/~casado/onix-osdi.pdf.

УДК 004
ГРНТИ 49.33.35

СОЗДАНИЕ ДЕЦЕНТРАЛИЗОВАННОЙ ТОРГОВОЙ ПЛАТФОРМЫ С ПРИМЕНЕНИЕМ ЭСКРОУ СМАРТ-КОНТРАКТА НА БАЗЕ ПЛАТФОРМЫ ETHEREUM. ЧАСТЬ 1

В. С. Елагин, Н. А. Мурашкин, П. А. Огорельцев, А. В. Помогалова

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

Работа посвящена разработке децентрализованного решения для проведения процедур купли-продажи товаров на основе эскроу смарт-контракта. Актуальность работы обоснована вопросами безопасности удаленного проведения платежей при проведении транзакций. В рамках данной работы предлагается децентрализованное решение, разработанное на базе блокчейн-платформы Ethereum, целью которого является решение вопросов безопасности осуществления дистанционных транзакций и гарантии доставки товаров. В работе рассматриваются особенности создания платформы безопасной оплаты с использованием эскроу смарт-контракта на платформе Ethereum. Приведены особенности построения структуры платформы, проведен анализ потенциальной проблематики платформы и ее функционирования, а также анализ обоснованности использования децентрализованных технологий и смарт-контрактов при решении задач схожей направленности.

блокчейн, Ethereum, смарт-контракт, децентрализованные приложения.

Технология «Блокчейн» – это совместно используемый распределенный реестр, состоящий из цепи блоков. Информация в реестре представляется в виде транзакций, записываемых в блоки, которые затем публикуются в общую сеть. Используемый актив (информация) может быть представлена как сведения о материальных вещах, так и сведения о нематериальных вещах, например, интеллектуальная собственность, патенты, авторские права.

По этой причине данная технология может быть применима к разным областям деятельности. В рамках данной работы сферой к применению данной технологии является торговля. Контролировать процесс поставок, а также проводить саму процедуру продажи с помощью блокчейна можно относительно всего, что имеет какую-либо ценность. Данная технология снижает риски и расходы для всех задействованных сторон. Каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока, а любое изменение хеш-суммы будет строго зафиксировано в последовательности блоков [1].

Децентрализованное приложение – это приложение, которое работает в распределительной вычислительной системе. Такие приложения обладают основными преимуществами блокчейна: прозрачность, надежность и неизменность данных. Подобные приложения позволяют избавиться от посредников (третьей стороны), позволяя взаимодействовать клиенту с поставщиком напрямую [2].

Для корректной работы распределенной вычислительной среды, где все устройства являются равноправными участниками ключевой проблемой являлся алгоритм принятия решения. Для разрешения данного вопроса были разработаны алгоритмы консенсуса – алгоритмы, которые позволяют в равноправной недоверенной среде принять общее одинаковое решение. К таким алгоритмам относятся:

Proof of work – алгоритм защиты распределенных систем от злоупотреблений, принцип работы которого сводится к двум основным пунктам: необходимости выполнения определенной достаточно сложной и длительной задачи и возможности быстрой и легкой проверки результата [3].

Proof of stake – альтернативный алгоритм консенсуса, идея которого состоит в использовании «доли» в качестве ресурса, который определяет, какая именно нода получает право добычи следующего блока. Сложность в данном случае распределяется пропорционально в соответствии с балансом данного узла, то есть большим шансом сгенерировать следующий блок обладает узел с большим балансом.

Можно сказать, что основным недостатком технологии блокчейн и децентрализованных приложений является сложность масштабируемости. С данной проблемой обычно сталкиваются платформы с алгоритмом консенсуса proof-of-work, к примеру, Ethereum, поэтому одним из простейших решений по минимизации данной проблемы является использование платформы, с алгоритмом proof-of-stake или delegated proof-of-stake, например, Cardano, EOS, Lisk [4]. Также решением может являться имплементация шардинга на уровне транзакций. Они разбиваются на отдельные части, которые отправляются в разные узлы и обрабатываются ими. В теории это позволит криптовалюте ускорить процесс обработки транзакции, но на практике применить его достаточно сложно [5].

Сложности реализации блокчейн-шардинга:

1. Не существует механизма, отслеживающего какой узел обрабатывают какую транзакцию. При этом нужен безопасный и эффективный механизм, который будет также работать и в блокчейн сети.

2. Не разработан алгоритм доверия между узлами. В блокчейне узлы должны приходить к независимому консенсусу, также нужно подтверждение того, что обе ноды закончили процесс обработки.

3. Эффективно применять шардинг можно в блокчейнах с алгоритмом proof-of-stake, а сейчас с проблемой масштабирования сталкиваются в основном криптовалюты с алгоритмом proof-of-work.

Существует множество различных платформ для разработки децентрализованных приложений. Некоторые из них – Ethereum, Cardano, EOS, Lisk, QTUM.

Кратко опишем каждую из платформ:

− Ethereum использует алгоритм консенсуса proof of work, что делает его довольно медленным, его скорость составляет всего 15 транзакций в секунду. Разработка смарт-контрактов может осуществляться на одном из языков программирования, которые спроектированы для трансляции в байт-код виртуальной машины Ethereum – Solidity, Vyper, Serpent, LLL, Mutan [2].

− Cardano использует протокол proof of stake, а его скорость составляет около 1000 транзакций в секунду. Блокчейн поддерживает язык Haskell. Из отличительных особенностей можно выделить интероперабельность [6].

− EOS основан на протоколе Delegated proof of stake, его работа отличается от обычного proof of stake. DPoS делает распределение монет и влияние в сети более равномерным и обеспечивает большую степень децентрализации. EOS может обрабатывать около 50 000 транзакций в секунду, а разработка осуществляется на C или C++. Данная платформа обладает высокой масштабируемостью и скоростью транзакций, но довольно сложна для использования [7].

− Lisk также основан на протоколе DPoS, обладает скоростью 10 000 операций в секунду, а разработка контрактов осуществляется на языке JavaScript. Из особенностей можно выделить, что приложения, созданные на основе Lisk, не будут существовать на главном блокчейне, а будут иметь свой собственный боковой блокчейн, который будут поддерживать сами пользователи. А главным преимуществом является удобство разработки [8].

− QTUM основан на алгоритме консенсуса proof of stake и обладает скоростью 50-100 операций в секунду. При этом в закрытой версии блокчейна Unita была достигнута скорость в 10 000 транзакций. Разработка контрактов в QTUM может осуществляться на языках программирования Solidity, C, C++, Rust, Python. Из особенностей стоит отметить, что QTUM основан на объединении кодов Bitcoin и Ethereum, что делает миграцию контрактов с Ethereum на QTUM очень доступной [9].

Из сравнения выше видно, что каждая из вышеперечисленных платформ имеет определенные преимущества над другими: EOS – обладает высокой масштабируемостью и скоростью транзакций, Lisk – удобством разработки, Cardano – интероперабельностью, а Ethereum высокой доступностью и популярностью, где QTUM является его немного улучшенной версией, из-за использования алгоритма PoS.

Но в качестве основы для разрабатываемого в рамках работы приложения авторы работы выбрали платформу Ethereum из-за наличия полной официальной документации и ее доступности. Язык программирования умных контрактов Solidity более сбалансирован и разработан с целью минимизации ошибок в логике программного кода, которые могут возникнуть при использовании других языков программирования. Для данного этапа развития проекта не требуется высокая масштабируемость. В случае продолжения развития проекта авторами работы будут использованы более подходящие платформы с точки зрения масштабируемости.

Разработка приложений на платформе Ethereum преимущественно осуществляется с помощью написания смарт-контрактов – самоисполняемых компьютерных алгоритмов, представленных в виде программного кода в блокчейн-сети, которые не требуют дополнительной активации после установки в сеть. Они предназначены для контроля и предоставления информации о владении чем-либо и описываются преимущественно на языке программирования Solidity [9].

Главными целями данного проекта является обеспечение сохранности средств покупателя во время доставки товара, с предусмотрением базовых функций по возврату средств в различных ситуациях, а также формирование системы с отсутствием посредников, хранящих средства клиента. Вместо классических посредников в системе выступает умный контракт.

После оплаты товара, средства поступают на контракт и хранятся там под уникальным идентификатором заказа, а продавец получает оповещение о том, что оплата прошла успешно (рис.). Далее, продавец передает товар службе доставки, которая изменяет статус заказа на соответствующий. Средства переходят продавцу только после подтверждения об успешной доставке от клиента или службы доставки (рис.).

Функциональные возможности клиента и продавца, а также особенности реализации приведены во второй части работы авторов.

Рис. Краткая схема взаимодействия со смарт контрактом обеих сторон

Основной проблемой, с которой столкнулись авторы работы – нестабильность криптовалюты, что является существенным риском и может повлечь осложнения функционирования платформы. Решением данной проблемы может являться, так называемый, «стейблкоин» или дополнительный «оракул» контракт, где

− Стейблкоин – псевдостабильная криптовалюта, стоимость которого привязана к устойчивому активу. Курс стейблкоина может колебаться к базовому активу, чаще всего незначительно.

− «Оракул» контракт является поставщиком информации, который по запросу основного контракта предоставляет из оффчейн мира достоверные данные, необходимые для корректной работы контракта.

«Оракул» контракт может позволить обновлять значение курса в режиме реального времени, что значительно упростит перерасчет стоимости товара при случае резких перепадов, что позволяет минимизировать данную проблему. При этом клиент получит только те средства, которые он изначально отправил в контракт, что исключает возможность отсутствия средств для возврата клиентам.

Стейблкоин позволяет решить эту проблему полностью, делая приложение централизованным и зависящим от курса валют, что противоречит децентрализованной природе криптовалют, понижая доверие.

В данной части работы были выделены положительные и отрицательные аспекты технологии блокчейн и смарт-контрактов, рассмотрены различные децентрализованные платформы для написания смарт-контрактов, а также была определена схема взаимодействия пользователей с контрактом.

Список используемых источников

1. Marco Iansiti, Karim R.Lakhani. The Truth About Blockchain. 2017. URL: https://hbr.org/2017/01/the-truth-about-blockchain

2. Ethereum Development Documentation. URL: https://ethereum.org/en/developers/docs/

3. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf

4. Max Wright. Delegated Proof of stake (DPoS) vs Proof of Work (PoW). 2015. URL: http://bytemaster.github.io/bitshares/2015/01/04/Delegated-Proof-of-Stake-vs-Proof-of-Work/

5. Alexander Skidanov. The authoritative guide to Blockchain Sharding. 2018. URL: https://medium.com/nearprotocol/the-authoritative-guide-to-blockchain-sharding-part-1-1b53ed31e060

6. Cardano Documentation. URL: https://docs.cardano.org/en/latest/

7. What is EOSIO. URL: https://developers.eos.io/welcome/latest/index

8. Aaron Mangal, Ryan Smith. What is Lisk? 2018. URL: https://coincentral.com/what-is-lisk/

9. Patrick Dai, Neil Mahi, Jordan Earls, Alex Norta. Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform. URL: https://qtum.org/user/pages/01.home/Qtum%20whitepaper_en%20v0.7.pdf

УДК 004
ГРНТИ 49.33.35

СОЗДАНИЕ ДЕЦЕНТРАЛИЗОВАННОЙ ТОРГОВОЙ ПЛАТФОРМЫ С ПРИМЕНЕНИЕМ ЭСКРОУ СМАРТ-КОНТРАКТА НА БАЗЕ ПЛАТФОРМЫ ETHEREUM. ЧАСТЬ 2

В. С. Елагин, В. Н. Бакатов, А. А. Громов, А. В. Помогалова

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

Работа посвящена разработке децентрализованного решения для проведения процедур купли-продажи товаров на основе эскроу смарт-контракта. Актуальность работы обоснована вопросами безопасности удаленного проведения платежей при проведении транзакций. В рамках данной работы предлагается децентрализованное решение, разработанное на базе блокчейн-платформы Ethereum, целью которого является решение вопросов безопасности осуществления дистанционных транзакций и гарантии доставки товаров. В представляемой части работы рассматриваются особенности реализации платформы безопасной оплаты с использованием эскроу смарт-контракта на платформе Ethereum. В качестве примера разработан интернет-магазин, в рамках которого смарт-контракт является посредником, выполняя функции хранения средств покупателя до наступления оговоренных условий, то есть, получения купленного товара. В работе приведены особенности разработки смарт-контракта, а также реализации связи между смарт-контрактом и front-end частью сайта.

блокчейн, Ethereum, смарт-контракт, децентрализованные приложения.

В настоящее время все больше покупок совершается дистанционной с использованием сети Интернет. Многие покупатели легкомысленно относятся к безопасности данных покупок. Из-за этого происходит множество злоумышленных действий со стороны продавцов. Также происходят ситуации, где злоумышленником является покупатель. Отсутствие должной безопасности торговых Интернет-площадок порождают чувство безнаказанности, что провоцирует у покупателей попытки обмануть продавца. Разрабатываемое в данном проекта децентрализованное приложение является одним из методов снижения вероятности обмана при покупке/продаже товара. Благодаря использованию технологии блокчейн, транзакции полностью защищены от перезаписи, внесения изменений или удаления. Смарт-контракт же выступает в качестве защищенного посредника (третьего незаинтересованного лица), что позволит пресечь кражу денежных средств. Использование смарт-контракта позволяет практически избавиться от посредника в известном смысле, так как чаще всего злонамеренные действия совершаются из-за посредников-злоумышленников. Когда речь идет о программном коде, который не поддается более никаким изменения после установки в блокчейн-сеть, то доверие к системе не может быть снижено, так как посредник абсолютно гарантированно не может принять ничью сторону и будет действовать строго по описанным в программном коде правилам.

Разработка децентрализованного приложения (DApp) является непростой задачей. Это связано с тем, что помимо разработки обычного web-приложения, нужно также разработать смарт-контракт и связать его с приложением.

Смарт-контракт данного проекта написан на контрактно-ориентированном языке программирования Solidity. Данный язык имеет полную официальную документацию. Но из-за узкой специализации языка и динамичного развития данной сферы разработка смарт-контрактов и их защита от потенциальных атак все же вызывают затруднения.

В первой части работы авторами проекта было проведено исследование различных существующих децентрализованных фреймворков. Для данного этапа разработки авторами работы была выбрана блокчейн-платформа Ethereum. Также была определена логика взаимодействия клиента и продавца в рамках платформы и изучены узкие места данной разработки.

После определения логики взаимодействия со смарт-контрактом было необходимо определить функциональные возможности клиента и продавца в рамках разрабатываемой платформы. Так, у клиента было выделено несколько возможностей взаимодействия со смарт-контрактом (рис. 1): оплата товара, отмена заказа, пока он имеет статус сборки, возврат средств, если товар не пришёл за определенное время и проверка статуса заказа, которая не требует оплаты комиссии.

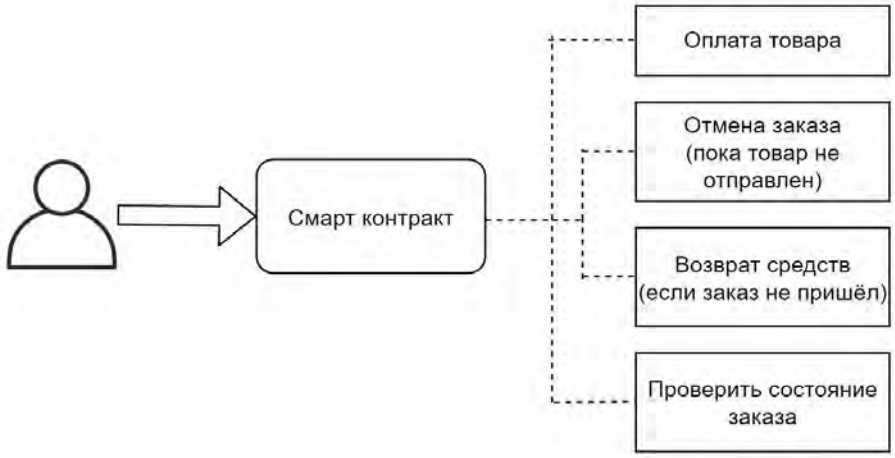


Рис. 1. Взаимодействие с контрактом со стороны клиента

Продавец, в свою очередь, должен иметь возможность обновлять статус доставки, отменять заказ, проверять состояние заказа (рис. 2). С помощью функции отмены заказа со стороны продавца, появляется возможность решения непредвиденных ситуаций. Безусловно, данный набор функций в дальнейшем может быть увеличен, так как на данный момент времени описанный функционал покрывает минимальные требования к корректной работе платформы.

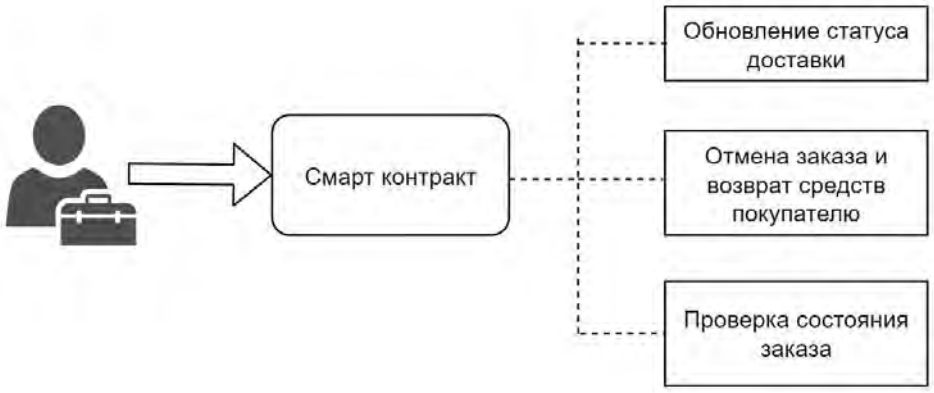


Рис. 2. Взаимодействие с контрактом со стороны продавца

Аутентификация пользователя

Помимо выделения необходимого функционала клиента и продавца необходимо также рассмотреть другие функции системы, которые необходимы для обеспечения в первую очередь безопасности системы. К таким функциям относится аутентификация продавца и пользователя. В случае платформы с применением технологии блокчейн для аутентификации необходимо использовать данные электронных кошельков и программные решения по работе с ними. Так, пользователю для корректной работы на сайте необходимо расширение для браузера MetaMask.

MetaMask [1] – это кошелек Ethereum с открытым исходным кодом, который поддерживает все виды токенов на основе Ethereum (например, токенов, соответствующих стандарту ERC-20 [2], и невзаимозаменяемых токенов, также известных как NFT [3]). Кроме того, появляется возможность покупать/обменивать их с другими пользователями сети с помощью встроенной интеграции с Coinbase и ShapeShift.

Регистрация и авторизация происходит с помощью этого расширения. Это позволяет разрабатываемой платформе автоматически получить публичный адрес криптовалютного кошелька покупателя, и при оформлении заказа появится окно с требуемой транзакцией на адрес смарт-контракта, что не требует от пользователя никаких посторонних действий и обеспечивает комфорт при работе с платформой.

Смарт-контракт хранит в себе структуру с адресом криптовалютного кошелька покупателя, то есть для смарт-контракта покупатель обезличен. Также смарт-контракт хранит информацию о сумме покупки, состоянии и времени заказа, для возможной отмены заказы со стороны покупателя или продавца.

Хранение заказов

Все заказы в обязательном порядке должны сохранятся в неизменяемом хранилище. При оформлении заказа происходит транзакция от покупателя, так смарт-контракт получает все необходимые данные для хранимой структуры. В структуре содержит адрес кошелька покупателя, сумму покупки, состояние заказа, а также время создания заказа.

Для экономии места и времени обработки запроса используются маппинги вместо массива. Маппинг [4] можно представить, как хэш-таблицу, которая инициализируются таким образом, что все возможные ключи существуют и сопоставляются со значениями, байтовое представление которых – нули (значение по умолчанию). В смарт-контракте предусмотрено два маппинга:

1. Для адресов покупателей:

Присваивается идентификатор, с помощью которого web-приложение может отслеживать все заказы одного покупателя;

2. Для заказов:

Присваивается идентификатор, с помощью которого web-приложение может отслеживать определенный заказ.

Взаимодействие смарт-контракта и web-приложения

Как описывалось ранее, наиболее трудоемким является процесс отладки взаимодействия между смарт-контрактом и итоговым веб-приложением (платформой). В нашем случае взаимодействие со смарт-контрактом

происходит с помощью библиотеки для javascript web3.js[5] на стороне клиента:

- Скрипт обращается к смарт-контракту, передавая в качестве аргумента адрес криптовалютного кошелька покупателя и получает все идентификаторы заказов, которые хранятся в структуре с этим адресом.
- После происходит повторное обращение к смарт-контракту и передается в качестве аргумента каждый из уникальных номеров заказа, и возвращается подробная информация о заказе, а также согласно шаблону в разметке сайта, добавляется отображения заказа для покупателя.

Возможности DApp

В результате разработки платформа реализует необходимый спектр функций. Так, функционал для пользователя включает в себя заказ продукта на сайте, отслеживание статуса заказа, отмену заказа в случае длительной доставки, отмена заказа по другим причинам. Со стороны продавца реализованы следующие функции: добавление различных товаров, изменение статуса заказа (ожидает оплаты, оплачен, отправлен в сборку, отправлен в службу доставки, доставлено, отменен). Веб-интерфейс приложения представлен на рис. 3.

В ходе разработки проекта были выделены определенные сложности, в частности, недостаточная гибкость при работе с библиотекой web3.js, которая может быть заменена на библиотеку wb3.py [6] и дальнейшее взаимодействие смарт-контракта с web-приложением будет происходить серверную часть приложения. Это также поможет ускорить отрисовку клиентской части. В дальнейшем авторы работы рассматривают возможность перехода на другой блокчейн-фреймворк с улучшенными показателями масштабирования.

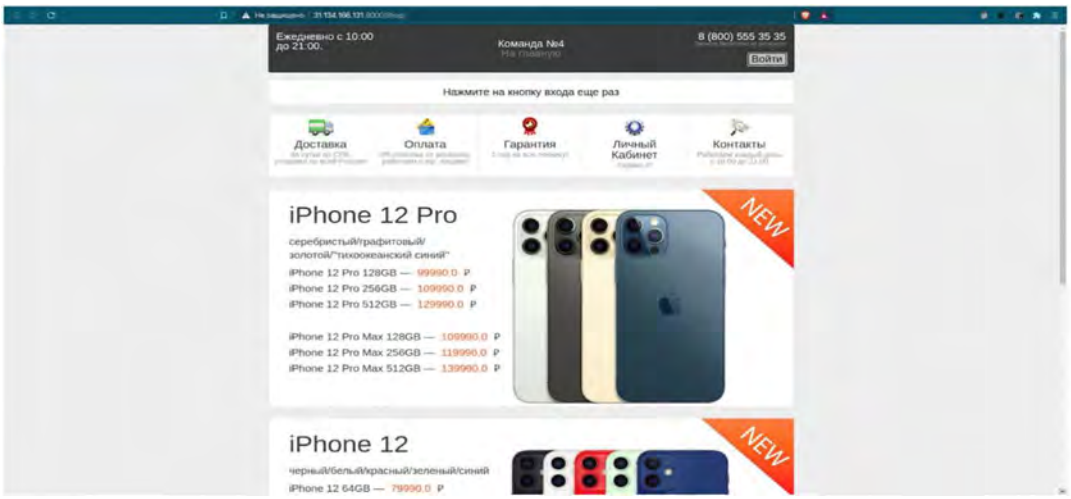


Рис. 3. Главная страница приложения

Список используемых источников

1. How to use Metamsk. 2021. URL: https://academy.binance.com/ru/articles/how-to-use-metamask
2. ERC-20 standart. 2020. URL: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
3. NFT token standart. 2021. URL:https://ethereum.org/ru/nft/
4. Mapping documentation. 2021. URL: https://docs.soliditylang.org/en/v0.8.3/types.html#mapping-types
5. Web3.js documentation. 2021. URL: https://web3js.readthedocs.io/en/v1.3.4/
6. Web3.py documentation. 2021. URL: https://web3py.readthedocs.io/en/stable/

УДК 004.77, 519.21
ГРНТИ 49.37.29, 49.03.09, 27.35.33

ФУНДАМЕНТАЛЬНЫЕ ОСНОВЫ МОДЕЛИРОВАНИЯ ТРАФИКА В ГЕТЕРОГЕННЫХ СЕТЯХ СВЯЗИ, С ПЕРСПЕКТИВОЙ КАНАЛЬНОЙ ИНДЕТИФИКАЦИИ ОТДЕЛЬНЫХ СЕРВИСОВ И ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ СЕТИ

В. С. Елагин, А. В. Спиркина, В. В. Фицов

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

Современные гетерогенные сети связи по сравнению с сетями коммутации каналов недостаточно изучены, с точки зрения проведения моделирования. Осложняет ситуацию наличие разнородных приложений и устройств, порождающих потоки трафика с различными характеристиками. В статье будут рассмотрены некоторые существующие подходы по моделированию трафика в пакетных сетях связи. А именно, применение для описания агрегированного пакетного трафика фрактального броуновского движения и движения Леви, а также метод сетевого исчисления.

моделирование, фрактальное броуновское движение, сетевое исчисление.

Введение

В XX веке была сформирована теория массового обслуживания, позволяющая рассчитать необходимое число коммутационного оборудования и каналов связи для предоставления услуг телефонии на сетях с коммутацией каналов. С переходом на мультисервисные сети на базе коммутации пакетов выяснилось, что применение моделирования на основе Пуассонов-

ских потоков не всегда дает близкие к реальности результаты. Математические подходы исследования сетей связи уступили имитационным моделям, по причине не достаточной проработанной теории математического моделирования разных видов пакетного трафика и оборудования мультисервисной сети.

С другой стороны со временем в мультисервисных пакетных сетях нарастала проблема классификации трафика и понимания – поток, каких именно данных обрабатывается сетевым оборудованием. Для сохранения контроля и управления над сетью связи потребовалось внедрять технологии классификации и инспекции пакетов. В том числе глубокую инспекцию пакетов *(*DPI, *Deep packet inspection)*.

Появление все новых потоков данных в гетерогенных сетях связи обостряет вопросы описания трафика и сетей с помощью моделирования для их построения, эксплуатации и модернизации.

В данной статье представлены некоторые существующие подходы по моделированию пакетного трафика в сетях связи. Первый из них описывается в ряде работ сотрудников РУДН, в частности в [1] и представляет собой способ использования классической теории массового обслуживания применительно к небольшим пакетным сетям. Для таких сетей осуществляется расчет вероятности блокировки при предоставлении очередной услуги в определенной точке на мультисервисной сети и среднее значение загрузки звена сети.

Ко второму подходу можно отнести применение распределений Парето и Вейбулла вместо Пуассоновского для описания поступающего потока заявок на систему массового обслуживания (СМО). В [2] выбор наиболее подходящего распределения (Парето или Вейбулла) рассматривается с учетом величины параметра Херста изучаемого самоподобного пакетного трафика.

Третьим подходом является применение фрактального броуновского движения *(*FBM*, fractional Brownian motion)* для описания пакетного трафика предложенное в [3] и развитое в ряде работ [4, 5, 6]. Подробнее об этом направлении будет написано ниже.

К последнему из представленных в данной статье подходов относится метод сетевого исчисления *(Network Calculus)* представленный в [7, 8] и описанный с точки зрения практического использования в [9]. Сетевое исчисление исходит из того, что максимальные значения длин очередей и величин задержек можно рассчитывать с помощью огибающих входящих потоков заявок и функций обслуживания, а не реальных кумулятивных функций. Описание подхода по использованию сетевого исчисления будет представлено далее.

Моделирование трафика с помощью его описания фрактальным броуновским движением

Ряд исследований сообщает, что сетевой трафик является самоподобным [3, 4, 5, 10] или фрактальным по структуре (пульсирующим в широких временных пределах) [4]. Еще в первой половине XIX века Р. Броун исследует движения цветочной пыльцы, ныне известное как броуновское движение (*Brownian motion*, BM), самоаффинное и обладающее фрактальными свойствами [11]. В начале XX века Г. Э. Херст наблюдая за рекой Нил вводит коэффициент (*H*), значение которого для реки говорило о длительной памяти и поддерживаемости процесса [11]. Н. Винер вводит математическую модель броуновского движения (Винеровский процесс, являющейся самоподобным). Степень самоподобия возрастает при значениях коэффициента Херста превышающих 0,5 и вплоть до 1 [4]. Коэффициент Херста для определенного трафика оценивается с помощью R/S статистики, дисперсионного анализа, оценки Виттла (частотная область) и др.

Б. Б. Мандельброт и Дж. У. Ван Несс в 1960-х годах для определения ценообразования на финансовых рынках применили фрактальное броуновское движение *FBM*. В качестве альтернативы классическому подходу для расчета системы с входящим потоком пакетного трафика в Bellcoregroup в 1990-х годах была разработана модель, основанная на работах Б. Б. Мандельброта. Описание данной модели привел И. Норрос в [3]. В частности число заявок в системе в [3] определяется по (1), а поступивший трафик по (2).

$$Xt = \sup\big(At - As - C(t-s)\big), \tag{1}$$

где *At* – поступающий трафик,
As – трафик в очереди,
C(t-s) – процесс обслуживания трафика, *sup* (или максимум) при высоком *t* [3, 12].

Применение и развитие модели Норроса описывается в [4, 5]. В [2, 12] проводится сравнение классических моделей и модели с описанием трафика с помощью *FBM*. *FBM* подразумевает Гауссовский самоподобный процесс *Bt(H)* [4], определяющий распределение поступающего трафика как показано в (2).

$$At = m \times t + \sqrt{a \times m} \times Bt(H), \tag{2}$$

где 0,5 < H < 1,

a – является характерным моментом для фрактального броуновского движения и задает моменты, форму дополнительного распределения,

m – средняя величина поступающего трафика.

Помимо фрактального броуновского движения (*FBM*), применяются модели с фрактальным движением Леви (FLM*, fractional Levy Motion,*), а также мультифрактальное броуновское движение (MFBM*, fractional Brownian motion*). Стоит добавить, что использование фрактальной размерности статистических характеристик трафика позволяет выявлять и проводить классификацию сетевых атак [6].

В ряде рисунков, приведенных в [4, С. 25–26], дается сравнение колебания потока трафика в IP-сети, с аналогичным описанием с помощью Пуассоновского потока и с помощью *FBM*. На них очевиден выбор в пользу *FBM*. Кроме того на рис. представлено сравнение колебаний трафика в IP-сети (число данных за единицу времени с учетом масштаба) с смоделированными колебаниями на основе математического описания из [3], которое показывает применимость такого подхода.

Представленный подход использует достаточно сложный математический аппарат для моделирования пакетного трафика. Однако, позволяет рассчитать некоторые показатели для устройств передачи данных с использованием формул из [3, 12].

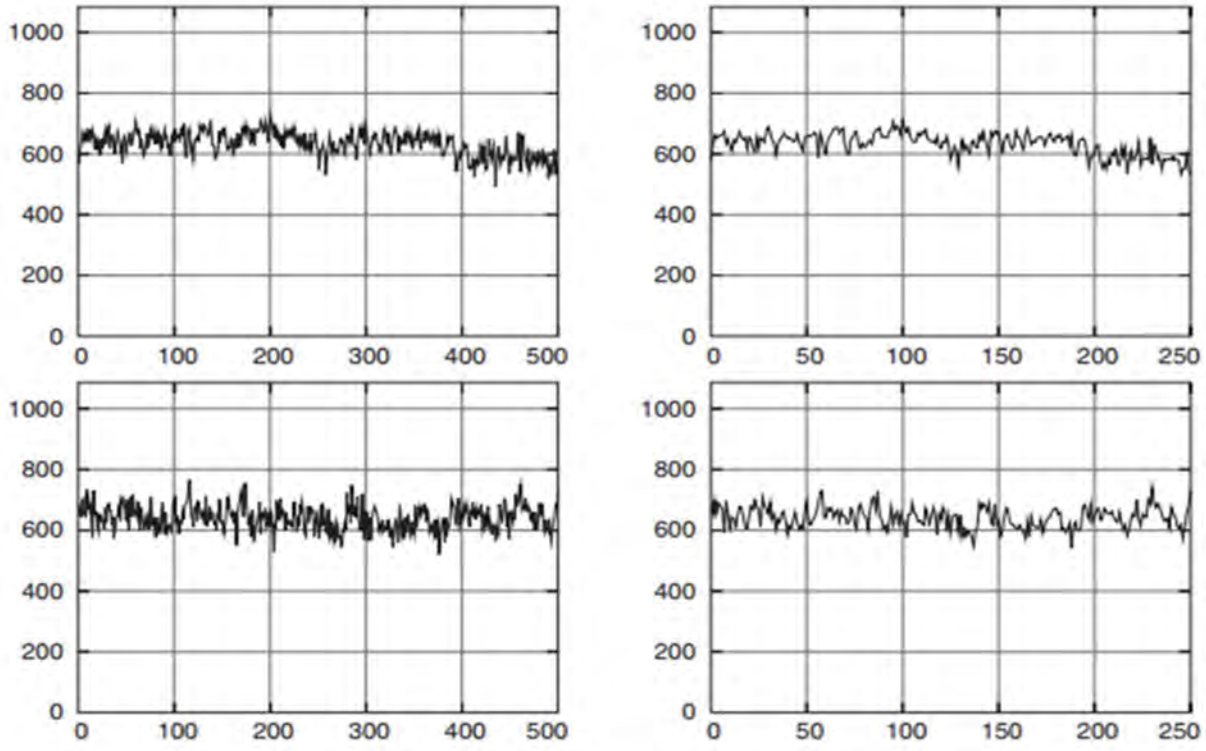


Рис. Измеренный трафик (вверху) по сравнению с смоделированным трафиком согласно модели Норроса (внизу), масштабирование t = 4 000 мс (слева) и t = 8 000 мс (справа) [Привод. по: 4, С. 226]

Сетевое исчисление

Оригинальный подход для определения максимального значения длин очередей и величин задержек с помощью огибающих входящих потоков заявок и функций обслуживания, а не реальных кумулятивных функций был представлен Рене Леонардо Крузом в диссертации [7]. Такой подход получил название сетевое исчисление, и позднее был опубликован в статье [8]. Математическое отношение кумулятивной функции и её огибающей показано в (3).

$$A(t) - A(s) \leq E(t - s), \tag{3}$$

где $A(t)$ – кумулятивная функция,

$E(t - s)$ – огибающая.

Спустя 10 лет Ле Будек создает руководство [9] по сетевому исчислению. Затем появляется программное обеспечение облегчающее использование сетевого исчисления, что дает возможность его применения на сетях связи. Описание сетевого исчисления также дается в статье [13].

Заключение

Проведен обзор подходов по моделированию трафика в пакетных сетях связи. В [1] дается метод расчета вероятности отказа в услуге на пакетной сети и среднего значения загрузки звена сети. В ряде работ, в том числе в [2] используются распределения Парето или Вейбулла для описания поступающего потока заявок. А в [3, 4, 5, 6, 12] для этого применяется *FBM*. Сетевое исчисление представлено работами [7, 8, 9, 13]. Описанные подходы остаются сложны для использования и недостаточно распространены.

Список используемых источников

1. Модели для анализа качества обслуживания в сетях связи следующего поколения : учебное пособие / Г. Башарин [и др.]. М. : РУДН, 2008. 137 с.

2. Одоевский С. М., Хоборова В. П. Методы прогнозирования качества обслуживания самоподобного трафика в устройствах коммутации мультисервисной сети // Труды учебных заведений связи. 2017. Т. 3, № 3. С. 86–92.

3. Norros I. A storage model with self-similar input // Queueing Syst. Theory Appl. 1994. No. 16. pp. 387–396.

4. Grimm C., Schluchtermann G. IP Traffic Theory and Performance // Heidelberg : Springer, 2008. - 501 p.

5. Krishna M., Gadre V., Desai U. Multifractal based network traffic modeling // Springer US, 2003. 210 p.

6. Sheluhin O., Kazhemskiy M. Influence of fractal dimension statistical charachteristics on quality of network attacks binary classification // Proceedings of the FRUCT'28. Vol. 1. 2021. pp. 169–175.

7. Cruz R. L. A calculus for network delay and a note on topologies of interconnection networks // PhD Dissertation, Report No. UILU-ENG-87-2246, University of Illinois, Urbana, Illinois, 1987.

8. Cruz R. L. A calculus for network delay. Part I: Network elements in isolation, Part II: Network analysis information theory // IEEE Trans. on Information Theory. Vol. 37. 1991. pp. 114–131, pp. 132–141.

9. Le Boudec J.-Y., Thiran P. Network calculus: a theory of deterministic queuing systems for the internet. // in Lecture Notes in Computer Science, Berlin, Germany: Springer-Verlag. 2001. № 2050. 273 p.

10. Косивцов П. Поведение IP-трафика в сетях NGN // Технологии и средства связи. 2009. № 5. С. 16–18.

11. Петров В. В. То, что вы хотели знать о самоподобном телетрафике, но стеснялись спросить. М. : МЭИ, ИРЭ, 2003. 48 с. URL: http://pi.314159.ru/petroff1.pdf , свободный.

12. Фицов В. В. Математическая модель DPI на основе классификации Норроса // 72 региональная научно-техническая конференция студентов, аспирантов и молодых ученых "Студенческая весна - 2018". 2018. С. 194–200.

13. Байбулатов А. А. От теории очередей к сетевому исчислению: исторический обзор // Труды 11-й Международной конференции "Управление развитием крупномасштабных систем" MLSD'2018. Москва, 1-3 октября 2018 г. М.: ИПУ РАН, 2018. Т. 2. С. 411–421.

УДК 004.085
ГРНТИ 47.35.41

ИССЛЕДОВАНИЕ ВОЛОКОННО-ОПТИЧЕСКОГО ЖГУТА

В. А. Ерёменко, Л. С. Шутова, Б. К. Резников

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

В статье проведен анализ способности передачи светового потока волоконно-оптическим жгутом в зависимости от изменения угла поворота центральной оси жгута относительно источника излучения. Рассмотрены на практике основные этапы формирования двоичного дискретного оптического сигнала с двумерной пространственной модуляцией. Проведены выводы относительно вводимого и выходного сигналов в исследуемом оптическом жгуте.

оптический жгут, волокно, оптический сигнал, эндоскоп.

Для передачи излучения отдельные оптические волокна объединяют в жгуты, которые могут иметь произвольное расположение волокон. На торцах волоконно-оптических жгутов единичные световоды склеены или сплавлены между собой, а сами торцы обрезаны перпендикулярно их

направлению и отполированы. Волоконные элементы жгута защищены гибкой оболочкой, предотвращающей их обрывы, разрушения при перегибах и проникновения влаги [1].

Эффект полного внутреннего отражения на границе световедущей жилы и оболочки оптического волокна позволяет передавать свет от высокоинтенсивного источника излучения, установленного в осветительном блоке, через тонкий гибкий жгут к эндоскопу и далее, через его рабочую часть, на выходной торец (дистальную часть) [2].

Существует две основные области применения оптических жгутов: передача изображения (эндоскопы) и передача света. Эндоскопы имеют широкое применение в медицинской технике и визуальном неразрушающем контроле. Волоконно-оптические жгуты, наиболее часто используемые в приборостроении, имеют диаметры от 0,5 до 400 мм и длину от 0,5 до 4 000 м и более [3].

Их гибкость позволяет соединять отдельные взаимно подвижные элементы, облегчает прокладку сети световодных каналов внутри приборов и механизмов.

Жгуты предназначены для передачи света в видимой области спектра.

Область применения:

- приборостроение,
- автомобилестроение,
- медицина.

Описание установки (рис. 1).

Цифрами на изображении обозначены:

1) Ноутбук, на который осуществлялся вывод изображения с цифрового микроскопа.

2) Блок питания лазера.

3) Лазер He-Ne с рабочей длиной волны $\lambda = 650$ нм.

4) Установка с коллиматором. Роль коллиматора в данном эксперименте исполняла линза, взятая из микроскопа, с очень малым фокусным расстоянием.

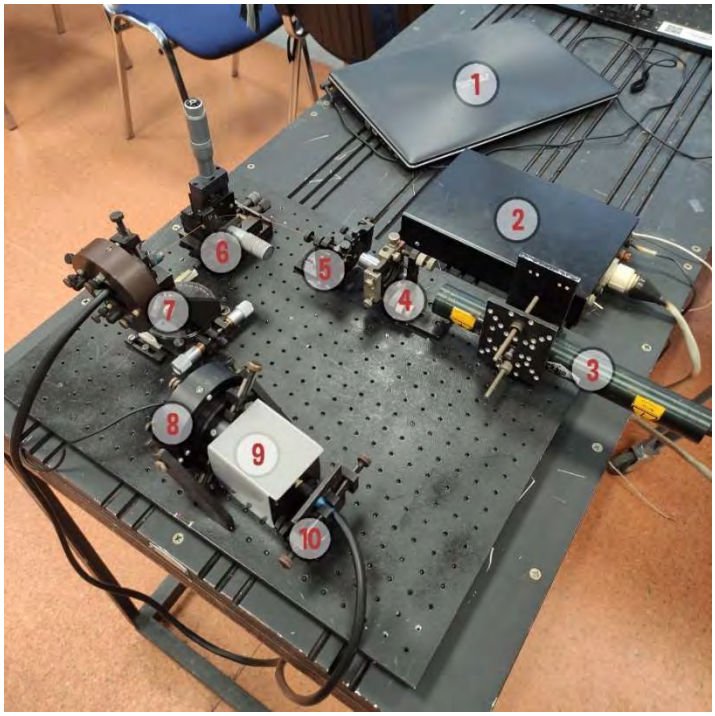


Рис. 1. Установка для исследования апертуры

5) Установка с зафиксированным в ней входом оптического волокна. Установка имеет возможность подстройки по двум осям для точечной подстройки сфокусированного лазерного излучения непосредственно в торец волокна.

6) Подвижка с зафиксированным в ней выходом оптического волокна. Данная подвижка имеет механизм точечной подстройки по трём осям, позволяя выполнить высокоточную подстройку выходящего пучка светового излучения на вход оптического жгута.

7) Тиски с зажатым в них входом оптического жгута, расположенные на поворотной платформе.

8) Цифровой микроскоп, сфокусированный на выход оптического жгута и выводящий изображение на экран ПК.

9) Металлических кожух, обеспечивающий отсутствие помех со стороны освещения лаборатории.

10) Тиски с закрепленным в них выходом оптического жгута.

Принцип работы установки:

Излучение лазера фокусируется коллиматором в торец оптического волокна. Выход волокна точечно юстируется со входом оптического жгута, размещённым на поворотной платформе. Посредством поворота платформы и фиксации полученного на выходе жгута изображения при помощи цифрового микроскопа и ПК была получена биекция значений углов поворота и картины на выходе оптического жгута. С помощью специального программного обеспечения были получены числовые значения интенсивности выходного излучения, позволяющие составить полноценную зависимость способности оптического жгута передавать изображение от угла ввода этого изображения в жгут.

Исходя из данных, полученных с помощью специального программного обеспечения, можно сделать выводы о том, что исследуемый оптический жгут имеет максимальное значение интенсивности выходного сигнала при точном перпендикулярном попадании в торец жгута (0 градусов поворота). Сигнал полностью пропадает при повороте торца на 28 градусов.

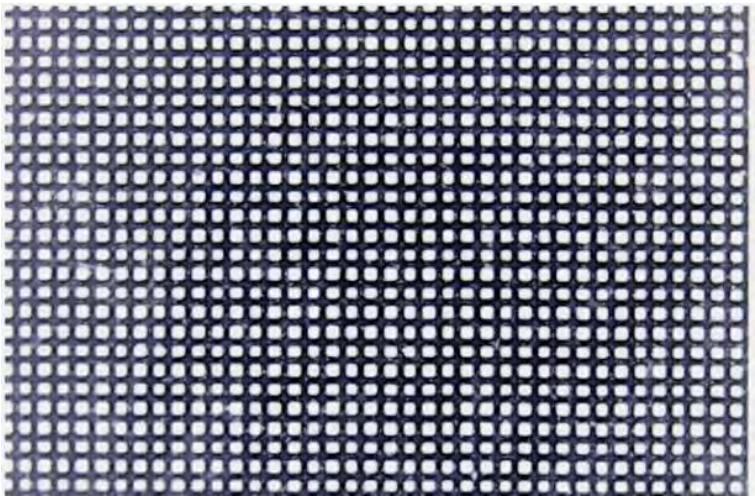


Рис. 2. Изображение, поданное на вход жгута

В зависимости от способа изготовления, жгуты с регулярной укладкой могут иметь площадь дефектов от 0,001 до 1 %. Эти жгуты допускают многократный изгиб с радиусом, равным 5–8 диаметрам жгута [4].

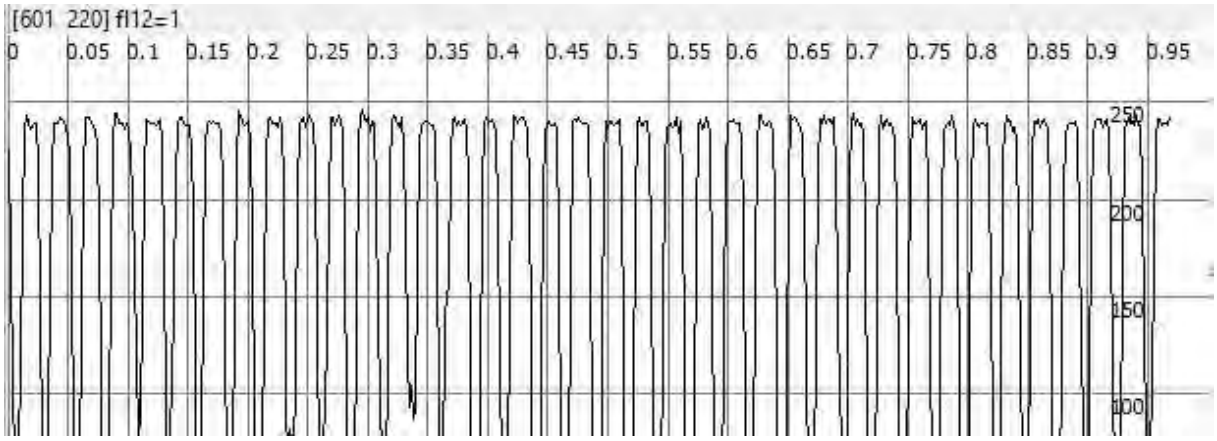


Рис. 3. Вид входного двоичного сигнала

На рис. 4 можно увидеть заметные искажения выходного сигнала относительно того, что был подан на вход, но тем не менее значительная часть сигнала всё ещё имеет ярко выраженные «нули» и «единицы», из чего можно сделать вывод, что при доработке данной технологии волоконно-оптический жгут подходит для передачи пространственно модулированных сигналов.

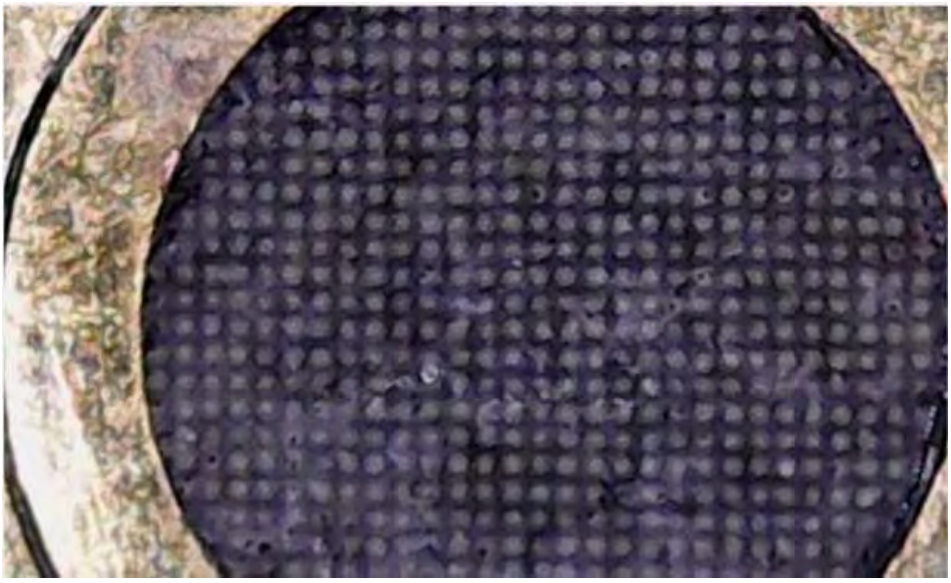


Рис. 4. Выход волоконно-оптического жгута с изображением

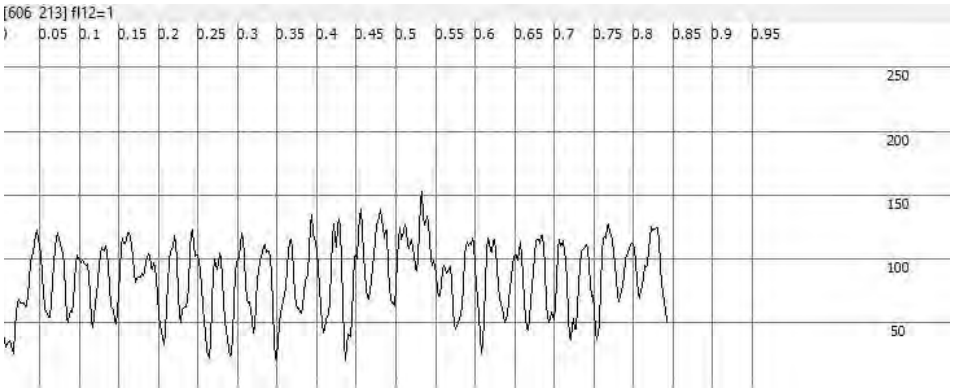


Рис. 5. Вид выходного двоичного сигнала

Список используемых источников

1. Чигорко А. Б., Чигорко А. А. Узлы и системы волоконно-оптических эндоскопов, 2007. 134 с.

2. Потери в оптических волокнах, вызываемые сильнейшие полями ионизирующего излучения. Саагел мл., да-ХТИИЭР. 1960. Том 68, Вып. 10. С. 81–86.

3. Апертура // Фотокинотехника: Энциклопедия / Гл.ред. Е. А. Иофис. М.: Советская энциклопедия, 1981. 447 с.

4. Лукомский Г. И., Березов Ю. Е. Эндоскопическая техника в хирургии. М.: Медицина, 1967. 400 с.

Статья представлена заведующим базовой кафедрой ССС СПбГУТ, доктором технических наук, доцентом В. В. Котовым.

УДК 65.011.56
ГРНТИ 50.41.23

АНАЛИЗ ИНСТРУМЕНТАРИЯ ДЛЯ ПОСТРОЕНИЯ КОРПОРАТИВНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ CARDANO

К. Э. Есалов[1], С. В. Кисляков[1,2], С. О. Шаляпин[3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]НТЦ АРГУС
[3]ООО "Естественный Интеллект"

Алгоритм консенсуса «Proof of Stake» (доказательство доли владения) является мощной альтернативой алгоритму «Proof of Work» (доказательство выполнения работы). Разработчики сети Cardano предложили, помимо самой новой блокчейн сети, также и новый алгоритм «Proof of Stake». В помощь сторонним исследователям разра-

ботчики предложили инструментарий для изучения и анализа работы своей сети работы алгоритма консенсуса. Представляемые здесь результаты исследования носят практический характер, цель исследования – показать практические аспекты запуска, настройки узлов, кошелька, а также инструмента «песочница» от Cardano.

блокчейн, Cardano, Proof of Stake

Введение

Основное внимание при работе протоколов блокчейн, основанных на алгоритме консенсуса доказательства выполнения работы (*PoW*), таких как Биткойн, – это энергия, необходимая для их выполнения. Это приводит к огромным потребностям в энергии. Такое положение дел мотивировало исследование альтернативных протоколов блокчейн, которые устранят необходимость в доказательстве работы, заменив его другим, более энергоэффективным механизмом, который может предоставить аналогичные гарантии.

Несмотря на то, что доказательство работы кажется безопасным, следует упомянуть некоторые недостатки:

- Возрастающая сложность, что может привести к централизации мощности майнинга, а это уже противоречит идее децентрализации блокчейна.
- Энергетические потери.

Естественный альтернативный механизм основан на понятии «доказательство владения/доли» (PoS). Вместо того, чтобы майнеры инвестировали вычислительные ресурсы для участия в процессе выборов лидера, они запускают процесс, который случайным образом выбирает одного из них пропорционально доле, которой каждый обладает в соответствии с текущим реестром блокчейна.

Поэтому применение алгоритма PoS интересно следующим:

- Энергия не тратится впустую, как в блокчейнах с подтверждением работы. Как правило, выбор новой подписывающей стороны производится с использованием случайных критериев и взвешивается в зависимости от доли, которую имеет узел.
- Алгоритм PoS предлагает более быстрый способ создания блока за счет сокращения времени на выбор нового узла, подписывающего блок.

Наиболее перспективным, по мнению авторов статьи, видится ветка консенсусных алгоритмов PoS, развиваемая Cardano [1]. Поэтому дальнейшие исследования в данной статье посвящены сети Cardano и алгоритмам консенсуса в рамках этой сети.

Алгоритмы PoS от Cardano

Основные требования к разработке алгоритмов консенсуса сети Cardano объявлены следующие [4]:

1) Каждый раз выбирается новый подписант блока. Этот выбор должен быть полностью случайным, чтобы его нельзя было предсказать и изменить заранее.

2) Алгоритм должен быть достаточно быстрым, чтобы поддерживать большое количество транзакций в минуту.

3) Алгоритм должен защищать блокчейн от сетевых атак.

В начале использовался алгоритм Ouroboros BFT (*Byzantine Fault Tolerance*) – простой алгоритм, который Cardano использовал на протяжении фазы Byron.

Сейчас платформа Cardano представляет собой гибридную цепочку, в которой префикс цепочки использует алгоритм BFT, а затем продолжается разработанным на фазе Shelley алгоритмом Ouroboros Praos [5, 7]. Это наиболее перспективное решение на сегодняшний день с точки зрения авторов этой работы.

Установка Cardano node

Основная документация по Cardano находится на официальной странице *https://cardano.org/* [6]. Установка узла начинается со скачивания исполняемого файла со страницы *https://docs.cardano.org/projects/cardano-node/en/latest/*. Требуется найти заголовок *Linux Executable* – здесь находится последняя версия для *Linux*- и *Windows*- систем. Для *Linux* нужен бинарный файл *cardano-node-1.25.0-linux.tar.gz*. Далее следует создать папку с именем *cardano-node-1.25.0-linux* и распаковать в неё архив с бинарным файлом. В этой папке требуется перейти в папку configuration/cardano и найти файл *mainnet-topology.json*. Этот файл можно открыть любым текстовым редактором и отредактировать: вместо строки “*relays-new.cardano-mainnet.iohk.io*” вставить *IP*-адрес нового узла (рис. 1–3).

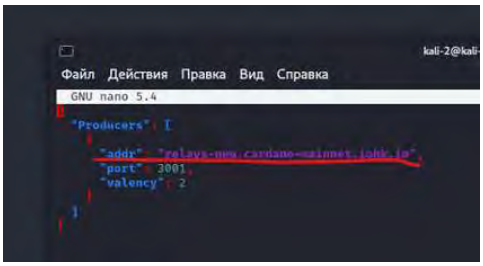


Рис. 1. Установка IP-адреса для узла Cardano

Рис. 2. Запуск установки узла

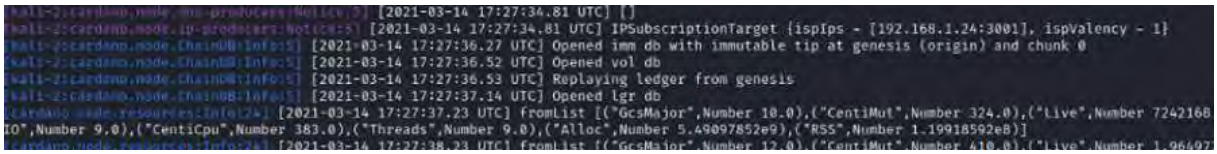


Рис. 3. Развёртывание узла – фрагмент процесса. Узел запущен и готов к работе

Инструменты Cardano для разработчиков и исследователей

Тестовая сеть *Cardano* (*Cardano Testnet*) дает возможность протестировать функциональность Shelley, включая пулы долей, делегирование долей и децентрализацию, прежде чем эти функции будут развернуты в основной сети Cardano. Цель тестовой сети – предоставить операторам пулов ставок возможность активно протестировать основные функции Shelley и подготовиться к запуску пулов ставок в основной сети Cardano. Поскольку тестовая сеть Cardano является независимой сетью, отдельной от основной сети Cardano, для нее требуются собственные токены (монеты).

The Cardano Testnet Faucet – это веб-сервис, который предоставляет тестовые бесплатные токены tADA пользователям тестовой сети, которые запускают пул ставок или другой узел. Токены позволяют пользователям экспериментировать с функциями Cardano, не тратя криптовалюту Ada в основной сети. В любом случае потребуются начальные средства, чтобы начать тестирование пулов ставок и делегирование ставок в тестовой сети. Testnet Faucet расположен по адресу *https://developers.cardano.org/en/testnets/cardano/tools/faucet/*. Для запроса тестовых токенов необходимо иметь установленный кошелёк, так как на этапе запроса токенов понадобится ввести адрес кошелька. Пример адреса: *addr_test1qqr585tvlc7ylnqvz8pyqwauzrdu0mxag3m7q56grgmgu7sxu2hyfhlkwuxupa9d5085eunq2qywy7hvmvej456flknswgndm3*. Начальный лимит тестовых токенов 1 000 в день для каждого пользователя тестовой сети.

Установка кошелька Cardano и получение тестовых токенов

Daedalus Wallet – тестовый кошелёк, который работает отдельно от главной сети. Установщик находится по адресу *https://developers.cardano.org/en/testnets/cardano/get-started/wallet/*.

Установка кошелька предполагает его уникальное название и его уникальный адрес. Чтобы принять транзакцию, необходимо передать адрес своего кошелька. Адрес можно взять в разделе Receive кошелька, выбрав один из доступных (рис. 4).

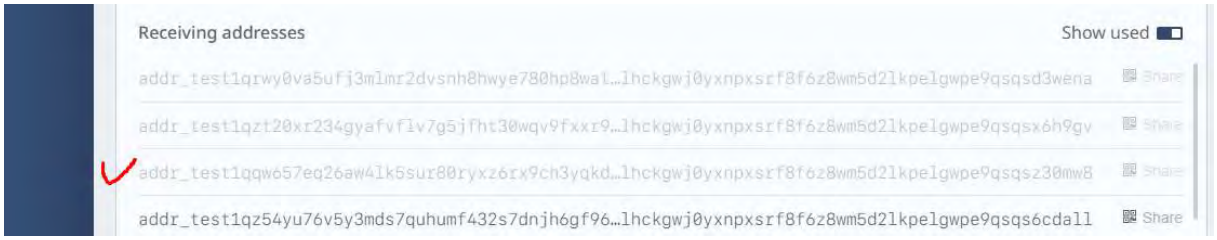


Рис. 4. Адреса кошелька для приёма тестовых токенов tADA.

В результате запроса тестовых токенов была получена 1 000 токенов. В разделе Transactions кошелька можно наблюдать полученные 1 000 токенов и 1 токен в результате ещё одной проведённой транзакции (рис. 5).

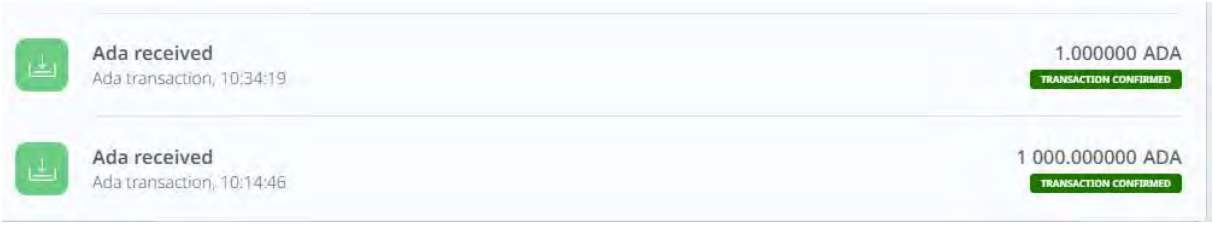


Рис. 5. В кошельке отражаются две принятых транзакции

В случае перевода токенов на другой кошелёк происходит оплата за транзакцию. На рисунке 6 приведен пример проведения транзакции в кошельке в размере 1 *tADA* с ценой перевода 0.175005 *tADA*.

Рис. 6. Цена транзакции

Проверку транзакции позволяет провести инструмент Cardano Blockchain Explorer. Для этого достаточно кликнуть по Transaction ID в кошельке. Переход по ссылке *https://explorer.cardano-testnet.iohkdev.io/en/transaction?id=68f220cc9c3a50f88854e1e1ff7afc80ff43264084f4370de72bfebb794c6c69* позволит увидеть подробную информацию о транзакции (рис. 7): время и дату, номер эпохи, номер блока в цепочке, исходящий и входящий адреса, количество, цену за транзакцию.

Как видно из копии экрана на рис. 7, данные по транзакции и остатку здесь и в кошельке полностью совпадают.

Рис. 7. Окно проверки транзакции

Разработка смарт-контрактов на платформе *Plutus*

Ещё один инструмент для поддержки разработчиков и исследователей – это Plutus Playground (песочница *Plutus*).

Plutus Playground предоставляет среду для написания и тестирования смарт-контрактов перед их выпуском в блокчейне Cardano. Plutus Core, язык смарт-контрактов, встроенный в реестр, основан на формальных принципах программирования Haskell и позволяет разработчикам писать высоконадежные приложения, взаимодействующие с Cardano. Haskell был выбран в качестве основы для платформы Plutus, потому что он отличается от других языков программирования тем, что предлагает возможность писать более безопасный код. Использование Haskell для развертывания смарт-контрактов гарантирует, что контракты запрограммированы так, чтобы делать именно то, что от них ожидается, и могут быть проверены на точность перед внедрением. Сама Cardano – многоуровневая блокчейн-платформа на базе Proof-Of-Stake – также написана на языке программирования Haskell.

Помимо веб-симулятора для написания и выполнения смарт-контрактов, новая площадка Plutus Playground также позволяет пользователям получать доступ к уже написанным популярным смарт-контрактам.

Plutus Playground состоит из редактора кода и симулятора. Приложения Plutus – это распределенные приложения с состоянием как в цепочке, так и вне ее. Их основная задача – создавать транзакции. Описание инструмента можно найти по ссылке *https://docs.cardano.org/projects/plutus/*.

Сама платформа (отладчик/симулятор) управляется через web-интерфейс и находится по адресу *https://playground.plutus.iohkdev.io/*. Интерфейс показан на рис. 8.

Рис. 8. Интерфейс платформы Plutus

Дальнейшие направления исследований

Одним из направлений развития Cardano объявлена поддержка нескольких пользовательских активов [7], что выглядит привлекательно с точки зрения расширения применения этой технологии за пределы криптовалютных/банковских операций. Например, это внедрение блокчейна Cardano в разработку OSS/BSS-решений для задач управления и эксплуатационной поддержки бизнес-процессов операторов связи.

Список используемых источников

1. Charles Hoskinson. Why we are building cardano. URL: https://docs.cardano.org/
2. Edsko de Vries, Thomas Winant, Duncan Coutts. The Cardano Consensus and Storage Layer. An IOHK technical report. February 26, 2021. URL: https://docs.cardano.org.
3. Kiayias, A., R ussell, A., D avid, B., and Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. Cryptology ePrint Archive, Report 2016/889, 2016. URL: https://eprint.iacr.org/2016/889.
4. Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. URL: https://docs.cardano.org/
5. Bernardo David, Peter Gazi, Aggelos Kiayias, Alexander Russell. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. URL: https://docs.cardano.org/
6. Официальный сайт Cordano. URL: https://cardano.org/
7. A Formal Specification of the Cardano Ledger. Deliverable SL-D5. 15th October 2019. URL: https://docs.cardano.org/

УДК 004.832.22
ГРНТИ 20.53.19

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ АЛГОРИТМОВ ГЛУБОКОГО МАШИННОГО ОБУЧЕНИЯ В ОБЛАСТИ ОБРАБОТКИ ЗВУКОВЫХ СИГНАЛОВ

К. Э. Есалов[1], Е. Ю. Куликов[1], А. Д. Онищук[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ООО "ЕСТЕСТВЕННЫЙ ИНТЕЛЛЕКТ»

Алгоритмы машинного и глубокого обучения все глубже проникают в каждую сферу нашей жизни, от сложного сырьевого производства, до сферы обслуживания. Так же алгоритмы такого типа широко используются в сетях связи, например для фильтрации сетевого трафика или обнаружения неполадок в сетях коммутации.

В данной статье описаны алгоритмы глубокого машинного обучения, используемые в современных системах голосовой верификации и идентификации пользователей. В этой работе будут описаны особенности подготовки данных для обучения алгоритмов на основе сверточных нейронных сетей, приведены архитектуры разработанных систем и показаны результаты работы.

нейронные сети, классификация, биометрия, речевые технологии.

Введение

Последнее десятилетие с развитием ЭВМ и интернета появляется все больше и больше дистанционных технологий от колл-центров службы поддержки до дистанционного образования. В 2020 году в связи с известными всем нам событиями мы были вынуждены сидеть дома и решать все наши дела дистанционно, через интернет и телефон.

При дистанционной работе важную роль играет безопасность. Вероятно все слышали про сервисы биометрической верификации и идентификации, можно смело предположить что такими технологиями пользуются большинство обладателей смартфонов, например FaceID или TouchID в *IPhone*, но когда речь идет об общении по телефону без возможности видеть и снимать отпечатки пальцев остается только один выход – определение личности по голосу, так как голос человека так же уникален как отпечаток пальца или сетчатка глаза [1].

Целью данной статьи является проектирование систем голосовой верификации и идентификации и определение максимально эффективного стека технологий для данных архитектур.

1 Основные понятия

Эмбеддинг – векторное представление образца голоса, выходящее из модели анализа голоса.

Верификация – производит сравнение двух образцов голоса: голос человека, чью личность необходимо подтвердить, с голосом, который храниться в базе данных системы и чья личность уже достоверно установлена. В качестве результата верификации система показывает степень совпадения одного голоса с другим в процентном отношении.

Идентификация – проверяет совпадение одного образца голоса со многими из базы голосов. В качестве результата идентификации система показывает список личностей с похожими голосами в процентном отношении. 100 % совпадение означает, что образец голоса полностью совпадает с голосом из базы данных и личность установлена достоверно.

Текстонезависимая верификация – вид верификации, когда подтверждение личности человека происходит по живой речи. Особенность этой технологии заключается в том, что ее можно применять «скрытно» от абонента. Данный подход анализирует речь на всем протяжении разговора и является самым надежным, т. к. заготовленные злоумышленниками фразы рано или поздно закончатся. Верификация производится по образцам разных размеров от 0,5 сек до бесконечности.

Текстозависимая верификация – вид верификации, когда подтверждение личности производится по определенной парольной фразе, которую на момент регистрации придумал абонент. Особенностью данной технологии является запрос конкретной фразы, что представляет собой дополнительную проверку личности, так-как злоумышленник может уметь синтезировать голос [2] конкретного человека, но может не знать определенную фразу.

Текстозависимая верификация по динамической парольной фразе – вид верификации, при которой подтверждение личности происходит по фразе, которую запрашивает система, допустим последовательность цифр или слов. Абонент повторяет за системой числа до тех пор, пока она не примет однозначного решения «свой/чужой». Это может быть и одно число или целая последовательность. Узким местом данной технологии является необходимость наличия алгоритмов распознавания речи [3].

2 Архитектура системы

Идеальным решением при проектировании системы голосовой верификации личности будет комбинация текстонезависимой верефикации для анализа речи абонента на протяжении всего разговора с оператором коллцентра или системой обслуживания и текстозависимой верификации по ди-

намической парольной фразе. Такая система имеет высокий уровень надежности и предусматривает противостояние современным методам мошенничества.

В этой статье будут рассмотрены системы текстонезависимой верификации и идентификации.

2.1 Система верефикации

Для функционирования системы верификации нам необходимо иметь:

– Базу данных, где мы будем хранить эмбеддинги наших абонентов.

– Алгоритм анализа голоса, который будет превращать образцы голоса наших абонентов в Эмбеддинг.

– Алгоритм сравнения эмбеддингов на основе Cosine Similarity [4] (1)

$$similarity = cos(\Theta) = \frac{A \cdot B}{\|A\|\|B\|} = \frac{\sum_{i=1}^{n} A_i \cdot B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}}. \quad (1)$$

Процедура регистрации абонентов в подобной системе представлена на рис. 1. Образцы голоса абонента проходят через алгоритм анализа голоса и хранится в базе данных.

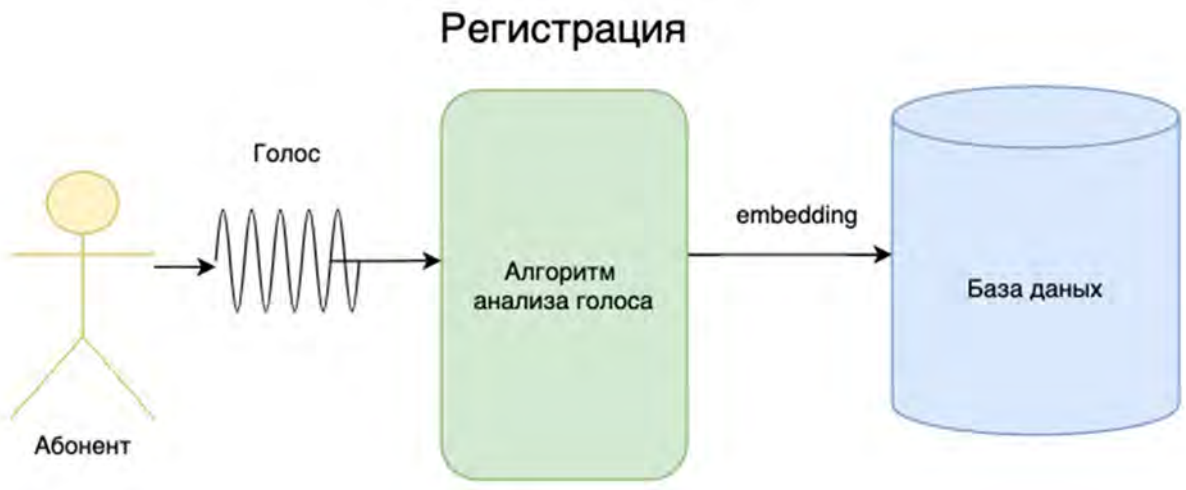


Рис. 1. Схема регистрации в системе верефикации

Процедура верификации в подобной системе представлена на рис. 2.

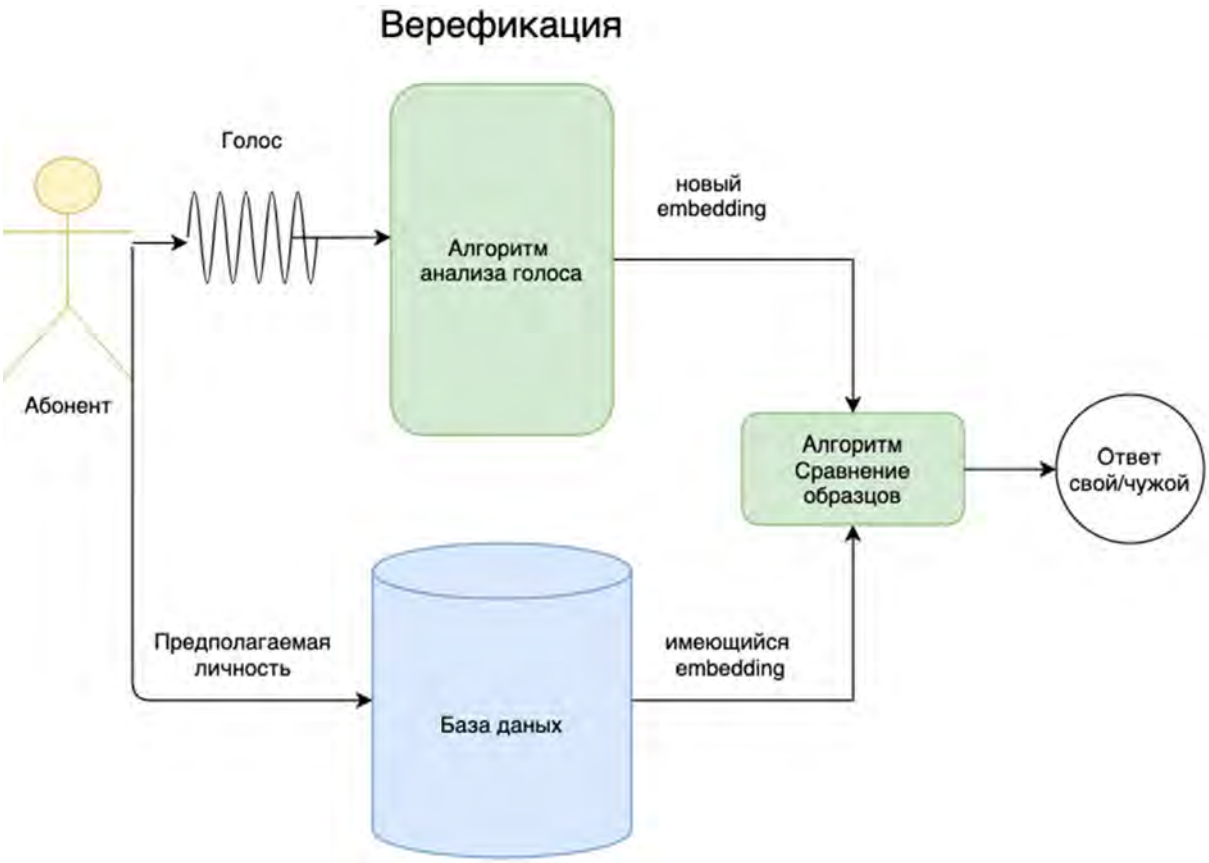


Рис. 2. Схема работы системы верификации

Первоначальное определение личности происходит по номеру телефона, с которого звонит пользователь, если это невозможно, то у абонента запрашивают ФИО или другую информацию, по которой можно идентифицировать личность, далее система берет образец голоса и отправляет его в алгоритм анализа голоса за тем получает новый эмбеддинг, из базы данных берется эмбеддинг созданный при регистрации, далее оба эмбеддинга сравниваются на основе cosine similarity [4] (1) и выдает ответ свой/чужой.

2.2 Система идентификации

Существует 2 разных метода построения систем идентификации, каждый из которых имеет свое узкое место. Однозначно нельзя сказать какой подход лучше, первый потенциально имеет большую точность и выше скорость работы, но требует более сложную процедуры регистрации и переобучение алгоритма классификации при добавлении новых пользователей, второй вариант имеет меньшую точность, ниже скорость работы, которая снижается по мере возрастания количества пользователей, но не требует регулярной поддержки и архитектурных правок.

2.2.1 Система идентификации 1

Процедура регистрации представлена на рис. 3. Предварительно идет этап сбора данных абонентов, после того как обьем данных стал пригодным для обучения, 10–15 секунд на пользователя или 5–7 эмбеддингов, классификатора, например Логистическая регрессия [5], Метод опорных векторов [6] и т. д. После того как алгоритм классификации обучен, система может функционировать на идентификацию (рис. 4).

Рис. 3. Схема регистрации в системе идентификации.

Рис. 4. Схема работы системы идентификации

2.2.2 Система идентификации 2

Процедура регистрации в подобной системе аналогична регистрации в системе верификации и представлена на рис. 1. Процедура работы подобной системы представлена на рис. 5 и представляет собой следующее:

1) Пользователь предоставляет образец голоса.

2) Образец проходит через алгоритм анализа голоса и получается эмбеддинг.

3) Алгоритм сравнения проходит по всем образцам из базы данных и находит ближайший.

4) Система выдает в качестве ответа личность абонента.

Рис. 5. Схема работы системы идентификации 2

3 Обработка данных

В качестве данных использовался набор данных VoxCeleb 2 [7], включающий в себя около 6 000 пользователей, общий обьем 2 000 часов (рис. 6, 7, 8).

Характеристики набора данных:

При обучении использовалась спектрограмма длинной 2,5 секунды случайно изымаемая из каждого образца. С вероятностью в 30 % фрагмент аудио выбирается в реверсивном виде. Спектрограмма получается путем краткосрочного преобразования Фурье [8] с окном 25 мс и шагом 10 мс. Далее к спектрограмме применяется z-масштабирование [9] (2).

$$z = \frac{x-\mu}{\sigma}, \tag{2}$$

где x – спектрограмма,

μ – среднее,

σ – среднеквадратическое отклонение.

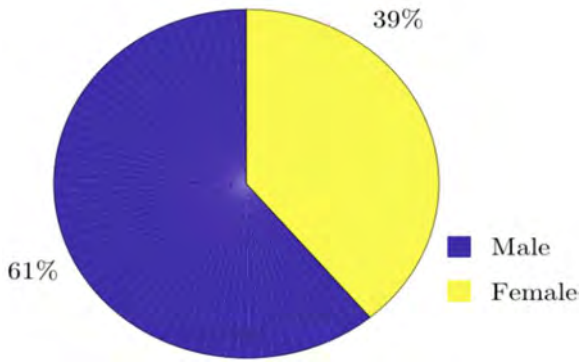


Рис. 6. График распределения пола

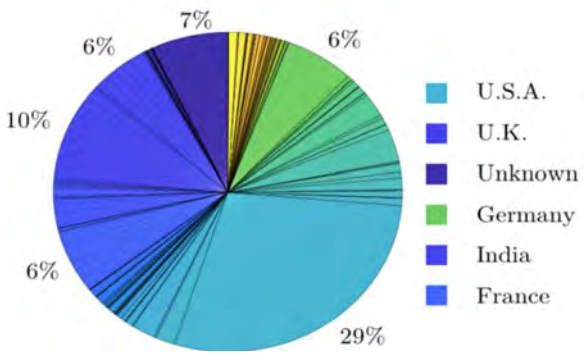


Рис. 7. График распределения национальностей

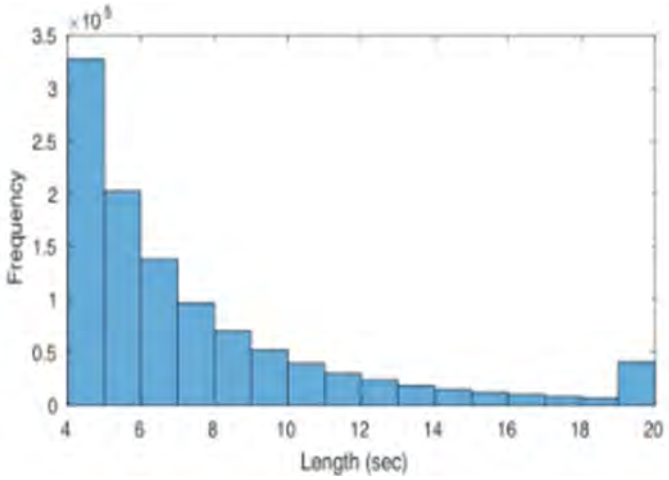


Рис. 8. График распределения длины образцов

3.2 Архитектура алгоритма

Алгоритм анализа голоса построен на основе сверточных нейронных сетей и разделен на 2 логические части (рис. 9):

1) Алгоритм извлечения признаков, который кодирует входящие спектрограммы и извлекает признаки.

2) Алгоритм агрегации признаков, который вычленяет важные признаки и обесценивает ненужные признаки.

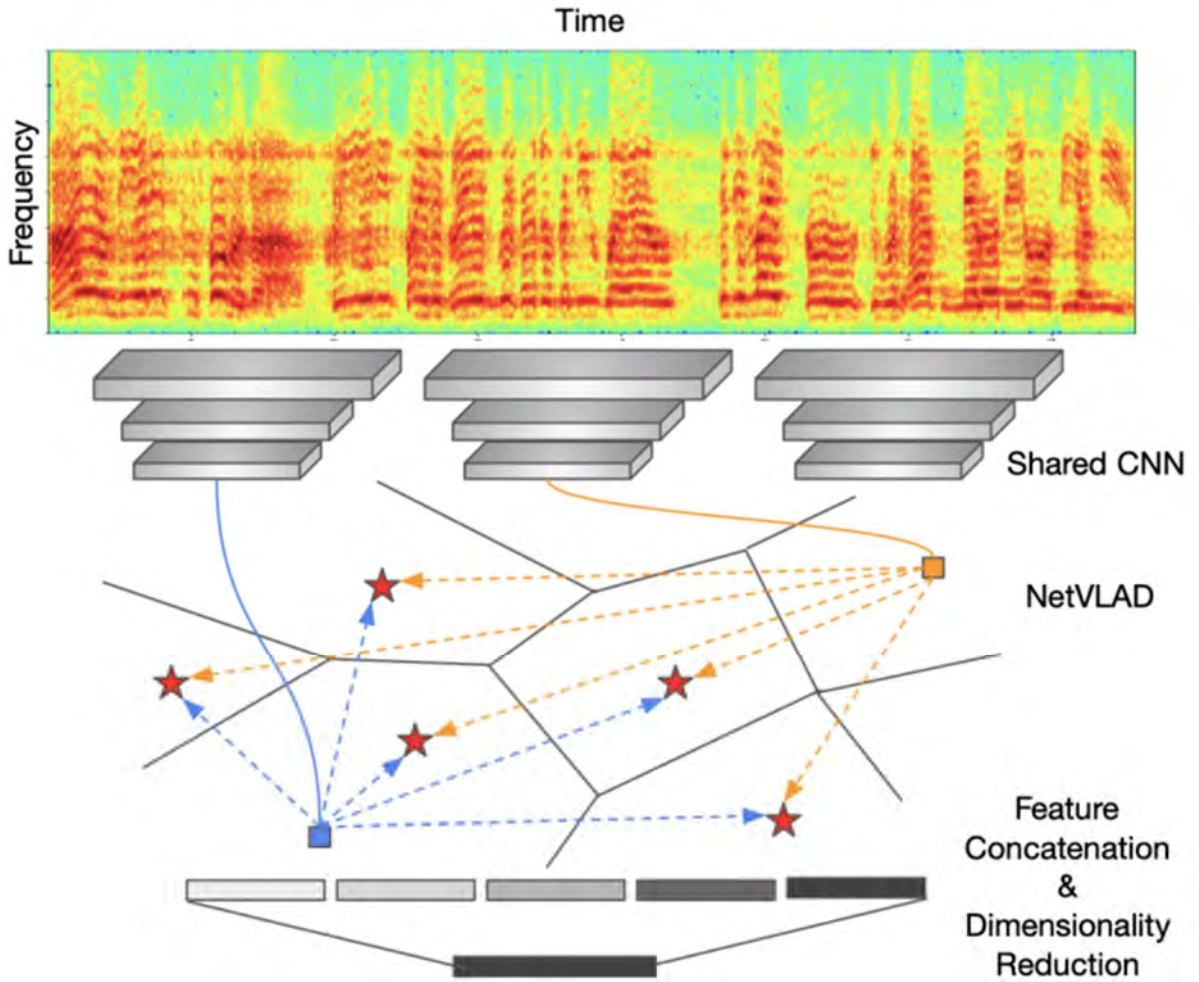


Рис. 9 Архитектура алгоритма анализа голоса

Вывод

Путем экспериментов было выяснено что оптимальная длина образца при обучении 2,5 секунды при достаточно богатом наборе данных, в ином случае, если набор данных представляет собой 3–5 секунды на спикера, то есть смысл уменьшить длину образца на обучении до 1 секунды, чтобы увеличить число уникальных образцов. При условии правильного обучения спроектированная система верификации может достигать точности 99 %.

Список используемых источников

1. Establishing the Uniqueness of the Human Voice for Security Applications. URL: http://www.csis.pace.edu/~ctappert/srd2004/paper08.pdf
2. Speech synthesis. URL: http://en.wikipedia.org/wiki/Speech_synthesis
3. Speech recognition. URL: https://en.wikipedia.org/wiki/Speech_recognition
4. Cosine Similarity. URL: https://en.wikipedia.org/wiki/Cosine_similarity
5. Logistic regression. URL : https://en.wikipedia.org/wiki/Logistic_regression
6. Support-vector machine. URL : https://en.wikipedia.org/wiki/Support_vector_machine
7. VoxCeleb dataset. URL: https://www.robots.ox.ac.uk/~vgg/data/voxceleb/

8. STFT. URL: https://en.wikipedia.org/wiki/Short-time_Fourier_transform
9. Z-scaling. URL:https://developers.google.com/machine-learning/data-prep/ trans-form/normalization#z-score
10. Utterance-level Aggregation For Speaker Recognition In The Wild (Xie et al., ICASSP 2019)
11. Convolutional neural network. URL: https://en.wikipedia.org/wiki/Convolutional_neural_network
12. Речевые технологии. Голосовая биометрия для чайников на примере работы в контактном центре. URL: https://habr.com/ru/company/speechpro/blog/205880/

УДК 004.832.22
ГРНТИ 20.52.19

РАЗРАБОТКА СИСТЕМЫ ОБРАБОТКИ ЕСТЕСТВЕННОЙ РЕЧИ НА ОСНОВЕ НЕЙРОКОГНИТИВНЫХ АРХИТЕКТУР ДЛЯ РЕАЛИЗАЦИИ ИИ СЕРВИСОВ ИНФОКОММУНИКАЦИОННЫХ УСЛУГ

К. Э. Есалов, А. В. Марочкина, А. С. Попонин

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

В данной статье приводится один из способов реализации системы обработки естественного языка, а именно: Автоматическое распознавание русской речи. В данной статье приводится описание сбора массива данных BigData, удовлетворяющих критериям для обучения, как обучалась модель, как улучшить результаты модели, например используя нейронные модели на этапе постпроцессинга результатов модели распознавания речи или препроцессинга входных данных. Данную систему распознавания речи можно использовать для реализации ИИ сервисов инфокоммуникационных услуг.

ИИ, нейронные сети, обработка естественной речи, нейрокогнитивные архитектуры.

Введение

На сегодняшний день существует потребность в оптимизации расходов абсолютно в любой области, касаемых консультационных процессов. В данный момент мы видим тренд замены живых сотрудников на ИИ-системы, направленные на консультацию клиентов. Одни из самых популярных решений являются «Алиса» от Yandex, «Олег» от Tinkoff, «Маруся» от Mail, голосового телефонного ответчика от «Sber».

Замена живых сотрудников на ИИ-системы позволит не только сократить расходы на зарплаты, но и освободить людей от работы, которую отлично может выполнять ИИ-система. Время этих людей можно тратить на решение творческих задач, которыми занимаются только около 20 % людей.

Есть совершенно простые системы, разрабатываемые для исследовательских задач, но в то же время есть современные и мощные системы, которые способны выполнять задачи промышленных масштабов. Цель данной статьи – определение максимально эффективного стека технологий для выполнения поставленной задачи.

1 Архитектура системы

Идеальным решением при проектировании системы распознавания речи будет пайплан, состоящий из Препроцессинга входных данных, акустической модели и постпроцессинга результата.

Общая структура система имеет более простой вид (рис. 1).

Рис. 1. Общая структура системы распознавания речи

1.1 Препроцессинг

Для улучшения результатов работы систем распознавания речи можно использовать инструменты препроцессинга входных данных (рис. 2). Одним из вариантов решения является система шумоподавления или Шумоподавитель (англ. *DeNoiser* [1]).

DeNoiser удаляет широкополосный шум из любых аудиозаписей. Алгоритм, на котором основана работа данного модуля, способен отслеживать и корректировать изменения в фоновом шуме.

Данный поход позволит Акустической Модели в нашей системе распознавания речи выдавать более качественные результаты.

Рис. 2. Структура работы системы с денойзером

1.2 Постпроцессинг

Акустическая модель чаще всего будет выдавать текст с ошибками, поэтому для исправления этих ошибок используют NLP [2] модели (рис. 3).

Самой популярной реализацией данной идеи являются N-gram [3] language model. Суть работы заключается в том, что на основе статистики модель может исправлять ошибки в словах.

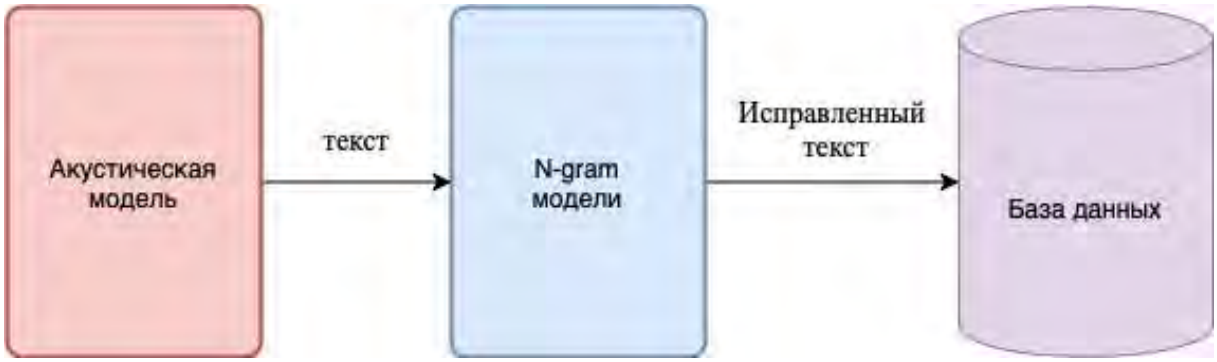


Рис. 3. Структура работы акустической модели вместе с N-gram моделями

1.3 Расширенная структура системы

На основе пунктов 1.1 и 1.2 можно улучить общую структуру системы, дополнив ее компонентами пре- и постпроцессинга с целью улучшения конечного результата (рис. 4).

Рис. 4. Расширенная структура систем

Основной упор в SoTa решениях делают не на улучшения качества Акустической модели, что конечно тоже является важной задачей, а на пре- и постпроцессинг. С помощью дополнительных компонентов можно значительно улучшить работу системы в целом.

2 Общие положения обучения акустической модели

Обычно программа обучения [5] CTC-ASR состоит из следующих блоков:

1) Предварительная обработка звука (извлечение функций): нормализация сигнала, построение спектрограмм или мелспектрограмм (MFCC [4]).

2) Нейроакустическая модель (которая предсказывает распределение вероятностей по словарным символам на каждом временном шаге с учетом входных характеристик на каждом временном шаге).

3) Функция потерь (обычно CTC *Loss*).

3 Данные для обучения акустической модели

Для обучения любой акустической модели нужно большое количество данных, которые нужно разделить на train, valid и test выборки.

2 000–5 000 часов качественных данных будет достаточно для достижения приемлемого результата.

Бывает так, что данных определенного языка бывает достаточно мало, в этом случае можно воспользоваться Аугментацией данных (рис. 5). Используя этот метод, мы можем размножить данные до нужного нам количества.

Рис. 5. Аугментация данных

4 Результаты

Собрав данные русской речи из открытых источников и обучив акустическую модель, используя методы из п. 2.1 и п. 2.2 (архитектура из п. 2.3), мы провели тесты получившейся системы распознавания речи. Для оценки результатов ASR системы мы использовали WER метрику.

На тестовой выборке наш WER получился равным 6,62 %.

Заключение

В данной работы было описано, как можно создать работающую систему распознавания речи в условиях, когда качественных данных недостаточно, как улучшить ее, используя пре- и постпроцессинг данных.

Акустическую модель можно улучшать используя итеративное обучение. С течением времени будет собираться всё больше и больше данных. Достаточно просто добавлять новые образцы в train выборку и переобучать акустическую модель.

Список используемых источников

1. DeNoiser. URL: it.wikireading: сайт. URL: https://it.wikireading.ru/59374
2. NLP. Wikipedia: сайт. URL: https://en.wikipedia.org/wiki/ Natural_language _ processing
3. N-gram. Wikipedia: сайт. URL: https://en.wikipedia.org/wiki/N-gram
4. Хабр. URL: https://habr.com/ru/post/140828/
5. Общие положения обучения акустичской модели. URL: https://docs.nvidia.com/ deeplearning/nemo/user-guide/docs/en/v0.11.0/asr/ tutorial.html

Статья представлена директором НИИ ТС СПбГУТ, кандидатом технических наук, доцентом А. Г. Владыко.

УДК 004.588
ГРНТИ 50.37.14

КОНЦЕПТ ПОСТРОЕНИЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СРЕДЫ ДЛЯ ПРОВЕДЕНИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ В ДИСТАНЦИОННОМ ФОРМАТЕ

К. Э. Есалов, А. В. Помогалова, А. А. Тян

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

Работа посвящена изучению концепции построения информационно вычислительной среды для проведения научных исследований и образовательных процессов в дистанционном формате. Вопрос проведения удаленных исследований по-прежнему остается актуальным, особенно в условиях борьбы с COVID-19. Тестирование высоконагруженных сетей, изучение принципов построения архитектуры и инфраструктуры сетей 2030 в дистанционном формате позволяет оптимизировать исследовательский процессы. Концепция, рассмотренная в рамках данной работы, позволяет проводить все виды сетевых исследований, а также образовательные процессы с использованием реального высокопроизводительного оборудования и технологий виртуализации.

COVID-19, ДОТ, дистанционно-образовательные технологии, сети 2030, дистанционные исследования, информационно-вычислительная среда.

Возможность проведения исследований сегодня – ключевой аспект для получения инновационных решений. А возможность проведения исследований дистанционно [1] – необходимость, как показали карантинные меры, связанные с пандемией COVID-19. Данная работа посвящена анализу и построению концепции построения информационно-вычислительной среды для проведения научных исследований в дистанционном формате на примере используемой научный центром дистанционно-образовательной платформы [4].

Архитектурная схема концепции представлена на рис. Для понимания концепции построения подобных информационно-вычислительных сред необходимо проанализировать каждый из представленных в рамках архитектуры блок.

Блок дистанционного доступа отвечает за предоставление удаленного доступа всем пользователям к системе согласно рекомендованным браузерам. Отвечает за предоставление доступа к веб-версии платформы, в рамках которой и происходит дальнейшее взаимодействие с ней.

Блок виртуализации отвечает за создание модельных стендов, в рамках которых производится обучение, тестирование и проведение исследований. Помимо исследований подобные модельные стенды могут быть использованы для проведения лабораторных практикумов, практических и факультативных занятий, а также в качестве тренажеров для школьников старших классов. Данный блок содержит производительный инструментарий для создания виртуальных версий оборудования. Виртуализация реализуется на базе реального оборудования, но позволяет виртуализировать любое необходимое сетевое оборудование: коммутаторы, маршрутизаторы, персональные компьютеры и многое другое. Данный блок представляет большое значение для платформы, так как именно на его основе создаются сети, которые имитируют реальные физические сети и позволяют проводить исследования, максимально приближенные к исследованиям на реальной физической производственной среде. Виртуализация происходит с использованием технологии qemu/kvm для управления виртуальными машинами.

Блок настройки курсов и практики отвечает за изменения, настройку и модификацию соответствующих разделов курсов. С помощью данного блока возможно постоянное улучшение предлагаемых платформой курсов и практических заданий, усовершенствование и настройка, в случае такой необходимости. В рамках блока также реализован UI-редактор, что упрощает взаимодействие с системой.

Блок интеллектуальных скриптов отвечает за автоматизацию таких действий [3], как предоставление доступа, разнотипные проверки состояний, тестирование и многое другое. Данный блок заменяет все рутинные процессы и автоматизирует их, что позволяет обеспечить подключение всех пользователей без усложнения данной процедуры. Оперативно тестировать различные участки сети с целью выявления некорректной работы, а также производить оперативное исправление ошибок и настройку среды. Скрипты реализованы на Shell и Python.

Рис. Схема архитектуры построения информационно-вычислительной среды для проведения научных исследований в дистанционном формате

База данных практик содержит формулировки практических заданий, автоматические проверки и другие технические настройки, необходимые для корректной работы практической части курсов. Реализовано с использованием реляционной базы данных MariaDB.

База данных курсов содержит в себе все данные о разработанных в рамках платформы курсов, согласно их топологии и архитектуре расположения. Содержатся не только описания курса и формулировки каждого его раздела, которые видит пользователь в рамках платформы, но и информация по настройке расписания предоставления доступа, разграничения прав доступа и многие другие настройки, которые необходимы при формировании индивидуальной траектории развития, а также персонализации курсов или адаптации под разные цели. Реализовано с использованием реляционной базы данных MariaDB.

База данных пользователей содержит в себе данные всех пользователей системы, включая разграничения прав, способ авторизации в системе, частоту входов в систему, дату последнего посещения и другую информацию, необходимую для создания корректного цифрового следа и корректной ав-

торизации в системе. Реализовано с использованием реляционной базы данных MariaDB и является частью общей реляционной базы данных платформы.

Блок логирования составляет важную часть платформы, так как позволяет фиксировать ошибки и подозрительные действия и события в рамках платформы. Данный блок содержит в себе логи работы всей платформы и фиксирует все неожиданные завершения сценариев, подозрительные, необычные ответы от оборудования, а также фиксирует ошибки, которые могут появляться при работе платформы. Этот блок позволяет оперативно разрешать случаи каких-либо поломок или некорректной работы платформы, а также позволяет однозначно распределить логирование информации, чтобы разработчики имели доступ ко всем выводам системы.

Блок статистического анализа отвечает за аналитику данных в рамках платформы. Статистический анализ может быть применим как к работе пользователей, так и работе самой системы. Данный блок отвечает за аналитику всех составляющих системы, корректность работы полигона и активность пользователей.

Интеллектуальный блок принятия решений отвечает за формирование цифрового следа. Данный блок разработан также для персонализации работы в рамках платформы, то есть расчета возможной индивидуальной траектории. Цифровой след – это уникальный набор действий и результатов взаимодействия с платформой каждого пользователя. Активность, успешность работы в рамках платформы, более активное решение определенного вида задач и более замедленное на другом виде – все эти данные позволяют с помощью интеллектуального блока принятия решений предложить индивидуальную траекторию развития с учетом всех персональных особенностей оставленного в рамках работы цифрового следа.

Блок подключения сторонних инструментов отвечает за подключение дополнительных утилит и программных решений, чтобы расширить функционал платформы дистанционного доступа. К таким сторонним инструментам относятся, например, WireShark. WireShark – это программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других [5]. Имеет графический пользовательский интерфейс и позволяет собирать статистику о передаваемых по сети пакетах данных, их частоте, типе, наполнении. Это позволяет проводить сетевые исследования в рамках формируемых стендов, анализировать характер и особенности трафика [2]. Для его генерации в качестве стороннего инструмента также подключается генератор трафика, формирующий передачу предустановленного трафика. Этот инструмент позволяет создавать гибкие сценарии и имитировать множество типов трафика, меняя характер и частоту появления пакетов, что позволяет проводить нагрузочное тестирование в рамках разработанных модельных стендов.

Также подключаются инструменты для измерения пропускной способности канала, анализа загруженности сети и другие генераторы трафика, которые могут быть необходимы для тестирования или проведения исследований. Примерами сторонних инструментов могут быть: iperf, anylogic, mininet, ns3, webshark и др.

Дальнейшим развитием концепции является построение распределенных лабораторий с использованием облачных технологий, таких, как OpenStack, что поможет усовершенствовать и вывести подобные решения на принципиально новый уровень.

Список используемых источников

1. Yesalov K., Lapiy A., Korytnikov O. 1. Adaptive learning system as a tool for increasing the effectiveness of distance learning // 2017 International Conference on Information Science and Communications Technologies, ICISCT 2017. 2017. pp. 1–4.

2. Елагин В. С., Спиркина А. В., Владыко А. Г., Иванов Е. И., Помогалова А. В., Аптриева Е. А. Основные сетевые характеристики Blockchain трафика и подходы к моделированию // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 39–45.

3. Есалов К. Э., Павленко М. Е. Программа автоматизации установки модельных полигонов. Свидетельство о регистрации программы для ЭВМ RU 2020613562, 18.03.2020. Заявка № 2020612625 от 10.03.2020.

4. Есалов К. Э., Белов А. С. Система дистанционного обучения QNet+. Свидетельство о регистрации программы для ЭВМ RU 2017619503, 25.08.2017. Заявка № 2017615079 от 25.05.2017.

5. Есалов К. Э., Помогалова А. В., Филипов В. В. Анализатор данных инфотелекоммуникационных систем с учетом кода регламентированных оператором услуг. Свидетельство о регистрации программы для ЭВМ 2020663614, 29.10.2020. Заявка № 2020662609 от 20.10.2020.

Статья представлена директором НИИ ТС СПбГУТ,
кандидатом технических наук, доцентом А. Г. Владыко.

УДК 004.51
ГРНТИ 81.93.29

МЕТОДИКА ПРОЕКТИРОВАНИЯ ЧЕЛОВЕКО-КОМПЬЮТЕРНЫХ ИНТЕРФЕЙСОВ ДЛЯ ПРИЛОЖЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К. Н. Жернова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук"

С учётом усложнения и увеличения общего объёма данных, передающихся по сети, а также увеличения количества подключенных к ней устройств, возрастает важность обеспечения информационной безопасности. Однако, при продолжительной работе с системами обеспечения информационной и компьютерной безопасности надёжность оператора снижается, уменьшается скорость принятия решений и эффективность работы. В данной работе представлена методика проектирования человеко-компьютерных интерфейсов, основанных на использовании сенсорных экранов, которые позволят повысить надёжность оператора при работе с приложениями информационной безопасности.

человеко-машинное взаимодействие, информационная безопасность, пользовательские интерфейсы, визуализация данных, сенсорные экраны.

Введение

В процессе работы с интерфейсами приложений информационной и компьютерной безопасности оператор может со временем утомляться и начать допускать ошибки, скорость и эффективность его работы снижается. Таким образом, уменьшается способность оператора выполнять поставленные задачи, т. е. снижается его *надежность* [1]. Повышением надёжности называется увеличение промежутка времени, в течение которого оператор сохраняет способность эффективно работать.

Для повышения эффективности работы оператора при работе с приложениями информационной безопасности разработана методика проектирования программно-аппаратных комплексов, реализующих интерфейсы человеко-компьютерного взаимодействия на основе сенсорных экранов. Методика состоит из трёх частей: (1) проектирование аппаратной части комплекса; (2) проектирование программной части комплекса; (3) оценка эффективности программно-аппаратного комплекса.

Проектирование аппаратной части комплекса

Для создания аппаратной части комплекса необходимо определить тип интерфейса: нужно ли создавать традиционный интерфейс, состоящий из привычных компонентов (кнопки, выпадающие списки, и т. п.), или интерфейс с управлением жестами на сенсорных экранах. Таким образом, разработчик имеет два возможных варианта устройств управления:

1) Клавиатура и мышь.

2) Сенсорный экран.

Остальные компоненты аппаратной части комплекса не имеют принципиального значения в рамках предлагаемой методики.

Проектирование программной части комплекса

Программная часть комплекса состоит из двух компонентов:

1) Компонент визуализации данных.

2) Компонент взаимодействия с этими данными через визуализацию посредством жестов на сенсорных экранах.

Проектирование компонента визуализации может происходить двумя способами.

1. Разработчик имеет возможность применять специальные библиотеки для визуализации данных, которые обеспечивают автоматический рендеринг изображения при изменении этих данных. Примеры таких библиотек: D3.js и C3.js.

2. Разработчик может прописывать необходимые компоненты визуализации самостоятельно. При этом визуализация будет лишена возможности автоматического изменения при изменении данных.

Проектирование компонента взаимодействия с отображаемыми данными происходит по трём возможным сценариям:

1. При разработке могут применяться готовые библиотеки, включающие в себя прописанные жесты взаимодействия с сенсорными экранами. Примерами таких библиотек могут служить Hammer.js и Interact.js.

2. Разработчик может прописывать жесты взаимодействия самостоятельно, что позволяет добавить в программную часть комплекса какой угодно жест, однако это повышает время, требуемое на разработку.

3. Также может использоваться метод машинного обучения, при котором для создания жеста требуется повторить один и тот же жест на сенсорном экране большое количество раз.

Оценка эффективности программно-аппаратного комплекса

Оценка эффективности полученного комплекса заключается в проведении эксперимента [2, 3] и последующего опроса [3] и состоит из нескольких этапов.

1. Подготовка к эксперименту. Должна включать в себя разработку нескольких сценариев, встречающихся при работе с системами информационной и компьютерной безопасности [4]. Сценарии состоят из различных заданий, оценивающих взаимодействие пользователя с визуализацией.

2. Проведение эксперимента. Приглашаются испытуемые для выполнения заданий из разработанных сценариев. Задания выполняются как с помощью оцениваемого интерфейса, так и с помощью традиционного. Пример интерфейса для сетевой безопасности приведен на рис.

Рис. Внешний вид прототипа интерфейса приложения сетевой безопасности

3. Проведение опроса испытуемых. Опрос состоит из нескольких заготовленных вопросов, на которые можно ответить, используя пятибалльную шкалу.

4. Оценка полученных результатов статистическими методами.

Выводы

В данной работе предложена методика проектирования программно-аппаратных комплексов, реализующих интерфейсы человеко-компьютерного взаимодействия на основе сенсорных экранов. Данная методика позволит создавать интерфейсы, повышающие надёжность оператора при работе с приложениями информационной безопасности.

Работа выполнена при финансовой поддержке РФФИ (проект 20-37-90130 Аспиранты).

Список используемых источников

1. Ломов Б. Ф. О путях построения теории инженерной психологии на основе системного подхода // Психологические основы профессиональной деятельности. 2007. С. 733–744.
2. Elmqvist N., Yi J. S. Patterns for visualization evaluation // Information Visualization. 2015. Vol. 14. No. 3. pp. 250–269.
3. Arendt D. L., Burtner R., Best D. M., Bos N. D., Gersh J. R., Piatko C. D., Paul C. L. Ocelot: user-centered design of a decision support visualization for network quarantine // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2015. pp. 1–8.
4. Коломеец М. В., Чечулин А. А., Котенко И. В. Методика визуализации топологии компьютерной сети для мониторинга безопасности // Известия высших учебных заведений. Приборостроение. 2016. Т. 59. № 10. С. 807–812.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Чечулиным.

УДК 004.51
ГРНТИ 81.93.29

УЯЗВИМОСТИ ИНТЕРФЕЙСОВ «ОПЕРАТОР – ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ» В БЕСПИЛОТНОЙ ТРАНСПОРТНОЙ СРЕДЕ

К. Н. Жернова, М. В. Коломеец

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Беспилотные транспортные средства являются неотъемлемой частью умного города. Данная технология непрерывно развивается, совершенствуется инфраструктура умного города, позволяющая взаимодействовать с беспилотными транспортными средствами. Однако по мере развития технологий умного города возрастает актуальность обеспечения безопасности беспилотной транспортной среды, а также необходимость разрабатывать меры противодействия возникающим угрозам. Данная работа даёт краткое описание интерфейса «оператор – искусственный интеллект» беспилотной транспортной среды, описывает основные уязвимости данной системы и возможные атаки, направленные на эти уязвимости.

человеко-машинное взаимодействие, информационная безопасность, пользовательские интерфейсы, визуализация данных, машинное зрение.

Введение

Для получения информации о ситуации на дороге беспилотные транспортные средства (БТС) часто используют машинное зрение. Машинное

зрение предполагает наличие фото- и видеокамер, которые получают изображение, и алгоритмов на основе машинного обучения, позволяющих определить, что именно изображено, и принять решение о дальнейших действиях БТС. При этом оператор, отслеживающий состояние системы БТС, должен получать данные о её состоянии, в форме графиков и схем. Каждый элемент интерфейса взаимодействия «оператор – искусственный интеллект» имеет уязвимости.

Схема взаимодействия оператора с системой

В начале, информация поступает из окружающего мира в компьютерную систему с помощью машинного зрения. Далее в компьютерной системе происходит обработка поступившей информации. После этого данные визуализируются и выводятся на экран оператора. Оператор изучает визуализацию и делает вывод о состоянии компьютерной системы. Таким образом, данная схема разделяется на две основные составляющие: (1) обработка информации с помощью машинного зрения и (2) визуализация информации о состоянии системы. Графически данная схема представлена на рис. 1.

Рис. 1. Схема взаимодействия человека с компьютерной системой

Ниже, на рис. 2, представлена блок-схема машинного зрения [1].

Рис. 2. Упрощённая схема обработки информации с помощью машинного зрения

Машина фиксирует изображение окружающей обстановки. Далее изображение обрабатывается, чтобы сделать его понятным для машины. Затем происходит извлечение признаков, необходимых для принятия решения о дальнейших действиях машины.

В упрощённом виде визуализация данных происходит следующим образом (рис. 3).

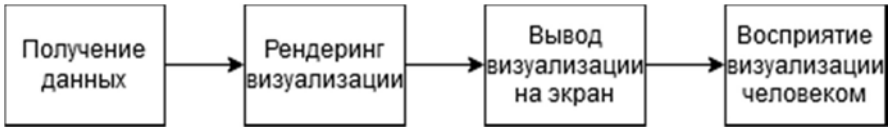


Рис. 3. Упрощённая схема визуализации полученных данных

Данные поступают в систему и обрабатываются ею. Далее на основе полученных данных строится визуализация. Затем визуализация выводится на экран, после чего оператор способен её воспринимать.

Уязвимости интерфейса взаимодействия оператор – система

Таким образом, уязвимости взаимодействия оператора с системой можно разделить на следующие категории:

1) Уязвимости со стороны системы.

2) Уязвимости со стороны оператора.

Со стороны системы проблемы обусловлены уязвимостями машинного зрения, которые также могут разделяться на следующие категории:

– физические уязвимости системы (позволяющие «обмануть» или ослепить камеры);

– сетевые уязвимости системы (позволяющие нарушить алгоритмы обработки информации, поступающей из окружающей среды, или подменить эту информацию).

Со стороны оператора уязвимости связаны со следующими проблемами:

– физические уязвимости оператора (оператор утомляется и допускает ошибки);

– сетевые уязвимости (позволяющие воздействовать на визуальные интерфейсы так, чтобы заставить оператора ошибаться или ухудшить его состояние, например, изменение данных визуализации, моргание экрана и т. д.).

Возможные меры противодействия атакам, основанным на уязвимостях интерфейса оператор – система

Зная уязвимости, можно предположить, какие атаки может попытаться предпринять злоумышленник. Например, к камерам машинного зрения может применяться спуфинг [2] или ослепление [3]. К визуальному интерфейсу на стороне оператора могут применяться побочные атаки глушением и сетевые атаки с целью подмены изображения.

Разрабатываются различные меры против атак, направленных на машинное зрение (дополнительная постобработка, основанная, например, на анализе качества изображения [4] и перефокусировке светового поля [5]),

а также направленных на визуализацию (например, в работе [6] предлагается экранирование устройства и глушение постороннего сигнала). Однако существует мало работ, направленных на изучение данных атак применительно к БТС.

Выводы

В данной работе показан интерфейс взаимодействия между оператором и системой управления БТС. Показано взаимодействие системы с окружающей средой посредством машинного зрения и взаимодействие оператора с системой посредством визуализации данных о состоянии системы. Дано краткое описание основных уязвимостей, как со стороны компонента машинного зрения, так и со стороны компонента визуализации, а также возможные атаки с использованием этих уязвимостей. В дальнейшем планируется разработать эффективные меры противодействия атакам [7], в том числе, основанным на уязвимостях, описанных в данной работе.

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099 мк).

Список используемых источников

1. Banić M. et al. Intelligent machine vision based railway infrastructure inspection and monitoring using UAV // Facta Universitatis, Series: Mechanical Engineering. 2019. Vol. 17. No. 3. pp. 357–364.
2. Li L., Correia P. L., Hadid A. Face recognition under spoofing attacks: countermeasures and research directions // Iet Biometrics. 2017. Vol. 7. No. 1. pp. 3–14.
3. Yan C., Wenyuan X., Jianhao L. Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle // In: DEF CON 24 (2016).
4. Wen, D., Han, H., Jain, A. K. Face spoof detection with image distortion analysis // IEEE Trans. Inf. Forensics Sec. 2015. 10 (4). pp. 746–761
2. Raghavendra, R., Raja, K. B., Busch, C.: Presentation attack detection for face recognition using light field camera // IEEE Trans. Image Process. 2015. 24 (3). pp. 1060–1075
3. Sayakkara A., Le-Khac N. A., Scanlon M. Accuracy enhancement of electromagnetic side-channel attacks on computer monitors // Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018. pp. 1–9.
4. Котенко И. В., Дойникова Е. В., Чечулин А. А. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. Инсайд. 2012. № 4. С. 54–66.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Чечулиным.

УДК 004.716
ГРНТИ 49.33.29

ФУНКЦИОНАЛЬНЫЕ ЭЛЕМЕНТЫ СИСТЕМЫ СЕТЕВОЙ ПОДДЕРЖКИ БЕСПИЛОТНОГО АВТОТРАНСПОРТА

А. А. Задорожняя, Р. В. Киричек

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

Одной из актуальных мировых технологий является беспилотные транспортные средства. Ожидается, что эта технология при внедрении сетей 2030 получит широкое распространение. Несмотря на то, что алгоритмы и сценарии взаимодействия беспилотных автомобилей с окружающей инфраструктурой и между собой каждый день развиваются и совершенствуются, беспилотным транспортным средствам рано выходить на дороги общего пользования. На сегодняшний день работа алгоритмов распознавания объектов и согласования с объектами окружающего мира далека от идеала. Для корректной работы всех элементов системы сетевой поддержки беспилотного автомобиля необходимо разработать единую однообразную функциональную архитектуру такой системы.

беспилотный автомобиль, функциональная архитектура, лидар.

Рассмотрим непосредственно базовые функциональные элементы системы сетевой поддержки беспилотного автотранспорта и их возможные приложения. Функции сетевой инфраструктуры при работе беспилотного автомобиля должны быть разделены в соответствии с различными требованиями к срочности и сложности, как показано на рис. 1 [1, 2, 3].

Функциональные базовые элементы кратко перечислены следующим образом:

- Бортовые службы, которые имеют низкую задержку из-за преимуществ локальной обработки: большинство срочных решений может быть принято непосредственно в транспортных средствах.
- Пограничные службы, которые могут обеспечить постоянную поддержку и помощь при движении транспортного средства между несколькими операторами: например, сложные приложения, такие как приложения, отвечающие за координацию между транспортными средствами и инфраструктурой, могут быть реализованы на пограничных хостах.
- Облачные сервисы, которые имеют широкий диапазон покрытия и обладают мощными вычислительными возможностями: учитывая большую

дальность передачи, некоторые функции с меньшим требованием к задержке могут быть реализованы в облаке, например, построение карт и планирование пути.

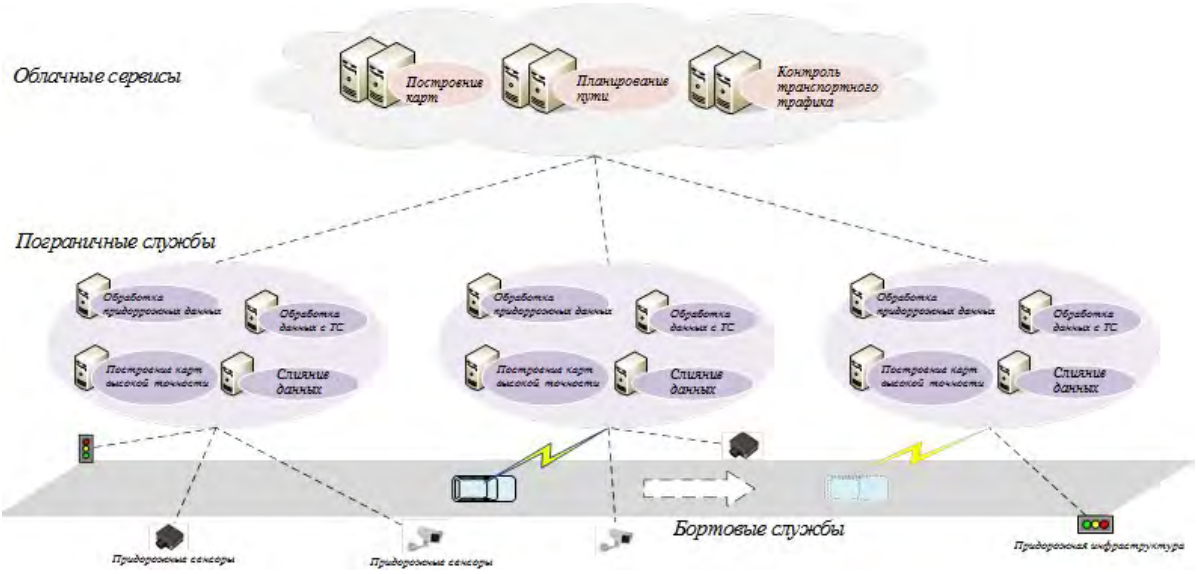


Рис. 1. Функциональная архитектура сетевой инфраструктуры беспилотного автотранспорта

На рис. 2 показана функциональная архитектура сетевой системы помощи при движении беспилотных транспортных средств, которая включает в себя функциональные возможности облачных и пограничных служб. В данной архитектуре функциональные элементы на уровне сервисной поддержки и поддержки приложений являются основными функциональными элементами. Они могут предоставить рекомендации по вождению транспортных средств, чтобы помочь скорректировать движение беспилотного автомобиля. Для удовлетворения требований связи со сверхнизкой задержкой необходимы высоконадежные сети. Сеть сквозная для информации о взаимодействии между различными объектами, включая транспортные устройства, пограничные и облачные сервисы.

Также на рис. 2 обозначены опорные точки между функциональными элементами. В архитектуре функциональные объекты системы сетевой поддержки беспилотных транспортных средств на разных уровнях соединяются через функциональные контрольные или опорные точки:

Контрольная точка 1 находится между объектом обработки данных на обочине дороги и объектом управления статическими данными в поддержку сбора данных и слияния статических данных. Она предназначена для связи между объектом обработки данных на обочине дороги и объектом управления статическими данными. Здесь передается инвариантная во времени информация, которая собирается из придорожных инфраструктур,

например, информация о дорожной сети, статическая информация о дорожном знаке и полосе движения.

Рис. 2. Функциональная архитектура сетевой системы поддержки беспилотного автотранспорта

Контрольная точка 2 расположена между объектом обработки придорожных данных и объектом управления динамическими данными в поддержку сбора данных и слияния динамических данных. Нужна для связи между объектом обработки придорожных данных и объектом динамического управления данными. Передается информация о временных вариантах, которая собирается из придорожной инфраструктуры, например, информация об обнаруженных участниках дорожного движения и фазе работы светофоров.

Контрольная точка 3 – между объектом обработки данных транспортного средства и объектом управления статическими данными в поддержку сбора данных и слияния статических данных. Связывает объект обработки данных транспортного средства и объект управления статическими данными. Передается инвариантная во времени информация, которая собирается с транспортных средств, например, основные параметры транспортных средств и их идентификация.

Контрольная точка 4 расположена между объектом обработки данных транспортного средства и объектом управления динамическими данными в поддержку сбора данных и слияния динамических данных. Обеспечивает связь между объектом обработки данных транспортного средства и объек-

том динамического управления данными. Передается информация о временных вариантах, которая собирается с транспортных средств, такая как состояние движения транспортного средства (например, скорость, крутящий момент двигателя, расход топлива) и данные от бортовых датчиков (например, бортовая камера и лидар).

Опорная точка 5 – между статическим объектом управления данными и объектом слияния данных в поддержку функции слияния данных. Для связи между статическим объектом управления данными и объектом слияния данных. Передаются предварительно обработанные статические данные, которые собираются из блока обработки данных транспортного средства и придорожных данных, в блок слияние данных для дальнейшей обработки.

Опорная точка 6 находится между объектом динамического управления данными и объектом слияния данных в поддержку функции слияния данных. Предназначена для связи между объектом динамического управления данными и объектом слияния данных. Передаются предварительно обработанные динамические данные, которые собираются из блока обработки данных транспортного средства и придорожных данных, в блок слияния данных для дальнейшей обработки.

Опорная точка 7 – между объектом слияния данных и объектом построения карты высокой точности в поддержку функции построения карты высокой четкости. Нужна для связи между объектом слияния данных и объектом построения карты высокой точности. Передаются результаты слияния для построения карт высокой точности, включая информацию о местоположении и информацию о составе участников дорожного движения (например, пешеходы, велосипедисты, транспортные средства).

Контрольная точка 8 – между объектом слияния данных и координационным органом транспортных средств в поддержку совместного контроля между транспортными средствами. Для связи между объектом слияния данных и объектом координации транспортных средств. Здесь в основном передаются результаты слияния информации транспортных средств для генерации предложений по координации движения транспортных средств в бортовые приложения.

Контрольная точка 9 расположена между объектом слияния данных и объектом координации транспортных средств и дорог в поддержку совместного контроля между транспортным средством и придорожной инфраструктурой. Предназначена для связи между объектом слияния данных и объектом координации транспортных средств и дорог. В основном передаются результаты слияния информации о транспортном средстве и информации о придорожной инфраструктуре, которые используются для генерации предложений по управлению транспортными средствами и дорожной координацией в бортовые приложения.

Опорная точка 10 – между объектом построения карты высокой точности и бортовыми приложениями для поддержки различных бортовых систем помощи при движении беспилотного ТС или автономных приложений вождения. Здесь обеспечивается связь между объектом построения карт высокой точности и бортовыми приложениями. В основном передаются части карты высокой точности, включая карту с уточнениями классификации дороги, полос движения и объектов.

Контрольная точка 11 – между блоком координации транспортных средств и бортовыми приложениями в поддержку различных бортовых систем при движении беспилотного ТС или автономных приложений вождения. Нужна для связи между блоком координации транспортных средств и бортовыми приложениями. Здесь в основном передаются оптимальные решения помощи при движении беспилотного транспортного средства, основанные на взаимосвязи дорожных транспортных средств, это может быть предупреждение о столкновении.

Контрольная точка 12 – между транспортным средством и дорожным блоком координации и бортовыми приложениями для поддержки различных бортовых систем помощи при движении беспилотного ТС или автономных приложений вождения. Здесь обеспечивается связь между транспортным средством и дорожным блоком координации и бортовыми приложениями. Здесь в основном передаются оптимальные решения по оказанию помощи при движении беспилотного транспортного средства на основе информации о придорожной инфраструктуре, такой как оптимальная скорость движения или маршрут движения [3].

На сегодняшний день, испытания показали, что беспилотный автотранспорт безопаснее транспорта, которым управляют люди и после массового внедрения вероятность таких случаев на дорогах снизится. В настоящее время использование облачных технологий предлагается повсеместно, это обусловлено тем, что для обработки больших объемов информации необходима удобная модель повсеместного сетевого доступа ко всем конфигурируемым ресурсам обработки данных [4]. Данные должны передаваться мгновенно между транспортными средствами и инфраструктурой (1 мс круговой задержки) и с высокой скоростью между собой. Для этого требуется введение нового высокоскоростного стандарта 5G, усовершенствованной дорожно-транспортной и телекоммуникационной инфраструктуры [5].

Анализ предлагаемой функциональной архитектуры сетевой системы поддержки беспилотного автотранспорта показывает возможность построения данной системы в ближайшем будущем.

Список используемых источников

1. Аль-Свейти М. А. М., Волков А. Н., Мутханна А. С. А. Проблемы и требования для реализации технологии V2X // Информационные технологии и телекоммуника-ции. 2020. Том 8. № 3. С. 20–26. DOI 10.31854/2307-1303-2020-8-3-20-26.
2. Кучерявый А. Е., Киричек Р. В., Маколкина М. А., Парамонов А. И., Дунайцев Р. А., Пирмагомедов Р. Я., Бородин А. С., Владыко А. Г., Мутханна А. С. А., Выборнова А. И., Владимиров С. С., Гришин И. В., Новые перспективы научных исследований в области сетей связи на 2021-2024 годы // Информационные технологии и телекоммуникации. 2020. Том 8. № 3. С. 1–19.
3. ITU-T Y.4471 (ex. Y.NDA-arch) "Functional architecture of network-based driving assistance for autonomous vehicles"
4. Al-Gaashani M., Muthanna M. S. A., Abdukodir K., Muthanna A., Kirichek R. Intelligent system architecture for smart city and its applications based edge computing // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2020. pp. 269–274.
5. Khayyat M., Alshahrani A., Alharbi S., Elgendy I., Paramonov A., Koucheryavy A. Multilevel service-provisioning-based autonomous vehicle applications Sustainability. 2020. Vol. 12. No. 6. P. 2497.

УДК 006.011
ГРНТИ 84.01.77

ЦИФРОВОЕ КАЧЕСТВО: РАЗРАБОТКА МОДЕЛЕЙ И МЕТОДОВ СРАВНИТЕЛЬНОЙ ОЦЕНКИ КАЧЕСТВА ПРЕДОСТАВЛЕНИЯ ЦИФРОВЫХ УСЛУГ

А. А. Зарубин, Н. М. Редругина, А. А. Савельева

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

В данной статье рассматривается подход автоматизированной оценки качества предоставления услуг программно-определяемых приложений инфокоммуникационных сетей с использованием сравнительного подхода и семантико-онтологический анализа и оценки качества восприятия. Данный подход рассмотрен как возможное дополнение к уже существующим рекомендациям.

качество обслуживания, QoS, инфокоммуникационные услуги, сравнительный подход, семантико-онтологический анализ.

Последние десятилетие в несколько раз преумножило номенклатуру предоставляемых инфокоммуникационных услуг и их функционального

разнообразия. Скорость роста и развития, как услуг, так и средств разработки различных приложений не позволяет оперативно вносить коррективы в системы контроля качества предоставления услуг.

Информация, приведенная в статье, является дополнением к существующим системам стандартизации, в которых заложены свойства системности и динамики улучшения системы управления качеством. Однако появление огромного количества приложений, требующих внимания, развитие которых опережает существующие стандарты, позволяет воспользоваться возможностью предложить дополнительные методы контроля качества предоставления услуг.

Развитие информационного общества, включая внедрение, расширение и разработку новых видов услуг зависит от обратной связи с пользователями данных услуг. Следовательно, важнейшим аспектом данного процесса является качество предоставления инфокоммуникационных услуг.

В данной статье описывается подход к разработке методов автоматизированной оценки качества предоставления услуг программно-определяемых приложений инфокоммуникационных сетей с использованием сравнительного подхода, а так же предлагается метод географического распределения средств вычисления и возможность использования средств семантического анализа качества восприятия пользователем.

Существуют публикации, такие как [1, 2], которые исследуют оценку вероятностно-временных характеристик коммутации пакетов, оценку доступности и времени отклика узлов телекоммуникационных систем, и варианты оценки параметров качества и ссылаются на известные стандарты, например [3, 4].

Стоит отметить что данные исследования основываются на анализе базовых показателей качества обслуживания. Польза, которых состоит в возможности получения качественных показателей, которые возможно взять за основу анализа качества новых разнообразных услуг, через общие измеримые показатели, имеющие вероятностно-временной характер.

Обозначим подходы к определению качества предоставления инфокоммуникационных услуг и их влияние на решение задач, связанных с проблемой быстроразвивающейся инфраструктуры.

Определим причины затрудняющие оценку параметров качества для появившейся инфокоммуникационной услуги.

- Высокая скорость обновления и разработки новых технологий, на которых основываются услуги.
- Увеличение разновидностей видов услуг
- Отсутствие эталонных или стандартизированных значений параметров качества обслуживания для отдельных интернет-услуг.
- Разные подходы для определения качественных характеристик в существующих рекомендациях.

Для решения затруднений, связанных с оценкой качества для недавно появившейся услуги, предлагается переход к комбинированному методу сравнительной оценки базовых объективных показателей качества услуг и результатов контент-ориентированного тестирования. Тем самым мы уходим от ограничений связанных с определением только базовых вероятностно-временных показателей качества обслуживания. В дополнение к численным значениям качества обслуживания предлагается подкрепить сравнением параметров полученных объективных методов оценки с результатами субъективных экспертных методов основанных на семантическом анализе качества восприятия.

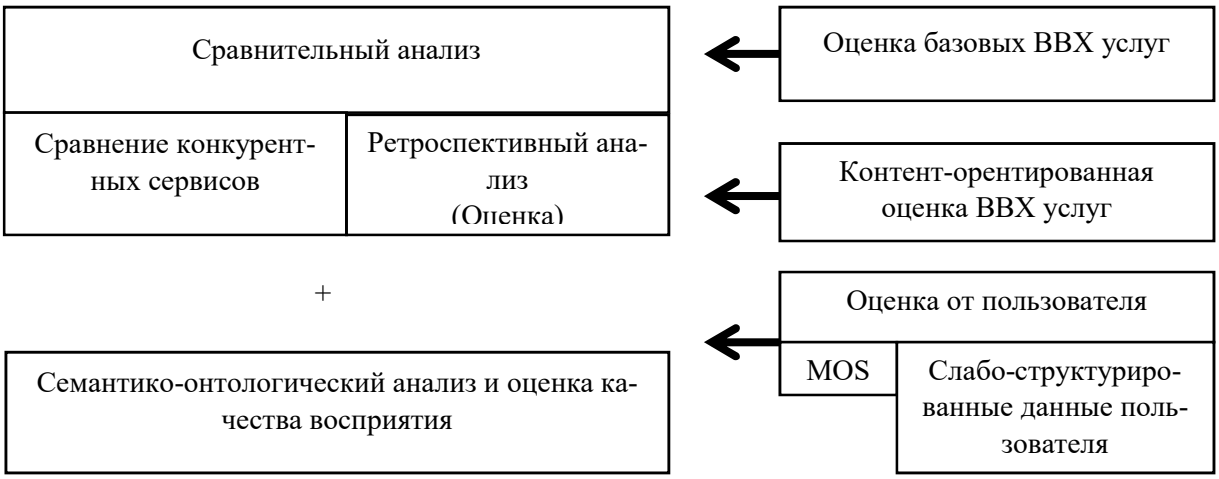


Рис. 1. Схема комбинированного метода оценки показателей качества услуг

Рассмотрим метод сравнительной оценки качества предоставления интернет-услуг. В данном методе оценки качества предлагается сравнивать качественные характеристики сервиса для определения изменений качества предоставления услуги с течением времени, либо в зависимости от предпринятых изменений в отношении сервиса (программной конфигурации или оборудования). На коротком промежутке времени возможно получить информацию о влиянии изменения нагрузки на качество обслуживания.

Сравнение базовых для всех сервисов сети Интернет показателей также может происходить среди аналогичных сервисов, либо с веб-сервисами не похожими по контенту.

При сравнении сервиса с самим собой следует обратить внимание на параметры изменяющиеся в зависимости от географического расположения оборудования, предоставляющего доступ к этому сервису. В зависимости от географической расположенности сервисов, их инфраструктура может обеспечивать неравномерное качество обслуживания(к примеру задержку или скорость передачи данных). При определении качества обслуживания пользователи могут определить эффективные качественные характеристики и выбрать сервер к которому они будут обращаться. Так же и разработчики

какой-либо услуги определяют корректность расположения серверного оборудования и слабые места гео-распределенной инфраструктуры.

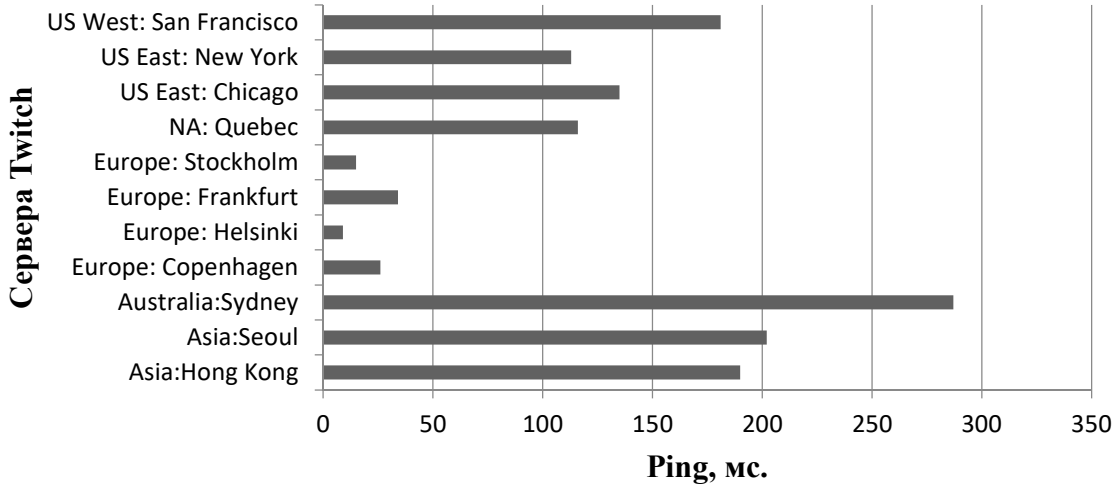


Рис. 2 Сравнение характеристики «ping»
для географически распределенных серверов сервиса Twitch

На рис. 2 показано сравнение качественной характеристики для географически распределенных по миру серверов стримингового сервиса Twitch для пользователей, находящихся в Санкт-Петербурге. Это один из основных параметров при определение качества обслуживания пользователей и выборе сервера для подключения.

Особое внимание в дальнейших исследованиях будет уделено семантико-онтологическому анализу для получения обратной связи от пользователей инфокоммуникационных услуг, качество обслуживания которых мы определяем.

Благодаря этому методу появится возможность работы с большими объемами данных, полученными в результате опроса и составления мнений пользователями, которые необходимо получить, обработать и получить набор актуальной и конкретизированной информации. На основе собранной информации возможно сделать вывод о качестве восприятия пользователями данной услуги и сравнение с качеством обслуживания полученными объективными методами.

Выводы

В связи с усложнением быстрым развитием и усложнением предоставляемых пользователю сервисов, появилась необходимость в изменении подходов оценки качественных характеристик современных инфокоммуникационных услуг. Подходы включающие в себя методы сравнительной оценки

как базовых вероятностно временных характеристик, так и контент-ориентированных. Новаторским решением станет использование семантико-онтологического анализа качества восприятия полученного через анализ слабоструктурированных данных от пользователей данных услуг.

Следует заметить что указанные выше методы будут эффективно работать если автоматизировать тестирование некоторых параметров.

Список используемых источников

1. Яновский Г. Г. Качество обслуживания в сетях IP // Вестник связи. 2008. № 1. 16 с.

2. Кучерявый Е. А. Управление трафиком и качество обслуживания в сети Интернет. СПб.: Наука и Техника, 2004. 336 с.

3. МСЭ-Т Recommendation G.1010. Series G:Transmission systems and media? Digital systems and networks // November 2001.

4. МСЭ-Т Recommendation Y.1540. IP Packet Transfer and Availability Performance Parameters // December 2002

5. Зарубин А. А., Кызюров О. Е., Савельева А. А. Разработка моделей и методов оценки качества цифровых услуг// Вестник связи. 2018. № 05. С. 37–40.

УДК 004.056
ГРНТИ 81.96

АНАЛИЗ МЕТОДОВ ВЫЯВЛЕНИЯ МНОГОШАГОВЫХ АТАК

И. Ю. Зеличенок, И. В. Котенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Многошаговые атаки – одна из основных угроз информационной безопасности на сегодняшний день. Базовые отличия от других типов атак – направленность атак на разные узлы информационной среды, нацеленность на наибольшее количество брешей системы информационной безопасности одновременно. Для выявления таких атак было предложено несколько методов. В докладе представляется анализ некоторых из них: на основе сходства, причинная корреляция, структурный подход, прецеденты и комбинация методов. Приводится описание каждого метода, его достоинства и недостатки. Для анализа используются актуальные исследования различных способов выявления многошаговых атак.

защита информации, кибератаки, многошаговые атаки, обнаружение атак.

Безопасность информационных систем являлась важнейшей их составляющей на протяжении всего их существования. Чем сильнее распространялись Интернет и локальные сети, тем большее внимание обращали на них злоумышленники. Со временем, информация, хранящаяся на серверах компаний или отдельных пользователей, стала достаточно ценна, чтобы начали появляться новые способы ее незаконной добычи. Сначала атаки были простыми, многие действия атакующего совершались в одно действие, иногда они просто повторялись. Такие атаки можно назвать «одношаговыми».

В наше время, взломщики используют сложные методы реализации атак. Они проводят атаки, состоящие из нескольких этапов для достижения конечной цели [1, 2]. Наборы таких этапов известны также как многоэтапные атаки или сценарии атак. Многоступенчатый характер этих атак препятствует обнаружению вторжений, так как для понимания стратегии атаки и определения угрозы необходимо проанализировать множество отдельных действий [1]. Примером успешной многошаговой атаки можно назвать вирус WannaCry, который 12 мая 2017 года распространился по миру, заблокировав работу персональных компьютеров (ПК) не только отдельных пользователей, но и многих компаний. Подобные атаки подтолкнули исследователей и разработчиков к разработке систем защиты, направленных на отслеживание многошаговых атак. Целью данной работы было исследование существующих методов выявления многошаговых атак, выделение их сильных и слабых сторон и приведение примеров исследований по каждому из рассматриваемых методов.

В основу классификации была положена работа [3]. Подходы к разработке этих систем можно представить следующим образом: на основе подобия (прогрессивное конструирование, кластеризация, обнаружение аномалий); причинная корреляция (предпосылки и последствия, статистический вывод, сопоставление моделей); структурный подход; основанный на прецедентах; смешанный.

В методах *на основе подобия* сценарий атаки восстанавливается на основе известных паттернов (следов) реализации атак.

При *прогрессивном конструировании* последовательности атаки строятся шаг за шагом на основе заданных разработчиком атрибутов и следуют логической последовательности [4, 5, 6, 7]. Совпадение сравниваемых полей может быть точным или частичным [5, 6]. В первом случае методы используют точное совпадение между некоторыми полями в событиях. Во втором – учитывается частичное сходство между рассматриваемыми атрибутами. В таких методах вычисляется коэффициент корреляции между событиями, и события помещаются вместе, если коэффициент выше определенного порога [7].

Цель *кластеризации* – выявить близкие группы событий. Обычно это делается посредством алгоритмов автоматической кластеризации. К этой категории относятся методы, применяющие алгоритм кластеризации для определения групп похожих действий. Эти группы или кластеры затем рассматриваются как потенциальные многоэтапные атаки. Сходство между следами, принадлежащих одному и тому же сценарию, должно быть выше, чем у следов, присущих другим сценариям [8].

Суть методов, основанных на *обнаружении аномалий*, заключаются в обучении систем защиты на наборах данных, очищенных от атак. Затем система рассматривает как угрозу последовательности, отличающиеся от нормального поведения. Далее выполняется сравнение сходства со всем базовым набором данных, а не только между элементами, составляющими сценарий. Результаты используются иначе, чем в других методах, основанных на сходстве: ищутся не сходства, а различия [9, 10]. Аномальное поведение не обязательно соответствует атаке. Частота ложных срабатываний может быть высокой, но методы обнаружения аномалий позволяют выявить ранее неизвестные атаки.

Основное преимущество методов на основе подобия: если процесс определения связи между трассировками событий выбран правильно, реализация будет простой и может возвращать неизвестные многоступенчатые атаки. Системы, реализующие эти методы, обычно имеют хорошую производительность. Однако выбор способа связывания следов является достаточно сложным процессом. Если процесс связывания остается простым – результаты будут содержать слишком много ложных срабатываний. Сложный процесс связывания, основанный на применении корреляционных матриц и использовании разных весов для каждого поля, может быть слишком трудоемким, чтобы охватить характеристики всего диапазона реальных многоступенчатых атак.

В методах *причинной корреляции* обнаружение атаки сосредоточено на структуре многоэтапных последовательностей атак и причинно-следственной связи между действиями атакующего.

«*Предпосылки и последствия*» – одно из направлений методов причинной корреляции. При таком подходе подразумевается, что каждое предупреждение имеет ряд предварительных условий, также называемых предварительными условиями и последствиями (или постусловиями). Предпосылки – это условия, которые необходимо создать для успешной атаки, а последствия – это возможные последствия атаки. Методы этой категории предполагают, что каждое возможное предупреждение имеет список известных связанных предпосылок и последствий. Оповещения об атаках объединяются в гипер-оповещения. Гипер-оповещения – это набор фактов, представленных предупреждениями, с одинаковыми предпосыл-

ками и последствиями. Затем гипер-предупреждения сопоставляются посредством автоматической идентификации предпосылок и последствий, возвращая последовательность атак, составляющих сценарий атаки [11, 12].

Статистический вывод – это процесс вывода из набора данных о распределении данных. Предполагается, что информация уже есть в наборе данных трассировок, но нужно знать, где искать. Методы этой категории работают с частотами действий и последовательностями действий. Статистическая модель автоматически извлекается из обучающего набора данных трассировок или из собственных данных, для которых выполняется процесс обнаружения. Полученная статистика служит для построения вероятностной модели, которую можно использовать для обнаружения и прогнозирования атак [13, 14, 15].

Методы *сопоставления моделей* предполагают, что каждая многошаговая атака следует определенной структуре. Данные методы моделируют эту структуру и пытаются найти последовательности, которые соответствуют этой структуре. Методы сопоставления моделей отличаются от методов на основе прецедентов, поскольку последние используют конкретные случаи реальных атак. Методы сопоставления моделей используют более высокий уровень абстракции, представляя шаблон и общие характеристики многоэтапной атаки [16].

У методов причинной корреляции есть важное преимущество: их процесс и результаты могут быть легко интерпретированы человеком-аналитиком. Они подчеркивают характер многоэтапных атак как последовательностей шагов, что на сегодняшний день является наиболее понятным представлением об этих атаках. Их гибкость позволяет вести поиск небольших вариаций известных атак (но не полностью неизвестных). По-прежнему может быть большое количество ложных срабатываний, но меньше, чем в методах, основанных на подобии, поскольку выдвигаются более безопасные гипотезы.

При использовании *структурного подхода* поступающие следы проецируются на модель сети, где можно предсказать будущие пути атаки [17, 18]. Приоритетная цель такого подхода – выявление неизвестных атак и прогнозирование путей уже начавшейся атаки.

Методы на основе *прецедентов* позволяют обнаруживать известные сценарии атак как ансамбли следов атак [19, 20, 21]. Явным преимуществом методов на основе прецедентов является то, что количество ложных срабатываний невелико. Однако если атаки нет в базе данных, она не обнаруживается, т. е. такие методы способны обнаруживать только известные многоступенчатые атаки.

В *смешанных методах* применяются несколько подходов, но ни один из них не выделяется среди других [22, 23]. При правильной реализации этих методов возможно сгладить недостатки отдельно взятых методов.

В статье была проведена структуризация подходов, используемых для обнаружения многошаговых атак, выделены положительные и негативные стороны каждого метода, а также приведены ссылки с актуальными разработками касаемо каждого метода.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science, Springer-Verlag. 2005. V. 3685. pp. 311–324.

2. 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. 4 (47). С. 5–27.

3. Navarro J., Deruyver A., Parrend P. A systematic survey on multi-step attack detection // Computers & Security. 2018. Vol. 76. pp. 214–249.

4. Chen C.-M., Guan D.-J., Huang Y.-Z., Ou Y.-H. Anomaly network intrusion detection using Hidden Markov Model // Int. J. of Innovative Comput. Inf. Control. 2016. No. 12. pp. 569–580.

5. Ebrahimi A., Zad Navin A. H., Mirnia K.M., Bahrbegi H., Ahrabi A.A.A. Automatic attack scenario discovering based on a new alert correlation method // 2011 IEEE International Systems Conference. 2011. pp. 52–58.

6. Wang C., Chen J., Cao W., Sun L., Sun H., Liu Y. Aurora-B and HDAC synergistically regulate survival and proliferation of lymphoma cell via AKT, mTOR and Notch pathways // European Journal of Pharmacology. 2016. Vol. 779. pp. 1–7.

7. Kawakani C., Barbon J., Miani R., Cukier M., Zarpelao B. Intrusion Alert Correlation to Support Security Management // Simposio brasileiro de sistemas de informação (SBSI). 2016. Vol. 12. pp. 313–320.

8. Friedberg I., Skopik F., Settanni G., Fiedler R. Combating advanced persistent threats: From network event correlation to incident detection // Computers & Security, 2015. Vol. 48. pp. 35–57.

9. Shin S., Lee S., Kim H., Kim K. Advanced probabilistic approach for network intrusion forecasting and detection // Expert Systems with Applications, 2013. Vol. 40, No. 1. pp. 315–322.

10. Pandey N., Gupta S., Leekha S., Zhou J. ACML: Capability Based Attack Modeling Language // 2008 The Fourth International Conference on Information Assurance and Security, 2008. pp. 147–154.

11. Alserhani F. A framework for multi-stage attack detection // 2013 Saudi International Electronics, Communications and Photonics Conference, 2013. pp. 1–6.

12. Lv Y., Xiang S., Geng J., Li Y., Xia C. An alert correlation algorithm based on the sequence pattern mining // 2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2015. pp. 1146–1151.

13. Li Y., Xue Y., Yao Y., Zhao X., Liu J., Zhang R. An attack pattern mining algorithm based on fuzzy logic and sequence pattern // 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), 2016. pp. 234–238.

14. Xuewei F., Dongxia W., Minhuan H., Xiaoxia S. An Approach of Discovering Causal Knowledge for Alert Correlating Based on Data Mining // 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing, 2014. pp. 57–62.

15. Holgado P., Villagrá V., Vazquez L. Real-time multistep attack prediction based on hidden markov models // IEEE Transactions on Dependable and Secure Computing. 2017. Vol. 17, No. 1. pp. 134–147.

16. Luo S., Wu J., Li J., Guo L. A multi-stage attack mitigation mechanism for software-defined home networks // IEEE Transactions on Consumer Electronics, 2016. Vol. 62, No. 2, pp. 200–207.

17. Luo Y., Szidarovszky F., Al-Nashif Y., Hariri S. A fictitious play-based response strategy for multistage intrusion defense systems // Security Comm. Networks, 2014. Vol 7. pp. 473–491.

18. Navarro J., Chavarriaga J. Using microsoft solver foundation to analyse feature models and configurations // 2016 8th Euro American Conference on Telematics and Information Systems (EATIS), 2016. pp. 1–8.

19. Jaeger D., Ussath M., Cheng F., Meinel C. Multi-step Attack Pattern Detection on Normalized Event Logs // IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015. pp. 390–398.

20. Giura P., Wang W. A Context-Based Detection Framework for Advanced Persistent Threats // 2012 International Conference on Cyber Security, 2012. pp. 69–74.

21. Shittu R. Mining intrusion detection alert logs to minimise false positives & gain attack insight: Unpublished Doctoral thesis, PhD / Shittu Ryaratt. London, 2016. 190 p.

22. Faraji Daneshgar F., Abbaspour, M. Extracting fuzzy attack patterns using an online fuzzy adaptive alert correlation framework // Security and Communication Networks, 2016. Vol. 9, No. 14. pp. 2245–2260.

23. Ahmadian R., Rasoolzadegan A. Causal knowledge analysis for detecting and modeling multi-step attacks // Security and Communication Networks, 2016. Vol. 9. No.18. pp. 6042–6065.

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

УДК 681.7
ГРНТИ 49.44.31

ИССЛЕДОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ЛИНИЙ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ НА БАЗЕ WDM И DWDM ТЕХНОЛОГИЙ

Б. Г. Ибрагимов, С. Р. Исмайлова, Э. М. Джафарова

Азербайджанский Технический Университет

Проанализированы показатели качества функционирования оптических телекоммуникационных систем, выполненных на основе волоконно-оптических систем передачи, использующих современные оптические технологии спектрального мультиплексирования по длине волны. На основе анализа существующих критериев эффективности функционирования волоконно-оптических систем передачи (ВОСП), выбраны показатели производительсти волоконно-оптических линий связи (ВОЛС) при оказании мультимедийных услуг на оптических транспортных сетях связи. В данной работе рассматриваются вопросы исследования производительности линий ВОСП на базе ВОЛС, использующие спектральные WDM (Wavelength Division Multiplexing) и DWDM (Dense WDM) технологии.

емкость линий связи, WDM, волоконно-оптическая линия связи, CWDM, волоконно-оптическая система передачи, длина волны, DWDM, производительность линий.

В настоящее время проблема интенсивного развития инфраструктуры цифровой экономики и формирования стратегических планов «Дорожной карты цифровизации» требует новых принципов и оптимальных подходов к построению высокоэффективных оптических телекоммуникационных систем на базе архитектурной концепции следующих поколений NGN и будущих сетей FN с повышенной пропускной способностью [1, 2, 3].

Данное направление развития переводит эти процессы из концептуальной в практическую плоскость реализации мероприятий для создания единого инфокоммуникационнного пространства и многооператорской среды, которые будут представлять пользователям мультимедийные услуги вторичных мультисервисных сетей связи общего пользования, сетей 5G/IMT-2020 и компьютерных сетей [4, 5].

Следует отметить, что вышеперечисленные направления, в первую очередь, охватывают вопросы оптической мультисервисной телекоммуникационной составляющей информационной инфраструктуры для развития цифровой экономики, которые позволяют решить одну из ключевых задач – создание единого инфокоммуникационного пространства, использующего

инновационные технологии волоконно-оптических сетей связи со спектральным разделением [2, 4, 5, 6, 7]. К ним относятся, прежде всего, технологии построения распределенных сетей связи как WDM (*Wavelength Division Multiplexing*), SDH (*Synchronous Digital Hierarchy*), SONET (*Synchronous Optical Network*), SDN (*Software Defined Networking*), NFV (*Network Functions Virtualization*), IMS (*Internet Protocol Multimedia Subsystem*), PON (*Passiv Optical Network*), CWDM (*Coarse* WDM) так и DWDM (*Dense* WDM).

На современном этапе в оптических телекоммуникационных системах используются технологии спектрального разделения WDM, CWDM (*Coarse* WDM), DWDM и HDWDM (Higher DWDM) системы, которые основываются на принципах волнового мультиплексирования с длиной волны $\lambda_i = (0,85,...,1,55)$ мкм, $i = \overline{1,n}$.

Проведенный анализ показал [3, 6, 8, 9], что одними из важных для критерия качества функционирования оптических телекоммуникационных систем выбраны показатели производительности линий ВОСП, которые отражают пропускные способности ВОЛС, состоящие из приемных оптических модулей (ПРОМ), волоконно-оптических кабелей (ВОК) и передающих оптических модулей (ПОМ).

Поэтому задача исследования показателей качества функционирования оптических телекоммуникационных систем как производительности линий ВОСП на базе перспективных оптических технологий спектрального разделения, битовых скоростных характеристик оптических средств ПРОМ, ВОК и ПОМ, угроза информационной безопасности ВОСП при передаче мультимедийных трафиков так и при оказании услуги «Triple Play services» и «Bandwith» является наиболее актуальной.

В работах [2, 3, 4, 5, 8, 10] проанализированы методы улучшения качества функционирования волоконно-оптических систем передачи на базе WDM&DWDM и CWDM технологий, определены передаточные характеристики волоконно-оптических линий связи.

В данной работе исследования посвящены решению проблемы анализа показателей качества связи и производительности линий ВОСП на базе ВОЛС, использующих эффективные технологии спектрального разделения оптического канала в волоконно-оптических сетях связи.

Теперь рассмотрим постановка задачи и анализ показателей емкости линий ВОЛС на базе мультиплексирования по длинам волны. На основе исследования установлено [3, 8, 9], что производительность линий волоконно-оптических систем передачи обеспечивает такие требуемые комплексные показатели как:

− емкости оптической системы, оптическое отношение сигнал-шум (OSNR) системы;

− полосы частот оптических спектральных каналов;

− защита информации от несанкционированных доступов;
− битовая скорость оптических средств;
− вероятность битовых ошибок приема оптических сигналов.

Эти показатели непосредственно оказывают влияние на качество функционирования волоконно-оптических сетей связи для гарантированного качества обслуживания QoS (*Quality of Service*) и мультимедийных приложений.

Системно-технический анализ показывает, что задача исследования показателей емкости WDM&DWDM системы на базе технологии спектрального разделения при использовании длины волны $\lambda_{i.1m} = (1.31,...,1.55)$ мкм, $i = \overline{1,n}$ еще полностью не решена [4, 7, 10, 11].

Емкость WDM&DWDM системы ВОСП на базе технологии спектрального разделения оптических каналов определяется следующей зависимостью:

$$E_B(\lambda_{i.1m}) = F[N_k(\lambda_{i.1m}), S(\lambda_i), V_b(\lambda_{i.1m})], \qquad i = \overline{1,n}, \qquad (1)$$

где $S(\lambda_i)$ – спектральные диапазоны оптических технологий волновым мультиплексированием по длине волны, где для передачи оптических сигналов используются множества спектральных диапазонов [3, 8]:

$$\text{C}(\lambda_i = 1.530,...,1565\ mkm),\ \text{S}(\lambda_i = 1.460,...,1.530\,mkm) \text{ и L } (\lambda_i = 1.565,...,1.625 mkm).$$

где $V_b(\lambda_{i.1m})$ – битовая скорость передачи оптических сигналов в каждом оптическом канале связи, *bit/s*;

$N_k(\lambda_{i.1m})$ – количество организуемых оптических каналов в ВОЛС на основе технологии спектрального разделения оптических каналов WDM&DWDM системы.

Функциональная зависимость (1) и проведенный анализ в [3] показали, что емкость WDM&DWDM и HDWDM системы можно наращивать, увеличивая как количество спектральных оптических каналов, так и битовую скорость передачи оптических сигналов в каждом канале связи.

Следует отметить, что в волоконно-оптических сетях связи оптические сигналы поступают от источника сообщений – от абонента (пользователя) по отдельным волокнам. Однако, передача оптических сигналов на основе WDM технологии производится по одному волокну при использовании разных длины волны, т. е. на разных несущих.

В зависимости от расстояния между несущими различают системы грубого мультиплексирования по длинам волны – CWDM и системы плотного мультиплексирования DWDM.

На базе выражения (1) рассмотрим емкости системы плотного мультиплексирования DWDM, где длина волны мультиплексирования $\lambda_i = 1,530, ..., 1,560\ mkm$. Емкость волоконно-оптических линий связи на базе спектральных DWDM технологий выражается следующим образом:

$$E_B(\lambda_{i.1m}) = N_k(\lambda_{i.1m}) \cdot V_b(\lambda_{i.1m}) \geq C_{\max}(\lambda_{i.1m}). \qquad (2)$$

Полученное выражение (2) характеризует пропускные способности волоконно-оптических систем передачи на базе технологии плотного мультиплексирования по длине волны и определяет емкости DWDM системы с использованием системы передачи спектрального диапазона $C(\lambda_{i.1m} \geq 1,530\, mkm)$.

Развитие и внедрение оптических спектральных технологий WDM, CWDM, DWDM и HDWDM позволяют на несколько порядков увеличить число спектральных каналов и скорость передачи в каждом канале связи. Среди этих технологий, наилучшим образом данные задачи решаются с помощью спектральных технологий мультиплексирования оптических каналов по длине волны DWDM системы [3], которые ориентируются на стандартное одномодовое волокно (SSMF, *Standart Single Mode Fiber*) или SM-волокно.

Число каналов организуемых на базе DWDM системы определяется отношением ширины полосы усиления оптического сигнала $\Delta\lambda_{i.1m}$ к ширине межканального интервала $\Delta\lambda_{i.k}$

$$N_k(\lambda_{i.1m}) = (\Delta\lambda_i / \Delta\lambda_k) \geq 1, \qquad i = \overline{1,n} \qquad (3)$$

Из (3) следует, что ширина полосы усиления зависит от типа усилителя оптического сигнала, а ширина межканального интервала определена частотным планом МСЭ-Т [3, 11]. Здесь, $\Delta f_k(\lambda_{i.1m}) = (50, 100, 200)$ ГГц. Если, в DWDM системе полоса частот $\Delta f_k(\lambda_{i.1m}) = 100$ ГГц , то ширина межканального интервала $\Delta\lambda_{k.1m} = 0,0008$ mkm, которому соответствует длина волны $\lambda_{i.1m} = 1,55\, mkm$.

Допустим, что $\Delta f_k(\lambda_{i.1m}) = 50$ ГГц при $\Delta\lambda_k = 0,00040$ mkm. Тогда, в межканальном интервале число спектральных каналов $N_k(\lambda_{i.1m})$ для С-диапозона $\lambda_i = (1,530, ..., 1,565)\, mkm$, ширина полосы усиления оптического сигнала $\Delta\lambda_i = 0,035 mkm$, равно $N_k(\lambda_{i.1m}) = 0,035 / 0,0004 = 87,5 \cong 88\ kanal$.

Однако, выявлено, что реально для DWDM системы из-за промежутка между полосами усиления оптического сигнала при использовании эрбиевых усилителей в (C+L) диапозоне используется $N_k(\lambda_{i.1m}) = 160$ каналов [3,

12]. Это соответствует емкости линий DWDM системы $E_B(\lambda_{i.1m}) = 16$ Тбит/с, где битовая скорость передачи оптических сигналов в каждом оптическом канале связи $V_b(\lambda_{i.1m}) = 100$ Гбит/с.

Результаты исследования показали, что одним из важных и перспективных показателей ВОСП на базе спектральных WDM, CWDM и DWDM технологий является производительность линий, который зависят от число спектральных каналов, емкости системы передачи, спектральный диапазон, а также пропускные способности с использованием спектрального волнового и частотного диапазонов.

Список используемых источников

1. Ефимушкин В. А., Козаченко Ю. М., Ледовских Т. В., Щербакова Е. Н. Будущий облик Единой сети электросвязь и Российской Федерации // Электросвязь. 2018. №10. С. 18–27.

2. Ибрагимов Б. Г., Джафарова Э. М. Показатели волоконно-оптических систем передачи с использованием перспективных технологий // Сборник трудов XIV Международной отраслевой научно-технической конференции «Технологии Информационного Общества» (18-19 марта 2020). МТУСИ, Москва. Том 1. ИД Медиа Паблишер, 2020. С. 43–44.

3. Листвин В. Н., Трещиков В. Н. DWDM–системы. М. : Техносфера, 2015. 256 с.

4. Ibrahimov B. G., Hasanov M. H. Research and analysis of indicators optical telecommunication networks based on PON, WDM and DWDM technology // 2020 International Conference «Engineering Management of Communication and Technology» IEEE Conference Record #49634, Vienna, Austria – Springer Schloessl. October 20-22, 2020. pp. 1–4.

5. Андреев В. А. и др. Направляющие системы электросвязи. М.: Горячая линия Телеком, 2010. 464 с.

6. Ибрагимов Б. Г., Мамедов И. М., Исмайлова С. Р. Исследование эффективности функционирования оптических телекоммуникационных сетей связи // Вестник компьютерных и информационных технологии. 2012. № 8. С. 3–7.

7. Портнов Э. Л. Волоконная оптика в телекоммуникациях. М.: Горячая линия – Телеком. 2018.392 с.

8. Ибрагимов Б. Г., Мамедов И. М. Эффективность волоконно-оптических линий связи с использованием WDM/DWDM технологий // Труды конференции «Телекомуникационные и вычислительныесистемы», Москва, МТУСИ, 2009. С. 179–180.

9. Chomez B. Planning Fiber Optic Networks. New-York: McGraw-Hill, 2009. 400 p.

10. Qiu Y., Chen S., Chen H. H., and Meng W. Visible light communications based on CDMA technology // IEEE Wireless Communications. 2018. 25 (2). pp. 178–185.

11. Ибрагимов Б. Г., Джафарова Э. М. Анализ передаточных, линейных и нелинейных эффектов в волоконно-оптических линиях передачи // Материалы XXIV-Международная НТК по «Современные средства связи», БГАС, Минск. 2019. С. 24–26.

12. Perlicki K., Wilczewski G. Fiber optics transmission for vehicle applications // Measurement Automation Monitoring. 2015. Vol. 61 (3). pp. 81–83.

УДК 004.056.55
ГРНТИ 81.93.29

АНАЛИЗ ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ ТЕХНОЛОГИИ СЕТЕВОЙ СТЕГАНОГРАФИИ

Б. Г. Ибрагимов[1], **К. М. Тахирова**[2]

[1]Азербайджанский Технический университет
[2]Военная Академия Вооруженных Сил Азербайджанской Республики

Проанализированы показателей информационной безопасности на базе технологии сетевой стеганографии при передаче полезного и служебного трафиков в мультисервисных телекоммуникационных сетях связи. С целью исследование информативных характеристик сетевой стеганографии приведена структурная схема физического процесса передачи секретного сообщения с использованием файла-контейнера. На основе исследование выбраны важные параметры информативные характеристики стеганографического система.

стеганография, полезный и служебный трафик, файл-контейнер, сокрытый пакет, цифровая стеганография.

В настоящее время использования современных информационных и компьютерных технологии в мультисервисных телекоммуникационных сетях при передаче, обработки и приема сообщений полезного и служебного трафиков появилась потребность в сокрытии как передаваемых данных, так и самого факта передачи информации. Именно этим вопросом занимается стеганография – наука о скрытной передаче любого вида информации [1, 2].

Однако, необходимость гарантированного качества ее обслуживания QoS требует нового подхода к созданию новых методов, технологий и средств криптозащиты информации от несанкционированного доступа. Это очень важна для применения сетевой стеганографии с целью обеспечения надежной и безопасной передачи информации смешанного типа [2, 3]. Кроме того, в связи с переходом к NGN (*Next Generation Network*) и FN (*Future Network*) появилась необходимость в сокрытии, как передаваемых данных, так и самого факта хранения и передачи сообщений полезного и служебного трафика.

Известно [1, 3], что стеганография – это наука о передаче некоторого секретного сообщения от отправителя (Алиса) к получателю (Боб) так, что сам факт передачи секретного сообщения должен оставаться скрытым от наблюдателя (Ева). В англоязычной литературе для методов и технологий скрытой передачи сообщения часто используется названия «data hiding», что

можно примерно перевести как «скрытие» или «сокрытие данных» (*Steqanogram packets*). Методы и технологии сетевой стеганографии позволяют не только скрытно передавать информации смешанного типа, но и решать задачи помехоустойчивой аутентификации, защиты информации от несанкционированного копирования, отслеживания распространения информации по мультисервисным сетям связи, поиска информации в мультимедийных базах данных.

Стоит отметить, что исследуемая система защиты информации должна обеспечивать свои функции даже при полной информированности противника о ее структуре и алгоритмах функционирования. Вся секретность системы защиты передаваемых сведений должна заключаться в ключе, то есть в предварительно – как правило разделенном между адресатами фрагменте информации [4, 5].

Учитывая выше изложенное, в данной работе рассматриваются задачи исследования и анализ показателей информационной безопасности на базе технологии сетевой стеганографии, а также приводится аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности в мультисервисных телекоммуникационных сетях.

Следует отметить, что информационный и служебный обмен трафика в мультисервисных телекоммуникационных сетях на базе методов и технологий сетевой стеганографии открывает массу разнообразных возможностей для скрытой связи с целью улучшения показателей системы защиты информации. Передаваемые полезного и служебного трафика с использованием протокола TCP/IP (*Transport Control Protocol/Internet Protocol*) и протокола установления сеанса SIP (*Session Initiation Protocol*) могут скрываться не только в обычных открытых сообщениях, как в традиционной стеганографии, но и в элементах управления протоколов сетей связи и в результатах изменения логики протокола [1, 4].

Однако, сетевая стеганография в качестве носителей секретных пакетов использует сетевые протоколы эталонной модели OSI, которые являются сетевой моделью взаимодействия открытых систем. Таким образом, они представляют в общем виде семейство методов модификации данных в заголовках сетевых протоколов RTR (*Real-time Transport Protocol*), SCTP (*Stream Control Transport Protocol*) и UDP. В простом варианте пакет состоит из двух полей – для передачи служебного и полезного трафиков.

В общем виде длина общего поля передаваемого пакета $L^n_{\text{об}}(\lambda_i)$ определяется как:

$$L^n_{\text{об}}(\lambda) = \sum_{i=1}^{n} [L^n_c(\lambda_{i.c}) + L^n_n(\lambda_{i.n})], \quad i = 1,2,3,...,n \qquad (1)$$

где $L^n_c(\lambda_{i.c})$ – длина поля служебного пакета с интенсивностью $\lambda_{i.c}$, $i = \overline{1,n}$;

$L^{n}_{i.n}(\lambda_{i.n})$ – длина поля полезной нагрузки пакетов (информационного пакета) с интенсивностью $\lambda_{i.n}$, $i=\overline{1,n}$.

В полях полезной нагрузки пакетов изменения структуры передачи пакетов в том или ином сетевом протоколе. Общей чертой всех методов сетевой стеганографии является создание с их помощью скрытых каналов передачи информации в любом открытом канале, в котором есть некая избыточность $R_{из}(t)$. В этой связи приоритетный характер приобретает исследование вопросов информационной безопасности.

В данном случае стеганография как технология реализует скрытия секретных данных в различных файлах: текстовых, изображениях, видео, аудио и сетевых пакетах. Внедрение секретной информации осуществляется путем изменения исходного файла-контейнера.

На рис. представлена структурная схема физического процесса передачи секретного сообщения с использованием файла-контейнера.

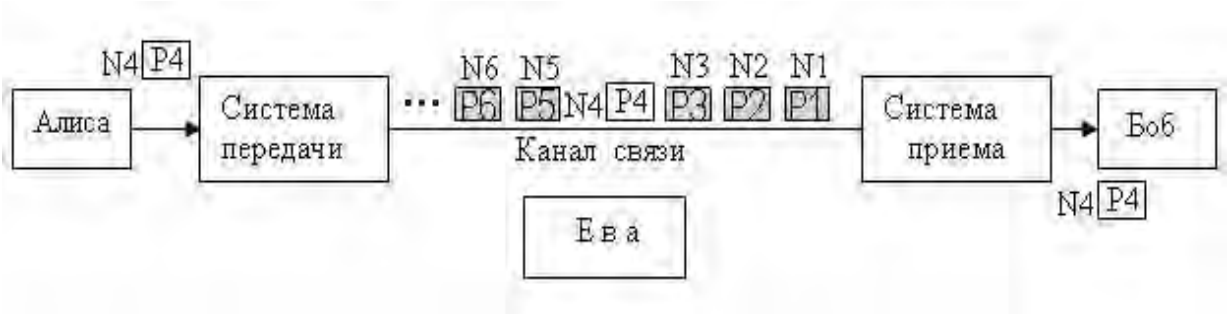


Рис. Структурная схема физического процесса передачи секретного сообщения с использованием файла-контейнера

Структурная схема физического процесса передачи секретного сообщения с использованием файла-контейнера состоит из системы отправителя, канала связи и системы приема. Примером такой системы передачи является упрощенная схема стеганографической системы.

Алгоритм работы стеганографической системы заключается в следующем. Из упрощенной схемы видно, что Алиса среди пакетов, т. е. файла-контейнера для скрытия данных, в качестве стеганограм использовала $N4$. Это заранее фиксированный пакет, который сообщен Бобу. Система передачи отправляет все пакеты через каналы связи, в том числе и пакет $N4$. На выходе канала связи система приема принимает все пакеты. Приемной стороне сообщено, что стеганограм – пакетом является пакет $N4$. В результате Боб выбирает только пакет $N4$.

На основе алгоритма физического процесса передачи секретного сообщения с использованием файла-контейнера, выражение (1) примет следующий вид:

$$L^n_{\text{об}}(\lambda) = \sum_{i=1}^{n}[L^n_c(\lambda_{i.c}) + \ell^p_{st}(\lambda_{i.st}) + L^n_n(\lambda_{i.n})], \quad i = \overline{1,n} \tag{2}$$

где $\ell^p_{st}(\lambda_i)$ – длина поля стеганографической нагрузки пакетов – сокрытого пакета с интенсивностью $\lambda_{i.st}$, $i = \overline{1,n}$.

Учитывая составные компоненты вектора сетевого стеганография в системе передачи полезного и служебного трафика, функционально описывается следующей зависимостью:

$$Q^k_{st}(\lambda_i) = W[P_{st}(\lambda_i, t,), C_{\max}(\lambda_i), I_{\text{н.б}}(\lambda_i), R_a(t)], \quad i = \overline{1,n}, \tag{3}$$

где $P_{st}(\lambda_i, t)$ – вероятность потерь пакетов стеганографического система с учетом скорости λ_i при передаче *i*-го потока пакетов полезного и служебного трафиков;

$C_{\max}(\lambda_i)$ – максимальная величина пропускная способность аппаратно-программных комплексов и терминальных средств стеганографического система с учетом скорости поступления входящего потока λ_i при передаче *i*-го потока пакетов полезного и служебного трафиков;

$I_{\text{нб}}(\lambda_i)$ – функция, учитывающие показателей система информационной безопасности с учетом интенсивности трафик λ_i;

$R_{\text{из}}(t)$ – коэффициент избыточности источника сообщения стеганографического система в момент времени *t* и определяется следующим функциональным зависимостью:

$$R_{\text{из}}(t) = E[H_{\text{сс}}(t, \lambda_i), H^{\text{сс}}_{\max}(t, \lambda_i)] \le 1, \tag{4}$$

где $H^{\text{сс}}_{\max}(t, \lambda_i)$ – максимальная величина энтропия источника сообщения стеганографического система в момент времени *t*;

$H_{\text{сс}}(t, \lambda_i)$ – энтропия источника сообщения стеганографического система в момент времени *t* и равно

$$H_{\text{сс}}(t, \lambda_i) = -\sum_{i=1}^{n} P(\lambda_i)\log P(\lambda_i), \tag{5}$$

В данном случае, предполагаем, что кодовые пакеты на входе λ_i, $i = 1, 2, ..., n$ не зависимы, а источник определен вероятностями $P(\lambda_i)$.

Как показаны в (4) и (5) энтропия источника сообщений стеганографического система, в основном определяется априорными вероятностями $P(\lambda_i)$ реализации этих сообщений, причем

$$H_{\text{cc}}(t,\lambda_i) \le H_{\max}^{\text{cc}}(t,\lambda_i) = \log n. \quad (6)$$

Выражения (1),…, (6) определяют сущность рассматриваемого нового подхода с целью анализа показателей аппаратно-программных комлексов стеганографического система, использующие ресурсов инновационных сетевых технологий при передаче стеганографического, полезного и служебного трафиков.

Реализация данной вышеизложенной задачи невозможна без разработки способов противодействия информационным атакам. Выявление и классификация угроз предусматривает изучение современных механизмов скрытой передачи информации. Одним из направлений, занимающихся исследованиями в этой области, является компьютерная стеганография [3, 4, 5].

Из вышепроведенного исследование видно, что аппаратно-программных комлексов стеганографического система может быть рассмотрена как система телекоммуникации [2, 5]. Основы данной системы является цифровой стеганографии, которое можно выделить две причины популярности исследований в области стеганографии в настоящее время:

− ограничение на использование методы криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Данная причина повлекла за собой большое количество исследований в духе классической стеганографии, то есть скрытия факта передачи информации.

− вторая – еще более многочисленные работы в области так называемых водяных знаков. Цифровой водяной знак (ЦВЗ) является специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом контролировать его использование.

Один из наиболее эффективных технических средств защиты мультимедийной информации и заключается во встраивании в защищаемый объект невидимых меток – ЦВЗ.

Исследования показывает, что цифровая стеганография в основном включает в себя следующие направления:

- Встраивание информации с целью ее скрытой передачи;
- Встраивание цифровых водяных знаков ЦВЗ – Watermarking;
- Встраивание идентификационных номеров – Fingerprinting;
- Встраивание заголовков – Captioning.

Учитывая основные направления цифрового стеганография, алгоритм встраивания ЦВЗ состоит из трех основных этапов: 1) генерации ЦВЗ, 2) встраивания ЦВЗ в кодере и 3) обнаружения ЦВЗ в детекторе.

Рассматриваемые алгоритмы стеганографического сокрытия информации обычно основаны на замещении шумовой составляющей цифрового сообщения некоторым тайным сообщением. Такое цифровое сообщение обычно называют контейнером, а биты, в которые происходит встраивание – собственными битами контейнера. Тайное сообщение называют встраиваемым.

Однако, сокрытие сообщение из собственных битов контейнера должно быть достаточно разнообразным, чтобы его небольшое изменение не было заметным. В качестве собственных битов контейнера обычно используются младшие биты некоторых неточных значений. При этом основной интерес при стеганографическом сокрытии сообщений представляет устойчивость алгоритма сокрытия к различного вида атакам.

В данном варианте, одним из значимых событий в последних лет стеганографического система следует считать открытие случайно-подобных процессов, которые также называются хаотическими детерминированным процессами.

Таким образом, в результате исследования и анализа показателей информационной безопасности на базе технологии сетевой стеганографии выбраны важные параметры информативные характеристики стеганографического система.

Список используемых источников

1. Шелухин О. И., Канаев С. Д. Стеганография. Алгоритмы и программная реализация / Под ред. профессора О. И.Шелухин. М.: Горячая линия –Телеком, 2018. 592 с.

2. Ибрагимов Б. Г., Тахирова К. М. Некоторые вопросы защиты информации в системе телекоммуникации с использованием цифровой стеганографии // Материалы Международной НТК – Инновационные технологии в телекоммуникации. Баку: АзТУ, 2019. С. 30–32.

3. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. 2-е изд. М.: Горячая линия – Телеком, 2020. 232 с.

4. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет // Технологический институт Южного федерального университета. 2013. С. 3–7.

5. Довгаль В. М., Гордиенко В. В., Елагин В. В. Методы и технологии подготовки защищенных от подделки электронных документов // Телекоммуникации. 2001. № 4. С. 43–48.

УДК 621.391.64
ГРНТИ 49.29.14

ВЛИЯНИЕ НЕКОТОРЫХ ХАРАКТЕРИСТИК СРЕДЫ ПРИ ПЕРЕДАЧЕ ОПТИЧЕСКИХ СИГНАЛОВ В ВОСП

В. С. Иванов, Б. К. Никитин, А. Н. Сергеев

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

Увеличение объёмов передаваемой информации приводит к необходимости учета характеристик оптической среды передачи, играющей основную роль в трансляции сигналов. Особенно важным такой учет становится при увеличении мощности отдельных передаваемых каналов и, соответственно, суммарной мощности группового сигнала. В статье рассматривается влияние показателя преломления на сигнал, передаваемый в оптической среде.

показатель преломления, нелинейный показатель преломления, фазовая самомодуляция, фазовая кросс-модуляция, дисперсия групповых скоростей.

Характеристики среды передачи играют определяющую роль в работе систем передачи по доставке сигналов из одной точки в другую. Их влияние определяет, как длину ВОЛС, что особенно актуально при проектировании протяжённых линий, так и скорость передачи в длинных и в коротких линиях. Ввиду обширности темы в этой статье будет рассмотрено влияние характеристик кварцевого оптического волокна, максимально применяемого в настоящее время.

Понятно, что существует определённый набор оптических волокон (стандартных и нестандартных) и приёмо-передающих устройств (таких, как, например, мультиплексоры), комбинируя технические характеристики которых всегда можно составить ВОЛП с требуемыми параметрами. Однако такой подход чаще всего займёт много времени и не всегда приведёт к желаемому результату. При этом нельзя забывать, что реальная ВОЛП предназначена для работы в условиях активного воздействия агрессивной среды и должна сохранять свои возможности по трансляции сигналов в течение достаточно продолжительного времени, обычно не менее 10 лет. Кроме внешних воздействий ВОСП должна обладать способностью устойчивости к влиянию внутренних процессов, сопровождающих её функционирование и иметь возможность для работы без ухудшения качества передачи при увеличении скорости, связанной с явной тенденцией роста передаваемого объёма информации и предоставления новых услуг связи.

Какие же основные характеристики среды влияют на работу волоконно-оптических систем передачи? Для одноканальных систем это коэффициент затухания, модовая и хроматическая дисперсии, поляризационно-модовая дисперсия, поляризационно-зависимые потери и дисперсия групповых скоростей (ДГС), связанная с дифференциальной групповой задержкой спектральных и модовых составляющих сигнала. Понятия, вроде бы несложные, если не углубляться в детали. Такая относительная «простота» характерна только лишь для одноканальных систем. Как только передаваемые объёмы информации увеличиваются до предельных возможностей систем, основанных на синхронной цифровой иерархии (SDH), приходится делать выбор в пользу применения новых технологий. В качестве основной технологии, внедряемой, в том числе, и в системах абонентского доступа, служит способ передачи множества сигналов в одном волокне при использовании систем передачи, основанных на спектральном разделении каналов. При этом для компенсации потерь мощности, которые весьма высоки в таких системах, и увеличения перекрываемого расстояния приходится использовать волоконно-оптические усилители. И тут все особенности используемой среды всплывают во всей своей красоте, ограничивая великолепные показатели внедряемых приёмо-передающих устройств.

Надо заметить, что с увеличением числа оптических каналов растет и общая мощность группового сигнала, вводимого в направляющую систему. К чему это ведёт? К проявлению эффекта Керра (изменения значения показателя преломления оптического материала пропорционально квадрату напряженности приложенного электрического поля), то есть к тому, что легко прогнозируемая среда передачи становится непредсказуемой в своей главной характеристике – показателе преломления. Он становится нелинейным, и приводит к появлению нелинейных эффектов, оказывающих крайне негативное воздействие на работу ВОЛП. В результате происходит уширение их спектра, появляются новые спектральные составляющие, в том числе и внутри рабочих каналов, возникают изменения фазы, джиттер и другие неприятные явления, приводящие в итоге к увеличению коэффициента ошибок в приёмном устройстве терминального или транзитного мультиплексора [1]. А если к тому же вспомнить, что значение показателя преломления связано с длиной волны передаваемого излучения – а передавать иногда приходится в широком спектральном диапазоне – то и вся картина становится крайне сложной и запутанной.

Увеличение мощности группового сигнала приводит и к другой группе эффектов, которые основаны на рассеянии передаваемого излучения. Такое рассеяние может быть линейным как, например, эффект Тиндаля, или нелинейным, таким, как рассеяние Мандельштама-Бриллюна или вынужденное комбинационное рассеяние, часто называемое рассеянием Рамана. Если рассмотреть первое явление, то окажется, что интенсивность рассеянного света

(рассеяние Рэлея), и, соответственно, потери, вызванные данным явлением обратно пропорциональны длине волны излучения, точнее, четвёртой ее степени. А поскольку при передаче в широком спектре большого числа каналов присутствуют многие длины волн, то и для разных каналов рассеяние Рэлея окажется разным [2]. Этот вид рассеяния связан с тем, что стекло оптического волокна является оптически неоднородной средой, то есть средой, показатель преломления которой не остаётся постоянным. За счёт флуктуаций он изменяется от точки к точке по расстоянию. Рассеяние Рэлея присутствует в любой оптической среде и приводит к уменьшению мощности сигнала в процессе передачи. Такое уменьшение мощности описывается законом Бугера-Ламберта [2]. Можно сравнить величину потерь на длине волны 1 470 нм и на 1 610 нм и убедиться, что интенсивность рассеянного света и связанные с ней потери из-за рассеяния Рэлея на длине волны 1 470 нм приблизительно в 1,5 раза или на 50 % больше. Если рассмотреть полный диапазон 1 270–1 610 нм, то окажется, что разница потерь составляет уже 2,5 раза, то есть, затухание сигналов в разных каналах значительно отличается. Если же учесть, что в стандартном одномодовом волокне коэффициент затухания на длине волны 1 550 нм составляет 0,2 дБ/км, то несложно оценить и коэффициент затухания на любой другой длине волны.

Несколько сложнее рассчитать поведение системы при нелинейном показателе преломления. Требования действующих нормативно-технических документов, инструкций и приказов разрешают проводить расчёт исходя из заранее ожидаемых норм, приводимых в виде чисел или расчётных формул. Это облегчает расчёт системы для работы в телекоммуникационных приложениях, но не дает ответа в нестандартных случаях. К таким случаям можно отнести расчёт распределённых по длине или в пространстве волоконно-оптических датчиков, многие из которых строятся на исследовании нелинейных изменений показателя преломления при воздействии контролируемого параметра на проходящее мощное оптическое излучение. В этом случае точное знание поведения системы, подтверждённое соответствующими расчётами, является крайне необходимым. Поскольку данный доклад ограничивается только системами передачи для телекоммуникаций, то вопросы, связанные с точными измерениями в распределенных системах мониторинга и контроля, останутся за его рамками.

Основной задачей телекоммуникаций является увеличение произведения $L*B$, где L – расстояние, на которое осуществляется передачи информации, а B – скорость передачи. Если сказать проще, то главное – это передать большой объём информации на максимально возможное расстояние. Если рассмотреть такую задачу с точки зрения возможностей среды передачи, то главным становится борьба за уменьшение потерь в линии и устранение влияния различных видов дисперсии передаваемого сигнала. Квантовый

предел потерь определяется законом Рэлея, действующим в пространственном измерении для одной спектральной составляющей. Дисперсия же связана с расширенным и более глубоким пониманием этого закона, и проявляется как в пространственном измерении, так и во времени [3].

Ниже приведена формула для оценки интенсивности рассеянного света, в которую косвенно входит закон Рэлея:

$$I_\vartheta = c\frac{N_0 V^2}{R^2\lambda^4} I_0(1+\cos^2\vartheta),$$

где V – объём одной частицы,

N_0 – число частиц в единице объёма среды,

R – расстояние от рассеивающего объёма до точки наблюдения,

λ – длина волны света,

I_0 – интенсивность падающего света,

c – коэффициент, зависящий от степени неоднородности среды, то есть от показателей преломления рассеивающих частиц и той среды, в которой они находятся. Отсюда видно, что при прохождении света через оптически неоднородную среду в рассеянном излучении преобладают коротковолновые составляющие, а в проходящем свете – длинноволновые [4].

Зависимость показателя преломления от интенсивности проходящего сигнала приводит к возникновению эффекта фазовой самомодуляции, при котором сигнал начинает влиять на своё фазовое положение, изменение фазы при этом:

$$\varphi(t) = \omega_0 t - \frac{2\pi}{\lambda_0} n(I) L,$$

где λ_0 – длина волны в вакууме,

L – расстояние, пройденное импульсом. Согласно эффекту Керра, при распространении излучения коэффициент преломления в каждой точке среды будет функцией интенсивности в этой точке:

$$n(I) = n_0 + n_2 \cdot I,$$

где n_0 – линейный показатель преломления,

n_2 – нелинейный показатель преломления второго порядка,

I – интенсивность излучения.

В результате действия этого эффекта проходящее оптическое излучение получает фазовый сдвиг, а импульсы уширяются по спектру и изменяются по длительности. В итоге спектр частот, составляющих передний фронт импульса, смещается в длинноволновую область, а спектр заднего

фронта смещается в коротковолновую область, то есть передний фронт растягивается, задний сокращается во времени, а спектральный состав всего импульса увеличивается. Вследствие того, что одновременно передается много длин волн, расстояние между отдельными каналами изменяется, и частотный канальный план системы со спектральным разделением нарушается. В системах с очень малым шагом между каналами ФСМ может привести к интерференции между соседними каналами.

Второй по нежелательности эффект вызван действием фазовой кросс-модуляции. Фазовая кросс-модуляция (ФКМ) всегда сопровождается фазовой самомодуляцией и возникает из-за того, что эффективный показатель преломления какой-либо волны зависит не только от интенсивности самой этой волны, но и от интенсивности других волн, распространяющихся с ней совместно. Отсюда можно рассматривать две причины возникновения ФКМ: 1) из-за взаимодействия волн, имеющих разные частоты; 2) из-за связи между компонентами вектора поляризации одной волны [1].

Первая причина возникновения ФКМ заключается в том, что показатель преломления оптической волны зависит не только от интенсивности самой волны, но также и от интенсивности других волн, распространяющихся вместе с данной волной.

$$\Delta n_j \cong n_2 \left(\left| E_j \right|^2 + 2 \left| E_{3-j} \right|^2 \right).$$

Так как волна распространяется по световоду, она приобретает зависящую от интенсивности нелинейную фазу:

$$\phi_j^{NL} = \frac{\omega_j z n_2}{c} \left[\left| E_j \right|^2 + 2 \left| E_{3-j} \right|^2 \right],$$

где j = 1 или 2. Первое слагаемое отвечает за ФСМ. Второе возникает из-за фазовой модуляции одной волны другой волной, распространяющейся вместе с ней, и отвечает за ФКМ. Коэффициент 2 в правой части показывает, что ФКМ в 2 раза эффективнее ФСМ при той же интенсивности.

Вторая причина ФКМ заключается в том, что компоненты вектора поляризации одной и той же волны имеют разные нелинейные значения показателей преломления и приводят к различному влиянию их друг на друга:

$$\Delta n_x = n_2 \left(|E_x|^2 + \frac{2}{3} \left| E_y \right|^2 \right),$$

$$\Delta n_y = n_2 \left(\left| E_y \right|^2 + \frac{2}{3} |E_x|^2 \right),$$

где Δn_x и Δn_y, – изменение показателей преломления ортогональных составляющих излучения, вызванное нелинейными эффектами [2].

ФКМ между двумя поляризационными компонентами одной волны менее эффективна, чем между двумя волнами на различных частотах, так как она включает коэффициент 2/3, а не 2. Но нелинейная связь между компонентами поля E_x и E_y, вызванная ФКМ, создает нелинейное двулучепреломление, которое изменяет состояние поляризации, если входное излучение эллиптически поляризовано. Это явление называется вращением эллипса поляризации и приводит к частотным сдвигам, известным под названием «чирп», т. е. смещению положения импульса в результате изменений в групповой скорости. Кроме того, ФКМ вызывает флуктуации амплитуды сигнала.

Список используемых источников

1. Агравал Г. Нелинейная волоконная оптика. М.: Мир, 1996, 325 с.
2. Агравал Г. Применение нелинейной волоконной оптики. Учебное пособие. СПб.: Издательство «Лань», 2011. 592 с.
3. Глаголев С. Ф., Иванов В. С., Кочановский Л. Н. Физические основы оптических направляющих систем. Учебное пособие. СПб.: СПбГУТ, 2008. 158 с.
4. Снайдер А., Лав Дж. Теория оптических волноводов. М.: «Радио и связь», 1987. 656 с.

УДК 004.051
ГРНТИ 50.41.23

АНАЛИЗ МЕТОДОВ БАЛАНСИРОВКИ НАГРУЗКИ СЕТЕВОЙ ПОДСИСТЕМЫ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ

К. Э. Иванов, А. А. Швидкий

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

Индустрия информационных технологий в направлении облачных технологий развивается активно, с каждым днем растет количество приложений и пользователей. Ввиду такого развития становится актуальным вопрос балансировки нагрузки в облачной инфраструктуре. Данная статья ставит своей целью рассмотреть существующие на сегодня подходы к балансировке трафика на различных уровнях и сравнить популярные программные решения для реализации в облачной инфраструктуре.

балансировка нагрузки, программная балансировка нагрузки, облачная инфраструктура.

Балансировка нагрузки в облаке полезна с точки зрения отказоустойчивости, а также повышает производительность инфраструктуры [1]. Отказоустойчивость проявляется при возникновении неисправностей на узле, увеличение производительности позволяет работать с большим количеством узлов одновременно.

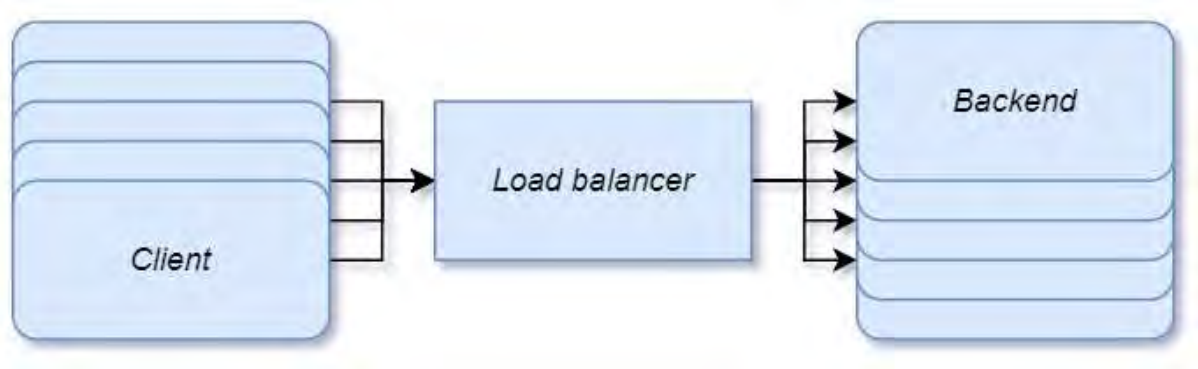


Рис. 1. Схема балансировки нагрузки

Упрощенная схема балансировки (рис. 1) показывает, что клиент запрашивает ресурс с бэкенда, а балансировщик должен обеспечить выполнение и упрощение запроса для клиента, путем решения таких задач: обнаружение сервисов, проверка состояний и непосредственно балансировка.

Обнаружение сервисов является функцией балансировщика нагрузки, позволяющей определить способ взаимодействия с бэкендом.

Проверка состояния позволяет понять к каким бэкендам можно обратиться.

Балансировка осуществляет распределение запросов среди доступных бэкендов и определяет какие именно алгоритмы для этого необходимы.

Использование балансировки в реализуемой системе дает ряд следующих преимуществ:

Устойчивость к отказам – за счёт возможности увеличения количества бэкенд-серверов;

Снижение стоимости и улучшение производительности – при помощи разбиения системы на несколько зон и регионов.

Абстрактность имен – это реализация заранее определенного механизма, когда клиенту не нужно знать о всех бэкендах, а процедура разрешения имён направляется к балансировщику.

Балансировка нагрузки осуществляется на нескольких уровнях модели OSI [2]: сетевой, транспортный и прикладной.

Балансировка нагрузки на сетевом (3) уровне позволяет решить задачу, в которой каждый отдельный IP-адрес сервера отвечают различные физические машины. Манипуляции непосредственно касаются протокола-IP, а балансировка имеет большое количество разнообразных способов, таких как:

- DNS – балансировка, когда на одно доменное имя предусматривается несколько IP-адресов и выбор сервера для обслуживания клиента осуществляется с помощью алгоритма перебора (*Round Robin*);
- Создание NLB-кластера, подразумевает объединение серверов в кластер, который состоит из вычислительных и входных узлов;
- Балансировка по IP с использованием дополнительного маршрутизатора;
- Балансировка на основе территориальной принадлежности, когда два одинаковых сервиса с одинаковыми адресами располагаются в разных регионах.

На сетевом уровне сессия происходит между бэкенд-сервером и клиентом, роль балансировщика состоит в решении – на какой из серверов передавать пакеты.

Балансировка на транспортном (4) уровне реализуется следующим образом: Клиент создает соединение с самим балансировщиком, информация о клиенте передается во вспомогательных заголовках и данных, когда балансировщик связывается с сервером. На этом уровне используются TCP/UDP – подключения и сессии.

Балансировка на прикладном (7) уровне происходит путем анализа запросов клиента. Балансировщик перенаправляет запрос на сервер на основании проанализированных данных о содержании запроса. На данном уровне происходят манипуляции с HTTP-трафиком и его подуровнями.

Для сравнения программных балансировщиков необходимо выделить их основные свойства: определение сервисов, проверка состояния, продвинутая балансировка, stiki-сессии, TLS-прерывание, прозрачность процесса, безопасность и разрешение последствий DoS, конфигурация и управляемость, поддержка протоколов, динамическая конфигурация, расширяемость.

Одними из самых известных программных балансировщиков нагрузки на сегодня являются HAProxy и Nginx. Оба обладают топологией с побочным прокси (рис. 2.), т. е. имеют встроенную клиентскую библиотеку, что немного увеличивает задержку при переходе между процессами, но упрощает настройку и описание алгоритмов взаимодействия.

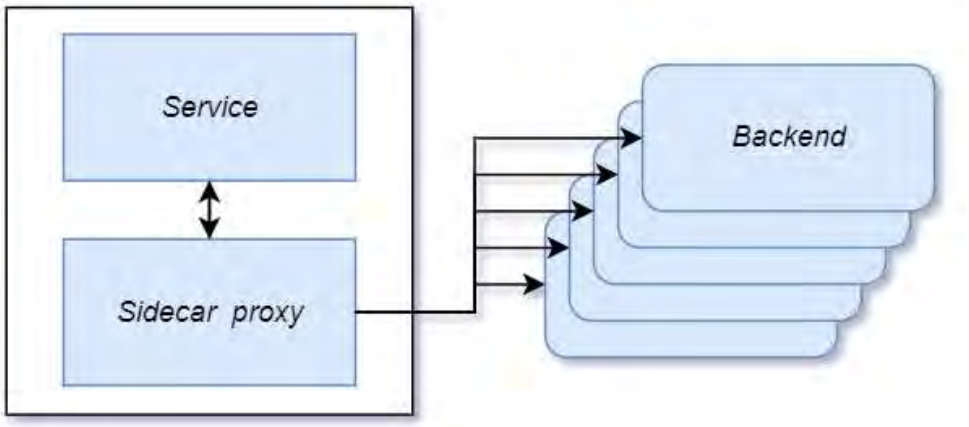


Рис. 2. Топология балансировки с побочным прокси.

HAProxy – является бесплатным, быстрым и надежным балансировщиком нагрузки с открытым исходным кодом, обеспечивающим высокую доступность, балансировку нагрузки и прокси для приложений на основе TCP и HTTP. Список возможностей HAProxy включает в себя [3, 4]:

- TCP-проксирование;
- обратный прокси сервер-HTTP;
- терминатор / инициатор / загрузчик SSL;
- нормализация TCP-трафика;
- нормализация HTTP-трафика;
- переключение на основе содержимого;
- балансировку нагрузки на сервере;
- регулирование трафика;
- защиту от DDoS-атак злоупотреблений службами;
- точку наблюдения для устранения неполадок в сети;
- загрузку сжатия HTTP;
- кэширующий прокси;
- шлюз FastCGI.

Nginx – это веб-сервер с открытым исходным кодом, обратный прокси-сервер, почтовый прокси-сервер, а также TCP/UDP прокси-сервер общего назначения. Основными функциями Nginx являются [5, 6]:

- обслуживание статических запросов, индексных файлов, автоматическое создание списка файлов, кэш дескрипторов открытых файлов;
- акселерированное обратное проксирование с кэшированием;
- акселерированная поддержка FastCGI, uwsgi, SCGI и memcached серверов с кэшированием;
- распределение нагрузки и отказоустойчивость;

− модульность, фильтры, в том числе сжатие (gzip), byte-ranges (докачка), chunked ответы, XSLT-фильтр, SSI-фильтр, преобразование изображений; несколько подзапросов на одной странице, обрабатываемые в SSI-фильтре через прокси или FastCGI/uwsgi/SCGI, выполняются параллельно;

− поддержка SSL и расширения TLS SNI;

− поддержка HTTP/2 с приоритизацией на основе весов и зависимостей.

Существует расширение Nginx до версии plus. Nginx plus предоставляет возможности централизованного мониторинга, защиты приложений и включает в себя внушительный список модулей расширяющих возможности приложения [6].

Различие обычной версии Nginx от коммерческой прослеживается на примере работы с неисправными бэкенд-серверами: если сервер перегружен, то он отдает неправильные ответы, но они не приходят и запросы на неисправный сервер будут продолжать поступать. Сервер исключается из списка только когда полностью перестает отвечать. В Nginx plus при помощи модуля upstream эта проблема решается путем совершения периодических проверок работоспособности серверов в группе.

По сравнению с Nginx в HAProxy предусмотрена возможность отслеживания детализированной статистики (рис. 3). В Nginx мониторинг доступен с инструментом Nginx Instance Manager, который входит в Nginx plus [6].

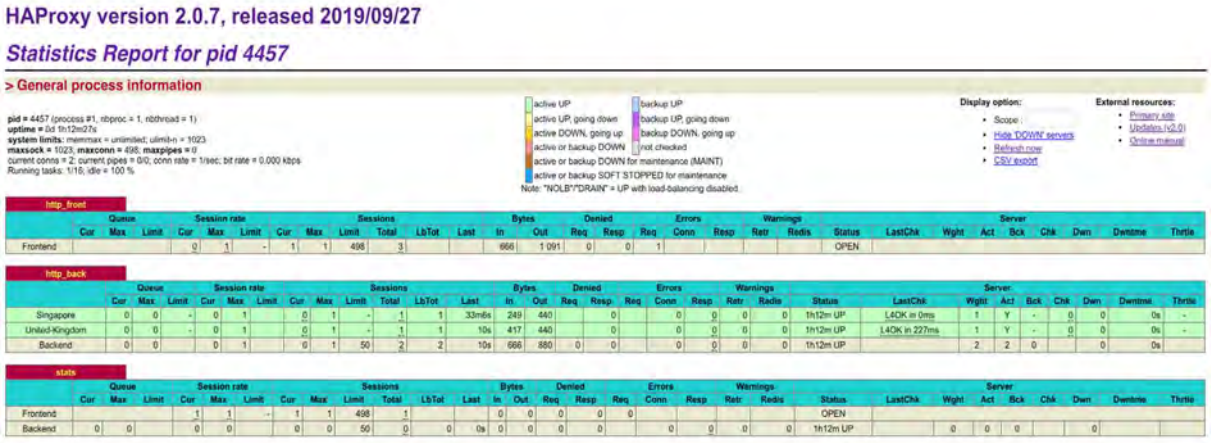


Рис. 3. Страница статистики HAProxy

Несмотря на то, что в Nginx отсутствует встроенный мониторинг, возможность экспорта статистики во внешние системы мониторинга на нем реализована, как и у HAProxy [3, 4].

В HAProxy отсутствует балансировка UPD-трафика. В отличии от Nginx, в нем не реализована балансировка на основе пакетов, поэтому HAProxy не будет видеть ни IP-пакеты, ни датаграммы UDP, не будет выполнять преобразование сетевых адресов и DSR [3].

Что касается доступности, то оба решения предоставляют большинство необходимых для балансировки нагрузки возможностей в бесплатной версии, однако по сравнению с HAProxy у Nginx функционал меньше.

Возможность расширения плагинами является важным аспектом, поскольку предполагает возможность усовершенствования, не прибегая к вмешательству в работу системы. В Nginx такая возможность предусмотрена при помощи инструментов и сервисов.

Исходя из описанных возможностей и недостатков систем, сравнение сводится к такому списку показателей (табл.):

− какое из приложений легче отслеживать;
− существующие различия в возможностях балансировки трафика;
− что более доступно;
− как приложения проявляют себя при возникновении неисправностей;
− возможности расширения.

ТАБЛИЦА. Сравнение параметров HAProxy и Nginx

Параметр\Наименование	HAProxy	Nginx
Встроенное средство мониторинга	Да	Нет
Экспорт статистики во внешние системы мониторинга	Да	Да
Балансировка UDP-траффика	Нет	Да
Доступность	Да	Да
Работа с перегрузками и неисправностями	Да	Да
Возможность расширения плагинами	Нет	Да

HAProxy поставляется с большинством основных дистрибутивов Linux и часто развертывается по умолчанию на облачных платформах, он подходит для сформированной и стабильной облачной инфраструктуры, поскольку предоставляет отлаженную работу, высокий уровень гарантий безопасности и без проблем отвечает основным требованиям отказоустойчивости и увеличения производительности.

Однако, облачная инфраструктура на данный момент активно развивается, расширяется и внедряется. Балансировщик Nginx будет более подходящим решением для реализации, поскольку необходимо предусмотреть разносторонние пути развития и иметь возможность быстро и качественно их реализовать.

Список используемых источников

1. Швидкий А. А., Спиркина А. В., Савельева А. А., Тарлыков А. В. Evaluation of the impact the hyper-converged infrastructure storage subsystem synchronization on the overall performance // 12th International congress on ultra modern telecommunications and control systems and workshops (ICUMT), 2020. pp. 248–252.
2. Елагин В. С., Николаев В. Е. Функциональное назначение балансировщика нагрузки в облачных микросервисных архитектурах // Информационные технологии и телекоммуникации. 2020. Том 8. № 1. С. 67–75. DOI 10.31854/2307-1303-2020-8-1-67-75.
3. HAProxy Starter Guide. 2020. URL: https://www.haproxy.org/download/2.4/doc/intro.txt (дата обращения: 29.03.21).
4. HAProxy Technologies. 2020. URL: https://www.haproxy.com (дата обращения: 29.03.21).
5. Nginx. 2020. URL: https://nginx.org/ru/ (дата обращения: 29.03.21).
6. Introducing NGINX Instance Manager. 2021. URL: https://www.nginx.com/blog/ introducing-nginx-instance-manager (дата обращения: 29.03.21).

Статья представлена научным руководителем, директором НИИ ТС СПбГУТ, кандидатом технических наук, доцентом А. Г. Владыко.

УДК 004.04(8)
ГРНТИ 49.01.85

ДИСТАНЦИОННЫЙ МОНИТОРИНГ ПАЦИЕНТОВ С COVID-19 С ИСПОЛЬЗОВАНИЕМ НОСИМОЙ ЭЛЕКТРОНИКИ

И. О. Игнатова, А. А. Парфенова, Р. В. Киричек

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

В статье рассматривается прикладное применение метода сбора данных с носимой электроники, которое используется для дальнейшего анализа и прогнозирования возможных болезней для медицинских приложений. Обработка полученных данных позволит прогнозировать болезни, такие как COVID-19.

дистанционный мониторинг, интернет вещей.

В наше время большой популярностью пользуются множество умных устройств, такие как смартфоны, смарт-часы и т. д., направленных на отслеживание базовых показателей физической формы человека. Каждый носит их по своим причинам. Фитнес-браслеты, как пример такого устройства, может иметь множество функций:

- Измерение пульса.

- Умное пробуждение.
- Измерение давления
- Подсчет числа шагов и пройденного расстояния.
- Подсчет калорий [1].

Получаемые показатели могут быть успешно использованы для отслеживания здоровья человека, анализа и прогнозирования возникновение некоторых болезней [2].

На сегодняшний день эпидемиологическая ситуация в стране оставляет желать лучшего. Количество заболевших растет и медперсонал не справляется с текущей нагрузкой. Поэтому потребность в разработке методов мониторинга больных в реальном времени многократно возросла. Развитие данной области поможет снизить время отклика врачей на изменения в состоянии пациента и снизить вероятность летального исхода последнего. Так отслеживание показаний пульса помогает оценить общее состояние человека и его степень интоксикации COVID-19.

Целью данной работы является рассмотрение модели дистанционного мониторинга пациентов с использованием носимой электроники.

В данной работе в качестве носимой электроники используются фитнес браслет со встроенным пульсометром и с возможностью постоянного измерения пульса. Получаемые данные должны быть обработаны и представлены в клиентском приложении с графическим интерфейсом. Интерфейс должен отображать имя наблюдаемого пациента, диагноз, его показания пульса, номер палаты. Так же должна быть реализована возможность уведомления медперсонала об ухудшении состояния пациента, с целью оказание немедленной помощи.

Стенд состоит из:

− браслета Xiaomi Mi Band 3;

− микрокомпьютера Raspberry Pi 3 B+;

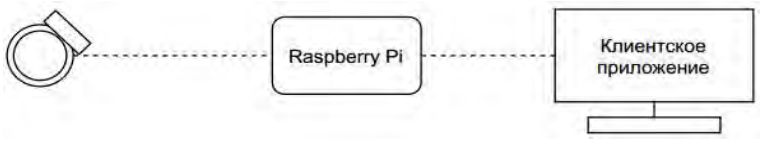


Рис. 1. Схематическое представление системы

− клиентского приложения.

Фитнес-трекеры. Фитнес-трекер представляет собой носимый гаджет компактного размера, предназначенный для контроля физической активности человека. В настоящее время производством таких устройств занимается большое количество производителей электроники такие как: Honor, Xiaomi, Garmin, Fitbit, Misfit и другие [3].

Основной задачей фитнес-трекера является мотивация своего владельца на активную деятельность и контроль получаемой нагрузки. Для выполнения поставленных задач в подобных устройствах установлены датчики, фиксирующие данные пульса, количества пройденных шагов, затраченных калорий, уровня стресса, качества сна, скорости перемещения и длины пройденного расстояния, уровня кислорода в крови. Полученная

информация может передаваться на смартфон или компьютер, а использование специально разработанного приложения позволит произвести расчеты активности человека, изменение показателей здоровья и при необходимости даст рекомендации для успешного достижения поставленной пользователем цели [4].

Наиболее распространённой формой фитнес-трекеров является браслет. Но существуют модели в виде клипс, очков и даже наушников. Браслет Xiaomi Mi Band 3 имеет следующие функции: измерение частоты пульса, шагомер, мониторинг физической активности и сна.

Скорость передачи данных и потребление энергии являются ключевыми факторами при выборе сетевой технологии для данного случая. 4G (LTE, LTE *Advanced*) наиболее подходит для тех устройств, которые обмениваются большими объемами данных. BLE применяется в устройствах с ограниченным объемом энергии и предполагают использование шлюза для инкапсуляции данных и отправки в IP-сеть. В рамках данной модели предполагается использование технологии Bluetooth LE. Bluetooth – это беспроводная технология, обеспечивающая передачу данных на небольших расстояниях между устройствами, поддерживающими эту технологию. Bluetooth позволяет общаться таким устройствам тогда, когда они находятся в радиусе до 10 метров друг от друга. Существенным достоинством Bluetooth LE является низкое энергопотребление. Использующие Bluetooth LE устройства потребляют меньше энергии по сравнению с Bluetooth-устройствами предыдущих поколений.

Микрокомпьютер Raspberry Pi 3 Model B+ представляет собой функциональную малогабаритную сборку, оптимальную для построения автоматизированных систем, сверхкомпактных настольных системных блоков и т. д. Изделие представляет собой материнскую плату, оборудованную процессором Broadcom 4×1 400 МГц и 1 ГБ оперативной памяти. Микрокомпьютер, снабженный контроллерами Wi-Fi, Bluetooth 4.2 (BLE) и сетевым адаптером для присоединения Ethernet-кабеля, Максимальная скорость сетевого подключения с помощью штатного адаптера – 300 МБит/с.

В данной системе Raspberry Pi 3 Model B+ будет использоваться как сервер для сбора данных с браслета Xiaomi Mi Band 3 и их обработки. Устройство будет обрабатывать полученные показания с помощью медицинской модели и выводить в клиентском приложении на веб-интерфейс имя наблюдаемого пациента, диагноз, его показания пульса, номер палаты в реальном времени. В случае, если показания пациента резко ухудшаться, то на интерфейс приложения поступает сообщение об этом с целью оповестить медперсонал, что человек нуждается в оказании немедленной помощи.

В рамках данного эксперимента поверка работоспособности модели проходила на здоровом человеке, поскольку доступа к зараженным пациентам не было.

Тестирование было разделено на три этапа:

1. Браслет считывал показатели с испытуемого, находящегося в спокойном состоянии. В этом случае уровень пульса находился в пределах допустимого для возрастной группы от 18 до 30 лет.

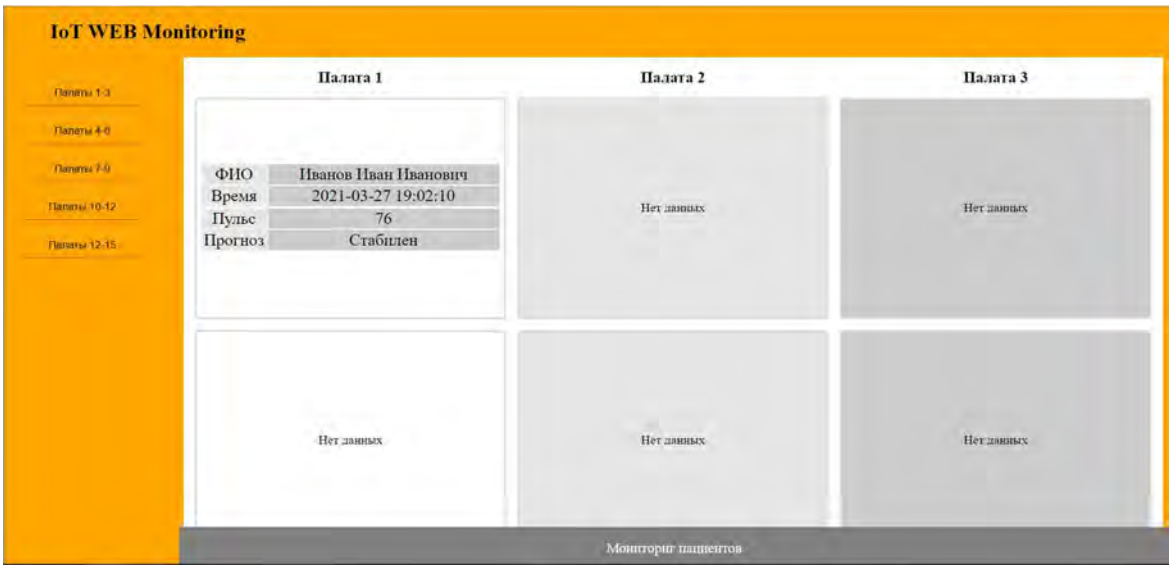


Рис. 2. Интерфейс при стабильном состоянии пациента

2. Браслет считывал показатели испытуемого, который выполнял физические упражнения разной интенсивности. Частота пульса при этом повышалась и выходила за рамки допустимого. В этом случае клиентское приложение выдает окно уведомления о необходимости оказания помощи пациенту.

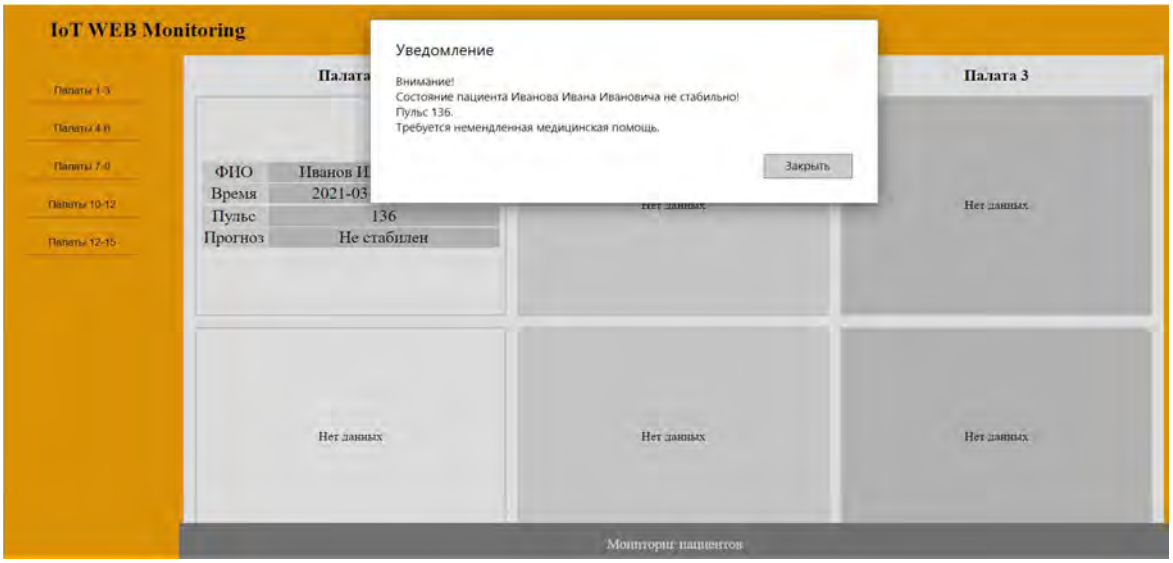


Рис. 3. Интерфейс при частоте пульса больше установленного диапазона

3. Чтобы проверить как поведет себя система при отсутствующих данных о частоте пульса, браслет снимали с испытуемого. В этом клиентское приложение выдавало уведомление о, том, что у испытуемого нулевой пульс.

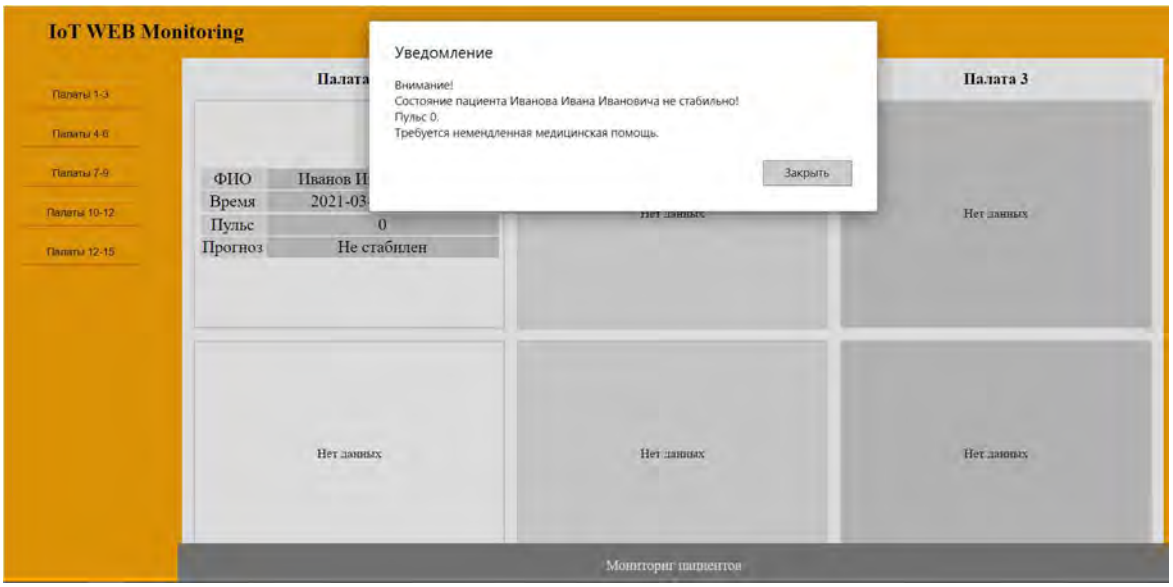


Рис. 4. Интерфейс при снятом с пациента браслете

Таким образом, предлагаема модель позволит оптимизировать процесс наблюдения пациентов, оказывать своевременную помощь на основе данных о каждом больном, тем самым увеличить продуктивность медучреждения. В будущем предполагается внедрение машинного обучения, с целью усовершенствования системы, что позволит достичь процесса распознавания и прогнозирования заболеваний, а также увеличение радиуса обхвата устройств для отслеживания состояния пациента не только в пределах палаты, но и медучреждения.

Исследование выполнено при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки ведущих научных школ Российской Федерации в рамках научного проекта НШ-2604.2020.9.

Список используемых источников

1. Гончарук С. В., Сечная А. Е. Современные технологии в спорте: фитнес-браслеты // Вестник научных конференций. 2019. № 12-2 (52). С. 46–48.

2. Орлова Е. Ю. Фитнес трекеры: понятие, функции, преимущества и недостатки // Евразийское научное объединение. 2020. № 6-6 (64). С. 459–460.

3. Фокин С. Ю., Киричек Р. В. Обзор медицинских приложений, устройств и технологий связи Интернета Вещей // Информационные технологии и телекоммуникации. 2016. Том 4. № 4. С. 67–80.

4. Захаров М. В., Киричек Р. В., Кучерявый А. Е. Обзор текущих исследований в области Mobile Health // Информационные технологии и телекоммуникации. 2020. Т. 8. № 3. С. 63–70.

УДК 004.056
ГРНТИ 19.31

ОСОБЕННОСТИ РАЗВЕРТЫВАНИЯ SECURITY OPERATIONS CENTER ПРИ ОРГАНИЗАЦИИ УДАЛЕННОГО ДОСТУПА К ИНФРАСТРУКТУРЕ КОМПАНИИ

П. В. Карельский, М. М. Ковцур, А. А. Миняев

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

С развитием технологий появляются угрозы информационной безопасности организаций, при создании удаленного доступа к ее инфраструктуре. Все больше растут требования к системам, обеспечивающим информационную безопасность компании, в связи с этим вопрос создания эффективного Security Operations Center встает особенно остро. В статье рассматриваются преимущества и недостатки SOC при организации удаленного доступа к инфраструктуре компании.

security operations center, информационная безопасность, удаленный доступ.

Одновременно с развитием технологий растет и количество угроз безопасности информации в информационных системах, в связи с этим проблема предотвращения и реагирования на угрозы информационной безопасности (ИБ) в организациях является актуальной задачей. Необходимо обеспечить бесперебойное функционирование каждого подразделения компании, что, в свою очередь, увеличивает требования к системам, обеспечивающим ИБ. Одним из решений данной проблемы в настоящее время является создание SecurityOperationsCenter (SOC) в организации [1].

На текущий момент не существует стандартов создания SOC, а в открытом доступе не в полной мере описаны методики организации и внедрения SOC. Одновременно с этим, в существующих условиях организация удаленного доступа к информационным системам организаций является актуальной задачей.

В таблице 1 представлены основные решения SOC согласно исследованиям компаний Softline и Anti-Malware в РФ на начало 2020 года [2] и количество типовых сценариев мониторинга для выявления компьютерных инцидентов и кибератак.

ТАБЛИЦА 1. Решения SOC

Решения SOC	Количество типов стандартных правил корреляции (use cases)
Solar JSOC	Более 200 сценариев
BI.ZONE	8 типов, 250 правил
IZ:SOC	30 типов, более 300 правил
JET CSIRT	9 типов

Изучив структуру SOC, выделим основные компоненты:

SIEM (*Security information and event management*) – система управления информацией и событиями в безопасности. Предназначена для анализа в реальном времени информации о событиях (тревог) безопасности, исходящих из различных источников, таких как сетевые устройства, средства защиты, приложения, журналы аудита и т. д., и реагирования на них до наступления существенного ущерба.

AV (*Antivirus*) – антивирусное программное обеспечение, предназначенное для обнаружения и удаления вредоносных программ, а также восстановления измененных вредоносными программами файлов.

EDR (*Endpoint Detection and Response*) – новая платформа, способная обнаруживать атаки на рабочие станции, серверы, любые компьютерные устройства и оперативно реагировать на них. EDR может включать различные технологии обнаружения, работающие в автоматическом или в полуавтоматическом режиме. Например, это может быть антивирус, «песочница», движок поведенческого анализа, индикаторы компрометации и др. EDR может являться дополнительным инструментом для SOC.

IPS/IDS (*Intrusion Prevention System* / *Intrusion Detection System*) – системы предотвращения вторжений / системы обнаружения вторжений. Системы IDS/IPS могут предупреждать операторов о фактах попыток компьютерных атак и внедрения вредоносных программ, обрывать соединение со злоумышленником, изменять настройку сетевого экрана для блокировки доступа к корпоративным информационным ресурсам.

LM (*Log Management*) – система управления сбором и запросом событий из разнородного набора журналов систем и приложений. У таких систем значительно меньше возможностей по анализу событий, чем у коммерческих SIEM-систем.

MA (*Malware Analysis*) – анализ (проверка) наличия вредоносного программного обеспечения в различных системах. Выполняется при расследовании инцидентов, исследовании вредоносного ПО и для определения признаков взлома (индикаторов компрометации) при разработке систем безопасности.

Рассмотрим типовое решение по организации удаленного доступа к инфраструктуре компании, представлено на рис. 1.

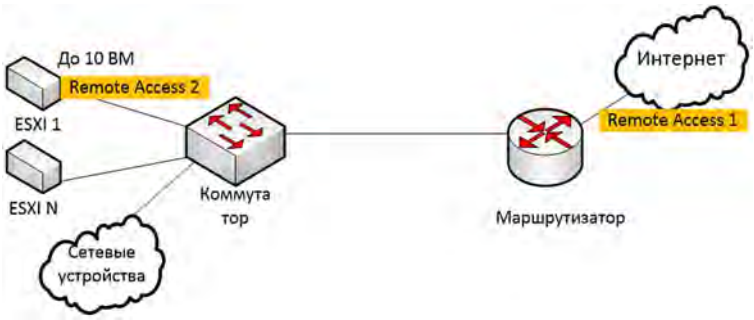


Рис. 1. Схема сети для мониторинга

Для мониторинга предлагается вынести следующие показатели:

– количество подключенных пользователей к RA 2;

– показатели сетевого оборудования: загрузка ЦПУ, трафик на интерфейсах, утилизация оперативной памяти;

– объем трафика сотрудников за интервал времени (удаленных и локальных);

– критичные ошибки в работе оборудования;

– попытки несанкционированного доступа.

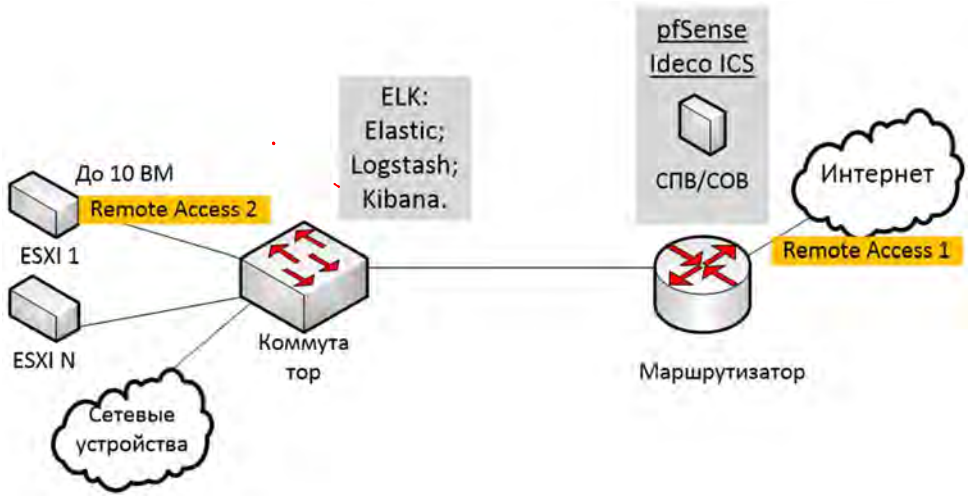


Рис. 2. Предлагаемое решение SOC

Предлагаемое решение SOC для организации удаленного доступа представлено на рис. 2.

pfSense – это программное обеспечение с открытым исходным кодом для маршрутизации и межсетевого экрана, основанное на дистрибутиве FreeBSD. Особенности решения представлены в таблице 2. Функционал включает: статическую/динамическую маршрутизацию, полноценный межсетевой экран, NAT, VPN, DHCP, DNS, Snort и suricata.

ТАБЛИЦА 2. Преимущества/Недостатки pfSense

Преимущества pfSense	Недостатки pfSense
Обильный функционал	Открытый исходный код

Преимущества pfSense	Недостатки pfSense
Бесплатный программный продукт	Нет гарантированной поддержки
Масштабируемость	Настройка через GUI

Ideco UTM – современное средство для защиты сетевого периметра производства РФ. К возможностям решения относят безопасное подключение удаленных пользователей, организация защищенных каналов между филиалами (поддержка VPN с использованием IKEv2, IPSec, SSTP) [3, 4]. К преимуществам решения относится наличие модуля IPS/IDS, наличие модуля антивируса, мощный контент-фильтр, встроенные средства безопасности, поддержка обновления ПО и русскоязычная поддержка. К недостаткам – ограничение бесплатной лицензии до 10 одновременных VPN сессий.

Для выбора подходящего обеспечения, необходимо определить, какие функции SOC наиболее важны для мониторинга в представленной сети. Например, мониторинг количества одновременно подключенных пользователей RemoteAccess, мониторинг трафика пользователей и т. д. Также требуется определить поддерживаемые протоколы для мониторинга (Syslog; Windows Event Log; NetFlow; SSH File Log; SNMP).

Необходимо реализовать следующую схему согласно рис. 3:

Рис. 3. Схема решения

Для работы с событиями можно использовать свободно распространяемый продукт, состоящий из трех компонентов: Elastic, Logstash, Kibana.

Elasticsearch – поисковый движок с jsonrestapi, использующий Lucene и написанный на Java. Kibana – это инструмент визуализации, обращающийся к журналам Elasticsearch и отображающий их пользователю в виде линейного графика, гистограммы, круговых диаграмм, т. д. Logstash – это ПО для сбора, фильтрации и нормализации логов. Оно является бесплатным и opensource приложением.

Внедряемое решение обеспечит необходимую защиту и безопасность, осуществит контроль доступа и защищенное удаленное подключение к инфраструктуре компании. Далее перечислены основные возможности представленного решения.

Система предотвращения вторжений IDS/IPS блокирует попытки несанкционированного доступа, эксплойты, ботнеты, DoS-атаки, вирусную активность в сети, TOR, анонимайзеры, криптомайнеры и помогает в расследовании инцидентов безопасности и поиске зараженных устройств [5].

Публикация сервисов с помощью DNAT port mapper. При этом сервис попадает под защиту системы IPS и становится устойчивым к попыткам взлома, использования вредоносных скриптов и эксплойтов.

Персональный полноценный доступ в интернет для каждого сотрудника. Авторизация по логину и паролю через VPN, PPPoE, через IdecoAgent или логин-пароль через веб-браузер, авторизация по IP-адресу (с возможностью привязки MAC-адреса).

Доступ сотрудников к сети предприятия из дома или командировки по защищенному каналу (IKEv2, IPSec, SSTP). В том числе с использованием мобильных устройств на базе ОС Android и iOS.

В результате проделанной работы, были изучены существующие решения SOC, определены основные компоненты SOC, на примере сети компании определены важнейшие функции SOC при организации удаленного доступа к инфраструктуре компании. Предлагаемое решение дает возможность объединить все удаленные подразделения компании в общую сеть на единой платформе с контролем защищенности инфраструктуры.

Список используемых источников

1. Фёдорова В. А., Колягина И. А., Руссак Д. А. Концепции и реализация центра операционной безопасности // Известия института инженерной физики. 2020. № 3. С. 68–73.

2. Сравнение услуг коммерческих SOC. URL: https://www.anti-malware.ru/compare/SOC-Security-Operations-Center, свободный. – Загл. с экрана.

3. Стрельников Р. В. SOC. Неэффективность внедрения // Вестник балтийского федерального университета им. И. Канта. 2019. № 4. С. 81–85.

4. Качалкова С. В., Садыков А. М., Касимова А. Р. Механизм создания системы защиты информации при разработке распределенного центра обработки данных // Вестник технологического университета. 2018. № 12. С. 176–180.

5. Казанцев А. А., Красов А. В., Катасонов А. И., Гельфанд А. М. Создание и управление Security Operations Center для эффективного применения в реальных условиях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 590–595.

УДК 004.451
ГРНТИ 81.96

РАЗРАБОТКА УНИВЕРСАЛЬНОГО АЛГОРИТМА ПО СОЗДАНИЮ ПРОСТЕЙШИХ МОДУЛЕЙ ЯДРА ДЛЯ РАЗЛИЧНЫХ ВЕРСИЙ ЯДРА LINUX

А. И. Катасонов, А. В. Красов, А. Ю. Цветков

Санкт-Петербургскийгосударственныйуниверситеттелекоммуникацийим. проф. М. А. Бонч-Бруевича

В наши дни с увеличением объемов передаваемой информации растут и требования к обеспечению безопасности этих данных. Злоумышленники разрабатывают все новые методы получения несанкционированного доступа к операционным системам с целью получения, нанесения ущерба секретной информации или для создания backdoor. Одним из таких способов является Rootkit уровня ядра. Для понимания специфики работы данного метода необходимо разобраться что из себя представляет ядро, каким оно бывает, каким образом функционирует, а также иметь представление по работе с модулями ядра и знание о том, каким образом происходит создание модулей ядра и принципа их функционирования. В данной статье разработан алгоритм, использующийся для реализации любых lkm модулей на различных версиях ядра Linux.

GNU/Linux, Rootkit, модули ядра, безопасность.

Существует большое количество различных версий и дистрибутивов известной операционной системы Linux, однако все эти системы объединяет одна общая черта – это ядро Linux, основная задача которого это общение аппаратного и программного обеспечения и наиболее эффективное управление ресурсами системы.

Ядра могут быть 3 различных типов: монолитное, микроядро и гибридное. Большинство ядер Linux именно монолитные, а Windows – гибридные. Рассмотрим каждый вид по отдельности.

Микроядро. Работа такого ядра основана на принципе, при котором ядро выполняет только функции управления памятью, процессором и производит межпроцессорное взаимодействие.

Основными преимуществами данного типа являются: малые размеры, низкое потребление памяти портативность, а также безопасность, поскольку большинство процессов выполняются в пространстве пользователя, где и реализованы большинство методов обеспечения безопасности [1].

Однако у такого ядра имеются и свои минусы. Для взаимодействия с аппаратными средствами необходимы драйвера, которые работают через пространство пользователя, где скорость обработки информации ниже, да и процессам приходится ожидать своей очереди при запросе.

Пытаясь устранить данные недостатки было придумано монолитное ядро. Оно в свою очередь охватывает не только процессор и память, но и включает в себя драйвера, систему ввода-вывода и файловую систему. Благодаря такому подходу обеспечивается быстрый доступ к аппаратным средствам, что не только увеличивает скорость взаимодействия, но и обеспечивает многозадачность, однако увеличивается размер данных ядер, необходимое количество оперативной памяти, а также возрастает вероятность угрозы, поскольку огромное количество действий требует прав суперпользователя.

Гибридные же ядра собирают в себе все лучшее из обоих типов ядер. Они могут работать как в режиме пользователя, так и в пространстве ядра, однако такой тип требует особого программного обеспечения, а именно драйверов, что сильно влияет на трудозатраты со стороны разработчиков и производителей [2].

Ядро Linux же имеет именно монолитную структуру, чтобы избежать его недостатки, для взаимодействия аппаратной части с ядром были созданы драйвера, которые могут быть дополнительно установлены и стать так называемыми модулями ядра.

Основное преимущество использования модулей ядра заключается в следующем. Само ядро Linux монолитное, поэтому при установке того или иного драйвера приходится пересобрать ядро, что является довольно трудоемким процессом. Благодаря использованию модулей ядра возможно установить тот или иной драйвер поверх самого ядра, а не внутрь его. На рисунке изображена структура операционной системы Linux и модель взаимодействия ядра с различными аппаратными компонентами при помощи модулей ядра [3].

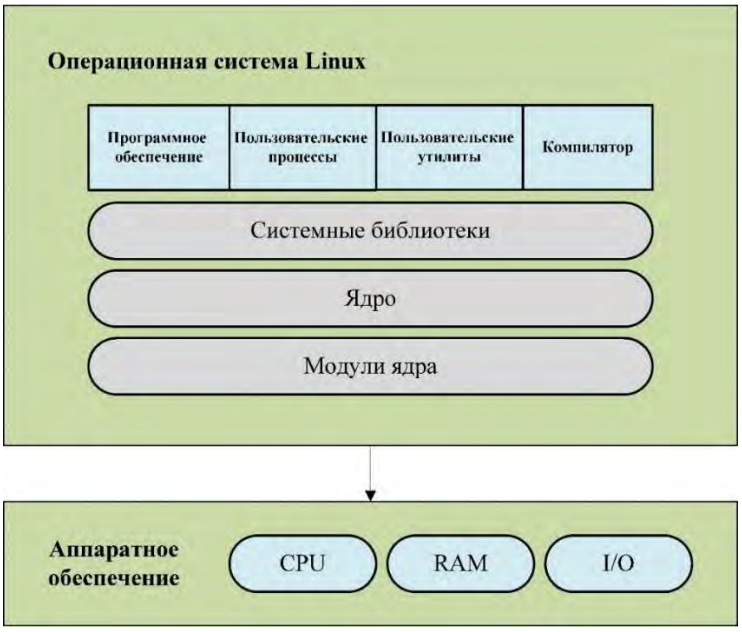


Рис. Структура операционной системы Linux

Однако написание модулей ядра тоже является довольно трудоемким и сложным процессом. Основной особенностью является то, что внутри кода ядра до сих пор нет стандартной защиты, как в обычных приложения Linux, что может привести к краху всей системы из-за одной ошибки.

Также при работе с модулями ядра нельзя пользоваться стандартными библиотеками, приходится использовать функции, которые использовались при сборке ядра.

Разработка алгоритма проводилась на различных версиях ядра Linux, а именно 2.6.32-5-amd64, 3.16.0-6-amd64, 4.19.0-6-amd64 дистрибутивов Debian 6,8,10, соответственно.

Первым делом при сборке модуля необходимо установить пакет под названием build-essential, при помощи следующей команды.

```
apt-get install build-essential linux-headers-`uname -r`
```

Заметим, что в конце команды находится *uname -r*, данная фраза необходимо для того, чтобы вы установили пакет build essential именно для той версии ядра, которую и использует ваша операционная система.

Далее первым делом необходимо создать файл с расширением *.c*, в который и будет загружаться код нашего модуля. Стандартный код модуля ядра. так называемый Hello World, выглядит следующим образом.

```
#include <linux/init.h>
#include <linux/module.h>
#include <linux/kernel.h>
 MODULE_LICENSE("GPL");
MODULE_AUTHOR("Robertinstaapt W. Oliver II");
MODULE_DESCRIPTION("A simple example Linux module.");
MODULE_VERSION("0.01");
 static int __init lkm_example_init(void) {
printk(KERN_INFO "Hello, World!\n");
return 0;
}
static void __exit lkm_example_exit(void) {
printk(KERN_INFO "Goodbye, World!\n");
}
 module_init(lkm_example_init);
module_exit(lkm_example_exit);
```

Разберем этот код подробнее. В первой части кода необходимо подключить стандартный набор библиотек.

Во второй части программы находятся данные, описывающие созданный модуль, по факту они могут быть любыми. В эти данные входит лицензия, автор модуля, описание модуля и версия.

Далее созданы 2 функции lkm_example_init и lkm_example_exit, которые выполняют код при запуске или при выключении модуля соответственно. В данном случае внутри кода находятся функции printk, которые выводят в лог фразы «Hello World» и «Goodbye World».

В последней же части находится вызов двух, созданных нами ранее функций init и exit.

Однако даже написав все вышеперечисленное еще пока нельзя скомпилировать даже наш стандартный модуль. Необходимо еще создать Makefile, в котором должны будут находится инструкции по сборке модуля. Стандартный и простой вариант makefile выглядит следующим образом

```
obj-m += lkm_example.o
 all:
  make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules
clean:
  make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
```

Важной особенностью является то, что данный файл очень привередлив к пробелам. Поэтому необходимо перед фразой make использовать именно табуляцию, а не пробелы. Также в первой строке необходимо указать точно такое же название файла, что и модуль, который мы создали, чтобы [4].

Рассмотрев данный файл видно следующее:

- *$* – получить в виде строки,
- *Shell* – вызвать команду из консоли,
- *Uname -r* – выводит имя текущей версии ядра Linux.

По сути внутри нашего файла Makefile находится путь к другому файлу в котором и находятся необходимые нам инструкции по сборке модуля. Если пройти по пути выше и открыть одноименный файл, то в нем будет следующее [5].

```
user@debian6:/lib/modules/2.6.32-5-amd64/build$ cat Makefile
VERSION = 2
PATCHLEVEL = 6
MAKEARGS := -C /usr/src/linux-headers-2.6.32-5-common O=/usr/src/linux-headers-
2.6.32-5-amd64
MAKEFLAGS += —no-print-directory
.PHONY: all $(MAKECMDGOALS)
cmd := $(filter-out all Makefile,$(MAKECMDGOALS))
all:
@$(MAKE) $(MAKEARGS) $(cmd)
Makefile:;
$(cmd) %/: all
@:
```

Далее необходимо запустить процесс сборки модуля простой командой *make*. После успешной компиляции модуля будет создано несколько файлов, одним из которых будет файл расширением .ko, который и содержит в себе основной модуль. Для загрузки его к ядру необходимо использовать

команду *sudo insmod lkm_example.ko.* Чтобы убедиться, что модуль подгрузился можно проверить логи при помощи *sudo dmesg*. Для дальнейшего отключения модуля используется команда sudo rmmod lkm_example.

Подводя итоги создадии универсальный алгоритм по созданию простейших модулей ядра. При разработке модуля ядра необходимо:

1. Установить пакет build-essential.
2. Определить версию используемого ядра.
3. Создать два файла:
    a. Файл, в котором хранится исполняемый код модуля,
    b. Makefile.
4. Запустить процесс сборки модуля.

Таким образом в данной статье рассмотрено создание стандартного модуля ядра и разработан алгоритм, использующийся для разработки любых lkm модулей на различных версиях ядра Linux.

Список используемых источников

1. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернбородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция6 сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 525–527.

2. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.

3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Материалы XVI Санкт-Петербургской международной конференции "Региональная информатика "РИ-2018" (Санкт-Петербург, 24-26 октября 2018 г.). СПб., 2018. С. 570–571.

4. Москальчук А. И. Практическое исследование методологии тестирования на проникновение в виртуальной среде // Молодежная научная школа кафедры "Защищенные системы связи". 2020. Т. 1. № 1 (1). С. 47–54.

5. Гельфанд А. М., Лансере Н. Н., Ложкина А. А., Фадеев И. И. Организация концептуальной модели критической информационной инфраструктуры // Методы и технические средства обеспечения безопасности информации. Санкт-Петербург, 2020. № 29. С. 39–40.

УДК 004.273
ГРНТИ 50.41.01

ОЦЕНКА ПОДХОДОВ К ТУННЕЛИРОВАНИЮ ЧАСТЫХ СЕТЕЙ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ

Р. Э. Катунин, А. А. Швидкий

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

В статье рассмотрены три подхода организации сети между виртуальными машинами, с учетом требований безопасности, описаны достоинства и недостатки каждого подхода, а также приведены примеры. Дано определение понятию туннелирование, приведены существующие протоколы туннелирования, из которых выбраны три наиболее используемых для сравнения и анализа. После сравнения протоколов сделан вывод, описывающий наиболее унифицированный протокол.

виртуальные машины, протоколы туннелирования, GRE, VXLAN, Geneve.

В мире современных технологий, где иерархия виртуальных машинных систем образует общую сеть устройств, без разделения трафика одних виртуальных машин от других, так как в таком случае отсутствует безопасность машин, что вызывает множество проблем в виде утечки информации, технической разведки, заражения вирусом сеть и прочих неприятностей. Были оверлейные сети на базе тоннелей, задача которых была организовывать частные сети на базе общественных сетей.

Для организации сети между виртуальными машинами, с учетом требований к безопасности, можно выделить три подхода:

1. Все виртуальные машины расположены в одной сети. Этот способ является самым простым и наименее безопасным, так как любая новая виртуальная машина в сети имеет такой же доступ к трафику, как и остальные. В данном случае, каждая виртуальная машина соединена между собой и не должна находиться вне этой сети.

2. Все виртуальные машины размещены в разных VLAN. Данный способ является более безопасным, по сравнению с первым, но имеет ограничение количество используемых машин (4 096), введу того, что технология имеет фиксированное 12-битное поле. В данном способе появляется разделение трафика на определенные группы VLAN. Можно, к примеру, разделить пользователей на 4 группы, 3 из которых имеют доступ к виртуальным машинам внутри своей группы, а пользователи 4 группы, имеют возможность подключаться как к виртуальным машинам своей группы, так и к ка-

кой-нибудь группе из трех или всем сразу. Это определяется при развертывании VLAN над сетью общего пользования. Трафик, передаваемый в VLAN сети, изолирован от сети общего пользования.

3. Все виртуальные машины полностью изолированы от сети, и соединены с другими виртуальными машинами с помощью туннелей. В данном случае на основе сети общего пользования создается туннель, соединяющий два оконечных устройства. Этот вариант позволяет организовать передачу трафика, изолированного от общей сети на любые расстояния, при этом имея хорошую безопасность, большее количество используемых виртуальных машин, а так же удобство мониторинга такой сети. Передача данных в этом способе выглядит следующим образом: пакет передается от устройства отправителя на маршрутизатор, где пакет инкапсулируется с помощью одного из протоколов туннелирования и отправляется в общую сеть, по полученным данным при инкапсуляции пакет попадает на маршрутизатор получателя, где происходит деинкапсуляция пакета, после этого пакет попадает на оконечное устройство получателя в исходном виде. Данный вариант является самым безопасным и удобным для использования. Данный подход является наиболее приемлемым для использования в частных и публичных облачных инфраструктурах

Можно сделать вывод о том, что туннелирование – это процесс, в результате которого создается защищенное логическое соединение между двумя оконечными устройствами посредством инкапсуляции различных протоколов. Смысл туннелирования состоит в том, чтобы «упаковать» передаваемую часть данных, вместе со служебными полями, в область полезной нагрузки пакета несущего протокола. Туннелирование может применяться на сетевом и на прикладном уровнях. Комбинация туннелирования и шифрования позволяет реализовать закрытые виртуальные частные сети.

Существует множество протоколов туннелирования, такие как IPIP, SIT, ip6tnl, VTI и VTI6, GRE и GRETAP, GRE6 и GRE6TAP, FOU, GUE, Geneve, VXLAN, ERSPAN и IP6ERSPAN [4]. Для оценки протоколов туннелирования наиболее используемые протоколы такие, как GRE, VXLAN, Geneve.

Протокол GRE (*Generic Routing Encapsulation*) описан в RFC 2784. При GRE-туннелировании между заголовками внутреннего и внешнего IP-пакета добавляется дополнительный заголовок GRE (рис. 1) [1].

В теории, GRE может инкапсулировать пакеты практически любого протокола 3 уровня с допустимым Ethernet-типом. Это отличает технологию GRE от технологии IPIP, которая использует лишь инкапсуляцию IP-пакетов, что урезает ее возможности. Туннели GRE позволяют использовать групповую передачу данных и поддерживают IPv6. Отличается от GRETAP тем, что работает на 3 уровне модели OSI в то время, как последний работает на 2 уровне.

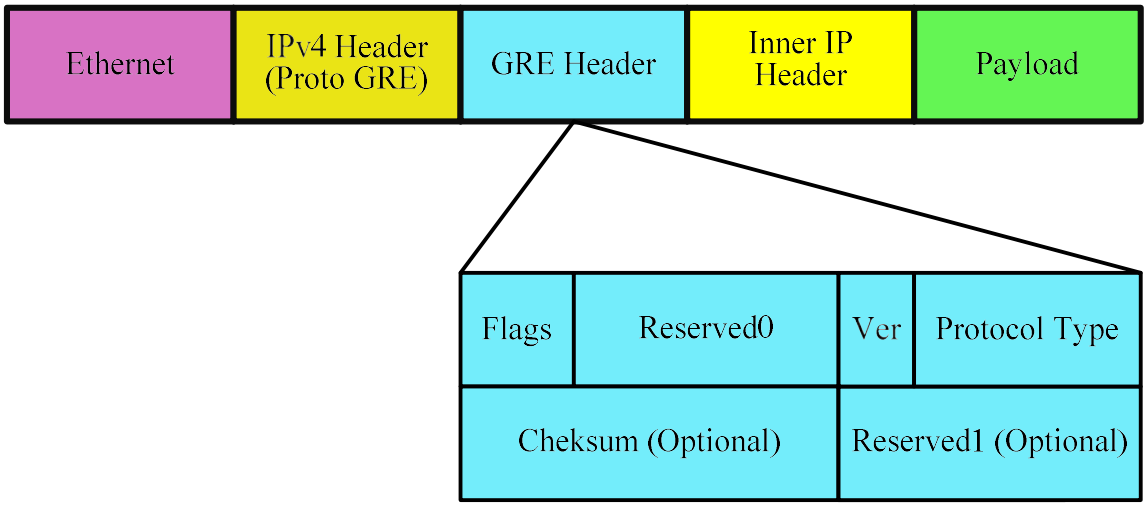


Рис. 1. Заголовок пакета туннеля GRE

Протокол VXLAN (*Virtual eXtensible Local Area Network*) – это туннельный протокол, предназначенный для решения проблемы ограниченных идентификаторов VLAN (4 096) в IEEE 802.1 q. Он описан IETF RFC 7348. С 24-битным идентификатором сегмента, он же VXLAN Network Identifier (VNI), VXLAN позволяет использовать до 2^{24} (16 777 216) виртуальных локальных сетей, что в 4096 раз превышает емкость VLAN. Является расширенным аналогом VLAN. VXLAN инкапсулирует кадры уровня 2 с заголовком VXLAN (рис. 2) в пакет UDP-IP [2].

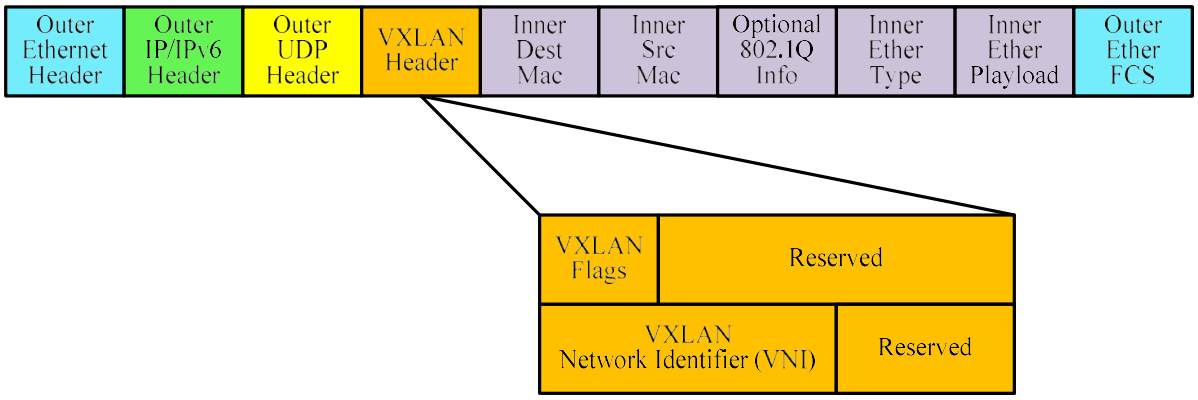


Рис. 2. Заголовок пакета туннеля VXLAN

Протокол Geneve (*Generic Network Virtualization Encapsulation*) поддерживают все возможности VXLAN, NVGRE и STT. Протокол Geneve спроектирован с учётом обхода выявленных ограничений этих трёх протоколов. Многие считают, что данный протокол способен, в перспективе, полностью заменить эти три более старых формата [5].

Заголовок Geneve (рис. 3) похож на заголовок VXLAN-пакета. Основное различие между ними заключается в том, что заголовок Geneve является более гибким. Он позволяет очень легко реализовывать новые возможности путём расширения заголовков с помощью полей Type-Length-Value (TLV) [3].

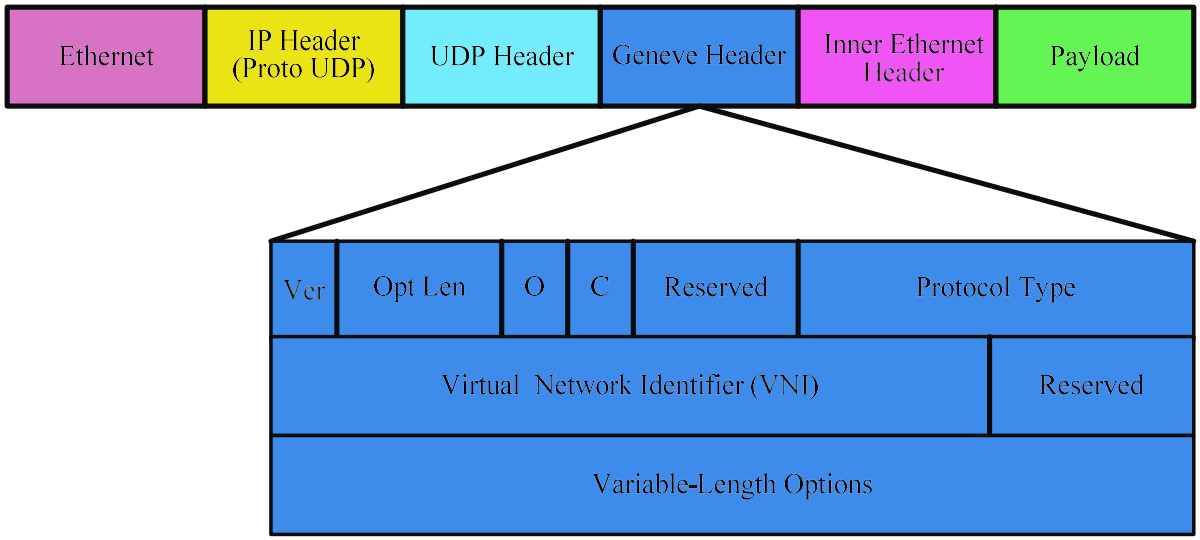


Рис. 3. Заголовок пакета туннеля Geneve

Разработчики могут включать в протокол необходимое количество опций динамически, не ограничиваясь 24-битными полями и не навлекая на себя накладные расходы 64-битного поля, когда требуется только часть этого размера. Все протоколы имеют свои преимущества и недостатки (табл.), что определяет их используемость в различных системах.

ТАБЛИЦА. Сравнение протоколов

Перечень	GRE	VXLAN	Geneve
Размер заголовка	20 бит	64 бита	Гибкий
Используемый уровень модели OSI	L3	L4	L4
Используемый протокол	IP	UDP	UDP
Поддержка версии протоколов IP	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6
Поддержка аппаратной разгрузки сетевыми картами	Да	Да	Нет
Поддержка сетевыми коммутаторами	Нет	Да	Нет
Встроенная реализация в ОС Linux	Да	Да	Да

Для проведения тестирования использовалось 2 сервера следующей конфигурации:

- CPU – 4 ядра 2.2 GHz,
- RAM – 32 GB,

•Сеть 10 Gb Intel XDA520.

Так же использовалась утилита IPerf3. Предварительно между двумя узлами были настроены тоннели с помощью набора утилит iproute2, был построен график скоростей (рис. 4).

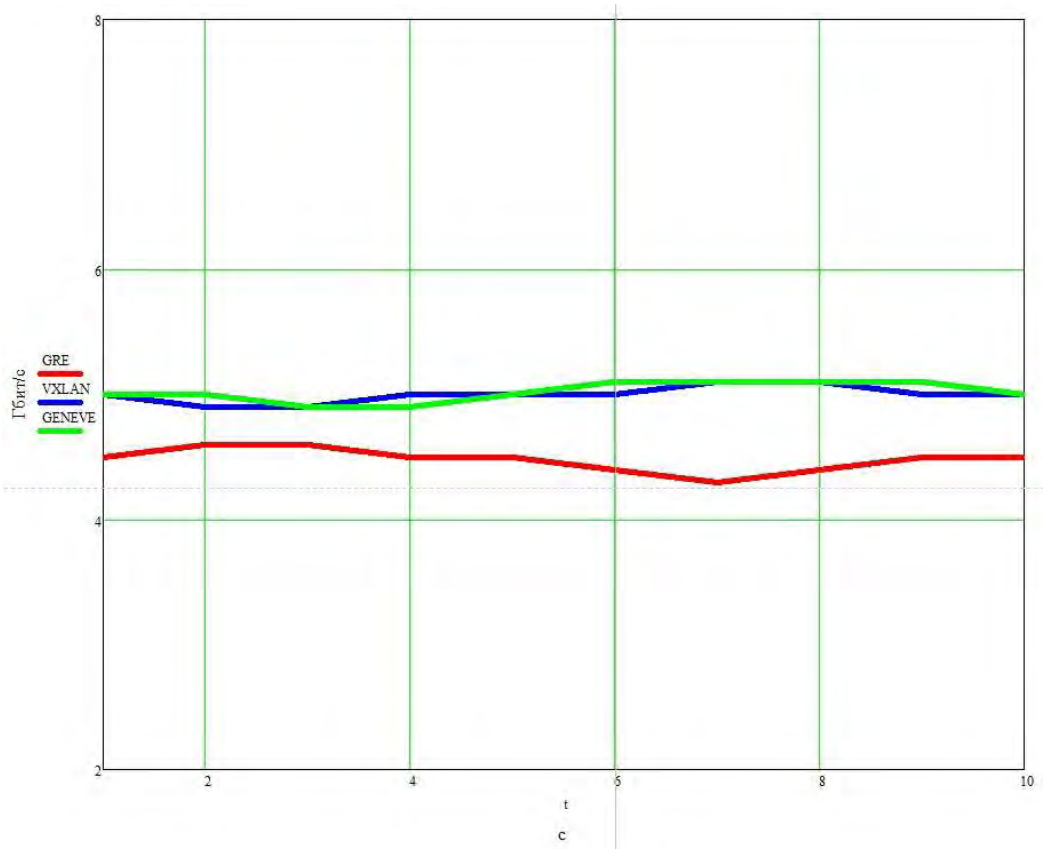


Рис. 4. График скоростей GRE, VXLAN, Geneve

Исходя из того, что протокол GRE имеет ниже скорость и меньше возможностей к передаче в разных сетях, можно сделать вывод, что в сравнении с остальными он уже устарел, а Geneve обладает преимуществом перед VXLAN. Развитие облачной инфраструктуры не стоит на месте, и один отдельный метод инкапсуляции не может стать общепринятым стандартом. Однако Geneve, с ее гибким опционным форматом и поддержкой всех возможностей других методов, будет сильным кандидатом на широкое распространение.

Список используемых источников

1. IETF Tools. 2020. URL: https://tools.ietf.org/html/rfc2784/ (дата обращения: 28.03.2021).

2. IETF Tools. 2020. URL: https://tools.ietf.org/html/rfc7348/ (дата обращения: 28.03.2021).

3. IETF Tools. 2020. URL: https://tools.ietf.org/html/rfc8926/ (дата обращения: 28.03.2021).

4. Хабр. 2006–2021. URL: https://habr.com/ru/company /ruvds/blog/457386/ (дата обращения: 28.03.2021).
5. Redhat. 2018. URL: https://developers.redhat.com/blog /2018/10/22/ introduction-to-linux-interfaces-for-virtual-networking/#vxlan/ (дата обращения: 28.03.2021).

Статья предоставлена директором НИИ ТС СПбГУТ, кандидатом технических наук, доцентом А. Г. Владыко.

УДК 004.75
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ И РАЗРАБОТКА АРХИТЕКТУРЫ ДЛЯ СИСТЕМЫ МОНИТОРИНГА ДАННЫХ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ НА ОСНОВЕ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ

К. Х. Киличева, А. С. Мутханна

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

Статья посвящена исследованию и разработке архитектуры для системы мониторинга данных медицинских учреждений на основе граничных вычислений. Граничные вычисления – это парадигма распределенных вычислений, осуществляемых в пределах досягаемости конечных устройств. Данный тип вычислений используется для сокращения времени сетевого отклика, а также более эффективного использования пропускной способности сети. В ходе работы было представлено концептуальное описание архитектуры инфокоммуникационного доступа к среде. Объектом изучения стало применение планировщика каналов доступа, в частности одного из методов управления – CSMA/CA, в качестве базиса предлагаемой сети. В терминологии компьютерных и сетевых технологий, коллизии определяются как наложение двух и более кадров от станций, пытающихся передать кадр в один и тот же момент времени. В статье также рассматривается роль выбранной технологии в сетевых компонентах, проводится анализ особенностей фреймворка передачи данных и ретрансляции. Проведённый эксперимент имеет высокую практическую ценность ввиду важности сферы здравоохранения и стремительного прогресса технологий беспроводных сетей. Созданная модель может быть интегрирована для дальнейшего прикладного проектирования и реализации сервисов приложений Интернета вещей.

Интернет вещей, IoT, Граничные вычисления, E-health, RFID, MEC.

Введение

Интернет вещей (IoT) – это система взаимосвязанных вычислительных устройств, механических и цифровых машин, объектов, животных или людей, которые снабжены уникальными идентификаторами и способностью передавать данные по сети, не требуя от человека взаимодействия между

компьютерами». Благодаря появлению сверх дешёвых компьютерных чипов и повсеместному распространению беспроводных сетей можно превратить все, от чего-то маленького, например, таблетки, до чего-то большого, как самолет, в часть IoT. Соединение всех этих различных объектов и добавление к ним датчиков добавляет уровень цифрового интеллекта к устройствам, которые в противном случае были бы глупыми, позволяя им обмениваться данными в режиме реального времени без участия человека [1].

Степень удаленного мониторинга позволяет операторам вышек и инфраструктуре отслеживать сигналы тревоги и управлять ключевыми показателями производительности через централизованную консоль. Это, в свою очередь, позволяет улучшить общее управление критически важной пассивной инфраструктурой на сотовых узлах, в то же время высвободив специалистов в области IoT-электросвязи, которые могли бы сосредоточиться на улучшении планирования сети и ресурсов [2].

Принцип работы

Непосредственная разработка и организация архитектуры беспроводных медицинских сетей была проведена с использованием планировщика каналов доступа. Так как, инфокоммуникационный доступ в среде возможен лишь для одного пользователя в конкретный момент времени, можно сделать вывод, что, при предоставлении доступа к системе первому пользователю, следующий пользователь обязан находится в ожидании до тех пор, пока пользователь не прекратит использовать канал [3]. После ожидания доступ к ресурсу перераспределяется для следующего пользователя. Ввиду этого в ходе эксперимента была выбрана система CSMA/CA, представляющая собой тип способа управления доступом к среде для размещения сигналов в сетях передачи основной полосы частот. Поскольку сети основной полосы частот могут одновременно передавать только один сигнал данных, должен быть какой-то способ управления тем, какая станция имеет доступ к медиа в любой момент времени.

Лабораторный стенд

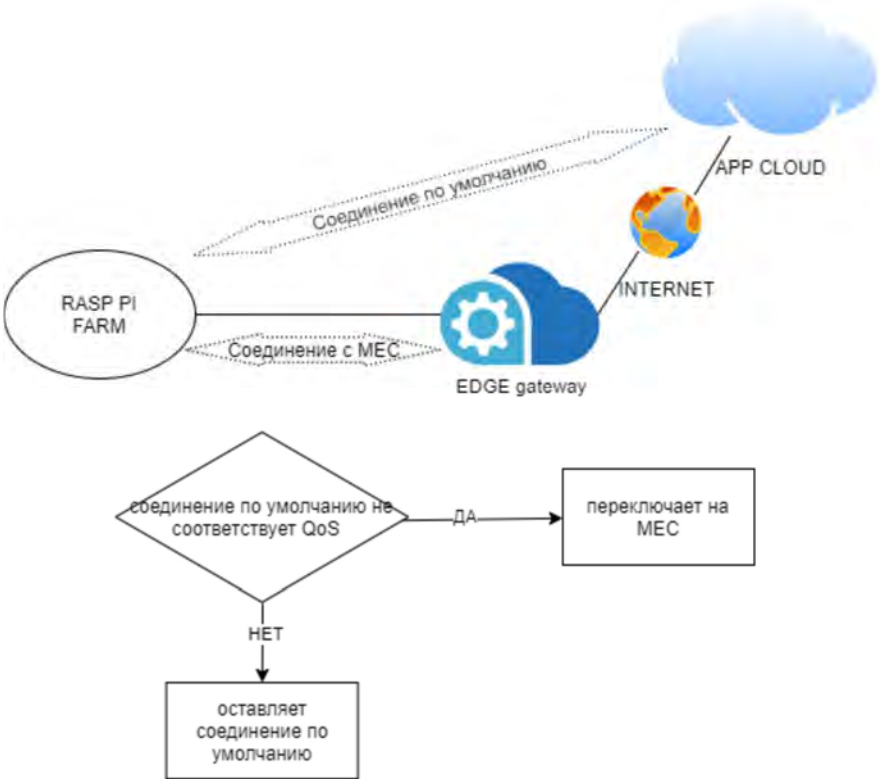


Рис. 1. Исследуемая модель передачи данных

1. Raspberry Pi – одноплатный компьютер, размеры 85,6 × 53,98 × 17 мм. Работает в основном на операционных системах, основанных на Linux ядре (рис. 2).

2. EDGE Gateway – шлюз граничных вычислений.

3. APP Cloud (Облако) – облачное хранилище данных.

4. Internet – Интернет.

Рис. 2. Ферма Raspberry Pi

ТАБЛИЦА 1. Исходные данные эксперимента

Распределение	Нормальное
Вероятность экстренных заявок	0,1
Интенсивность	2 пакета/сек
Доверительный интервал	3 сигма
Потеря пакетов	0,005
Протокол	MQTTS/UDP

Было произведено два эксперимента:

1) Создавалась генерация множества устройств ИВ с запросами на облака.

2) Создавалась генерация множества устройства ИВ с запросами на граничные вычислительные системы. Создавались виртуальные устройства с 1 до 14 000 устройств. в первом случае показал, что при 14 000 устройств в рамках лабораторного стенда. вероятность ошибки достигал чуть больше 0,8. а при обращениях к граничным серверам вероятность при таких же условиях достигал 0,6.

В целом, вероятность ошибок на всех количествах устройств получилась меньше на 20 %. На участке Edge – Cloud коэффицент Херста стремится к 0,5.

ТАБЛИЦА 2. Результаты эксперимента

Вычислительная мощность MEC сервера	2,10 GHz
Мощность передатчика	23dBm
Длина тайм слота	0,125 ms
Ширина поднесущей	60 KHz
Длина пакета	[32,100] Bytes
Задержка	1 ms
Допустимая потеря	10^{-7}

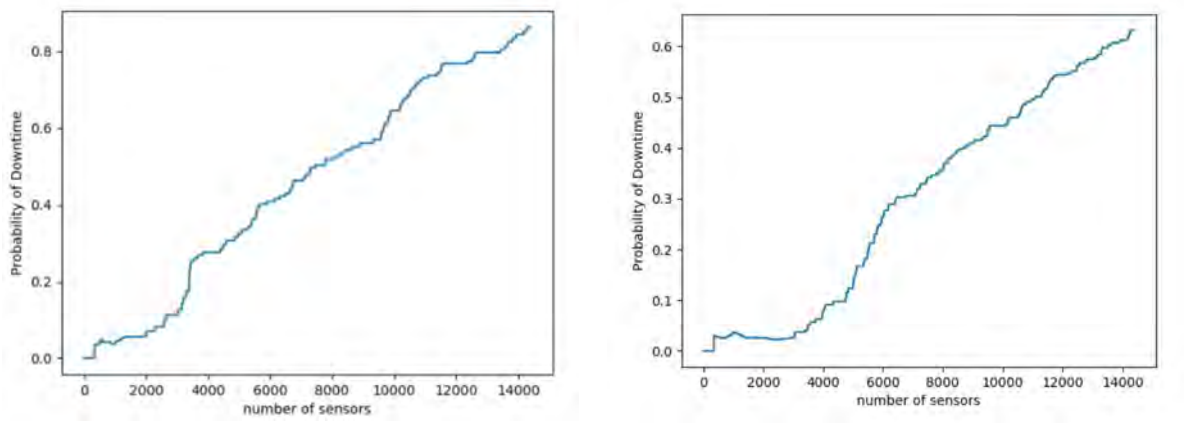


Рис. 3. Зависимость вероятности отказа от количества устройств на Облаке и граничных вычислениях

Первый эксперимент представлял из себя сравнение полной выгруженной базой приложения с частичной. Было взято приложение, которое организовывало свою работу следующим образом:

1. Сообщение, состоящее из ID – 32 bit (целое число A (16bit) и целое число B (16bit)) принимается по протоколу MQTT.

2. Производится операция OP 2bit.

3. Далее происходит поиск по ID номер пациента и осуществляется операция вычисления SQRT (A OP B).

4. Результат записывается в таблицу базы данных и при необходимости отправляется обратно пациенту [4].

Рис. 4. График зависимости энергопотребления от числа пользователей

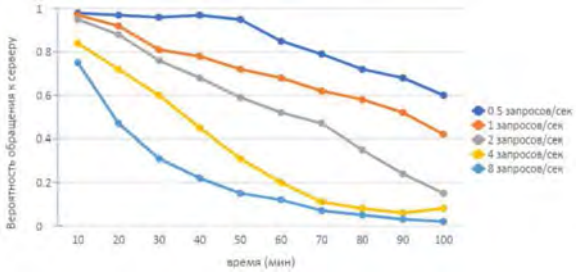


Рис. 5. График зависимости вероятности обращения к серверу от времени

Заключение

В ходе эксперимента были выявлены проблемы реализации носимых устройств, провелось обсуждение различных подходов к их решению и опрос исследований, посвящённый методам повышения энергоэффективности [5]. Главная задача проекта состояла в разработке архитектуры модели сети на основе граничных облачных вычислений и также в проведении натурного эксперимент для вычисления трафика носимых устройств. Результаты теста показали, что выбранный вид компьютерного вычисления несёт большую точность и производительность, ввиду меньшей потери сообщения с сенсоров [6]. Так же стоит отметить, что частичная выгрузка способна оптимизировать время получения данных на сервер с носимого устройства, за счет сокращения вписываемых в базу данных строк. Наконец, одно из существенных преимуществ выбранного граничного вычисления состоит в том, что при сокращении нагрузки на центральный сервер, уменьшается количество флуда и атак.

Список используемых источников

1. 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.

2. Naphade M. et al. Smarter Cities and Their Innovation Challenges // Computer, 2011.vol. 44, no. 6.

3. 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. Том. 4. № 2. С. 77–85.

4. Bowerman B., Braverman J., Taylor J., Todosow H., and Von Wimmersperg U. The vision of a smart city // In 2nd International Life Extension Technology Workshop, Paris, volume 28, 2000.

5. Jaeseok Yun Interoperability between IoT Platforms // Workshop on the Future of IoT Standard Technology, Dec. 2015.

6. Radek Fujdiak, Pavel Masek, Petr Mlynek, Jiri Misurec, Ammar Muthanna: Advanced optimization method for improving the urban traffic management // FRUCT 2016.

УДК 004.056.2
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ПОДХОДОВ АНАЛИЗА ТРАФИКА БЕСПРОВОДНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕКИ PANDAS

М. М. Ковцур, Д. И. Кириллов, А. В. Михайлова, П. А. Потемкин

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

В данной статье представлен подход анализа трафика беспроводных сетей, реализованный с помощью инструментов языка программирования Python, в частности библиотеки Pandas. Основной целью работы является оптимизация анализа трафика сетей семейства IEEE 802.11. Для обеспечения доступности беспроводных сетей необходим постоянный мониторинг сети для выявления угроз, поэтому актуальностью данной работы является увеличение производительности отслеживания аномальных действий при анализе дампов трафика. Основным инструментом является стек модулей языка Python, а именно NumPY, Pandas, StatsModels, MatPlotLib, math и Scipy.

Pandas, Python, трафик, беспроводные сети, анализ, мониторинг.

В настоящее время увеличивается объем трафика за счет подключений новых абонентов и развития каналов связи. По результатам статистики Cisco Visual Network Index за последние 5 лет количество новых подключений выросло в 4 раза [1]. В статистику вошли мобильный трафик, трафик проводных подключений, трафик Wi-Fi. Приоритетной задачей на данный момент является быстрый анализ трафика во избежание кражи паролей пользователей, взломов, хакинга и так далее. В данной статье проводится эксперимент по представлению больших данных различными методами. В анализе были задействованы такие программы как, Excel, анализатор трафика Wireshark и библиотека Pandas. Для исследования был взять дамп трафика объемом 3 Гб. Самый быстрый результат анализа – 2 минуты при использовании библиотеки Pandas языка программирования Python. 25 минут

понадобилось для анализа дампа программе Wireshark. И на последнем месте оказалась программа Excel – 45 минут.

Главным направлением анализа трафика стало качество Wi-Fi соединения, а именно количество пакетов с флагом retry=1. На основе выбранного направления исследования была составлена методика анализа трафика методами библиотеки Pandas (рис. 1).

Рис. 1. Методика исследования трафика беспроводной сети

Во-первых, для построения модели исследования данных необходимо получить историю отправки и получения пакетов за определенный период [2]. Для реализации данного шага можно воспользоваться двумя различными подходами – получить данные, используя программно-аппаратный комплекс для перехвата беспроводного трафика, или загрузить уже готовый dump-файл из открытых источников. При выборе первого метода получения данных используются следующие устройства и технологии:

– использование специализированных программно-аппаратных комплексов;

– использование беспроводных адаптеров в режиме мониторинга;

– использование программ мониторинга беспроводных сетей (Wireshark, Tcpdump, T-Shark).

При выборе второго варианта можно воспользоваться бесплатным online сервисом Google Dataset Search [1]. В данной работе использованы оба метода, как и метод захвата трафика, так и метод загрузки истории в виде dump-файла за семидневный период работы беспроводной сети.

Во-вторых, для того чтобы сделать показатель эффективности модели исследования наиболее высоким, необходимо было провести конвертацию и нормализацию данных, состоящую из следующих шагов:

– загрузка dump-файла в формате JSON;

– обработка и нормализация данных;

– приведение dataframe в виде таблицы.

В рамках работы данные преобразовываются в формат JSON, загружаются в виде словаря и конвертируются в формат DataFrame (двумерной матрицы) [3]. А после конвертации переименовываются столбцы, удаляются лишние данные (заголовки кадра).

Следующим шагом является – задание правил исследования, используя математический и статистический аппарат языка Python, а именно используя модули Pandas и SimPy.

Перед использованием математических функций полученная матрица должна быть сгруппирована и разбита на выборку, в которой хранятся основные параметры при отправке.

После этого полученная выборка претерпевает трансформацию, в результате использования статистических и математических функций. Итоговый DataFrame (рис. 2) группируются по MAC-адресам всех устройств и содержит в себе следующие параметры:

- скорость передачи данных,
- длительность передачи,
- уровень сигнала,
- количество Retry пакетов,
- количество устройств (уникальных MAC-адресов).

Пример матрицы анализа трафика представлен на рис. 2.

mac_addr	number_frame	length	duration	\
00:00:00:00:00:00	4	74.000000	135.537102	
00:0c:29:a8:a5:04	263	263.825095	135.896842	
02:00:00:00:00:00	22	133.000000	73.120347	
02:00:be:5e:e6:c4	2	166.000000	40.765865	
02:11:44:bd:26:69	3	131.000000	50.681867	

mac_addr	signal_dbm	speed	retry
00:00:00:00:00:00	-70.500000	27.500000	0.0
00:0c:29:a8:a5:04	-68.223214	5.570342	191.0
02:00:00:00:00:00	-51.181818	1.000000	0.0
02:00:be:5e:e6:c4	-79.000000	1.000000	0.0
02:11:44:bd:26:69	-63.000000	1.000000	0.0

Рис. 2. Матрица анализа трафика беспроводной сети

Последним шагом является обработка результатов. В данной работе полученная аналитика переведена в формат графиков для более наглядного представления [4]. Визуализация результатов получена в 4 различных графических представлениях.

- группировка и выявление устройств с наибольшим количеством отправки Retry пакетов в сети;
- статистика устройств, имеющий низкий уровень сигнала;

− количество пакетов, отправленных со скоростью меньшей средней скорости отправки пакетов в беспроводной сети;

− сравнение работы различных ПО при анализе трафика.

Преимущества использования данной модели в сравнении с программами снятия и анализа трафика (WireShark, T-shark и т. д.).

Автоматизация всего процесса анализа данных, начиная разбиения статистики по MAC-адресам и заканчивая построением графиков. Время выполнения анализа инструментом Pandas в 6,5 раз меньше относительно Wireshark и в 19 раз меньше времени анализа методами Excel. Построение аналитики по всем параметрам кадра, с заданием любых правил и любой настройки визуализации.

В заключении, в данной работе была разработана и описана методика исследования трафика беспроводной сети с использованием библиотеки Pandas. Рассмотрены задачи, связанные с изучением методов получения трафика беспроводных сетей. Реализован и описан метод исследования трафика беспроводных сетей с использованием библиотеки Pandas. Проведен сравнительный анализ работы Pandas и ПО Wireshark.

Список используемых источников

1. Красов А. В., Верещагин А. С., Цветков А. Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013. № S7. С. 27–29.

2. Kovtsur M. M., Mikhailova A. V., Potemkin P. A., Ushakov I. A., Krasov A. V. Guidelines for using machine learning technology to ensure information security // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2020. pp. 285–290.

3. Ковцур М. М., Миняев А. А., Потемкин П. А., Хамза Д. Д. Обеспечение информационной безопасности web-приложений с использованием машинного обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 597–601.

4. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

5. Хейдт Майкл, Груздев А. В. Изучаем pandas. Высокопроизводительная обработка и анализ в Python. ДМК-Пресс, 2019 г. 153 с.

УДК 004.491
ГРНТИ 50.41.27

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ РУТКИТОВ УРОВНЯ ЯДРА В РАБОТАЮЩИХ LINUX-СИСТЕМАХ

К. С. Кирилова, А. В Красов, А. Ю. Цветков

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

С развитием и распространением информационных технологий нельзя не заметить, что вместе с ними распространяются и свойственные им угрозы. Например, с вредоносными программами нередко сталкиваются и пользователи, и администраторы компьютерных систем. В данной статье рассматриваются вредоносные программы для UNIX-подобных систем типа руткит уровня ядра, а также способы их поиска в зараженной системе. Упор делается на обнаружение вредоносных программ в запущенных системах.

linux, модули ядра, анализ вредоносных программ, руткиты.

Руткит – это разновидность вредоносного программного обеспечения (ПО), скрывающего факт своего присутствия в системе, а также используемого для маскировки присутствия других вредоносных программ. Это понятие появилось в мире UNIX, где под этим термином понимается набор утилит или специальный модуль ядра, которые злоумышленник устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. Иногда под руткитом понимают утилиту, предназначенную для получения этих прав, но в данной работе рассматриваются руткиты с первой точки зрения [1]. Скрытие необходимой информации достигается путем скрытия файлов, процессов и сетевых соединений [2].

Уровни привилегий

В операционных системах (ОС) код может выполняться в двух режимах, каждому из которых соответствует свой уровень привилегий [3]:

- Режим пользователя – обычно на этом уровне выполняется прикладное и системное ПО, которое не обладает правами вмешиваться в работу ядра. Этот уровень также называется кольцом защиты 3 (Ring 3);
- Режим ядра – на этом уровне выполняется код драйверов устройств, обработчиков прерываний и непосредственно ядра ОС. Данный уровень именуется также нулевым кольцом защиты (Ring 0). Код, исполняющийся в этом режиме, обладает максимальными привилегиями в ОС.

Руткиты могут быть предназначены для выполнения в любом из этих режимов в зависимости от целей атакующего. Таким образов, различают руткиты уровня пользователя и руткиты уровня ядра. Поскольку руткиты уровня ядра обладают максимально возможными привилегиями в зараженной системе, они трудно обнаруживаемы непосредственно в этой системе. В системах Linux руткиты уровня ядра реализуются в виде модулей ядра, и потому именуются LKM-руткитами (*Loadable Kernel Module* – загружаемый модуль ядра). Модуль ядра Linux – это скомпилированный двоичный код (перемещаемый объектный файл), который вставляется непосредственно в ядро Linux, работая таким образом с привилегиями ядра. Загружаемые модули ядра получили широкое распространение в системах Linux, поскольку позволяют динамически расширять функционал ядра без необходимости пересобирать его целиком [4].

Загрузка модулей ядра в Linux

При загрузке модуля ядра происходит следующее:

− ядро выделяет память под структуру-описатель (дескриптор) модуля и заполняет его;

− данная структура добавляется во внутренний связный список ядра, содержащий информацию обо всех загруженных модулях;

− выделяется память под код модуля, модуль загружается туда и начинает исполняться с функции init_module().

В данном процессе следует обратить внимание на связный список, в котором перечисляются все загруженные модули. Он используется системой для дальнейших манипуляций с ними (например, для вывода информации об активных модулях или для их выгрузки из памяти). Таким образом, если запись о модуле не присутствует в этом списке, то ядро ОС считает, что этот модуль не загружен. Этим пользуются LKM-руткиты, после своей загрузки удаляя из этого списка ссылку на свой описатель. Такая техника называется манипулированием внутренними объектами ядра (DKOM, *Direct Kernel Object Manipulation*) [5]. После этого действия LKM-руткит не отображается при выполнении команды lsmod, а также его становится невозможно выгрузить. Чтобы избавиться от вредоносного модуля в системе, необходимо сначала вернуть ссылку на его описатель в список загруженных модулей.

Итак, задача обнаружения LKM-руткита сводится к поиску в памяти системы объекта, похожего на описатель модуля ядра, но при этом отсутствующего в системном списке загруженных. Возникающая при этом проблема заключается в том, что поиск происходит в виртуальном адресном пространстве, а объем этого пространства зачастую может может превосходить физически доступную память. Например, на 32-битных системах виртуальное адресное пространство имеет размер 4 ГиБ (однако с PAE могут

быть доступны и 64 ГиБ). На более современных 64-битных архитектурах поддерживаются 64-битные виртуальные адреса, хотя в реализациях и используются, как правило, 48-битные. Это даёт виртуальное адресное пространство размером 256 ТБ, поровну поделенных между пространствами ядра и пользователя [6]. Полный перебор пространства такого объема в поисках структур, похожих на описатели модуля ядра – трудоемкая задача. К счастью, виртуальная память в Linux устроена так, что для нахождения нужной структуры перебирать все адреса нет необходимости.

Во-первых, из исходных текстов ядра Linux известно, что память под описатели загружаемых модулей выделяется функцией vmalloc(). Эта функция может возвращать адреса (виртуальные) из определенного диапазона, ограниченного значениями VMALLOC_START и VMALLOC_END, которые также определяются в исходных текстах ядра и специфичны для разных архитектур.

Во-вторых, выделяемая память всегда выровнена по размеру страницы памяти, определяемому в исходных кодах ядра значением PAGE_SIZE, по умолчанию равному 4 КБ [7, табл. 19.4]. Это значение также может быть сконфигурировано при компиляции ядра.

Учитывая вышесказанное, количество адресов, по которым может находиться искомая структура-описатель, ограничено размером области, доступной vmalloc(), поделенному на размер страницы памяти. Для архитектуры x86_32 это всего 32 кБ, а для x86_64 – 8 ГБ вместо изначальных 128 ТБ. Важно отметить, что реализация решения рассматриваемой задачи для первой платформы была опубликована в 2003 году [8], но в данный момент, поскольку за почти 20 лет в ядре произошли значительные изменения, данная реализация является устаревшей и компиляция представленного там кода не является возможной без его адаптации к современным версиям ядер Linux.

Заключение

Присутствие руткита в атакованной системе во многом развязывает руки злоумышленнику [9, 10]. Более того, работа руткита в пространстве ядра предоставляет наиболее широкие возможности для маскировки своего присутствия в системе, поскольку в таком случае руткит обладает максимально возможными привилегиями. Такие руткиты сложнее обнаружить непосредственно в атакованной системе, чем руткиты пространства пользователя [11].

Тем не менее, существует способ поиска LKM-руткитов, и он был рассмотрен в статье. Заметим, что обращение к памяти, если у обращающегося процесса имеется к ней необходимый доступ, перехватить можно только в случае ошибки отсутствия страницы, что требовало бы изменения логики

обработчиков прерываний. Для этого, в свою очередь, понадобятся глубокие знания процесса прерываний и работы виртуальной памяти в Linux, что сильно затрудняет задачу атакующему. Поэтому предполагается, что предлагаемый способ поиска руткитов не встретит препятствий [12, 13].

Дальнейшая работа по теме заключается в том, чтобы адаптировать и реализовать рассмотренное решение для современных ядер Linux на архитектуре x86_64.

Список используемых источников

1. Raúl Siles Peláez. Linux kernel rootkits: protecting the system's "Ring-Zero" // SANS Institute. GIAC Unix Security Administrator. 2004. URL: https://www.giac.org/paper/gcux/243/linux-kernel-rootkits-protecting-systems-ring-zero/105411 (дата обращения: 15.12.2020).

2. Hiding out under UNIX // Phrack Magazine. 1989. URL: http://phrack.org/archives/issues/25/6.txt (дата обращения: 15.12.2020).

3. Таненбаум Э., Остин Т. Архитектура компьютера: пер. с англ. 6-е изд. СПб.: Питер., 2019. 816 с. ISBN 978-5-4466-1103-9.

4. Hiding with a Linux Rootkit. Exploit development. URL: https://0x00sec.org/t/hiding-with-a-linux-rootkit/4532 (дата обращения: 15.12.2020).

5. Jamie Butler. Direct Kernel Object Manipulation. URL: https://www.blackhat.com/presentations/win-usa-04/bh-win-04-butler.pdf (дата обращения: 15.12.2018).

6. Linux x86_64 Memory Management Documentation // Исходные тексты ядра Linux на ресурсе github.com. 2020. URL: https://github.com/torvalds/ linux/blob/master/Documentation/x86/x86_64/mm.rst (дата обращения 17.11.2020).

7. Love R. Linux Kernel Development. Novell Press by Pearson Education, Inc., 2010. 496 p. 3rd ed. ISBN 0-672-32946-8.

8. Finding hidden kernel modules (the extrem way) // Phrack Magazine. 2003. URL: http://phrack.org/archives/issues/61/3.txt (дата обращения: 15.11.2020)

9. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернбородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 525–527.

10. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.

11. Построение доверенной вычислительной среды: монография / Красов А. В., Гельфанд А. М., Коржик В. И., Котенко И. В., Петрив Р. Б., Сахаров Д. В., Ушаков И. А., Шариков П. И., Юркин Д. В. СПб.: Индивидуальный предприниматель Петрив Р. Б., 2019. 108 с.

12. Кушнир Д. В., Шемякин С. Н., Орлов Г. А. Представление некоторых аспектов отсеивания составных чисел для криптографических приложений // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 25–28.

13. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Материалы XVI Санкт-Петербургской международной конференции "Региональная информатика "РИ-2018" (Санкт-Петербург, 24-26 октября 2018 г.). СПб., 2018. С. 570–571.

УДК 004.04(8)
ГРНТИ 49.01.85

РАЗВИТИЕ ГОСТИНИЧНОЙ ИНДУСТРИИ ПУТЕМ ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Р. В. Киричек, А. Е. Круглова

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

В статье рассматривается внедрение интеллектуальных решений в номера отелей и гостиниц. Автоматизированные номера обеспечат создание более комфортного пребывания посетителей. Рассматриваются технологии передачи данных в системе «умных зданий». Рассмотренные информационные технологии могут быть использованы для оснащения гостиничных номеров.

гостиница, гостиничная индустрия, интеллектуальные решения, интернет вещей.

Гостиничная индустрия – одна из самых инновационных, энергозатратных и постоянно модернизирующихся отраслей.

Эпоха информационных технологий дает возможность развития нового формата в мире – «умного отеля». Эта система характеризуется непосредственным управлением всего оборудования, подключенного к глобальной компьютерной сети.

Главное требование к «умной гостинице» – это соблюдение стандартов качества оказываемых услуг. Технология «умного отеля» должна обеспечить оптимальные для проживания гостей условия, а также повысить безопасность и снизить расходы предприятия. Важнейшим элементом, влияющим на инфокоммуникационные технологии, является взаимодействие между сотрудниками отеля и его гостями.

Вся концепция администрирования отеля построена на стандарте KNX. Этот стандарт позволяет объединить все инженерные сети и коммуникации в одну систему. Благодаря этому стандарту мы можем:

- Повысить качество обслуживания клиентов в умном здании.
- Разработать эффективные руководящие принципы для оказания эффективной помощи предприятиям в выполнении соответствующей работы.

Благодаря стандарту KNX значительно сокращаются затраты на проектирование электроустановок в здании. В случае изменений в системе, происходит перепрограммирование устройства шины без прокладки новых проводов. Созданные KNX – устройства позволяют управлять системами как в отдельном помещении, централизованно – с диспетчерского пульта (планшета) или компьютера, так и удаленно – с мобильного телефона.

Система «Умная гостиница» направлена на повышение уровня комфорта и безопасности проживания. Как уже было сказано выше, важным условием комфорта является соответствие системы человеческим потребностям. Поэтому, при проектировании системы автоматизированного номера необходимо учитывать факторы, составляющие жизненные принципы проживающих.

Система состоит из одного или нескольких взаимосвязанных устройств. Все виды устройств, подключенные через интернет-технологии, производят действия согласно установленному режиму. В каждой комнате есть датчики и сенсоры, которые считывают информацию о состоянии номера и формирующие входные данные для компьютерной системы.

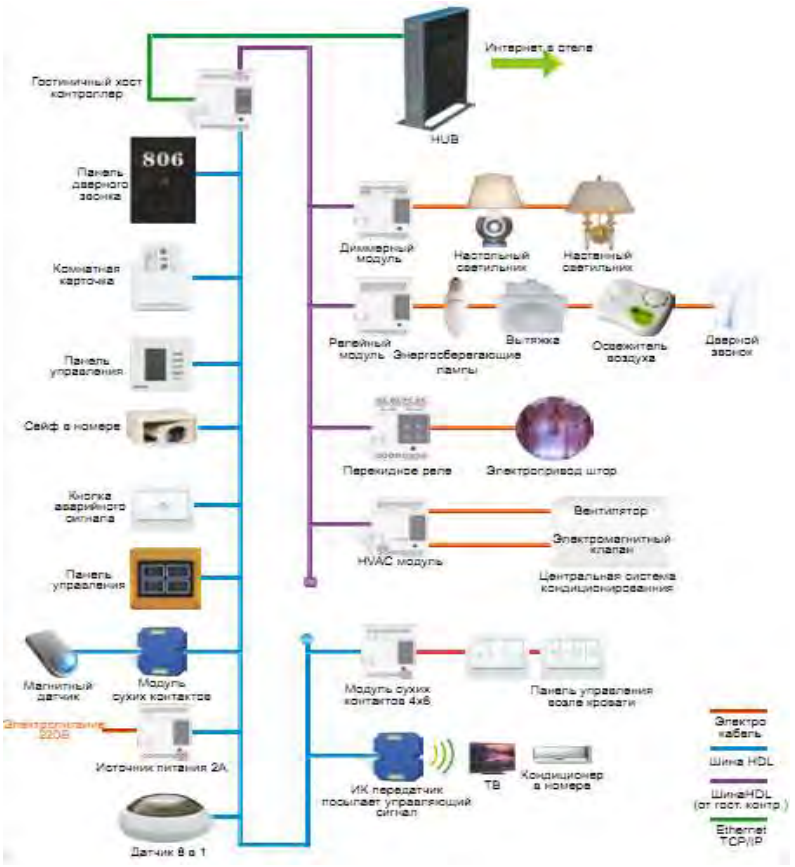


Рис. Пример интеллектуального решения для отеля

В системе «Умная гостиница» можно выделить такие подсистемы, как электроснабжение, освещение, управление электроприводами (регулировка жалюзи, штор), развлечения (домашний кинотеатр, аудиосистема), связь, контроль температуры, система безопасности и общая система контроля. Осуществляется различная логика интеллектуальной ID идентификации по карточке владельца или обслуживающего персонала.

Технология «умной гостиницы» способна не только обеспечивать оптимальные комфортные условия для гостей, а также позволяет повышать безопасность и понижать производственные расходы.

Централизованный контроль номеров базируется на основе сетевого протокола TCP/IP и дает большую стабильность и удобство в управлении всей гостиницей.

Сетевым управлением с помощью ПО легко проверяется нахождение кого-то в номере, запрашивается время на расчет по окончании срока пребывания; отправляется на стойку администратора клиентский запрос о расчете по окончании срока пребывания. Администратор видит полную картинку состояния датчиков в номере единым интерфейсом.

Также сетевое управление с помощью ПО позволяет: определять статус обслуживающего персонала, осуществлять удаленный контроль за системами функционирования, анализировать мониторинг неисправностей.

Рассмотрим беспроводные технологии передачи данных, использующиеся в «Умных зданиях» (табл. 1). Связь между узлами системы и устройством обработки данных основана на беспроводных технологиях Wi-Fi (передача видеопотока), Bluetooth (связь элементов аудиосистемы), ZigBee (передача данных с датчиков).

ТАБЛИЦА 1. Характеристики беспроводных технологий передачи данных

	WiFi	Bluetooth	ZigBee
Диапазон (м)	50–100	10–100	10–100
Частота (ГГц)	2,4	2,4	2,4
Потребление мощности	Высокий уровень	Низкий уровень	Очень низкий уровень
Предполагаемая область применения	Передача видеопотока с камер	Передача аудиосигнала	Беспроводное соединение между датчиками и системой

Исходя из табл. 1, можно сделать вывод, что использование технологии Bluetooth и ZigBee наиболее удобно для передачи данных. Использование Wi-Fi технологии допускается, но с учетом энергоемкости потребляемого ресурса.

Рассмотрим наиболее популярные устройства обработки данных (табл. 2).

ТАБЛИЦА 2. Характеристики устройств обработки данных

	Coubietruck	Raspberry Pi
Стоимость	От 3100 руб.	От 1400 руб.
Процессор	CPU: 1G ARM Cortex – A7 Dual Core	CPU 0.7 Ghz ARM 1176JZF – S
Видеокарта	GPU: Mali400M P2	GPU Broadcom VideoCore IV
Оперативная память	RAM 2GB DDR3	RAM 512 MB
Поддерживаемые интерфейсы	Ethernet 1000M, 2USB, SATA	2USB

	Coubietruck	Raspberry Pi
Встроенная память	4 Гб NAND Flash	Нет
Входы – Выходы для подключения датчиков	54 контакта	26 контактов
Максимальная потребляемая мощность	9 Вт	3,5 Вт

При анализе данных таблицы 2 можно увидеть преимущества Coubietruck: мощность процессора, поддержка Gigabit Ethernet, большое количество периферийных контактов для подключения устройств.

Raspberry Pi более дешевое и экономичное устройство, но менее производительное, следовательно, Coubietruck – больше подходит как устройство для обработки данных системы.

Связь между элементами системы поддерживается при помощи проводной или беспроводной связи. Как ни странно, но вариант с проводными соединениями меньше подвергается поломкам и сбоям системы.

В настоящее время самые продвинутые технологии в отелях имеются у трех гостиничных корпораций – IHG, Mariott и Hilton.

В ноябре 2017 года международная компания по управлению гостиничными сетями Marriott International представила интеллектуальную лабораторию, которая тестирует прототип умного гостиничного номера. В лаборатории IoTRoomroom, принадлежащей Mariott International используются как собственные разработки, так и решения Samsung и Legrand.

Сеть отелей представила два варианта: подключение комнат с нуля и после ремонта. Номер гостиницы управляется мобильными приложениями. Системы отеля «запомнят» предпочтения посетителя на основе предыдущих визитов.

К примеру, голосовой ассистент Amazon Alexa сможет выполнить такие команды, как «нагрев воды в душе до нужной температуры», «настроить оптимальное освещение для чтения» и т. д. Кроме того, предустановки можно задать на сайте программы лояльности Marriott. Внедрять новшества планируется в течение следующих пяти лет.

Marriott также задействовала гарнитуры с поддержкой технологий виртуальной реальности Oculus Rift, чтобы гости еще на этапе бронирования могли оценить интерьер понравившегося номера.

Не далеко ушли и разработчики сети отелей Hilton. Было создано инновационное решение ConnectedRoom – это платформа, которая позволяет гостям контролировать различные параметры в номере.

Connected Room, спроектированный и созданный с нуля, является естественным продолжением существующих возможностей приложения Hilton Honors. Его создание было основано на уникальных потребностях гостей, которые выразили желание персонализировать свое пребывание. С помощью мобильного приложения и сервиса Hilton Honors можно управлять

освещением, кондиционированием и медиаконтентом. В сервисе Hilton Honors можно предварительно, до заселения в номер, настроить все параметры.

Помимо оснащения системами «умных номеров», есть различные технологии, благодаря которым гостиница становится «умной». А именно – приложения на планшете в номере или в смартфоне выступают в качестве виртуального консьержа; инфракрасные датчики позволяют узнать персоналу, когда гости покинули свои комнаты и начать уборку; зеркало в ванной комнате кроме основной функции работает и в качестве интерактивного дисплея, на котором выводят информацию о новостях, погоде и т. д.; умные подушки с электрочувствительными волокнами контролируют кровяное давление, структуру сна и уровни стресса.

Таким образом, благодаря внедрению интеллектуальных решений в повседневную жизнь, руководители гостиничной индустрии смогут адаптировать и приблизить удобство проживания гостей в средствах размещения к тому уровню, который привычен людям дома.

Список используемых источников

1. Джанджугазова Е. А. Маркетинговые исследования в индустрии гостеприимства. Москва; Берлин: Директ-Медиа, 2020. 191 с. С. 90–93. ISBN: 978-5-4499-1541-2.

2. Устелемова М. С. Основы построения системы «Умный дом»: курс учебное пособие. Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2010. 45 с.

УДК 004.054
ГРНТИ 49.37

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ ТЕСТИРОВАНИЯ ФРАГМЕНТА СЕТИ, ИСПОЛЬЗУЮЩЕЙ ПРИЛОЖЕНИЯ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Р. В. Киричек, Е. А. Кузнецова

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

Дополненная реальность с каждым годом становится более популярной и востребованной в разных областях, начиная со сферы развлечения и заканчивая медицинской сферой. Сервисы и услуги, использующие дополненную реальность, более требовательны к параметрам сети из-за этого встает вопрос о качестве сети связи. Для каче-

ственного предоставления услуги дополненной реальности, требуется протестировать сеть на соответствие параметров сети требованиям, при которых сеть будет работать стабильно и удовлетворять пользователя. В статье рассмотрены существующие программно-аппаратные комплексы для тестирования сети.

тестирование сети, SLA, QoS, дополненная реальность.

В настоящее время трафик, связанный с приложениями Виртуальной и Дополненной реальности обладает достаточно высокими требованиями к сетевым характеристикам. Дополненная реальность AR (*Augmented Reality*) является одним из наиболее перспективных приложений сетей связи пятого поколения (5G). Для корректной работы сети, использующую услугу дополненной реальности, требуется убедиться, что сеть удовлетворяет характеристикам качества обслуживания (QoS – *Quality of Service*), для этого следует протестировать доставку данных от сервера до устройства дополненной реальности. Есть приложения, у которых сервер находится в другой стране, в таком случае, пока данные прогрузятся на устройство, информация может потерять одно из своих свойств – актуальность.

Для контроля клиентом показателей предоставляемых услуг появился термин SLA. SLA – Service Level Agreement (соглашение об уровне обслуживания) – внешний документ (существующий между заказчиком и исполнителем), описывающий параметры предоставляемой услуги. «Соответствие SLA» эквивалентно тому, что сервис работает так, что реальные параметры соответствуют заявленным в соглашении значениям метрик.

Рассмотрим существующие программно-аппаратные комплексы для измерения параметров сети.

Iperf

Iperf – кроссплатформенная консольная клиент-серверная программа – генератор трафика для тестирования пропускной способности сети.

Утилита позволяет генерировать трафик с разными настройками, можно выбрать протокол TCP/UDP, размер пакета, порт, время теста. Клиент и сервер могут иметь несколько одновременных подключений, но на разных портах.

Для выполнения тестирования программа должна быть запущена на двух устройствах (это могут быть как компьютеры, так и смартфоны, планшеты). Одно из них будет выполнять роль сервера, а другое роль клиента. Между ними и будет происходить передача данных для измерения пропускной способности соединения (рис. 1).

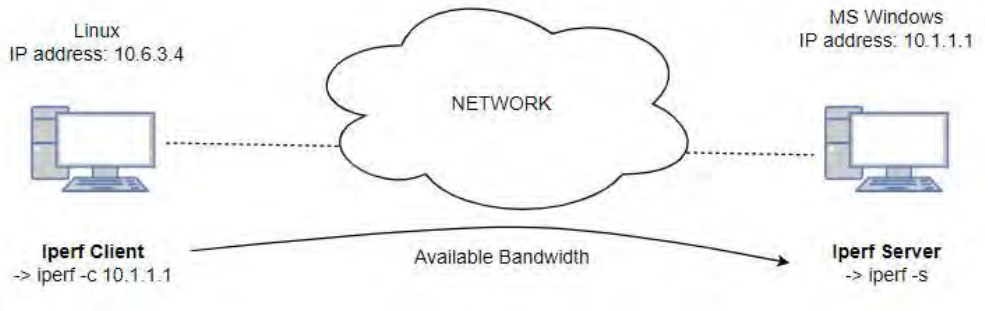


Рис. 1. Работа утилиты Iperf

Cisco IOS IP SLAs

Cisco IOS IP Service Level Agreements (SLAs) – функция на оборудовании Cisco. Cisco IOS IP SLAs использует активный метод контроля, генерируя непрерывный трафик, позволяя таким образом измерить производительность и качество сети. Технология Cisco IP SLA позволяет маршрутизаторам и коммутаторам Cisco выполнять различные сетевые тесты путём обмена данными с другими устройствами Cisco («ответчиками») или обычными хостами сети. Минусом данной технологии является то, что нельзя настроить ответчик IP SLA на устройствах сторонних производителей [1].

IP SLA начинается, когда исходное устройство отправляет сгенерированный пакет устройству назначения. После того, как устройство-адресат получит пакет, в зависимости от типа операции IP SLA, оно отправляет в ответ информацию о временной отметке, чтобы источник произвел вычисление показателей производительности. Операция IP SLA выполняет измерение сети от исходного устройства до пункта назначения в сети с использованием определенного протокола, такого как UDP (рис. 2).

IP SLA собирает уникальное подмножество этих показателей производительности: задержка (как в оба конца, так и в одну сторону), джиттер (направленный), потеря пакетов (направленная), последовательность пакетов, путь (за переход), время загрузки сервера или веб-сайта.

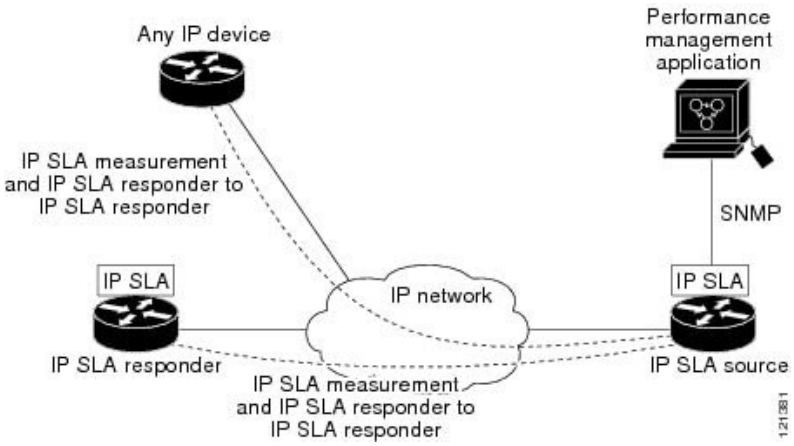


Рис. 2. Работа Cisco IOS IP SLA

Juniper RPM

Juniper RPM (*Realtime Perfomance Monitoring*) – эта технология является аналогом механизма SLA у производителя Cisco, и как и у Cisco предназначена для измерения характеристик каналов в реальном времени.

Когда на устройстве настроен RPM, устройство рассчитывает производительность сети на основе времени ответа пакета, джиттера и потери пакетов. Эти значения собираются с помощью запросов GET протокола передачи гипертекста (HTTP), запросов протокола управляющих сообщений Интернета (ICMP) и запросов TCP и UDP, в зависимости от конфигурации. Запросы ICMP, TCP и UDP являются расширенными и требуют поддержки RPM со стороны устройства с ролью Server, чтобы он генерировал ответы. Кроме поддержки RPM в железе, для этих тестов так же требуется и расширенная лицензия [2].

Устройство с одной стороны канала (*Client*) периодически посылает ряд запросов на устройство (*Server*) на другой стороне канала, получает ответы (или неполучает) и сохраняет результаты (рис. 3).

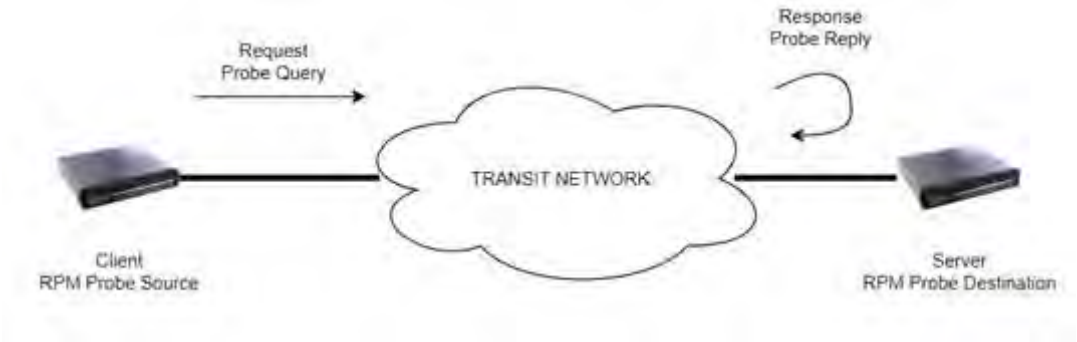


Рис. 3. Принцип работы Juniper RPM

IxChariot

IxChariot – полностью оснащенная система от компании IXIA, для оценки функционирования и надежности сетей и приложений, работающих через различные транспортные интерфейсы. Система имеет базу шаблонов для тестов по стандартам Минкомсвязи и Россвязи. Это эффективное средство оценки использует программные агенты (называемые оконечными точками) для имитации трафика приложений и предоставления центральной консоли информации о ключевых параметрах сети или приложения, таких как пропускная способность, задержки, джиттер и потери пакетов. Конечные точки поддерживают свыше 30 операционных систем, включая мобильные платформы, но все тестируемые точки должны быть зарегистрированы в консоли.

Принцип проведения тестирования IxChariot, рис. 4. Консоль передает скрипт теста на оконечную точку 1, которая передает копию скрипта оконечной точке 2 и уведомляет консоль, что конечные точки готовы. Консоль дает указание начать тестирование, оконечная точка 1 собирает результаты и в конце возвращает в консоль для их отображения.

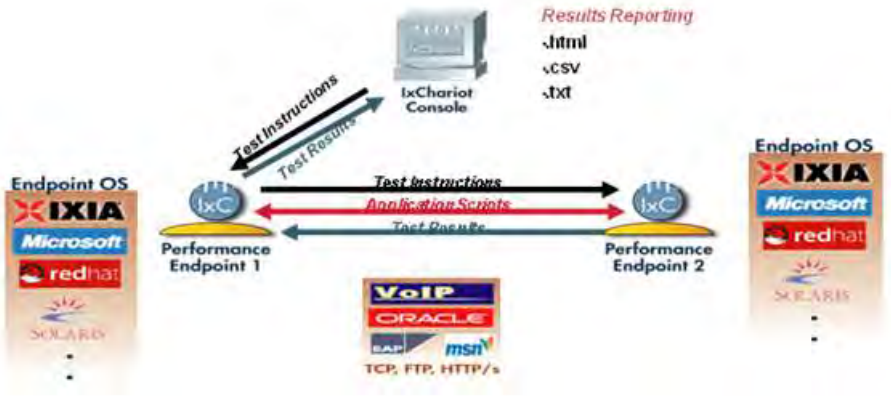


Рис. 4. Проведение тестов IxChariot

IXIA Hawkeye (IxChariot Pro)

Hawkeye – платформа активного сетевого мониторинга, использует реалистичное моделирование трафика для точного измерения производительности. Hawkeye это модификация уже упомянутого IxChariot, который раньше имел название IxChariot Pro, но итоговая версия сильно отличалась от оригинала, что решили сделать отдельным продуктом, но в основе лежит та же технология, что и в IxChariot. Отличием от оригинала является наличие не только программных агентов, но и аппаратных (IXIA XR2000 и IXIA XRPi2), которые могут запускать тест не только до зарегестрированных агентов, но и до внешних сервисов (к примеру, серверов Google).

Система контроля SLA каналов связи компании «Treatface»

Treatface – компания, является дистрибьютором Ixia, разработала систему контроля SLA собственного производства. В систему входит разработанный ими же многофункциональный ПАК TOFSLAN, который утвержден Росстандартом как тип средства измерений качества каналов связи и внесен в Госреестр средств измерений под № 60891–15. Поэтому получаемые результаты измерений могут быть официально использованы в качестве доказательной базы в спорных ситуациях с поставщиками услуг и операторами связи [3].

В разработанной системе контроля SLA имеется большая база шаблонов тестов, компактные пробники, устанавливаемые на любые операцион-

ные системы, а так же это единственная на рынке система, имеющая метрологический сертификат Росстандарта. Особенностью является управление агентами компании, так и агентами IxChariot.

Контроль выполняется посредством активного тестирования каналов связи синтезируемым трафиком. Трафик передается от одного устройства TOFSLAN до другого (или до программного агента IxChariot), и на принимающей стороне измеряются показатели доставки (рис. 5).

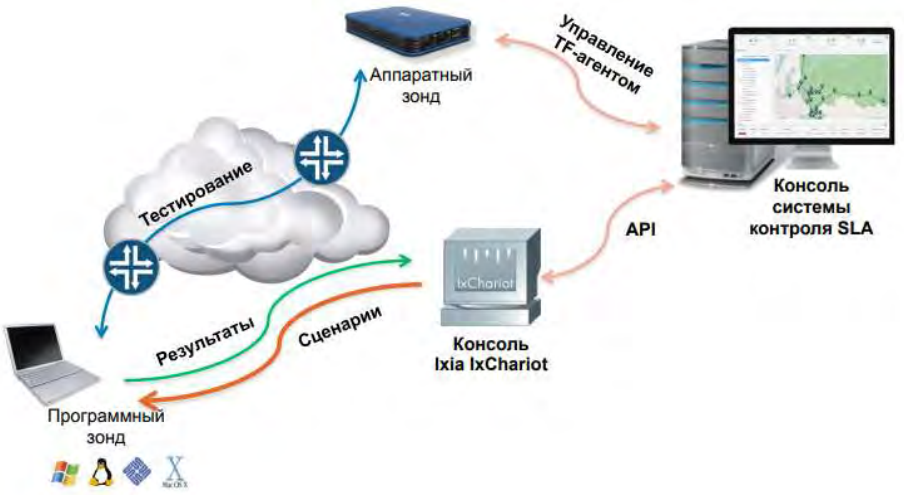


Рис. 5. Базовая схема работы

Представленные комплексы предусматривают установку программных агентов на конец тестируемой сети или использование специального оборудования, что невозможно реализовать при тестировании приложений дополненной реальности, со стороны пользователя, так как нет доступа на сервера.

Список используемых источников:

1. Catalyst 4500 Series Switch Software Configuration Guide, 12.2(44)SG. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/44sg/configuration/guide/Wrapper-44SG/swipsla.html

2. Real-Time Performance Monitoring. URL: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/real-time-performance-monitoring.html#id-understanding-real-time-performance-monitoring-on-switches

3. Зонд контроля качества каналов связи ПАК TOFSLAN. URL:. http://treatface.ru/solutions/sistemy-setevogo-monitoringa/tofslan/

УДК 004.738
ГРНТИ 49.43.29

ОБЗОР АРХИТЕКТУРЫ СЕТЕЙ ПЯТОГО ПОКОЛЕНИЯ O-RAN

Р. В. Киричек, М. А. Рожков

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

Развитие сетей мобильной связи пятого поколения (5G) привело к появлению требований операторов, являющихся основными потребителями оборудования сетей 5G, касающихся обеспечения взаимозаменяемости и интероперабельности между решениями от разных разработчиков. В статье рассматривается принципы и проблемы стандартизации элементов и интерфейсов сетей пятого поколения, в качестве их решения предполагается использовать архитектуру O-RAN при построении сетей нынешнего и будущих поколений.

сети пятого поколения, радиодоступ, беспроводные сети, виртуализация, стандарт.

Существующие на данный момент сети радиодоступа, не являются «открытыми», и почти все операторы вынуждены использовать оборудование одного производителя. В случае же если оператор использует оборудования различных производителей то, как правило оно изолировано друг о друга, и не взаимодействует между собой. Единственное исключения представляет собой верхние уровни сети (ядра сети), реализованные на универсальном оборудовании и использующие стандартизированные интерфейсы (S1 в сетях 4G и NG в сетях 5G) [1]. Что же касается уровня радиодоступа то несмотря на существование открытых стандартов для интерфейсов между базовыми станциями различных производителей, их взаимодействие между собой крайне редко. Как оказалось одних стандартов для унификации сетей нового поколения оказалось недостаточно. В связи с этим было сформировано множество синергетических проектов, альянсов и рабочих групп, у каждой из которых есть свои задачи и направления. Все эти усилия имеют общую цель – создание открытой среды RAN с помощью стандартизованных элементов и интерфейсов.

Open RAN – это группа проектов, запущенная Telecom Infra Project в 2017 году с заявленной целью определения и создания решений 2G, 3G и 4G RAN на основе универсальных, независимых от поставщиков аппаратных и программно-определяемых технологий. Сюда входит создание программируемых виртуализированных решений RAN на основе микропроцессоров общего назначения.

Несмотря на то что обычно «O-RAN» используется в качестве абревиатуры «Open RAN», дефисная номенклатура эволюционировала, чтобы более конкретно представлять Альянс O-RAN с момента основания группы. Наряду с публикацией спецификаций архитектуры Open RAN, инициатива группы была сосредоточена на внедрении искусственного интеллекта (AI), определении интерфейсов и API для обеспечения соответствующей стандартизации и создании необходимой инфраструктуры цепочки поставок. Эти усилия обеспечивают поддержания принципов открытости и интеллекта при построении сетей нового поколения на базе Open RAN.

Открытая сеть радиодоступа (O-RAN) – это концепция, основанная на взаимодействии и стандартизации элементов RAN, включая унифицированный стандарт взаимодействия для аппаратного обеспечения «белого ящика» и элементов программного обеспечения с открытым исходным кодом от различных поставщиков. Архитектура O-RAN объединяет модульный программный стек базовых станций на готовом оборудовании, что позволит взаимодействовать компонентам радио модулей различных производителей [2].

Архитектура O-RAN является основой для создания виртуализированных RAN на открытом оборудовании с интегрированным управлением сетью на базе искусственного интеллекта. Архитектура O-RAN основана на стандартизованных интерфейсах, обеспечивающих открытую, функционально совместимую экосистему различных компонентов и модулей, отвечает требованиям преемственности и дополняет стандарты консорциума 3GPP и других организаций, разрабатывающих отраслевые стандарты. Схема архитектуры O-RAN приведена на рис. [3].

Архитектуру O-RAN можно разделить на следующие ключевые следующие функциональные модули:

− уровень управления и оркестрации/NMS, включая уровень функций Non-RT RIC;

− уровень функций Near-RT RIC;

− уровень функций стека протоколов управляющего модуля Multi-RAT;

− уровень функций стека протоколов узла O-DU;

− уровень функций стека протоколов узла O-RU.

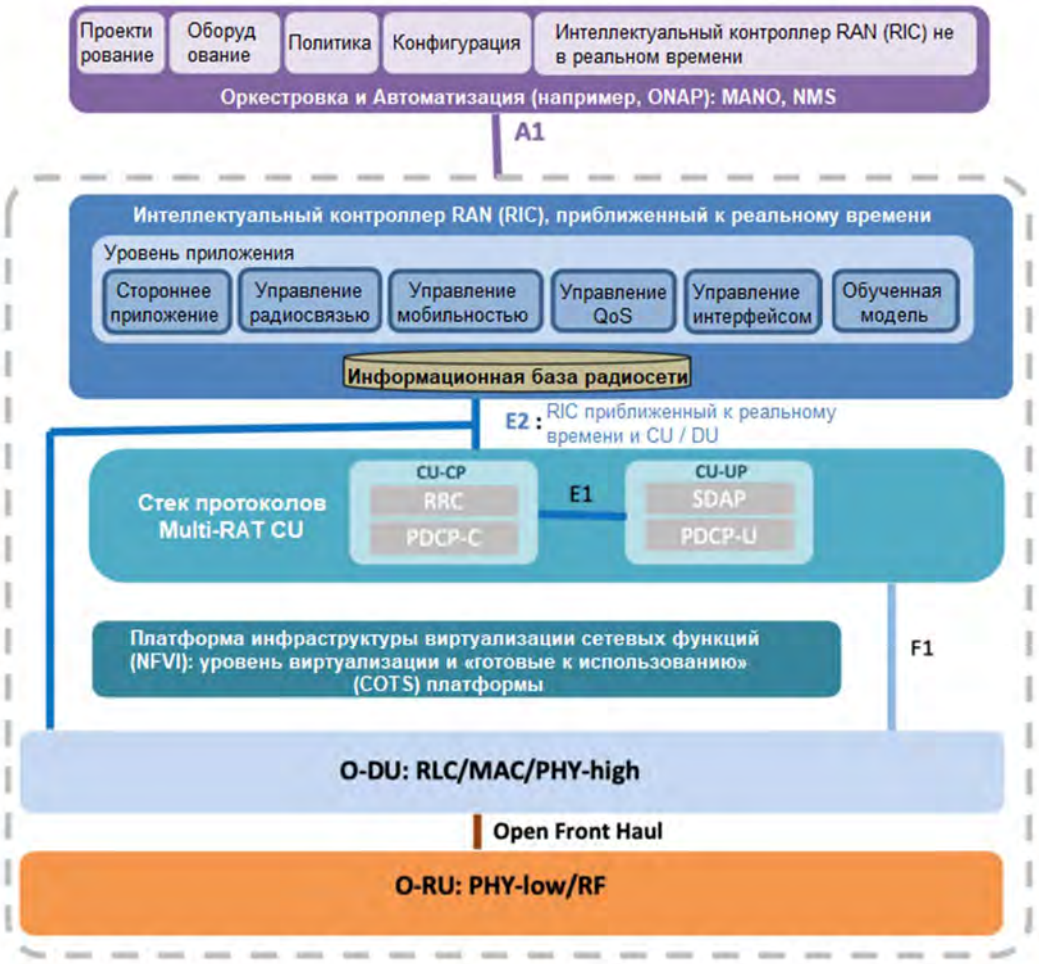


Рис. Схема архитектуры O-RAN

Функции Non-RT RIC включают в себя управление службами и политиками, сбор аналитики RAN и обучение моделей для оптимизации работы RAN в режиме реального времени.

Near-RT RIC представляет собой надежную, безопасную и масштабируемую платформу, которая позволяет гибко устанавливать сторонние управляющие приложения. Функции Near-RT RIC включают в себя чувствительные ко времени функции, такие как балансировка нагрузки, передача обслуживания и контроль интерференции и помех. Интеграция уровней позволяет уровню Near-RT RIC использовать обученные модели и функции управления, хранящиеся в Non-RT RIC, в режиме реального времени.

Функции стека протоколов управляющего модуля Multi-RAT разворачиваются на платформе виртуализации или на любой аппаратной платформе. Задачей управляющего модуля Multi-RAT является реализацией протоколов сети радиодоступа уровня L3 для различных технологий мобильной связи. В рамках функций данного модуля может быть обеспечена поддержка как технологии 4G LTE, так и технологий 5G NewRadio.

Функции стека протоколов узлов O-DU и O-RU включают в себя функции стека протоколов базовых станций уровня L2 и L1, а также основные алгоритмы цифровой обработки сигналов и распределения радио ресурсов в составе базовой станции. Интерфейс между узлами O-DU и O-RU обеспечивает стандартизированное функциональное разделение функций стека протоколов, включая интерфейс разделения нижнего уровня «распределенный модуль – удаленный приемопередающий модуль» и интерфейс разделения верхнего уровня «управляющий модуль – распределенный модуль» (интерфейс F1AP), что обеспечивает взаимодействие и совместимость между оборудованием от разных изготовителей.

Все сетевые функции O-RAN могут быть реализованы как VNF, т. е. как виртуальные машины или контейнеры, размещенные на облачной платформе, и/или как PNF с использованием конкретной аппаратной платформы или оборудования [4].

Заключение

Отход от парадигмы RAN, зависящей от производителей, не только обеспечит большую гибкость при построении пятого и будущих поколениях сетей для операторов, но повысит конкуренцию и развитие сетей в результате появления новых участников. Что потенциально может снизить стоимость оборудования O-RAN. Аспекты межоператорской совместимости Open RAN также могут использоваться для повышения эффективности существующих сетей LTE, поскольку они продолжают включать виртуализацию и дезагрегацию, которые являются предварительными условиями развертывания 5G RAN.

В Российской Федерации построение сетей нового поколения на базе открытой архитектуре O-ran облегчит задачу импортозамещения в связи с тем, что позволит строить и развивать радиосети с применением «отечественного» оборудования и компонентов.

Список используемой литературы

1. Sasha Sirotkin. 5G Radio Access Network Architecture: The Dark Side of 5G. Wiley-IEEE Press, 2020. 448 p. ISBN: 978-1-119-55088-4.

2. Ian Wong. The O-RAN ALLIANCE, Open RAN Architecture, 5G, and Testing Solutions // Innovations in open ran: a technical deep dive., Fierce wireless 23-25 march 2021. URL: https://www.viavisolutions.com/en-us/literature/o-ran-open-ecosystem-power-5g-applications-white-papers-books-en.pdf (дата обращения: 27.03.2013).

3. O-RAN ALLIANCE e.V, O-RAN.WG1.OAM-Architecture-v04.00, Buschkauler Weg 27, 53347 Alfter, Germany, Register of Associations, Bonn VR 11238, VAT ID DE321720189, 2021.

4. O-RAN ALLIANCE e.V, O-RAN.WG1.O-RAN-Architecture-Description-v03.00, Buschkauler Weg 27, 53347 Alfter, Germany, Register of Associations, Bonn VR 11238, VAT ID DE321720189, 2021.

УДК 004.735
ГРНТИ 49.37.29

АНАЛИЗ ТЕХНОЛОГИЙ УЗКОПОЛОСНЫХ БЕСПРОВОДНЫХ СЕТЕЙ СВЯЗИ ДАЛЬНЕГО РАДИУСА ДЕЙСТВИЯ: LoRaWAN, NB-Fi и OpenUNB

Р. В. Киричек, Е. Д. Филин

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

С ростом применения и повышения значимости проектов Интернета вещей, основанных на использовании энергоэффективных сетей дальнего радиуса действия LPWAN (Long-power Wide-area Network), возрастает значение обеспечения информационной безопасности используемых технологий, а именно, таких ключевых принципов как конфиденциальности, целостности и доступности информации, передаваемой между устройствами. В данной работе будет проведен обзор и сравнение технологий LPWAN, работающих в нелицензируемом диапазоне частот, а также проведен анализ особенностей в контексте обеспечении защиты информации, передаваемой по беспроводным каналам связи.

Интернет вещей, энергоэффективные сети дальнего радиуса действия.

В рамках выполнения национальной программы «Цифровая экономика Российской Федерации», 29 марта 2019 г. был подписан приказ об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации. Основной задачей государственного регулирования рынка беспроводных сетей связи Интернета вещей является реализация системы регулирования, которая будет создавать условия для эффективной конкуренции, направлена на своевременное создание и развитие рынка новых услуг и улучшения качества сервиса [1]. На февраль 2021 года Росстандартом утверждены два предварительных национальных стандарта (далее – ПНСТ) – на протоколы NB-Fi [2, 3, 4] и LoRaWAN [5, 6]. В декабре 2020 г. техническим комитета 194 «Кибер-физические системы» на базе Российской венчурной компании (РВК) при участии компании WAVIoT (торговая марка ООО «Телематические Решения») и Ассоциации Интернета вещей разработан ПНСТ на протокол NB-Fi. В феврале 2021 г. центром компетенций НТИ «Сквозные технологии беспроводной связи и интернета вещей» АНОО ВПО «Сколковского института науки и технологий» при участии Технического комитета 194 «Кибер-физические системы» и компании GoodWAN была представлена вторая версия ПНСТ на протокол OpenUNB [7, 8].

Технология LoRaWAN (*LoRa of Wide Area Network*) позволяет осуществлять передачу информации на большом расстоянии с приложениями Интернета вещей, объединяя технологии двух уровней сетевой модели OSI – физического уровня, основой которого является технология LoRa (*Long Range*) [9, 10, 11] и канального уровня, основой которого является открытый протокол LoRaWAN, версия 1.0 которого была представлена в 2015 г., а версия 1.1 в 2017 г. [12]. Для развития и поддержки технологии LoRaWAN была создана некоммерческая организация LoRa Alliance. Основными достоинствами технологии являются: большая дальность передачи информации, высокая проникающая способность, высокая помехоустойчивость, высокая масштабируемость сети, низкое энергопотребление, низкая стоимость конечного устройства и низкая стоимость развертывания [13, 14]. Данная технология является оптимальной для реализации задач, в которых требуется обеспечить большую дальность передачи данных устройствами с низким энергопотреблением с допустимыми временными задержками. Одной из главных особенностей технологии LoRaWAN является способность принимать сигналы, лежащие ниже уровня шума. Маломощные сигналы в линейно-частотной модуляции трудно обнаружить и перехватить, но при этом LoRa чувствительна к широкополосным помехам. Если две базовые станции, находящиеся рядом, работают на одной частоте, то они будут сильно мешать друг другу. LoRaWAN поддерживает двунаправленную связь. LoRaWAN использует два уровня безопасности: один для сети и второй – для приложения.

NB-Fi обеспечивает связь между устройствами в труднодоступных местах на больших расстояниях (до 10 км. в городской среде) при плотной застройке, обеспечивая долгий рок работы устройств на одной батарее (до 10 лет). Являясь результатом российских разработок, технология адаптирована к использованию на территории Российской Федерации, соответствует требованиям регулирующих органов и позволяет осуществить интеграцию с решениями других отечественных производителей. Исполнительные устройства собирают и передают информацию на базовые станции сети, которые в дальнейшем осуществляют передачу на сервер для обработки и отображения данных в клиентских приложениях посредством API IoT-платформы WAVIoT. В устройствах используется чип ON Semiconductor AX8052F143, поддерживающий стандарт NB-Fi на физическом уровне, обладающий высокой чувствительностью, низким энергопотреблением и возможностью применения в диапазонах частот 430–500 МГц и 860–925 МГц. Базовые станции и чип NB-Fi имеют чувствительность приемника до −148 дБм (на скорости 50 бит/с). Рабочая полоса частот для восходящих сигналов, от устройства к базовой станции (Uplink), составляет 50 кГц, для нисходящих сигналов, от базовой станции к устройству (*Downlink*), составляет 100 кГц. Все устройства с двухсторонней связью поддерживают адаптивное

изменение скорости передачи сигнала – при достаточном уровне приема сигнала устройства автоматически переходят на более высокую скорость передачи данных. Базовая станция NB-Fi позволяет принимать сигнал с уровнем сигнала, не превышающем уровень шума.

OpenUNB является открытым протоколом с открытой архитектурой, при создании которого был отброшен ряд требований с целью создать технологию, которая бы позволила максимально удешевить надежный и безопасный сбор информации от множества датчиков. OpenUNB – это технология односторонней передачи без обратного канала, есть только канал от исполнительных устройств до базовой станции. Технология спроектирована таким образом, чтобы в исполнительных устройствах было возможно использование разнообразных чипов мировых производителей, поэтому устройства получается не дороже устройств с Sigfox и LoRaWAN. Сетевые шлюзы реализованы на программно определяемых радиосистемах (SDR), в которых используются доступные компоненты от ведущих мировых производителей, поэтому цена на них является конкурентоспособной. В нелицензируемом диапазоне частот максимальная мощность сигнала ограничена, поэтому дальность передачи зависит от многих условий. Используя сигналов в полосе 100 или 200 кГц, позволяет обеспечивать пропускную способность сетевого шлюза аналогичную Sigfox, и большую, чем у LoRaWAN. За счет использования методов помехоустойчивого кодирования сигнала были получены высокие показатели защиты от естественных и искусственных помех, что обеспечивает необходимую дальность связи в реальных условиях эксплуатации. Ключевым элементом обеспечения безопасности является система динамического кодирования, которая обеспечивает защиту передачи адреса устройства в сети [15].

Фактически, LPWAN, работающие в нелицензируемом диапазоне частот, делятся на две группы – сверхузкополосные (далее – UNB) и сверхширокополосные (далее – UWB) технологии связи. На территории Российской Федерации устройства, работающие в нелицензируемых диапазонах частот для неспециализированных устройств малого радиуса действия, передают информацию на частотах 866–868 МГц при мощности до 25 мВт с рабочим циклом 1 % (или режимом LBT), а также запретом на работу вблизи аэропортов, и 868,7–869,2 МГц при мощности до 100 мВт с рабочим циклом 10 % (или режимом LBT) без такого ограничения [16].

В системах UWB канал занимает полосу шириной 125–250 кГц, в UNB 50–100 Гц, то есть в диапазоне 868,7–869,2 МГц доступна полоса частот 500 кГц, и при полосе шириной в 125 кГц возможно разместить три канала, в то время с шириной 50 Гц тысячи. Если в эфире сильная помеха, устройство UWB не имеет возможности перестроиться на другую частоту, в то время как устройство UNB имеет возможность оперативно изменить частоту передачи информации для защиты от помех. Системы UNB передают

информацию на определенной скорости, в то время как системы UWB позволяют осуществлять передачу на адаптивной скорости. Системы UWB позволяют осуществлять передачу на больших скоростях, создавать дуплексный канал связи и менее восприимчивы к температурным колебаниям, а также обладают большим количеством параметров для настройки, чем в системах UNB.

Системы UWB обеспечивают симметричный канал связи, поэтому каждый чип может быть приёмником и передатчиком. В системах UNB для организации приема информации исполнительным устройством от базовой станции, базовая станция должна работать на частоте исполнительного устройства, однако, системы UNB чувствительны к точности установки частоты, поэтому, высокая относительная нестабильность частоты кварцевого резонатора является одной из главных проблем систем UNB – невозможности организации симметричной обратной связи. В системе UNB частота исполнительного устройства не определена, так как на плате установлен кварц, который может разносить сигнал на частоты в сотни герц. Для передачи информации исполнительному устройству, базовая станция в момент выхода исполнительного устройства в эфир должна установить частоту передачи и передать информацию на определенной частоте. В системе UWB, благодаря ширине полосы, устройства без каких-либо проблем могут принимать сигналы, смещенные на двадцать-тридцать килогерц, обеспечивая обратную связь для всех классов устройств.

Заключение

Каждая из систем обладает достоинствами и недостатками, которые напрямую зависят от того, является система сверхузкополосной или сверхширокополосной, и однозначного ответа, какая из систем является наилучшей, нет. В зависимости от задач, которые должна решать система, определяется и оптимальный выбор системы LPWAN. В дальнейших работах будет проведен анализ технологий, приведенных выше, на устойчивость к преднамеренным электромагнитным воздействиям, оказываемым на линии передачи информации.

Исследование выполнено при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки ведущих научных школ Российской Федерации в рамках научного проекта НШ-2604.2020.9.

Список используемых источников

1. Концепция построения и развития узкополосных беспроводных сетей связи Интернета вещей на территории Российской Федерации. Утв. М-вом от 29.03.2019 № 113. Москва. 2019. 6 с.

2. Интернет ресурс. URL: https://iot.ru/promyshlennost/rosstandart-utverdil-predvaritelnyy-natsionalnyy-standart-dlya-nb-fi (дата обращения: 10.03.2021).

3. Интернет ресурс. URL: http://tc194.ru/nb-fi. (дата обращения: 10.03.2021).

4. Проект национального стандарта Российской Федерации. Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi). Москва. Стандартинформ. 2020.

5. Интернет ресурс. https://rossma.ru/news/росстандарт-утвердил-стандарт-п. (дата обращения: 10.03.2021).

6. Предварительный национальный стандарт Российской Федерации. Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением. Москва. Стандартинформ. 2019.

7. Интернет ресурс. URL: https://www.openunb.org/openunb-text (дата обращения: 10.03.2021).

8. Предварительный национальный стандарт Российской Федерации. Информационные технологии. Интернет вещей. Протокол передачи данных для высокоемких сетей на основе сверхузкополосной модуляции радисигнала. Москва. Стандартинформ. 2019.

9. Кумаритова Д. Л., Киричек Р. В. Обзор и сравнительный анализ технологий LPWAN сетей // Информационные технологии и телекоммуникации. 2016. № 4. С. 33–48.

10. Фам В. Д., Кисель В. С., Киричек Р. В., Овчинников А. О., Бородин А. С. Метод передачи изображений в энергоэффективной сети дальнего радиуса действия с ячеистой топологией // Труды научно-исследовательского института радио. 2021. № 1. С. 2–15.

11. Kirichek R., Pham V.D., Koucheryavy A., Vishnevsky V. Analytic model of a Mesh topology based on LoRa technology // 22, Digital Security Global Agenda for Safe Society. 22nd International Conference on Advanced Communications Technology: Digital Security Global Agenda for Safe Society, ICACT 2020 - Proceeding. 2020. С. 251–255.

12. LoRaWAN 1.1 Specification. LoRa Alliance, Inc. 2017

13. Dina M. Ibrahim. Internet of Things Technology based on LoRaWAN Revolution // 10th International Conference of Information and Communication Systems (ICICS). 2019.

14. Jelena Culic Gambiroza, Toni Mastelic, Petar Solic, Mario Cagalj // Capacity in LoRaWAN Networks: Challenges and Opportunities. IEEE. 2019.

15. Интернет ресурс. URL: https://habr.com/ru/post/523866 (дата обращения: 10.03.2021).

16. Решение ГКРЧ № 18-46-03-01 от 11 сентября 2018 г. «О выделении полос радиочастот, внесении изменений в решения ГКРЧ и продлении срока действия решений ГКРЧ». Приложение № 12.

УДК 004.048
ГРНТИ 50.43.15

АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПРОГНОЗИРОВАНИЯ ПОТРЕБЛЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ КОНТЕЙНЕРНЫХ ПРИЛОЖЕНИЙ В КЛАСТЕРЕ

С. В. Кисляков, Е. Ю. Мордвинов

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

При разворачивании приложений с применением технологий контейнеризации в кластере возникает необходимость дальнейшего непрерывного контроля за потребляемыми ресурсами. В статье предлагается использовать методы машинного обучения для анализа данных об использовании ресурсов CPU/RAM, собранных в процессе работы приложения, для составления прогноза на их основе. В ходе работы рассматривается создание тестового окружения с приложением, использование системы мониторинга и сторонних модулей для сбора необходимых данных из системы. В результате производится оценка применения выбранных методов прогнозирования и выбор наиболее подходящих для решения поставленной задачи.

машинное обучение, мониторинг, DevOps.

Микросервисный подход является одним из главных направлений при разработке программного обеспечения на данный момент. Вместе с этим развиваются подходы с использованием контейнеризации, которые реализуют микросервисные архитектуры [1] и позволяют ускорить процесс разработки, тестирования и разворачивания приложений. Поддержка лишь одного контейнера для каждого из приложений является недостаточным условием в силу необходимости обеспечения постоянной и бесперебойной работы приложений. В связи с этим возникают сопутствующие контейнеризации понятия оркестрации и кластеризации. Объединяя набор контейнеров в единый кластер с применением определенных правил и инструментов оркестрации можно обеспечить выполнение необходимых требований по качеству поддержки приложений, а также упростить работу с системой на протяжении всего жизненного цикла контейнеров.

Оркестрация контейнеров во многом повлияла на традиционные PaaS (*Platform-as-a-Service*), почти полностью изменив процессы упаковки, разворачивания, масштабирования и обновления приложений. Вместе с этим появились новые платформы, которые уже основываются на этих новых принципах. Одним из таких решений уровня PaaS является Kubernetes [2],

предоставляя фреймворк для управления большим набором контейнеров в распределенных системах.

Архитектура кластера Kubernetes состоит из двух типов узлов: master и worker. Master узел является единой точкой входа для управляющих команд от пользователей, содержит в себе модули для конфигурации кластера, а также выполняет задачи организации работы worker узлов, на которых происходит запуск приложений с использованием pod – модулей, который в большинстве случаев содержат в себе по одному контейнеру с приложением. Worker узел содержит в себе модули для обработки запросов от master узла и оконечных пользователей, и запущенные pod, контейнеры в которых используют выбранную среду исполнения, например Docker.

Для поддержания заданного состояния кластера и предотвращения выхода из строя приложения Kubernetes реализует механизмы вертикального и горизонтального масштабирования. Вертикальное масштабирование происходит в рамках существующего объема вычислительных ресурсов и предполагает внутреннее перераспределение ресурсов между узлами и pod, в то время как горизонтальное предлагает их расширение (добавление новых виртуальных машин). В условиях ограниченных ресурсов и требований по качеству обслуживания приложений, необходимость в вертикальном масштабировании возрастает. В целях автоматизации этого процесса предлагается использовать алгоритмы машинного обучения для анализа потребления вычислительных ресурсов уже запущенных приложений и дальнейшего прогноза, который поможет выбрать оптимальное распределение ресурсов. Для этого необходимо решить ряд задач: создание тестового окружения на базе Kubernetes; размещение системы мониторинга для учета выбранной метрики; разработка модуля для сбора данных из системы мониторинга и их подготовка для анализа; выбор и анализ методов машинного обучения с полученными данными для формирования вывода о возможности их использования для прогнозирования.

Для реализации этих задач на практике был выбран провайдер облачных сервисов AWS (*Amazon Web Services*). На базе сервиса EC2 (*Elastic Compute Cloud*) был развернут виртуальный сервер с образом операционной системы Ubuntu v20.04, 2 CPU, 2GB RAM. Для Kubernetes был выбран дистрибутив Minikube, позволяющий создать кластер на одной виртуальной машине. Для мониторинга в кластере был размещен Prometheus [3] – отдельный pod, осуществляющий комплексный мониторинг всех модулей кластера. В созданный кластер также был добавлен тестируемый pod, данные о потреблении ресурсов которого будут собираться системой мониторинга. В качестве метрики контейнера для анализа было выбрано значение потребления ресурсов CPU.

Первым этапом анализа данных является получение первоначального набора данных в формате «время – значение» из системы мониторинга с помощью REST API Prometheus и составление CSV файла. На втором этапе необходимо произвести проверку на стационарность, так как полученные данные представляют временной ряд, а прогнозирование нестационарных данных невозможно из-за изменения их статистических характеристик со временем. Данные были проверены с помощью расширенного теста Дики-Фуллера из библиотеки Python Statsmodels, который показал стационарность временного ряда. Дальнейший анализ сводится к выбору методов машинного обучения, которые позволят прогнозировать значения выбранной метрики. Такой тип задач и исходных данных предполагает использование методов регрессии [4], которые позволяют прогнозировать вещественные значения зависимой переменной *Y* по независимой *X*. Исходя из этого были выбраны три алгоритма для анализа: случайный лес, градиентный бустинг и стекинг. В общем виде они состоят из трех шагов: формирование набора данных, использование алгоритма и обработка результатов. Случайный лес является примером использования метода бэггинга (*bagging – bootstrap agregation*). На первом этапе из исходного набора данных формируются разные наборы данных (*bootstrap* выборки), которые далее параллельно используются в одинаковых алгоритмах, а обработка результата происходит усреднением полученных значений от каждого алгоритма. Метод бустинга последовательно выстраивает этапы формирования данных, использования алгоритма и обработки результата, каждый раз повторяя этот цикл с результатом от предыдущего, уделяя внимание случаям в которых была допущена ошибка. Метод стекинга предполагает наличие одинаковых наборов данных на входе, а алгоритмы используются разные, имея один решающий для обработки результатов. Объединяет эти подходы использование ансамблей алгоритмов машинного обучения – объединении слабых моделей и их комбинирование с помощью усреднения для получения лучшего результата. В качестве слабой модели используется дерево принятия решений. Дерево принятия решений для задач регрессии строится на основе последовательного деления набора значений *Y* по условию переменной *X* с целью минимизации суммарного значения сумм квадратов ошибок (1). Если имеется набор значений переменных $x_{1,2,3\ldots n}$ $y_{1,2,3\ldots n}$, то условие для деления и составления первой пары узлов будет следующим:

$$\min\left(\sum_1^i (y_i - \frac{\sum_1^i y_i}{i})^2 + \sum_{i+1}^n (y_n - \frac{\sum_{i+1}^n y_i}{n-i})^2\right). \quad (1)$$

Алгоритмы для обучения были получены из библиотеки Python Sklearn [5]. Данные предварительно были разделены на обучающую и тестовую выборку в отношении 80/20. Первая выборка используется для обучения алгоритма, а тестовая для проверки и дальнейшей оценки. В результате

были получены графики (рис. 2, 3, 4), показывающие зависимость уровня использования CPU pod в кластере Kubernetes от времени для реальных спрогнозированных данных.

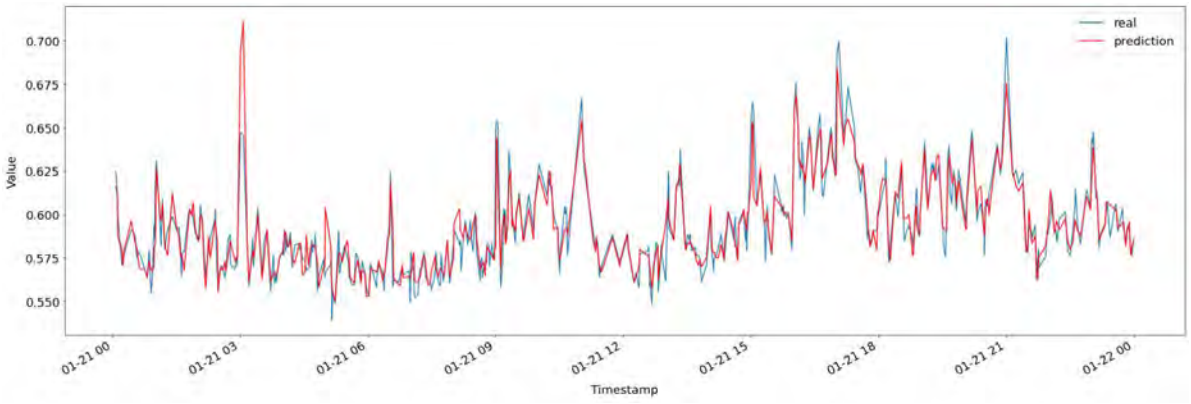


Рис. 2. Случайный лес

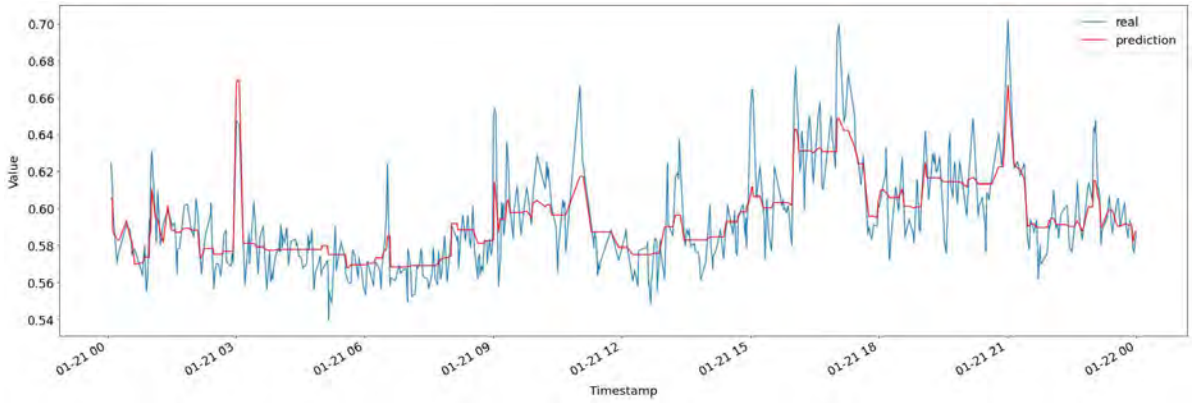


Рис. 3. Градиентный бустинг

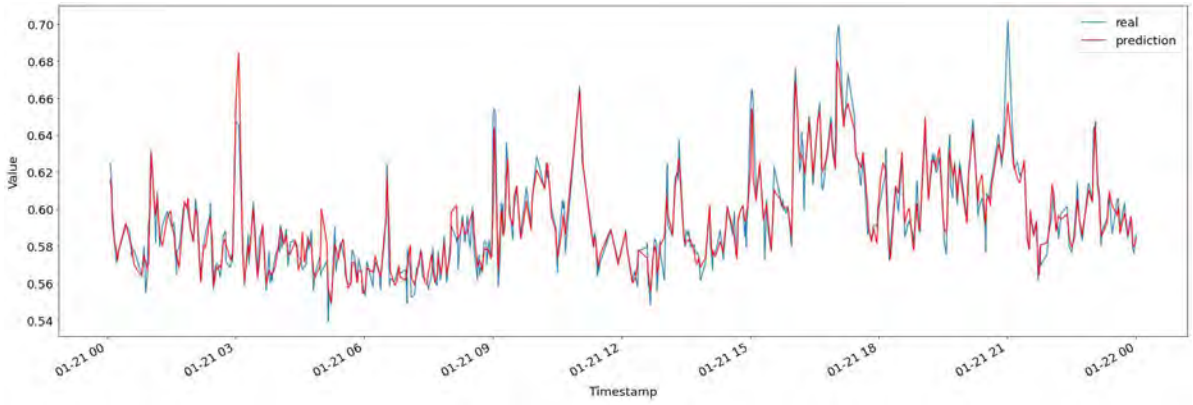


Рис. 4. Стекинг регрессии

Для оценки качества полученных результатов алгоритмов используется коэффициент детерминации (2). Эта метрика принимает значения от 0 до 1

и показывает насколько полученный прогноз отражает целевую переменную (табл.1). Если модель делает максимально точный прогноз, то значение коэффициента детерминации будет равно 1.

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - y_i^*)^2}{\sum_{i=1}^{n}(y_i - y_i^+)^2}, \quad (2)$$

где $(y_i - y_i^*)^2$ – сумма квадратичной ошибки,
$(y_i - y_i^+)^2$ – сумма разниц между значением и средним.

ТАБЛИЦА. Результаты оценки прогнозов для исследуемых алгоритмов

	Случайный лес	Градиентный бустинг	Стекинг
Коэффициент детерминации	0,856806	0,691057	0,896197

На основе полученных результатов можно сделать вывод о преимуществе алгоритма стекинга регрессии для решения задачи прогнозирования временного ряда данных об использовании ресурсов CPU pod внутри кластера Kubernetes.

Список используемых источников

1. Irakli Nadareishvili, Ronnie Mitra, Matt McLarty, Mike Amundsen Microservice Architecture: Aligning Principles, Practices, and Culture: O'Reilly Media, Inc., 2016. 146 p.

2. Nigel Poulton, Pushkar Joglekar The Kubernetes Book: The fastest way to get your head around Kubernetes: Packt Publishing, 2019. 228 p.

3. Brian Brazil Prometheus: Up & Running : Infrastructure and Application Performance Monitoring: O'Reilly Media, Inc., 2018. 369 p.

4. Бринк Х., Ричардс Дж., Феверолф М.. Машинное обучение. СПб.: Питер, 2017. 336 с.

5. Элбон К. Машинное обучение с использованием Python. СПб.: БХВ-Петербург, 2020. 384 с.

УДК 004.056.53
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ ТОЧЕК ДОСТУПА В РЕЖИМЕ PSK К DOS АТАКАМ НА БЕСПРОВОДНУЮ СЕТЬ

А. Ю. Кистуга, М. М. Ковцур, А. Г. Оганесян

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

Одним из элементов, лежащих в основе сети IEEE 802.11, является беспроводная точка доступа. Атаки, которым могут подвергаться точки доступа, можно условно разделить на три группы, в соответствии с тремя фундаментальными принципами информационной безопасности: атаки на нарушение конфиденциальности, целостности и доступности. Цель последних – организовать вынужденный простой, чтобы пользователь не смог получить доступ к услугам сети. Атаки на доступность часто представлены различными DoS-атаками. Статья посвящена исследованию влияния атак на беспроводные точки доступа, функционирующие в режиме PSK.

точка доступа, PSK, DoS, Wi-Fi.

Беспроводные сети часто подвергаются атакам. В частности, причина состоит в том, что доступ к физической среде в беспроводных сетях получить значительно проще, чем в проводных. Злоумышленнику достаточно находится в зоне действия сети и иметь при себе сетевой адаптер, отвечающий его целям [1]. Одним из распространенных видов атак на беспроводные сети являются DoS-атаки [2, 3]. Актуальность DoS-атак обусловлена еще и тем, что злоумышленнику достаточно иметь лишь одно устройство с беспроводным сетевым адаптером, чтобы полностью нарушить работу точки доступа [4, 5].

Чем выше устойчивость точки доступа, тем сложнее злоумышленнику вызвать в ее работе отказ в обслуживании [6]. Для оценки устойчивости точки доступа проводятся различные DoS-атаки и в зависимости от того, как точка доступа на них реагирует, делаются выводы о наличии уязвимостей в данной точке доступа. Будем считать, что чем больше уязвимостей к определённым DoS-атакам обнаружено, тем ниже устойчивость точки доступа.

Точка доступа (ТД) содержит в себе таблицу ассоциаций, которая имеет ограниченный размер [7, 8]. В ходе тестирования устойчивости исследуются 3 атаки. Все три атаки направлены на переполнение таблицы ассоциаций на точке доступа, однако делают это немного разными способами.

1 атака – Authentication flood. При данной атаке на ТД отправляется много фреймов типа Authentication Request со случайными MAC-адресами

источников. Получая запросы на аутентификацию, ТД создаёт в таблице ассоциаций записи. Однако, в силу ограниченности размера таблицы ассоциаций, постепенно ТД полностью заполняется и подключение новых легитимных клиентов не представляется возможным [9]. ТД может отправить в ответ фрейм Authentication Response и ждать получения от клиента подтверждения – фрейма Ack. Время ожидания согласно стандарту IEEE 802.11 составляет по умолчанию 43 мкс, однако это значение может варьироваться. Затем ТД выполняет повторную передачу фрейма с указанием флага R (*retransmit*). После 15 повторных передач ТД прекращает попытки связаться с клиентом и высылает в его адрес фрейм деаутентификации, тем самым извещая (пусть и не существующего) клиента о завершении коммуникации с ним.

2 атака – Association flood. В этой атаке на ТД также отправляются запросы на ассоциацию со случайными MAC-адресами источников. Если ТД уязвима к данной атаке, получив от злоумышленника фрейм Association Request, ТД также создаст запись в таблице ассоциаций [10]. Также она может прислать в ответ фрейм Association Response, в котором указывается Association ID – порядковый номер клиента, зарегистрированного на ТД.

3 атака – Association table overflow. Также ее можно назвать Authentication Association flood. Главное отличие от атаки 2 заключается в подложном выполнении стадии аутентификации и требуется в ситуации, когда ТД не реагирует на атаку 2 в чистом виде.

Методика тестирования включает в себя следующие этапы:

- организация сети;
- проведение мониторинга сети без атак;
- подготовка инструментария для исследования атаки на сервере;
- тестирование DoS-атаки Authentication flood;
- тестирование DoS-атаки Association flood;
- тестирование DoS-атаки Association table overflow;
- анализ результатов.

Под сервером подразумевается виртуальная машина на Kali Linux 2020.4. К ней подключается два сетевых адаптера EDUP 802.11n Nano Adapter. Один адаптер используется для мониторинга сети, другой для запуска фреймов в беспроводную среду. В качестве исследуемой точки доступа выступает беспроводной маршрутизатор Tp-Link AC1750, который работает в диапазоне 2,4 ГГц и в режиме PSK. Схема лабораторного стенда представлена ниже на рис. 1.

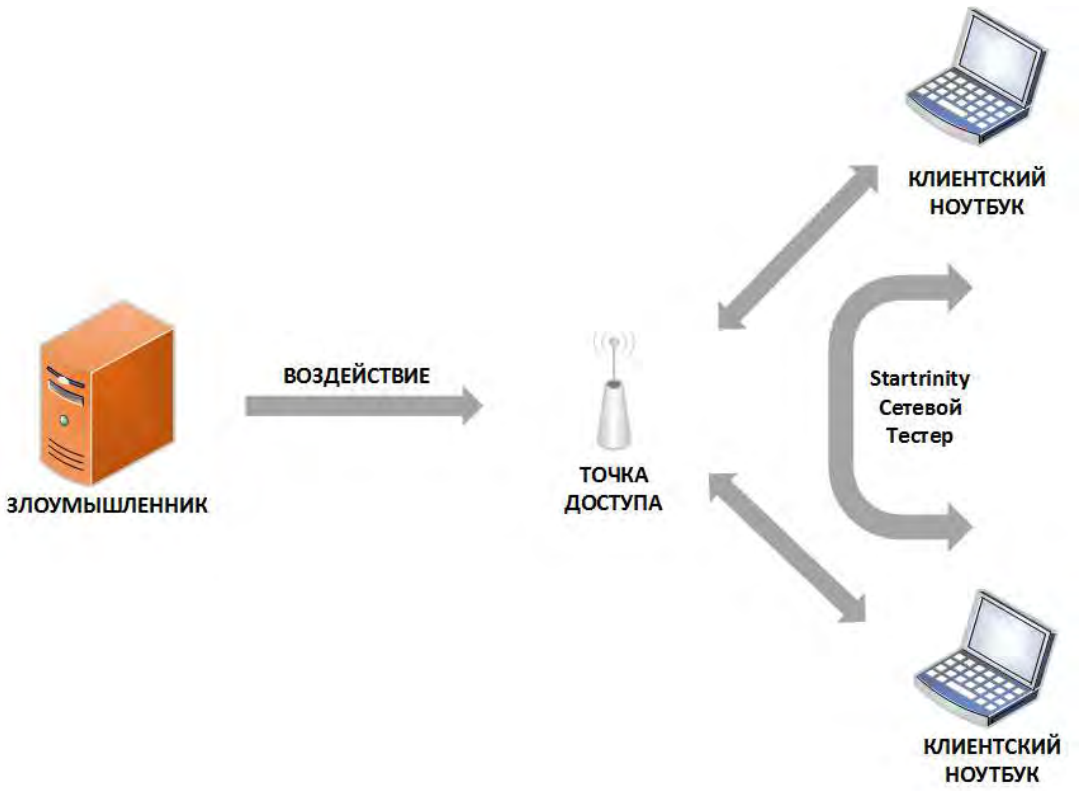


Рис. 5. Схема стенда

Как видно из схемы стенда, клиенты связываются между собой посредством утилиты Startrinity Network Tester, которая наглядно демонстрирует статистику касательно качества связи до проведения атак и во время их проведения.

Также для проведения тестирования разработана программа на языке Python с использованием библиотеки Scapy для генерации фреймов, которые потом отправляются в сеть.

Демонстрация работы программы представлена на рис. 2. В данном случае представлен пример ввода параметров для генерации фреймов для моделирования атаки Association table overflow.

```
┌──(ararat㉿pc)-[~/Рабочий стол]
└─$ sudo python3 FrameGen.py
Введите количество фреймов: 100
Введите MAC-адрес цели в формате "AA:BB:CC:11:22:33": 7d:d9:2f:67:2e:cf
Введите тип атаки "Auth", "Asso", "AuthAsso" или "AuthAckAsso": AuthAsso
Введите имя и расширение для pcap-файла дампа в формате "Dump.pcap": AuthAsso.pcap
Введите имя сети: SadWiFi
Ждите! Генерируется дамп дла атаки "Authentication+Association flood"...
Ура! Дамп сгенерирован!
```

Рис. 6. Образец ввода параметров в программу

Результаты проведённого исследования продемонстрировали, что в режиме PSK на оборудовании Tp-Link AC1750 эффективной оказалась только

1 атака – Authentication flood, так как эффект сохранился и после прекращения атаки, а также клиенты потеряли доступ к Интернету. Если сравнить снимки экрана из утилиты Startrinity Network Tester до начала атаки (рис. 3) и во время (рис. 4), то можно заметить, как выросло среднее значение задержки и джиттера. Также изменения видны на графике, отражающем распределение джиттера.

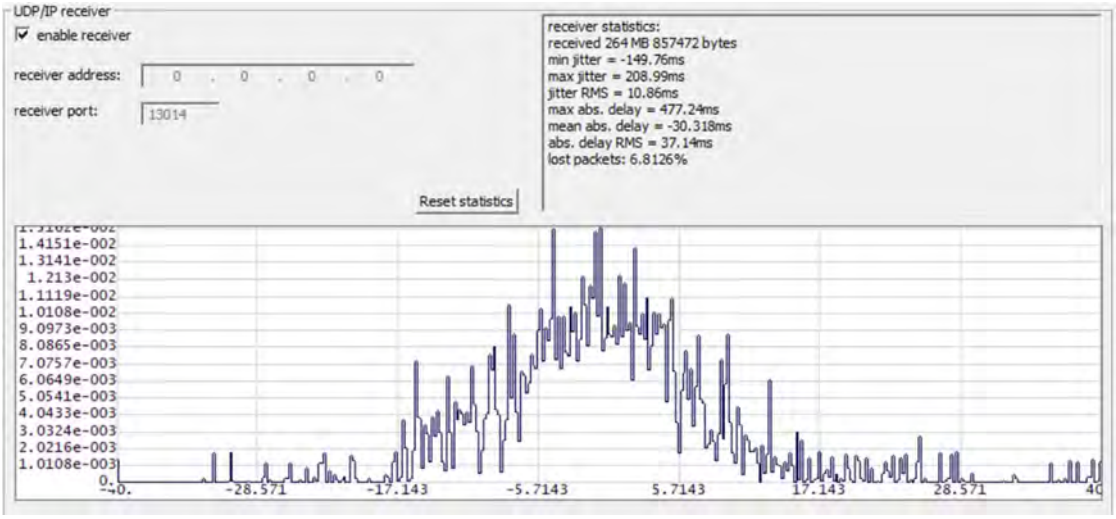


Рис. 7. Показания утилиты до атаки

Снимок экрана во время проведения атаки:

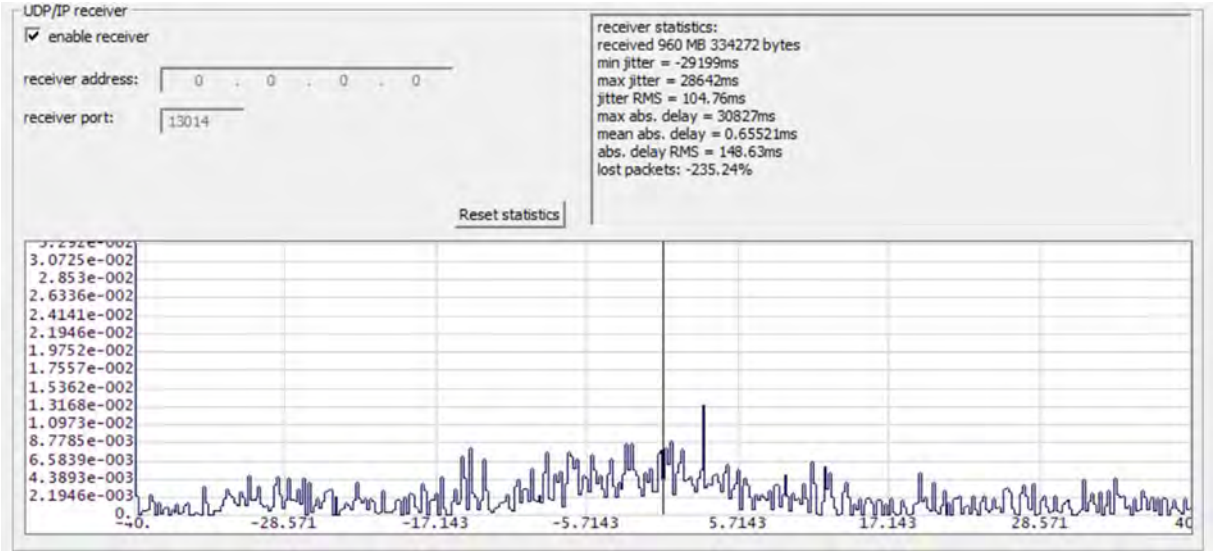


Рис. 8. Показания утилиты во время атаки

Можно сделать вывод, что исследуемая точка доступа оказалась неустойчива к атаке Authentication flood и устойчива к атакам Association flood и Association table overflow. В качестве защиты эффективнее всего приме-

нять Wireless IPS. Также можно использовать второй маршрутизатор, работающий на частоте 5 ГГц. Стоить отметить, что рассмотренные атаки также могут быть актуальны для открытых сетей и для IEEE 802.1x сетей, т. к. все атаки выполняются на процедуры, существующие в том числе и в указанных режимах работы.

Список используемых источников

1. Гамидов Т. О., Виткова Л. А., Ковцур М. М. Разработка моделей и алгоритмов анализа данных для исследования хода инцидентов и кризисов в социальных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 3–10.

2. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70–76.

3. Миняев А. А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информатизация и связь. 2020. № 6. С. 29–36.

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. Ушаков И. А. Обнаружение инсайдеровв корпоративной компьютерной сетина основе технологий анализа больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 38–43.

6. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

7. Штеренберг С. И., Щеголева Д. И., Виноградова О. М. Синхронизированное использование систем защиты информации для контроля учёта рабочего времени // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 3–8.

8. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства Linux / // Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657–662.

9. Ильина-Сидорова И. Специфика защиты беспроводных сетей // Беспроводные технологии. 2017. № 2. С. 50–53.

10. Бирюков А., ZYXEL NWA1123-AC-PRO. Тестируем защищенность // Системный администратор. 2017. N 11. С. 50–53.

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

УДК 004.056.53
ГРНТИ 81.93.29

СОСТЯЗАТЕЛЬНЫЕ АТАКИ В НЕЙРОННЫХ СЕТЯХ

И. А. Ковалев, Н. А. Косов

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

В статье обозреваются известные методы состязательных атак на модели машинного обучения, в частности, на нейронные сети, их возможные варианты реализации, методы защиты от подобных атак, приводятся примеры существующих практик данных так. Дается оценка возможности их применения. Дается определение и практическая оценка применения методов состязательных атак

состязательные атаки, нейронные сети, модель, машинное обучение, белый ящик, черный ящик.

Глубокое обучение превратилось в сильную и эффективную структуру, которая может быть применена к широкому спектру сложных проблем обучения, которые в прошлом было трудно решить с помощью традиционных методов машинного обучения. За последние несколько лет глубокое обучение радикально продвинулось вперед, так что оно может превзойти производительность человеческого уровня по ряду задач. Как следствие, глубокое обучение широко используется в большинстве современных повседневных приложений. Однако безопасность систем глубокого обучения уязвима для созданных состязательных примеров, которые могут быть незаметны для человеческого глаза, но могут привести модель к неправильной классификации результатов. В последнее время различные типы противников, основанные на их модели угроз, используют эти уязвимости для компрометации системы глубокого обучения, где противники имеют высокие стимулы. Следовательно, чрезвычайно важно обеспечить устойчивость алгоритмов глубокого обучения против этих противников. Однако существует лишь несколько сильных контрмер, которые могут быть использованы во всех типах сценариев атак для разработки системы глубокого обучения. В этой статье мы попытаемся подробно обсудить различные типы состязательных атак с различными моделями угроз, а также рассмотрим механизмы защиты против подобных сценариев атак [1].

Состязательные атаки – это совершение попытки злоумышленника повлиять на вывод модели машинного обучения изменении входных данных незаметным для человека образом. В результате можно манипулировать выходными данными модели в целях атакующего.

Данные атаки имеют огромное практическое значение и потенциальную опасность, ведь модели машинного обучения очень быстро распространяются и внедряются во все сферы нашей жизни, так что актуальность этой темы достаточно высока на данный момент и будет расти со временем дальше.

Таким образом, можно обмануть классификатор объектов в беспилотных автомобилях, вызвав аварию или другие разрушительные события; есть возможность нарушить логику системы распознавания лиц, выдав себя таким образом за другого человека, затруднив работу соответствующих государственных органов; изменить входные данные для голосового ассистента с целью дальнейшего манипулирования устройством и так далее [2].

Рассмотрим несколько типовых состязательных атак на модели машинного обучения:

1. Fast Gradient Sign Method (FGSM). Данный метод основан на наложении некоторой шумовой карты на входные данные модели, с умножением на некоторый коэффициент.

2. DeepFool. Этот метод очень схож с предыдущим, однако лучше работает на данных низкого разрешения и пытается изменить решение классификатора моделей путем минимального изменения исходных данных.

3. OnePixel. Как видно из названия, этот метод атаки работает с картинками и создает состязательный пример путем изменения всего лишь одного пикселя исходной картинки.

4. Карта градиентов: многие методы состязательных атак вычисляют градиент и антиградиент данных, чтобы понять какая минимальная единица данных или их группа способна вызвать наибольший вклад в решение классификатора модели машинного обучения и, соответственно, выходные данные. Если по такой карте единица данных находится в пике, значит, ее изменения повлечет большие последствия в результат анализа классификатора модели.

Эти методы являются одними из самых популярных на данный момент в сфере атак на нейронные сети и прочие виды моделей машинного обучения и анализа данных. Они очень просты в использовании и достаточно эффективны: с помощью пакетов art.attacks и foolbox.attacks на языке программирования Python представляется возможность всего за 3 строчки кода внедрить вышеперечисленные атаки и получить весьма удовлетворительный результат [3].

Дополнительно стоит обратить внимание на то, что вышеперечисленные методы атак могут быть применимы только к моделям с заранее известным устройством архитектуры, так как подход в таких атаках является крайне индивидуальным. В том случае, если внутреннее устройство модели неизвестно атакующему, необходимо рассматривать такую модель как

«чёрный ящик». Суть проста: мы стараемся создать самостоятельно максимально точно модель, похожую на целевую. Создать такую модель можно с использованием выходных данных черного ящика, обучая свою систему подражать выходным данным черного ящика. Таким образом, развертывая атаки, перечисленные выше, на своей модели, можно говорить об определенной вероятности того, что эта же атака сможет сработать и с черным ящиком. Эта вероятность тем выше, чем точнее скопирована модель, точность которой, в свою очередь, зависит от количества и качества данных для обучения.

Рассмотрим некоторые методы защиты от подобных атак:

1. Можно создать несколько моделей с разной архитектурой, выполняющих одну и ту же задачу и работающих одновременно. Смысл этого заключается в том, что состязательные атаки крайне индивидуальны, общий подход найти крайне сложно. Этот факт можно использовать, чтобы затруднить злоумышленникам совершение атаки. Можно обмануть одну модель, но куда сложнее обмануть все сразу – в этом заключается суть данного метода защиты. Однако, стоит отметить, что такая защита является крайне ресурсоемкой, поскольку нужно одновременно поддерживать несколько моделей с разной архитектурой.

2. Если заранее ввести обработку входных данных модели, то можно существенно снизить вероятность совершения состязательной атаки, поскольку целостность внесенных злоумышленником данных очень важна для успешности нападения. Например, можно добавить случайного шума, незаметного для человека, чтобы нивелировать потенциальное воздействие атакующего. Или, например, работать с входными данными в сжатом виде, что тоже может воспрепятствовать совершению состязательных атак.

3. И один из самых мощных методов – это обучение защищаемой модели на состязательных примерах. Идея заключается в том, что мы сами создаем атакующие примеры для своей модели и обучаем её на этих примерах, таким образом, можно научить модель не только избегать воздействий злоумышленника через изменение входных данных, но и даже детектировать потенциальные атаки и предупреждать об этом администратора, чтобы он мог предпринять дальнейшие действия по защите всей инфраструктуры, в которой находится защищаемый объект.

Список используемых источников

1. Чакраборти А. Состязательные атаки и защита от них. 31 с.

2. Состязательные атаки в соревновании Machine Can See 2018. URL: https://habr.com/ru/post/413775/ (дата обращения: 20.02.2021).

3. Безопасность алгоритмов машинного обучения. URL: https://habr.com/ru/company/dsec/blog/437092/ (дата обращения: 20.02.2021).

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

УДК 004.413
ГРНТИ 50.41.01

МЕТОДИКА ОРГАНИЗАЦИИ РАСПРЕДЕЛЕННОЙ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

М. М. Ковцур, А. А. Миняев, В. А. Петров, А. И. Таргонская

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

Одним из важнейших направлений в сфере информационных технологий является разработка и внедрение программного обеспечение для нужд различных компаний. Помимо вопросов разработки и внедрения, стоит также вопрос обеспечение информационной безопасности. Различные атаки, электронное мошенничество и утечка данных – актуальная проблема в настоящее время, поэтому внедрение и сопровождение программного обеспечения с учетом аспектов безопасности становится важной задачей. Правильно подобранная концепция разработки безопасного программного обеспечения позволяет сократить возможные риски для проекта. В статье рассмотрена популярная практика DevOps, которая получила свой виток развития. DevSecOps – это развитие концепции DevOps, где помимо процессов разработки (Development) и эксплуатации (Operation), затрагивается аспекты информационной безопасности (Security).

DevSecOps, жизненный цикл программного обеспечения, методика разработки программного обеспечения.

Ключом успеха для готовых приложений являются отлаженные методы и подходы к разработке программного обеспечения. В современном мире есть различные методологии организации разработки программного обеспечения. Выбор зависит от специфики проекта, системы бюджетирования, субъективных предпочтений. В рамках работы были рассмотрены популярные международные практики. Это Agile, Waterfall model и DevSecOps. В таблице 1 отображены основные недостатки и преимущества этих методик.

ТАБЛИЦА 1. Сравнение международных практик по разработке ПО

Практики	Преимущества	Недостатки
DevSecOps	Объединение в единый процесс разработку, тестирование и эксплуатацию Ускореный Time to Market. Автоматизация процессов с самого начала позволяет снизить вероятность неправильного администрирования и ошибок.	Для эффективного функционирования DevOps нужен эффективный менеджмент – для успешного взаимодействия отделов.

Практики	Преимущества	Недостатки
Agile	Нет четкого обозначения этапов и упора на требования, у исполнителей проекта появляется возможность экспериментировать и вносить изменения постепенно. Методология Agile подразумевает регулярное получение обратной связи от участников и последующее внесение изменений.	Определение точной даты окончания может быть довольно сложным, так как вам не хватает тщательной документации. Отсутствие четкого плана означает.
Waterfall model	Полное документирование каждого этапа. Четкое планирование сроков и затрат. Прозрачность процессов для заказчика.	Необходимость утверждения полного объема требований к системе еще на первом этапе. Внесение изменений требований позднее – это возврат к началу и переделка проделанной работы.

Перед началом подготовки методики организации распределенной разработки безопасного веб-приложения были выделены основные критерии, которым должна будет отвечать созданная практика: учитывать аспект информационной безопасности; возможность введения распределенной разработки (распределение программного обеспечение на составляющие компоненты, распределение команды в пространстве по дистанционной работе); возможность организации коллективной разработки посредством онлайн совещаний, контроля работы, системы контроля версий и ведения документации; время на выпуск релиза.

Проанализировав данные критерии и разбор современных методологий, за основу была взята практика DevSecOps. DevSecOps – это развитие концепции DevOps, где помимо процессов разработки (*Development*) и эксплуатации (*Operation*), затрагивается аспекты информационной безопасности (*Security*) [1].

Прежде чем перейти к непосредственной подготовки методики необходимо дать определение распределенной разработки безопасного программного обеспечения:

Распределенная удаленная разработка – это разработка, которая выполняется в нескольких рабочие местах, и участники проекта могут не видеть друг друга лицом к лицу, но совместно работать над достижением результата.

Безопасное программное обеспечение – это программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы. (ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. 2016. 18 с.)

Поскольку за основу была взята методология DevSecOps, обратимся к практикам, которая она предлагает для тестирования: DAST, IAST и SAST. В рамках работы рассмотрено динамическое тестирование. DAST (*Dynamic Application Security Testing*) – тестирование «черного ящика», которое может обнаруживать уязвимости и слабые места в работающем приложении, обычно веб-приложениях. Это достигается за счет использования методов внедрения ошибок в приложении [2]. В качестве доступных приложений были выбраны OWASP ZAP и Arachni. В ходе исследования был проведен их сравнительный анализ (табл. 2).

ТАБЛИЦА 2. Сравнительный анализ OWASP ZAP и Arachni

Программное обеспечение	Время (мин)	Загрузка RAM (МБ)	Загрузка CPU (%)	Количество найденных уязвимостей
Тестируемый ресурс: http://google-gruyere.appspot.com				
OWASP ZAP	5:17	526,8	12,9	7
Arachni	45:43	1 021,5	27,8	10
Тестируемый ресурс: http://router.asus.com				
OWASP ZAP	0:11	538,6	15,4	1
Arachni	1:43	704,5	25,8	8
Тестируемый ресурс: https://relands.ru				
OWASP ZAP	8:40	1 033,1	40	11
Arachni	03:11	738,2	27	14

Проведя анализ, можно сделать вывод что ПО OWASP ZAP проводит тестирования быстрее, однако Arachni находит большее количество уязвимостей [3] (рис. 1). Таким образом, можно проводит тестирования OWASP ZAP на начальных этапах для ускорения разработки. Arachni же оставит как инструмент для последних этапов.

Учитывая критерии для методики и концепцию DevSecOpsa, была создана методика с предложенными решениями для распределенной разработке безопасного программного обеспечения. А также реализована функциональная схема (рис. 2) [4].

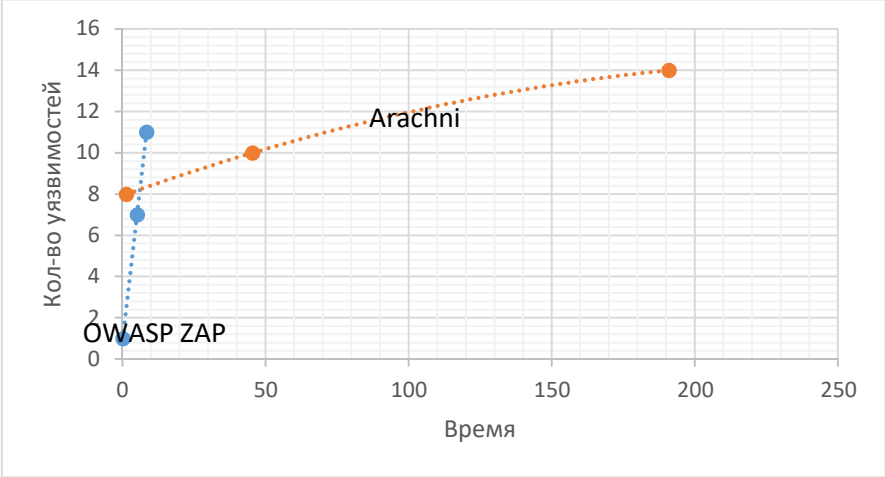


Рис. 1. Сравнительный анализ OWASP ZAP и Arachni

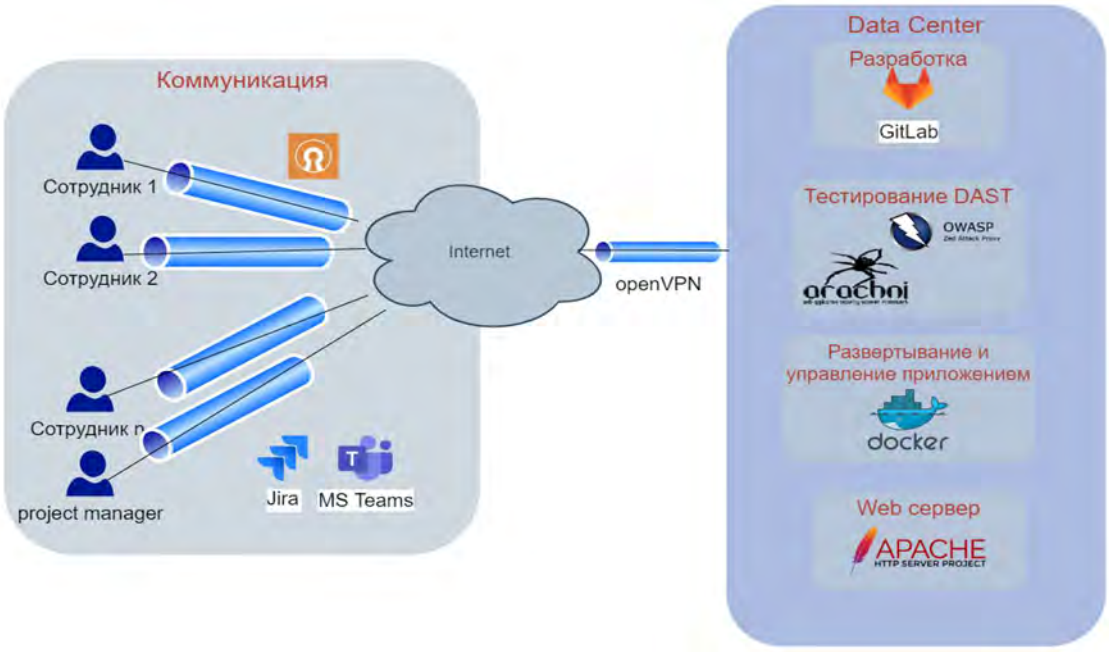


Рис. 2. Функциональная схема для методики

В данной схеме затронуты сферы [5, 6]: удаленного подключения, коммуникации, инструментов координирования, совместной разработки, тестирования, веб-сервера для развертывания приложений.

Результатом работы является созданная методика для организации распределенной разработки безопасного программного обеспечения:

- Учитывая аспект информационной безопасности и время на выпуск релиза, необходимо использовать методологию DevSecOps.
- Безопасную разработку ПО обеспечить посредством тестирования DAST – предложенное доступное ПО Arachni и OWASP ZAP.
- Проводит тестирования OWASP ZAP на начальных этапах для ускорения разработки. Arachni на последние этапы.

● Безопасное подключение для распределенной разработки обеспечить посредством VPN. Например – использовать OpenVPN.

● В качестве системы контроля версий и хранение документации использовать GitLab (для обеспечения безопасности – хранение репозиториев локально). Коллективная разработка – Jira, MS Teams.

● Для избежание недостатков практики DevSecOps необходимо сохранить роли аналитиков, тестировщиков и внедрения в команде. Однако обеспечить их тесное взаимодействие.

Список используемых источников

1. Ковцур М. М., Миняев А. А., Потемкин П. А., Хамза Д. Д. Обеспечение информационной безопасности WEB-приложений с использованием машинного обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1. С. 597–601.

2. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

3. Израилов К. Е. Система критериев оценки способов поиска уязвимостей и метрика понятности представления программного кода // Информатизация и связь. 2017. № 3. С. 111–118.

4. Пиховкин Н. Л., Сахаров Д. В. Обеспечение безопасности распределенной информационно-вычислительной сети с учетом управления рисками // Труды учебных заведений связи. 2016. Т. 2. № 2. С. 93–97.

5. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.

6. Багомедова А. Р., Ушаков И. А., Цветков А. Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 58–63.

УДК 621.395
ГРНТИ 49.33.35

СИМЕТРИЧНОЕ ШИФРОВАНИЕ ДЛЯ КОММЕРЧЕСКОГО ИСПОЛЬЗОВАНИЯ

Ю. Ф. Кожанов

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

Рассматривается способ симметричного шифрования с закрытыми ключами для коммерческого использования. Хранение секретных ключей пользователей производится в сервере ключей. Для шифрования открытого текста предлагается использовать формулу Эрланга.

шифрование, дешифрование, формула Эрланга.

Классическая модель криптосистемы приведена на рис. 1. В модели присутствуют три участника: два легальных пользователя и злоумышленник.

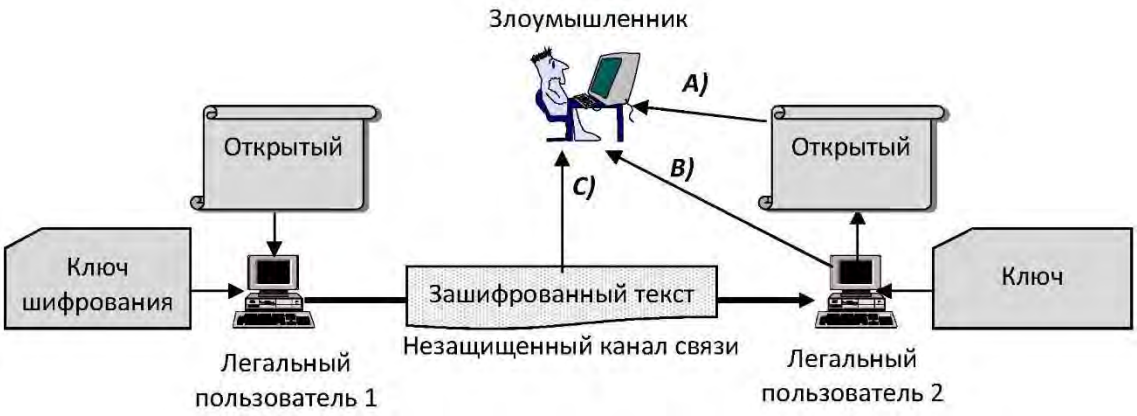


Рис. 1. Классическая модель криптосистемы

Легальные пользователи обмениваются между собой конфиденциальной информацией. Для того чтобы она была недоступна посторонним лицам, сообщение на передаче преобразуется в нечитаемый (зашифрованный) текст, который получается перемешиванием открытого текста с элементами ключа шифрования по определенному алгоритму (программе).

На приеме легальный пользователь, используя ключ дешифрования, восстанавливает исходный текст. Ключи шифрования и дешифрования могут совпадать или отличаться.

Задача злоумышленника заключается в перехвате и чтении всех передаваемых сообщений. При этом предполагается, что злоумышленник имеет возможность подключения к каналу связи и ему доступны

A) Некоторые открытые тексты.

B) Алгоритм шифрования\дешифрования передаваемых сообщений.

C) Зашифрованный текст.

Первое предположение основано на том, что злоумышленник может быть знаком с ***некоторыми*** открытыми текстами, которые могут быть похищены, подсмотрены или скопированы его соучастником.

Алгоритм шифрования\дешифрования в принципе не может быть секретом.

Зашифрованный текст легко перехватывается при использовании незащищенного канала связи.

Поэтому единственным секретом является только ключ дешифрования, который при его дискредитации и позволяет злоумышленнику читать ***все*** передаваемые зашифрованные сообщения.

При перечисленных предположениях алгоритм взлома ключа дешифрования состоит в подборе такого его значения, чтобы при перехваченном зашифрованном тексте ***C)*** и известном алгоритме шифрования ***B)*** получить известный открытый текст ***A)***.

В 1883 г. голландский криптограф Огюст Керкгоффс изложил шесть принципов проектирования военных шифров в своей книге «Военная криптография». Шесть основных требований к криптосистеме, все из которых до настоящего времени определяют проектирование криптографически стойких систем, в переводе с французского звучат так:

1. Система должна быть физически, если не математически, не вскрываемой.

2. Нужно, чтобы не требовалось сохранение системы в тайне. Попадание системы в руки врага не должно причинять неудобств.

3. Хранение и передача ключа должны быть осуществимы без помощи бумажных записей. Корреспонденты должны располагать возможностью менять ключ по своему усмотрению.

4. Система должна быть пригодной для сообщения через телеграф.

5. Система должна быть легко переносимой, работа с ней не должна требовать участия нескольких лиц одновременно.

6. От системы требуется, чтобы она была проста в использовании, не требовала значительного умственного напряжения или соблюдения большого количества правил.

Аналогично постулатам Керкгоффса к системе сформулируем постулаты к алгоритмам шифрования\дешифрования.

1. Каждый пользователь должен иметь индивидуальный секретный ключ шифрования. Дискредитация (вскрытие) ключа одного пользователя не должна вести к дискредитации ключей других пользователей.

2. Ключ дешифрования должен иметь достаточную длину. Если для проверки (подбора) одного бита ключа требуется время T, то для гарантированного перебора всех символов ключа длиной N бит потребуется время в 2^N раз больше. Поэтому для надежного шифрования длина ключа выбирается не менее 16 символов (128 бит).

3. В шифровании каждого символа открытого текста должны участвовать все элементы ключа шифрования. Поэтому «угадывание» даже части ключа делает невозможным чтение открытого текста.

4. Число операций (время дешифрования) не должно быть слишком малым. Увеличение времени дешифрования на t секунд приводит к увеличению времени подбора в 2^N $(T+t)/t$ раз. С другой стороны для удобства пользования оно не должно быть слишком большим (не более нескольких секунд).

Ниже предлагается алгоритм симметричного шифрования с закрытыми ключами, удовлетворяющий указанным требованиям.

Система использует три вида ключей:

– секретный ключ пользователя X с элементами $X[i]$, $i = 0, 2, \ldots 15$;

– сеансовый открытый ключ R с элементами $R[i]$, $i = 0, 2, \ldots 15$;

– сеансовый закрытый ключ Rx с элементами $Rx[i]$, $i = 0, 2, \ldots 15$.

Для шифрования текста используется блочный метод шифрования [1]. Для этого открытый текст разбивается на блоки по 16 байт и каждый блок шифруется отдельно.

Сеансовый открытый ключ R содержит элементы ключа $R[i]$ в виде случайных чисел в диапазоне от 100 до 99 990. Элементы ключа $R[i]$ пересчитываются в другое случайное число по формуле $E[i]=R[i]/100\,000$. Таким образом, случайное число $E[i]$ находится в диапазоне от 0,001 до 0,9999.

Открытый текст T с элементами $T[i]$ шифруется формулой Эрланга

$$E[i] = \frac{T[i]^{Tx[i]} / Tx[i]!}{\sum_{j=0}^{Tx[i]} \frac{T[i]^j}{j!}}. \qquad (1)$$

Запишем кратко эти преобразования в виде $Tx = f(E,T)$.

Восстановление исходного значения T происходит подбором такого его значения, чтобы выполнялось (1) – $T = f(Tx,E)$.

Сеансовый открытый ключ R шифруется в несколько этапов:

– используется преобразование с использованием секретного ключа пользователя X в виде $sum = X[0] \oplus X[1] \oplus \ldots X[15]$, $Rx[i] = R[i] \oplus sum \oplus X[i]$, где $\oplus$ – операция суммирования по модулю 2 (XOR);

– элементы $Rx[i]$ размещаются в матрицу 4×4;

– производится перемешивание строк путем циклического сдвига каждой строки со значением $Rx[8+i]$;

– производится перемешивание столбцов путем циклического сдвига каждого столбца со значением $Rx[12+i]$;

– матрица преобразуется в строку $Rx[i]$.

Запишем кратко эти преобразования в виде $Rx = f(R,X)$.

Восстановление исходного значения R происходит в обратном порядке – $R = f(Rx,X)$.

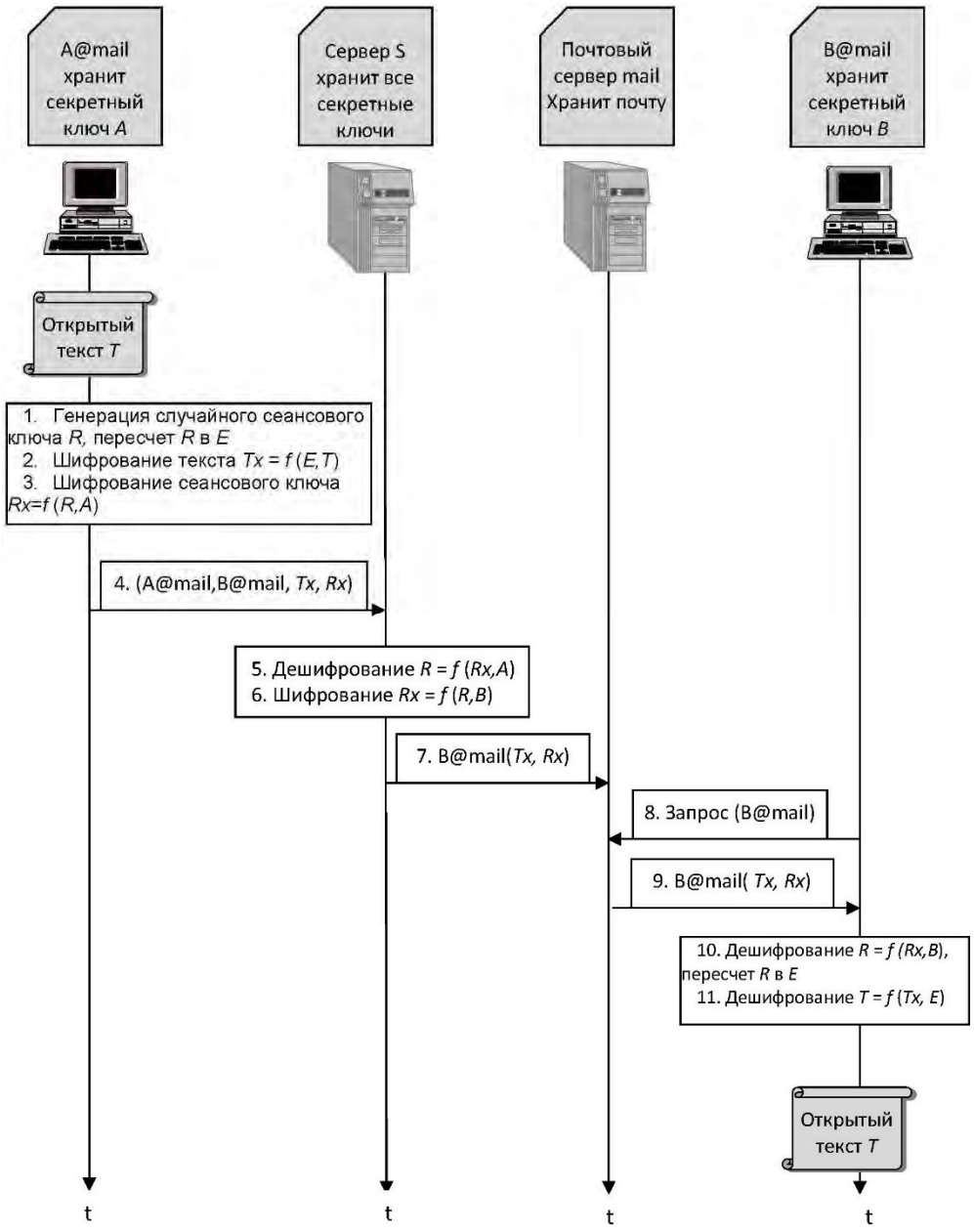


Рис. 2. Сеанс связи

Сеанс связи между пользователями с почтовыми адресами A@mail и B@mail упрощенно показан на рис. 2.

1. Для передачи открытого текста *T* пользователь A@mail генерирует случайный открытый сеансовый ключ *R* и пересчитываются в другое случайное число *E*.

2. Шифрует открытый текст *T* по формуле (1): $Tx = f(E,T)$.

3. Шифрует открытый сеансовый ключ *R* секретным ключом пользователя *A*: $Rx = f(R,A)$.

4. На адрес сервера ключей *S* пользователь *A* передает адрес источника A@mail, адрес получателя B@mail, зашифрованный текст *Tx* и зашифрованный сеансовый ключ *Rx*.

5. Сервер ключей *S* своей базе данных находит секретный ключ пользователя *A* и дешифрирует сеансовый ключ $R = f(Rx,A)$.

6. Шифрует открытый сеансовый ключ *R* секретным ключом пользователя *B*: $Rx = f(R,B)$.

7. По адресу получателя B@mail перенаправляет сообщение на его почтовый сервер зашифрованный текст *Tx* и зашифрованный сеансовый ключ *Rx*.

8. В удобное время пользователь B@mail обращается к почтовому серверу mail.

9. Почтовый сервер возвращает ему зашифрованный текст *Tx* и зашифрованный сеансовый ключ *Rx*.

10. Пользователь B@mail расшифровывает сеансовый ключ $R = f(Rx,B)$, пересчитываются в другое случайное число *E,* а затем восстанавливает зашифрованный текст: $T = f(Tx,E)$.

Для каждого сеанса связи пользователь генерирует новый сеансовый ключ.

Ниже на рис. 3 представлен пример использования предложенного метода шифрования с соответствующими ключами.

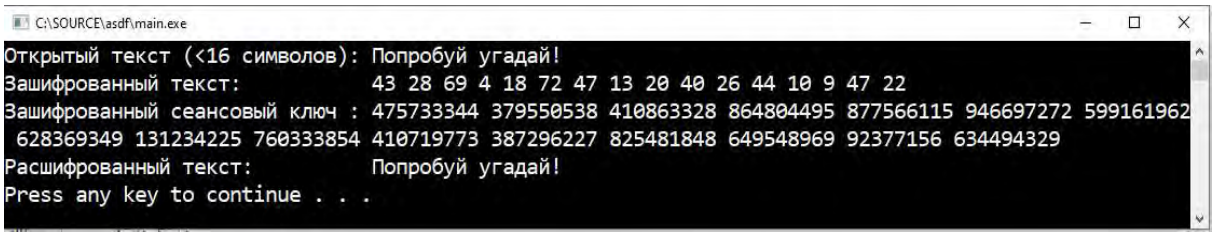


Рис. 3. Процесс шифрования\дешифрования фразы «Попробуй угадай!»

Список используемых источников

1. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 600 с.

УДК 004.7
ГРНТИ 81.93.29

МОДЕЛЬ DDOS/DOS АТАК НА ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Д. В. Колмыков, В. А. Липатников

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

Представлен анализ методов защиты информационных сетей от наиболее актуальных типов атак, основанных на отражении и усилении трафика. Выявлены преимущества и недостатки. Предложена модель защиты информационных сетей от DDoS-атак с прогнозированием.

DDoS-атака, статистический анализ, анализ трафика, распределенные сети.

Актуальность

Анализ инцидентов информационной безопасности (ИБ) является чрезвычайно важным источником информации для формирования мер противодействия, однако не может в достаточной мере обеспечивать своевременность, адекватность и эффективность мер противодействия, поскольку строится на изучении произошедших событий. Атаки типа «отказ в обслуживании» приводит к перегрузке ресурсов системы, поэтому она не может отвечать на запросы обслуживания. DDoS-атака также является атакой на ресурсы системы, но запускается с большого количества других хост-машин, зараженных вредоносным ПО, контролируемым злоумышленником. В отличие от атак, которые предназначены для того, чтобы позволить злоумышленнику получить или расширить доступ, отказ в обслуживании не дает злоумышленникам прямого доступа к системе, лишь только выводит ее из строя. Если атакованный ресурс относится к критической информационной инфраструктуре, то выгода для злоумышленника может быть достаточно реальной. Другой целью DoS-атаки может быть отключение системы, чтобы можно было запустить другой вид атаки. К DOS/DDOS атакам также относят следующие их под виды: TCP SYN Flood атаки, атаки фрагментированными пакетами со смещением (*Teardrop Attack*), Smurf-атаки, атаки сети ботнет [1]. Характерными признаками данной атаки являются: необычно низкая производительность сети, недоступность конкретного веб-сервиса, невозможность доступа к любому веб-сервису, резкое увеличение количества полученных спам-писем, отключение беспроводного или проводного подключения к интернету, долгосрочный отказ в доступе к сети или другим интернет-услугам.

Известные работы

Метод защиты от DDoS/DoS атак маршрутизации в «черные дыры», рассмотренный в работе [1] является не удачным решением, так как с вредоносным трафиком отбрасывается и полезный, тем самым легитимные пользователи не имеют доступа к ресурсу.

Предотвращение DDoS/DoS атак рассматриваемое в работе [2] посредством межсетевых фильтрации сетевыми экранами, является не актуальным из за того, что в межсетевых экранах отсутствует механизм выявления аномалий, межсетевые экраны в первую очередь предназначены для контроля доступа в частные сети, в них отсутствуют возможности для выявления аномалий. Межсетевые экраны не могут распознать ситуацию, в которой носителем атаки служат корректные разрешенные протоколы [2].

Цель: Разработать модель процесса передачи информации в информационно-вычислительные сети (ИВС) при атаках типа «отказ в обслуживании» для анализа вероятностно-временных характеристик нарушения безопасной передачи информации и выявления закономерностей. Задача – разработать модель, отражающую вероятностно-временные характеристики процессов нарушения безопасной передачи информации в ИВС.

Решение

Атаки типа «отказ в обслуживании» приводит к перегрузке ресурсов системы, поэтому она не может отвечать на запросы обслуживания. DDoS-атака также является атакой на ресурсы системы, но запускается с большого количества других хост-машин, зараженных вредоносным ПО, контролируемым злоумышленником. В отличие от атак, которые предназначены для того, чтобы позволить злоумышленнику получить или расширить доступ, отказ в обслуживании не дает злоумышленникам прямого доступа к системе, лишь только выводит ее из строя. Если атакованный ресурс относится к критической информационной инфраструктуре, то выгода для злоумышленника может быть достаточно реальной [3]. Другой целью DoS-атаки может быть отключение системы, чтобы можно было запустить другой вид атаки. К DOS/DDOS атакам также относят следующие их под виды: TCP SYN Flood атаки, атаки фрагментированными пакетами со смещением (*Teardrop Attack*), Smurf-атаки, атаки сети ботнет. Характерными признаками данной атаки являются: необычно низкая производительность сети, недоступность конкретного веб-сервиса, невозможность доступа к любому веб-сервису, резкое увеличение количества полученных спам-писем, отключение беспроводного или проводного подключения к интернету, долгосрочный отказ в доступе к сети или другим интернет-услугам.

Алгоритм данной атаки выглядит следующим образом:

- Злоумышленник собирает информацию о цели атаки. Собирает список открытых портов, и подключенных служб на стороне жертвы.

• Злоумышленник формирует вредоносное воздействие на систему, при помощи распределенной сети зараженных компьютеров, объединённых в ботнет сеть.

• Злоумышленник начинает атаку, при необходимости корректирует вредоносные пакеты, для усиления вредоносного воздействия и противодействия СЗИ сети [4].

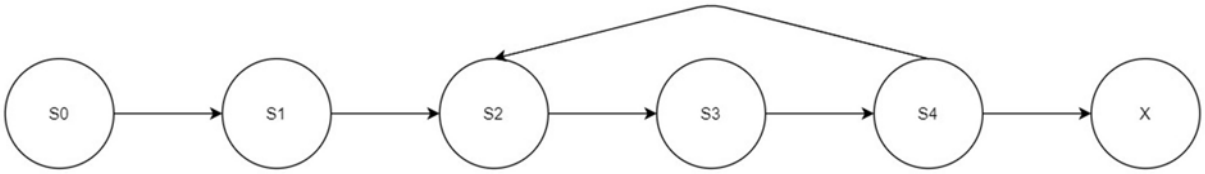


Рис. 1. Граф осуществления DDoS/DoS атак

Алгоритм действий злоумышленника для осуществления DDoS/DoS атак описан в таблице.

ТАБЛИЦА. Алгоритм действий злоумышленника для осуществления DDoS/DoS атак

Событие	Описание
S0	Защищенное состояние ИВС (бездействие нарушителя)
S1	Начало действий нарушителя
S2	Сбор информации о ИВС, для реализации атаки (сбор данных о портах, подключенных службах)
S3	Формирование вредоносных пакетов на ИВС
S4	Внесение изменений в отправляемые пакеты, направленное на противодействие СЗИ
X	Реализация отказа в обслуживании

Дерево событий выглядит таким образом: Sx1 = {S1, S2, S3, S4, X}.

Представлена математическая модель активного нарушителя, учитывающая возможность нарушителя реализовать атаку позволяющая рассчитать вероятностно-временных характеристик атаки, нацеленной на отказ в обслуживании [5].

Для решения задачи по определению вероятности реализации отказа в обслуживании используется следующий граф состояний.

В данной работе используется аппарат Марковских случайных процессов, с помощью дифференциальных уравнений, в которых неизвестными функциями являются вероятности нахождения DDos/Dos атак в различных состояниях $P_{0,}\, P_{1,}\, P_{2,}\, P_{3,}\, P_{4}$.

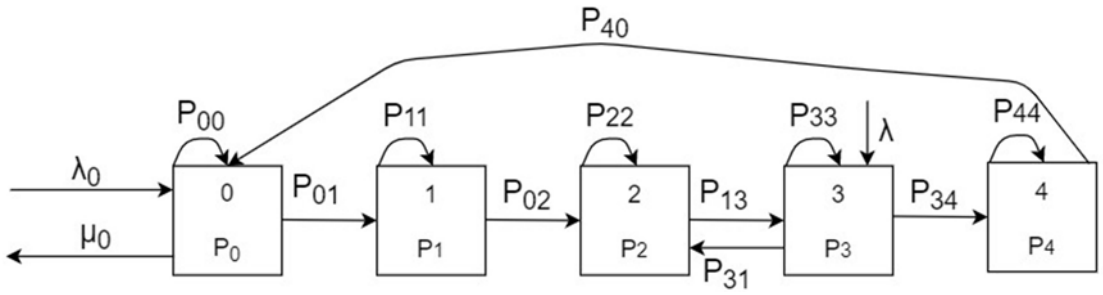


Рис. 2. Граф состояний DDos/Dos атак

Зафиксировав некоторый момент времени *t.* можно найти вероятность $P_0(t + \Delta t)$ того, что в момент времени $t - \Delta t$ система будет находиться в состоянии «0». Это событие может произойти двумя способами: в момент времени *t* система находилась в состоянии «0» и за время Δt не перешла в состояние «1», в момент времени *t* система находилась в состоянии «4» и за время Δt перешла в состояние «0» [6]. Учитывая теоремы сложения и умножения вероятностей $P_0(t + \Delta t)$ будет находиться следующим образом:

$$P_0\,(t + \Delta t) = \; P_0\,(t) \cdot P_{00}\,(t + \Delta t) + P_4(t) \cdot P_{40}(t + \Delta t).$$

Далее для остальных состояний:

$$\begin{cases} P_0(t + \Delta t) = P_0(t) \cdot P_{00}(t + \Delta t) + P_4(t) \cdot P_{40}(t + \Delta t) \\ P_1(t + \Delta t) = P_1(t) \cdot P_{12}(t + \Delta t) + P_2 \cdot P_{22}(t + \Delta t) \\ P_2(t + \Delta t) = P_2(t) \cdot P_{23}(t + \Delta t) + P_3 \cdot P_{33}(t + \Delta t) \\ P_3(t + \Delta t) = P_{21} \cdot P_3(t + \Delta t) + P_2(t) \cdot P_{33}(t + \Delta t) + P_3(t) \cdot P_3(t + \Delta t) \\ P_4(t + \Delta t) = P_3(t) \cdot P_{34}(t + \Delta t) + P_4 \cdot P_{44}(t + \Delta t) \end{cases}.$$

Определены переходные вероятности. Вероятность того, что за время Δt не поступит ни одной задачи на вторжение равна $e^{-\lambda_0 \Delta t} \approx 1 - \lambda_0 \Delta t$, а вероятность того, что за время *At* система проведёт кибервторжение равна $\mu_0 \Delta t$. И, наконец, вероятность того, что за время *At* не поступит ни одной задачи и система не освободится $e^{-\lambda_0 \Delta t} * e^{-\mu_0 \Delta t} \approx 1 - (\lambda_0 + \mu_0)\Delta t$ [7].

Исходя из этого и учитывая, что λ_0 – плотность потока задач на вторжение, μ_0 – плотность потока успешных вторжении: $\mu_0 = \frac{1}{t_в}$, где $t_в$ – среднее время вторжения нарушителя.

β_1 – плотность выполнения задач на сбор информации о системе (СИ): $\beta_1 = \frac{1}{t_{пп}}$, где $t_{пп}$ – среднее время СИ;

β_2 – плотность выполнения задач формирование вредоносного воздействия (ФВ) в системе: $\beta_2 = \frac{1}{t_{ав}}$, где $t_{ав}$ – среднее время ФВ [8];

β_3 – плотность выполнения задач на внесение изменений в отправляемые пакеты, направленное на противодействие СЗИ (ВИ) на роутере для дальнейшего создания двойника на своём устройстве: $\beta_3 = \frac{1}{t_{пс}}$, где $t_{пс}$ – среднее время ВИ [9];

λ – плотность заявок на вторжение сети VoIP:

$\lambda = \frac{1}{t_{сзи}}$, где $t_{сзи}$ – среднее время реакции сети VoIP на вторжение, определим:

$$P_{01}(t+\Delta t) = \lambda_0 \cdot \Delta t, \qquad P_{11}(t+\Delta t) = (1-(\lambda_0+\beta_1)) \cdot \Delta t,$$
$$P_{23}(t+\Delta t) = \beta_1 \cdot \Delta t, \qquad P_{22}(t+\Delta t) = (1-(\lambda_0+\lambda+\beta_2)) \cdot \Delta t,$$
$$P_{21}(t+\Delta t) = \lambda \cdot \Delta t, \qquad P_{33}(t+\Delta t) = (1-(\lambda_0+\beta_3)) \cdot \Delta t,$$
$$P_{23}(t+\Delta t) = \beta_2 \cdot \Delta t, \qquad P_{44}(t+\Delta t) = (1-(\lambda_0+\beta_4)) \cdot \Delta t.$$

Отличительной особенностью модели является прогнозирование изменения рисков в соответствии с динамикой действий нарушителя и изменениями, а также данными накопленными ранее, что позволяет повысить точность прогноза [10].

Практическая значимость

Предложенная модель DDoS–атак на ИВС, позволяющая проводить проактивное противодействие.

Заключение

DDoS нападения опасны для ИВС. Исследованы основные программы для анализа DDoS атак, большинство из них применимо для небольших сетей или провайдеров.

Предложено усовершенствование метода выявления и противодействия угрозам безопасности информации киберфизических систем при DDOS-атаках.

Предлагаемый способ анализа и прогнозирования, обеспечит защиту от DDoS нападения. Использование предложенного способа позволяет поддерживать защищённость от DDoS атак выше требуемого значения в пределах каждой итерации цикла проактивного управления ИБ.

Кроме того, разработанные подходы не учитывают формирование системно-аналитического ядра технологического сопровождения процессов проектирования математического обеспечения КБ систем крупномасштабных гетерогенных сетей, обеспечивающего соблюдение гарантий безопасности. Данные направления выведены авторами в область дальнейших исследований.

Список используемых источников

1. Предотвращение атак с распределенным отказом в обслуживании (DDoS): официальный сайт компании Cisco. URL: http:// www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd8011e927_.html

2. Ferguson P. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. 2000. URL: http://tools.ietf.org/html/rfc2827.html.

3. Li J. SAVE: Source address validity enforcement protocol // INFOCOM 2002. Twenty-First Annual Joint Conf. of the IEEE Computer and Communications Societies.Proceedings.IEEE. 2002. Vol. 3. P. 1557–1566.

4. Chen R., Park J. M., Marchany R. TRACK: A novel approach for defending against distributed denial-ofservice attacks. 2006. URL: http://www.researchgate.net/profile/Jung-MinJerry_Park/publication/228471222 TRACK_A_ Novel Approachfor Defending Against Distributed Denial of Service_Attacks/ links/0a85e53454bbb9a d32000000.pdf.

5. Argyraki K., Cheriton D. R. Scalable network-layer defense against internet bandwidth-flooding attacks // IEEE/ACM Transactions on Networking (TON). 2009. Vol. 17, No. 4. pp. 1284–1297.

6. Furfaro A. Modelling and simulation of a defense strategy to face indirect DDoS flooding attacks // Internet and Distributed Computing Systems Conf., Calabria, Italy. Springer International Publishing, 2014. pp. 263–274.

7. Липатников В. А., Шевченко А. А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2016. № 2 (94). С. 128–140.

8. Липатников В. А., Омаров Р. Г., Шевченко А. А. Способ защиты информационных сетей транспортных систем от DDoS-атак с прогнозированием // «Транспорт России: проблемы и перспективы-2019». Материалы Международной научно–практической конференции. 2019. С. 413.

9. Korshunov G. I., Lipatnikov V. A., Omarov R. G., Frolova E. A. Предотвращение атак с распределенным отказом в обслуживании информационных сетей киберфизических систем // International scientific conference, ICMSIT-2020: Metrological support of innovative technologies.

10. Липатников В. А., Омаров Р. Г. Способ предотвращения атак с распределенным отказом в обслуживании информационно-телекоммуникационных сетей // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сборник статей II Всероссийской научно-технической конференции. Федеральное государственное автономное учреждение «Военный инновационный технополис "ЭРА"». Анапа, 2020. С. 147–158.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ СТАТИСТИЧЕСКИХ ПРИЗНАКОВ ПРОФИЛЕЙ В СОЦИАЛЬНЫХ СЕТЯХ ДЛЯ ОБНАРУЖЕНИЯ БОТОВ

М. В. Коломеец

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В работе рассматривается статистические признаки, собранные из профилей социальной сети, а также их полезность в задаче обнаружения ботов. Для этого на основе аккаунтов ботов и пользователей были сгенерированы две группы аккаунтов – группы, содержащие ботов и группы без ботов. Предложены статистические признаки и проведен анализ их корреляции между собой и с меткой бота.

обнаружение ботов, анализ социальных сетей, информационная безопасность, машинное обучение.

Обнаружение ботов в социальных сетях – одна из наиболее востребованных защитных функций социальной сети, которая активно исследуется как коммерческими компаниями, так и правоохранительными органами. Во многих случаях боты используются для накрутки репутации, ведения недобросовестной конкуренции, распространения дезинформации, мошенничества и кражи конфиденциальной информации. В некоторых случаях активность ботов может представлять серьезную угрозу целостности онлайн-сообществ. Например, недавние исследования [1, 2, 3] показывают, что вмешательство в выборы, распространение теорий заговора и идей антивакцинации, а также манипуляции на фондовых рынках осуществляются именно с помощью ботов.

Как правило, для обнаружения ботов используют различные методы машинного обучения, для которых необходимо определить большое количество признаков ботов. Таким образом, необходимо определить какие признаки могут быть полезны в задаче обнаружения ботов, а какие нет.

В данной работе представляется анализ статистических признаков ботов социальной сети ВКонтакте на основе корреляции признака с меткой бота.

В качестве источника данных предлагается использовать численные метрики аккаунтов социальной сети. Для анализа использовался датасет [4], который содержит список ботов и список реальных пользователей. На основе данного датасета были сгенерированы 2 типа групп аккаунтов:

1) Группа аккаунтов, состоящая только из реальных пользователей;

2) Группа аккаунтов, состоящая из реальных пользователей и ботов. Количество ботов в группе равномерно варьируется от 30% до 70% от всех аккаунтов группы.

Всего было сгенерировано 90 групп, из которых 45 групп с ботами. Каждая группа содержит 200 аккаунтов. Пересечение аккаунтов между группами составляет не более 15 %. Для каждой группы аккаунтов были определены следующие источники данных:

1. Распределение количества друзей. Чтобы подружиться, пользователь должен отправить запрос, а другой пользователь должен его подтвердить.

2. Распределение количества групп. Группы могут быть посвящены какому-либо событию или теме.

3. Распределение количества подписок. Разница между подпиской и дружбой в том, что для подписки не нужно подтверждение другого пользователя.

4. Распределение количества подписчиков – людей, которые подписался на аккаунт.

5. Распределение количества фотографий. Пользователь может загружать фотографии на свою страницу.

6. Распределение количества альбомов. Пользователь может объединять фотографии в альбомы.

7. Распределение количества постов. У каждого пользователя ВКонтакте есть свой микроблог. Количество постов – это количество записей в этом микроблоге.

Данные распределения являются характеристиками группы аккаунтов. Для каждого распределения высчитываются следующие признаки:

1. Среднее (mean).

2. 1, 2 и 3 квартиль (q1, q2, q3).

3. Стандартное отклонение (dev).

4. Индекс Джини (gini).

Индекс Джини – это статистическая мера, которая очень популярна в экономике для выражения неравенства доходов. Иногда индекс Джини используют и в других областях, например, для оценки биоразнообразия [5]. Предполагается, что значения количества друзей, фотографий и т.д. можно интерпретировать как «богатство» пользователя социальной сети, потому что для увеличения этого числа пользователям необходимо совершать больше действий. Таким образом, индекс Джини может указывать на равенство или неравенство пользователей в выборке.

Для анализа была построена матрица корреляции со значениями по модулю. Далее из матрицы были исключены признаки, которые имеют высо-

кую (> 0.7) корреляцию с другими признаками. Высокая корреляция указывает на то, что признаки дублируют друг друга и один из них может быть исключен. Итоговая матрица изображена на рис.

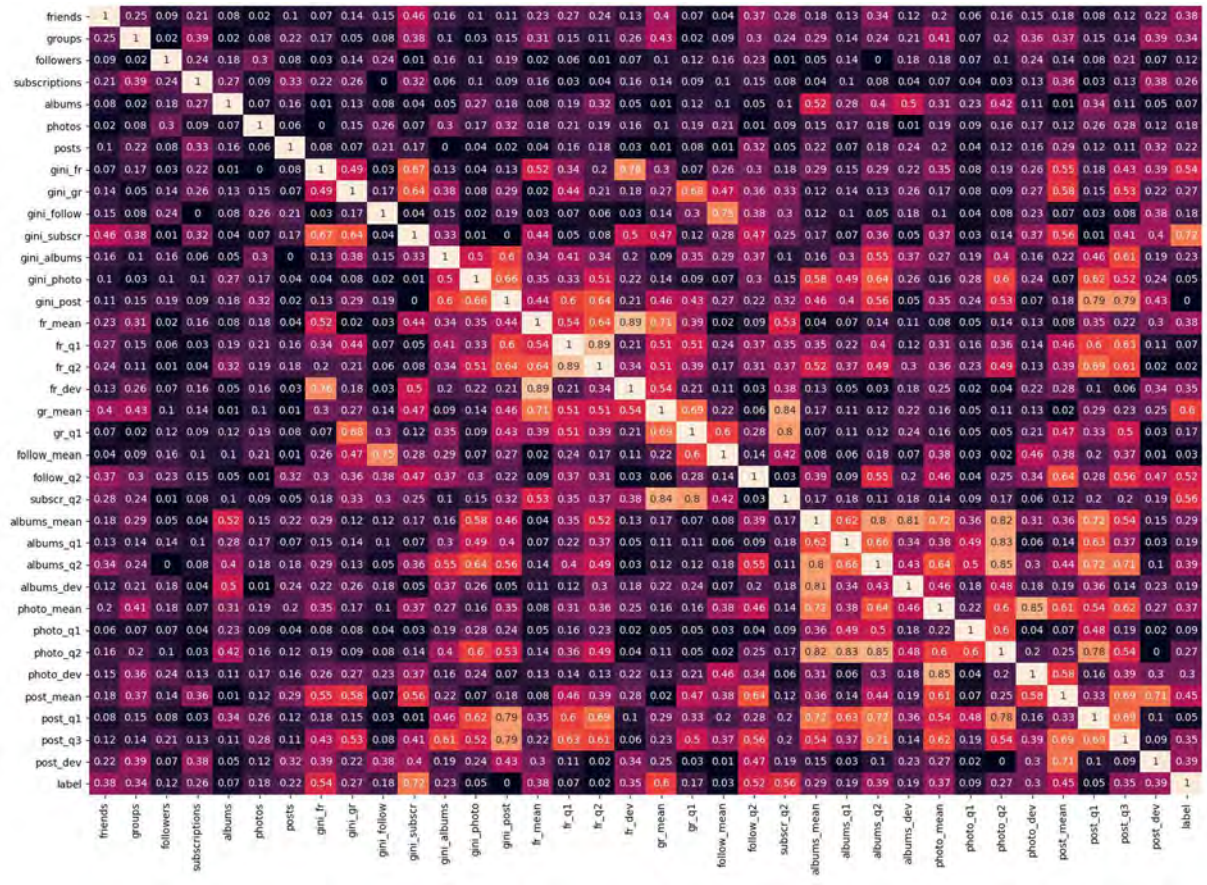


Рис. Матрица корреляции для признаков и метки ботов

Последняя строка / столбец соответствует корреляции признака и метрики (0 для пользователя и 1 для бота). Признаки способные в явном виде разделить датасет на 2 части имеют большее значение корреляции.

Работа выполнена при финансовой поддержке РНФ (грант № 18-71-10094).

Список используемых источников.

1. Subrahmanian V. S. et al. The DARPA Twitter bot challenge // Computer. 2016. Vol. 49. Iss. 6. pp. 38–46.

2. Pierri F., Artoni A., Ceri S. Investigating Italian disinformation spreading on Twitter in the context of 2019 European elections // PloS one. 2020. Vol. 15. Iss. 1. P. e0227821.

3. Котенко И. В., Саенко И. Б., Чечулин А. А. Защита от нежелательной и вредоносной информации в глобальных информационных сетях // Информационно-психологическая и когнитивная безопасность. Коллективная монография / Под ред. И. Ф. Кефели, Р. М. Юсупова. СПб.: Изд-во «Аврора» 2017. 345 с. С. 207–229.

4. Guiasu R. C., Guiasu S. The weighted Gini-Simpson index: revitalizing an old index of biodiversity // International Journal of Ecology. 2012. T. 2012.
5. Kolomeets M., Tushkanova O., Levshun D., Chechulin A. VKontakte bots dataset // GitHub. URL: https://github.com/guardeec/datasets.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Чечулиным.

УДК 004.021
ГРНТИ 50.41.25

АВТОМАТИЗИРОВАННОЕ ТЕСТИРОВАНИЕ ИНФОРМАЦИОННЫХ БАЗ СИСТЕМЫ 1С:ПРЕДПРИЯТИЕ 8

В. Ю. Комарьков, Д. В. Окунева

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

На данный момент система 1С:Предприятие 8 является одним из самых популярных и удобных средств для создания бизнес-приложений. Платформа 1С: Предприятие 8 позволяет создавать гибкие и быстро настраиваемые приложения, является кроссплатформенной, обладает средствами для поддержки крупных корпоративных систем, работает на мобильных устройствах. Объемы разработки бывают достаточно крупными, и для тестирования разработанных решений приходится тратить очень много времени. Но есть решение – это автоматизированное тестирование. В статье рассмотрены механизм автоматизированного тестирования платформы 1С: Предприятие 8.3, цели его создания, способы написания автоматизированного теста, описана возможность написания комплексного тестирования в рамках одной или нескольких информационных баз.

автоматизированное тестирование, 1С:Предприятие 8.

Технологическая платформа 1С:Предприятие 8 позволяет разрабатывать прикладные решения самого разного масштаба. Это могут быть как несложные решения для одного или нескольких пользователей, так и сложные многопользовательские тиражные решения, обладающие широкой функциональностью и обрабатывающие большие объемы данных. Важным моментом является то, что состав задач, решаемых разработчиком в одном и другом случае, существенно отличается. При реализации сложных многофункциональных проектов на первый план выходит целый ряд задач, которые для простых конфигураций не являются критичными и решаются

обычно, минимальными производственными затратами. Для удобства решения проблем при разработке, в системе 1С:Предприятие 8 реализован механизм автоматизированного тестирования [1].

В системе 1С:Предприятие 8 автоматические тесты имитируют действия пользователя и проверяют результаты этих действий. Данный механизм позволяет разработчикам написать тест для проверки и отладки написанного ими кода. Это позволяет уменьшить время на проверку и отладку созданной ими конфигурации.

Конфигурация это – совокупность созданных разработчиком объектов, их свойств, методов и алгоритмов поведения, отражающих хозяйственную деятельность предприятия [2].

Данный механизм может быть использован при разработке любых конфигураций. Механизм немного сложен в изучении, но очень полезен для разработчиков.

Процесс автоматизированного тестирования заключается во взаимодействии двух специальным образом запущенных клиентских приложений: ***менеджера тестирования*** *и* ***клиента тестирования.***

Создаётся две конфигурации, одна будет клиентом тестирования, вторая будет менеджером тестирования. В параметрах конфигурации задается соответствующий тип запуска приложения (рис.).

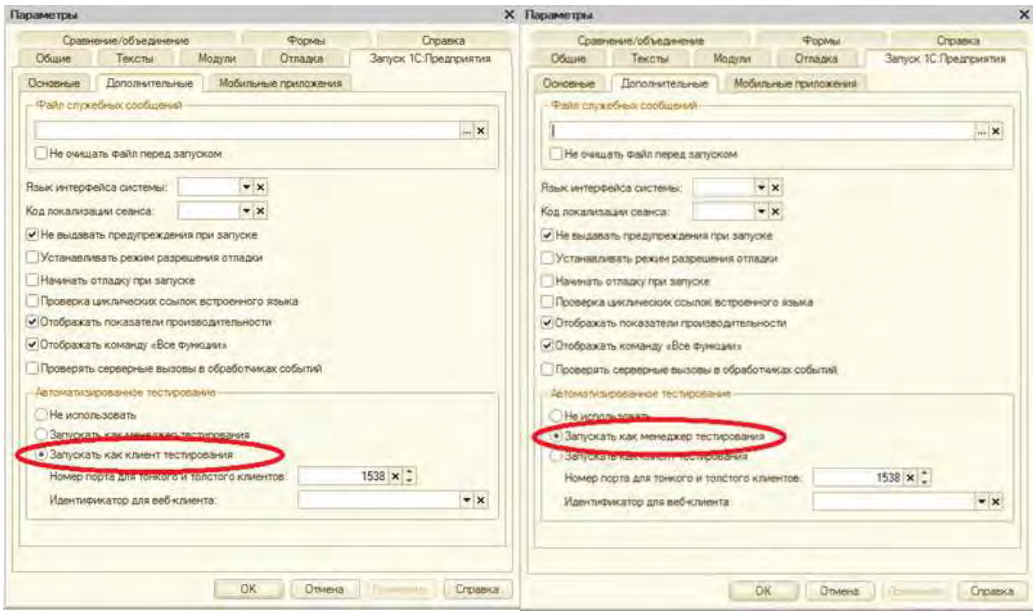


Рис. Выбор типа запуска автоматизированного тестирования для двух конфигураций

После выбора типа запуска, необходимо создать внешнюю обработку, в которой будет выполняться программный код. Ниже представлен код на внутреннем языке, который запускает тестируемое приложение, то есть клиент тестирования. Все действия будут выполняться на клиенте.

```
    &НаКлиенте
Процедура Тест(Команда)
    АдресEXE = "C:\Program Files (x86)\1cv8t\8.3.12.1529\bin\1cv8t.exe";
    АдресБазы = "C:\Users\Мария\Desktop\1109";
    ЗапуститьСистему(АдресEXE + " ENTERPRISE /F " + АдресБазы + "
/TESTCLIENT");

    ТестовоеПриложение = Новый ТестируемоеПриложение("localhost");

    ВремяОкончания = ТекущаяДата() + 60;

    Подключен = Ложь;

    Ошибка = "";

    Пока не ТекущаяДата() >= ВремяОкончания Цикл
        Попытка
            ТестовоеПриложение.УстановитьСоединение();
            Подключен = Истина;
            Прервать;
        Исключение Ошибка = ОписаниеОшибки();
        КонецПопытки;
    КонецЦикла;

    Если не Подключен Тогда ТестовоеПриложение = Неопределено;
        Сообщить("Не установлено" + Ошибка);
        Возврат;
    КонецЕсли;

    ПроцедураТеста(ТестовоеПриложение);
КонецПроцедуры
```

Функция «ЗапуститьСистему()», запускает приложение в тестируемом режиме. Выше описанный код запускает тестируемое приложение и выполняет подключение менеджера тестирования к тестируемому клиенту. В случае если соединение не будет установлено, программа сообщит об ошибке.

Процедура «ПроцедураТеста(ТестовоеПриложение)» вызовет клиента тестирования «ТестовоеПриложение» и выполнит на нём действия, описанные в процедуре «ПроцедураТеста()».

Результат выполнения автоматизированного теста может контролироваться визуально, либо программным путем, сравнивая полученные результаты с эталонными значениями.

Написание длинных и сложных тестов может оказаться довольно трудоемким занятием, поэтому в платформе реализована возможность автоматической записи интерактивных действий пользователя в XML файл.

У механизма есть следующие варианты использования:

1. Сотруднику службы технической поддержки приходит заявка, в которой сообщается о появлении у пользователя сложной проблемы, и он хочет посмотреть, что именно пользователь выполняет в системе.

Для решения подобной задачи, можно создать bat-файл для запуска базы, в которой произошла проблема в режиме клиента тестирования и использовать методы тестового приложения «НачатьЗаписьЖурналаДействийПользователя» и «ЗавершитьЗаписьЖурналаДействийПользователя» для получения журнала действий пользователя. В результате получится XML текст, который в дальнейшем может быть преобразован в обработку для повторения ошибки пользователя. После исправления ошибки данную обработку можно использовать для тестирования.

2. При разработке новых возможностей системы появляются ошибки в ранее разработанном функционале. Для полноценного тестирования можно заранее создавать тестовые сценарии исправного функционала и выполнять их перед выпуском новых релизов.

3. Для разрешения проблем ожиданий на блокировках или дедлоков. Можно создать несколько тестов, которые явно приведут к проблеме производительности для дальнейшего исследования.

4. Проведение нагрузочного тестирования. Фирма 1С позиционирует функционал как механизм сценарного тестирования, но по большому счету не запрещает запускать большое количество клиентов тестирования. В обработчики можно вставить генераторы случайных чисел для разнородности вводимой информации.

Для того чтобы написать один автоматизированный тест для нескольких конфигураций должны быть соблюдены условия идентичности среды, один программный код может совершить те действия, для которых был создан автоматизированный тест. К примеру, заполнить справочник. Получается так, что в нескольких тестируемых информационных базах должны быть созданы справочники, имеющие одинаковые наименования, наименования реквизитов, типы этих реквизитов, одинаковые кнопки, выполняющие одно и то же действие.

Реквизит объекта метаданных, такого как справочник или документ – это дополнительная информация об объекте, доступная только в пределах этого объекта. Можно сказать, что с помощью реквизитов определить дополнительные свойства объекта.

Всё, с чем работает автоматизированный тест, должно быть одинаково во всех системах. Иначе следует ожидать некорректные результаты или их отсутствие.

Ниже два правила, соблюдая которые, можно написать автоматизированный тест для нескольких информационных баз системы 1С:Предприятие 8.

1. У тестируемых клиентских приложений (1С:Предприятие 8), должны быть версии программного обеспечения, не ниже версии 8.3.8;

2. У тестируемых клиентских приложений, должны быть созданы абсолютно идентичные: реквизиты, справочники, документы, регистры, константы и т. п., с которыми будет работать автоматизированный тест.

В правила не были добавлены такие обязательные пункты, как выбор типа запуска тестируемого приложения, так как без соответствующей настройки информационных баз невозможно даже запустить автоматизированный тест.

Автоматизированное тестирование очень удобный механизм для разработчиков и администраторов информационных баз системы программ 1С:Предприятие 8, при помощи данного механизма можно совершать отладку программного обеспечения и выявление его уязвимостей.

Список используемых источников

1. Габец А. П., Гончаров Д. И., Козырев Д. В., Кухлевский Д. С., Радченко М. Г. Профессиональная разработка в системе 1С: Предприятие 8. М.: «1С-Паблишинг», СПб.: Питер, 2006. 698 с. ISBN 5-9677-0268-7.

2. Родченко М. Г., Хрусталева Е. Ю. 1С: Предприятие 8.3 Практическое пособие разработчика. Примеры и типовые приемы. М.: ООО «1С-Паблишинг», 2013. 945 с. ISBN 978-5-9677-2041-3.

УДК 004.056
ГРНТИ 81.3.29

ВЕРОЯТНОСТИ ОШИБОК ПРИ РАСПРЕДЕЛЕНИИ КЛЮЧЕЙ ПО БЕСШУМНЫМ ПОСТОЯННЫМ КАНАЛАМ С ИСПОЛЬЗОВАНЕМ ДОБАВЛЕНИЯ ИСКУССТВЕННОГО ШУМА

В. И. Коржик, В. А. Яковлев

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

Исследуется протокол распределения ключа по постоянным бесшумным каналам (типа Интернет). В ранее исследованных протоколах легальные пользователи формировали биты сырого ключа путем взаимного обмена зашумленными матрицами, состоящими из гауссовских случайных чисел. На основе моделирования были получены оценки

вероятностей совпадения бит ключа у пользователей и нарушителя. В предлагаемом простом протоколе корреспонденты обмениваются непосредственно случайными гауссовскими числами. Получены аналитические соотношения, для вычисления вероятности несовпадения бит ключей у легальных пользователей и вероятности несовпадения бит ключа у легального пользователя и нарушителя, которые подтверждаются экспериментальными исследованиями.

криптография, распределение ключей.

В работах [1, 2] был представлен протокол скрытного распределения ключей по постоянному каналу в условиях возможно бесшумного перехвата нарушителем передаваемых данных. Суть протокола заключаются в том, что два корреспондента сети А и В генерируют случайные гауссовские матрицы, принудительно зашумляют их, суммируя с матрицами, тоже случайными гауссовскими, но имеющими меньшую дисперсию и обмениваются результирующими матрицами по каналу связи. Канал связи предполагается постоянным (типа сети Интернет). Получив зашумленную матрицу, каждый корреспондент умножает ее на свою матрицу (без шума). Далее проводится многоэтапная обработка матриц произведений с целью получения ключа в следующем порядке:

– извлечение собственных чисел матрицы и их квантование с целью получения бинарных последовательностей – получение бит сырого ключа;

– выполнение процедуры «очистки» полученных последовательностей от ошибок на основе использования процедуры преимущественного улучшения основного канала и помехоустойчивого кодирования на основе эффективных низкоплотностных кодов;

– выполнение процедуры усиления секретности.

Нарушитель может вычислять биты сырого ключа из матрицы, полученной перемножением двух перехваченных зашумленных матриц. Так как у злоумышленника при такой обработке присутствует шум сразу от двух корреспондентов, то это дает основание полагать, что условия выделения сырого ключа у него заведомо хуже, чем у легальных корреспондентов.

В [2] были получены результаты, показывающие, что данный протокол обеспечивает теоретический уровень секретности при обмене по постоянному бесшумному каналу при отсутствии любых преимуществ у перехватчика за исключение требования аутентификации легитимных пользователей. При этом вероятность ошибки (несовпадения ключей) может быть достаточно малой.

Первая часть данного протокола (формирование бит сырого ключа) была осуществлена на основе моделирования процессов: генерации матриц размера от 4 до 64, обмена ими, перемножения матриц и вычислении собственных чисел. Поскольку каждая матрица состояла из гауссовских случайных чисел, то закономерен вопрос о возможности построения протокола на основе непосредственного обмена гауссовскими числами и нахождения

аналитических соотношения для вероятности ошибок (несовпадения) бит сырого ключа между легальными пользователями и между легальным пользователем и нарушителем, которые впоследствии могут быть использованы на других этапах протокола.

Рассмотрим следующий протокол формирования бит сырого ключа (рис.).

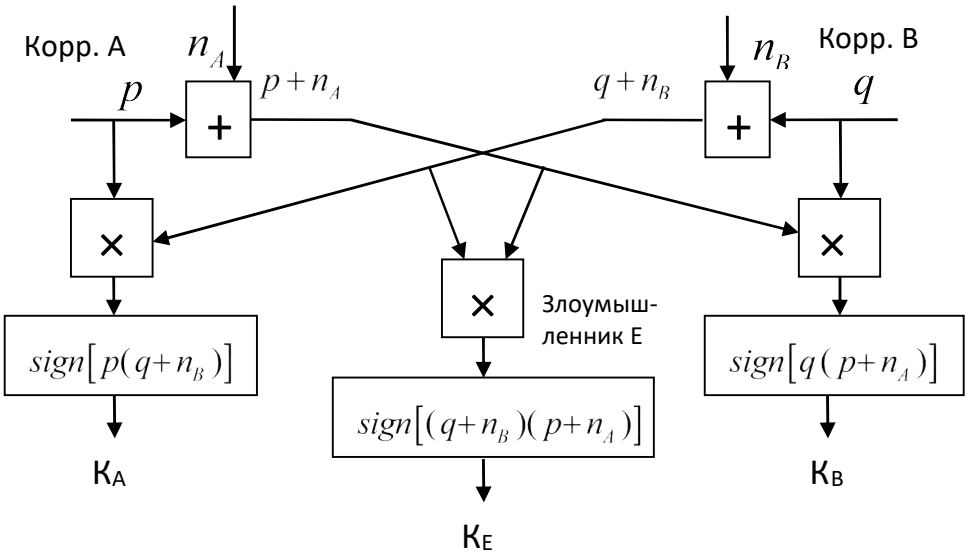


Рис. Сценарий формирования бит сырого ключа корреспондентами A и B в присутствии нарушителя E путем обмена гауссовскими числами

Корреспондент А генерирует случайное число p суммирует его с другим случайным числом n_A («шумом») и передает сумму $(p+n_A)$ по постоянному бесшумному корреспонденту В. Корреспондент В выполняет аналогичные операции: генерирует случайное число q суммирует его с другим случайным числом n_B и передает сумму $(g+n_B)$ корреспонденту А. Здесь: p, q гауссовские СВ с параметрами (0,1). n_A, n_B – гауссовский шум (0,σ). Далее каждый корреспондент вычисляет произведение своего случайного числа и числа принятого вместе с «шумом» от противоположного корреспондента, квантует его на два уровня и получает бит сырого ключа. У корреспондента А бит сырого ключа обозначим как $K_A = sign[\,p(g+n_B)]$. У корреспондента В бит сырого ключа обозначим как $K_B = sign[\,q(\,p+n_A)]$. Нарушитель Е перехватывает в обоих каналах зашумленные числа $(p+n_A)$ и $(g+n_B)$ перемножает их, квантует на два уровня и получает бит сырого ключа $K_E = sign[(\,p+n_A)(g+n_B)]$. Знак квантования $sign[s]$ определяется следующим образом $sign[s] = \begin{cases} 1, \text{ если } s \le 0 \\ 0, \text{ если } s > 0 \end{cases}$.

Наша задача состоит в определении вероятностей событий:

$$\tilde{K}_A = \tilde{K}_B,\ \ \tilde{K}_A \neq \tilde{K}_B,\ \ \tilde{K}_E = \tilde{K}_A,\ \ \tilde{K}_E \neq \tilde{K}_A.$$

Рассмотрим сначала ситуацию $\tilde{K}_A = \tilde{K}_B$. Это событие может произойти, когда выполняются следующие неравенства:

$$p\left(g+n_B\right)>0,\ \ g\left(p+n_A\right)>0 \tag{1}$$

или

$$p\left(g+n_B\right)<0,\ \ g\left(p+n_A\right)<0. \tag{2}$$

В свою очередь (1) можно записать, как выполнение неравенств

$$p>0,\left(g+n_B\right)>0 \quad g>0,\left(p+n_A\right)>0, \tag{3}$$

$$p<0,\left(g+n_B\right)<0 \quad g<0,\left(p+n_A\right)<0, \tag{4}$$

$$p>0,\left(g+n_B\right)>0 \quad g<0,\left(p+n_A\right)<0, \tag{5}$$

$$p<0,\left(g+n_B\right)<0 \quad g>0,\left(p+n_A\right)>0. \tag{6}$$

Заметим, что условие (3) может быть переписано в виде

$$\begin{aligned} &p>0,\left(p+n_A\right)>0 \Rightarrow p>0, n_A>-p \\ &g>0,\left(g+n_B\right)>0 \Rightarrow g>0, n_B>-q \end{aligned}, \tag{7}$$

Тогда, обозначив плотности распределения СВ p, q, n_A, n_B соответственно $w(p), w(q), w(n)_A, w(n_B)$, запишем выражение для вероятности совместного выполнения неравенств (7)

$$P1=\int_0^{\infty} w(p) \int_{-p}^{\infty} w\left(n_A\right) dn_A dp \cdot \int_0^{\infty} w(q) \int_{-q}^{\infty} w\left(n_B\right) dn_B dq \cdot \tag{8}$$

Для неравенств (4)–(6) можно аналогично записать вероятности их выполнения:

$$P2 = \int_{-\infty}^{0} w(p) \int_{-\infty}^{-p} w(n_A)\, dn_A dp \cdot \int_{-\infty}^{0} w(q) \int_{-\infty}^{-q} w(n_B)\, dn_B dq \cdot, \quad (9)$$

$$P3 = \int_{0}^{\infty} w(p) \int_{-\infty}^{-p} w(n_A)\, dn_A dp \cdot \int_{-\infty}^{0} w(q) \int_{-q}^{\infty} w(n_B)\, dn_B dq \cdot, \quad (10)$$

$$P4 = \int_{-\infty}^{0} w(p) \int_{-p}^{\infty} w(n_A)\, dn_A dp \cdot \int_{0}^{\infty} w(q) \int_{-\infty}^{-q} w(n_B)\, dn_B dq \cdot. \quad (11)$$

Неравенства (2) могут по аналогии с (1) переписаны как четыре группы неравенств, подобных (3)–(6), и для них могут быть записаны вероятности их выполнения, которые мы обозначим как $P5$, $P6$, P7, $P8$.

Тогда вероятность правильного выделения бита ключа $P\left(\tilde{K}_A = \tilde{K}_B\right) = \sum_{1}^{8} Pi$.

Очевидно, что вероятность несовпадения бит ключей у А и В равна $P\left(\tilde{K}_A \neq \tilde{K}_B\right) = 1 - \sum_{1}^{8} Pi$.

Рассмотрим теперь события, когда у нарушителя формируется совпадающий с А бит ключа независимо от того какой бит ключа выделил В.

$K_A = K_E$, если $sign\left[p\left(g + n_B\right)\right] = sign\left[\left(p + n_A\right)\left(g + n_B\right)\right]$, что равносильно выполнению неравенств

$$p\left(g + n_B\right) > 0 \text{ и } \left(p + n_A\right)\left(g + n_B\right) > 0 \text{ или } p\left(g + n_B\right) < 0 \text{ и } \left(p + n_A\right)\left(g + n_B\right) < 0.$$

Эти неравенства можно переписать в виде

$$p > 0 \text{ и } n_A > -p \text{ или } p < 0 \text{ и } n_A < -p.$$

Тогда можно записать выражение для вероятности $P\left(K_A = K_E\right)$

$$P\left(K_A = K_E\right) = \int_{0}^{\infty} w(p) \int_{-p}^{\infty} w(n_A)\, dn_A dp + \int_{-\infty}^{0} w(p) \int_{-\infty}^{-p} w(n_A)\, dn_A dp. \quad (12)$$

А вероятность несовпадения бит ключа у нарушителя и корреспондента А равна

$$P\left(K_A \neq K_E\right) = 1 - P\left(K_A \neq K_E\right).$$

Аналогичным путем можно получить выражения для вероятности совпадения (несовпадения) бит ключа у нарушителя и корреспондента А при условии, совпадения несовпадения бит у корреспондентов А и В:

$$P\left(K_A = K_E / K_A = K_B\right),\ P\left(K_A = K_E / K_A \neq K_B\right) \text{ или } P\left(K_A \neq K_E / K_A = K_B\right),$$
$$P\left(K_A \neq K_E / K_A \neq K_B\right).$$

В таблице представлены вероятности совпадения (несовпадения) бит ключа для разных значений дисперсии шума σ^2, рассчитанные с использованием соотношений (8)–(12).

Из таблицы следует, что с увеличением σ^2 вероятность правильного выделения бита ключа уменьшается как у легального пользователя, так и у нарушителя. Причем вероятность правильного приема бита ключа у нарушителя даже несколько больше чем у легального пользователя. Это объясняется более широкой областью интегрирования в (12), однако обоснование с физической точки зрения пока не ясно. Вероятности совпадения (несовпадения) ключей у легальных пользователей и нарушителя по отношению к легальному пользователю являются зависимыми. Это видно из сравнения столбцов 4,5 и 6 таблицы. Видим, что если бит ключа у В совпадает с битом ключа у А, то вероятность того, что биты ключа у А и Е совпадут увеличивается. В тоже время расчеты показывают, что если бит ключа у В не совпадает с битом ключа у А, то вероятность того, что биты ключа у А и Е совпадут равна 0,5, то есть $P\left(K_A = K_E / K_A \neq K_B\right) = 0.5$.

ТАБЛИЦА. Вероятности совпадения (несовпадения) бит ключа для разных значений дисперсии шума σ^2

σ^2	$P\left(\tilde{K}_A = \tilde{K}_B\right)$	$P\left(\tilde{K}_A \neq \tilde{K}_B\right)$	$P\left(\tilde{K}_E = \tilde{K}_A\right)$	$P\left(\tilde{K}_E \neq \tilde{K}_A\right)$	$P\left(K_A = K_E / K_A = K_B\right)$	$P\left(K_A \neq K_E / K_A = K_B\right)$
1	2	3	4	5	6	7
0.1	0.82403	0.17597 0.17557 эксп.	0.90251	0.09749 0.09754 эксп.	0.98847	0.01153
0.2	0.76812	0.23188 0.2318 эксп.	0.86614	0.13386 0.13387 эксп.	0.97667	0.02333
0.3	0.73188	0.26812 0.26762 эксп.	0.8405	0.1595 0.15912 эксп.	0.96524	0.03476
0.5	0.68494	0.31506	0.80409	0.19591	0.94396	0.05604
0.7	0.65483	0.34517	0.77823	0.22177	0.9249	0.0751

В таблице также представлены результаты, моделирования схемы на рис., полученные М.М. Кабардовым. Как видим, результаты моделирования и результаты, полученные аналитическим путем, имеют хорошее совпадение.

В качестве направлений дальнейших исследований можно отметить следующие:

– разработка метода преимущественного уменьшения вероятности ошибки бита ключа у легального пользователя по отношению к нарушителю с учетом зависимости ошибок у легального пользователя и нарушителя;

– получение аналитических оценок для вероятностей совпадении (несовпадения) бит ключа для протокола на основе обмена матрицами между корреспондентами A и B.

Список используемых источников

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

2. Герасимович А. С., Кабардов М. М., Коржик В. И., Старостин В. С., Яковлев В. А. Скрытное распределение криптографических ключей по постоянному каналу, в условиях возможного бесшумного перехвата и перспективы использования квантовых компьютеров // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т. 1.С. 5–15.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ УЯЗВИМОСТИ СИСТЕМ ХРАНЕНИЯ ПАРОЛЕЙ В ВЕБ-БРАУЗЕРАХ

Н. А. Косов, И. П. Павлоцкий

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

В современном мире, в котором Интернет стал неотделим от жизни человека, невозможно представить обычного пользователя, не использующего веб-браузер для доступа к Всемирной паутине. За последние годы браузеры претерпели значительные изменения, и теперь это не просто удобные инструменты для просмотра веб-страниц. Сегодня браузер предлагает пользователю множество дополнительных функций, в том числе встроенный менеджер паролей, позволяющий сохранять пароли и другие учетные данные к различным сервисам в базе данных и синхронизировать ее между различными устройствами, такими как ПК и смартфон. Такое решение одновременно создает угрозу безопасности, так как порождает возможность кражи учетных данных пользователей. В данной статье рассмотрено, какие уязвимости могут содержать в себе системы хранения паролей в наиболее популярных браузерах, как злоумышленники могут ими воспользоваться, и возможные решения выявленной проблемы.

информационная безопасность, веб-браузер, менеджер паролей, DPAPI, уязвимость.

В наше время довольно трудно представить человека, обладающего персональным компьютером или мобильным гаджетом, который не пользовался бы браузером. Согласно статистике интернет-портала LiveInternet за январь 2021 года общее количество пользователей браузеров в России составило почти 90 млн, при этом тройку лидерства занимают такие браузеры, как Google Chrome, Яндекс.Браузер и браузер для ОС компании Apple – Safari (рис. 1) [2].

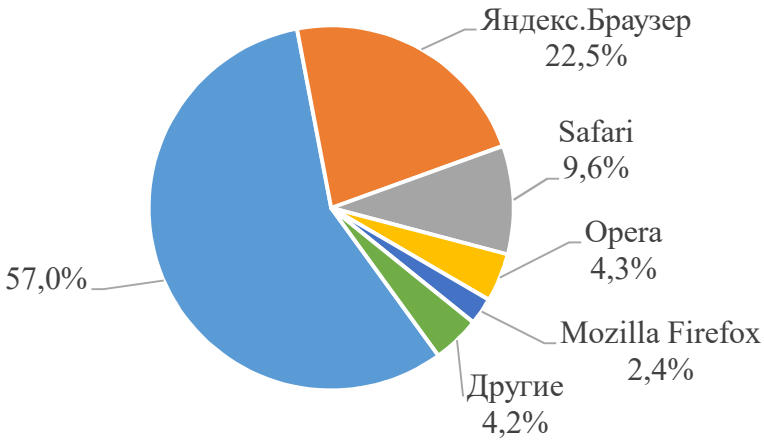


Рис. 1. Статистика наиболее популярных браузеров в России по количеству пользователей (январь 2021 г.)

Помимо основной функции – предоставление пользователю удобного интерфейса для просмотра веб-сайтов, веб-браузер предлагает множество дополнительных функций, одной из которых является встроенный менеджер паролей. Данная система хранения паролей избавляет пользователя от необходимости помнить огромное количество паролей от каждого сайта. Благодаря этому данная функция становится очень заманчивой и быстро набирает популярность. А потому становится актуальным вопрос безопасности таких систем.

Рассмотрим, как устроен менеджер паролей в браузере Google Chrome в рамках операционной системы Windows. Как будет показано далее, именно в нем в первую очередь наблюдается слабое место, представляющее угрозу информационной безопасности.

Учетные данные Google Chrome хранит в локальной базе данных типа SQLite, которая по умолчанию находится по следующему пути: %LOCALAPPDATA%\Google\Chrome\User Data\Default. Файл базы данных называется Login Data, а нужная информация содержится в таблице logins (рис. 2) [1].

Наиболее интересными для злоумышленника полями являются origin_url (url сайта, где регистрировались), username_value (логин пользователя) и password_value. Последнее имеет тип данных BLOB (*Binary Large OBject*) – по сути байтовый массив. Это поле и есть непосредственно сам пароль, но в зашифрованном виде. Соответственно, перед хакером встает задача расшифровки паролей.

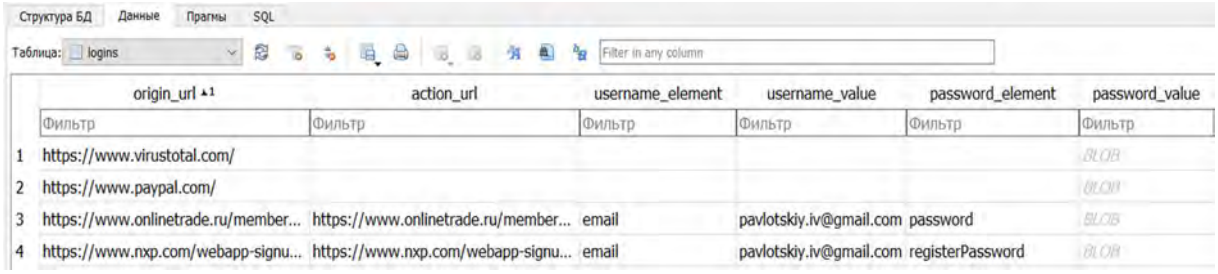

Структура БД | Данные | Прагмы | SQL

Таблица: logins | Filter in any column

	origin_url	action_url	username_element	username_value	password_element	password_value
	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр
1	https://www.virustotal.com/					BLOB
2	https://www.paypal.com/					BLOB
3	https://www.onlinetrade.ru/member...	https://www.onlinetrade.ru/member...	email	pavlotskiy.iv@gmail.com	password	BLOB
4	https://www.nxp.com/webapp-signu...	https://www.nxp.com/webapp-signu...	email	pavlotskiy.iv@gmail.com	registerPassword	BLOB

Рис. 2. Пример содержимого таблицы logins

На момент написания данной статьи алгоритм работы менеджера паролей следующий. Google Chrome шифрует каждый пароль алгоритмом AES-256 в режиме GCM (*Galois/Counter Mode*) с помощью ключа, генерируемого случайным образом. В дальнейшем будем называть этот ключ EncKey. Данный ключ в свою очередь также шифруется с помощью DPAPI (*Data Protection Application Programming Interface*) – криптографического интерфейса в системе Windows. При этом используется так называемый мастер-ключ, формируемый на основе пароля пользователя на вход в систему [1, 3]. Зашифрованный ключ EncKey сохраняется в папке User Data в файл Local State, имеющий формат JSON (*JavaScript Object Notation*).

Уязвимость данного алгоритма кроется в использовании DPAPI. Суть в том, что вся работа с данным интерфейсом реализуется с помощью двух простых в использовании функций: CryptProtectData, шифрующей данные и CryptUnprotectData, выполняющей, соответственно, расшифровку (рис. 3). При этом разработчику ПО, использующему DPAPI, не нужно знать мастер-ключ и прочие параметры криптографической системы. Операционная система сделает все за него. Единственным обязательным аргументом, который подается на вход этих функций, являются данные в формате BLOB, которые нужно зашифровать или расшифровать [3].

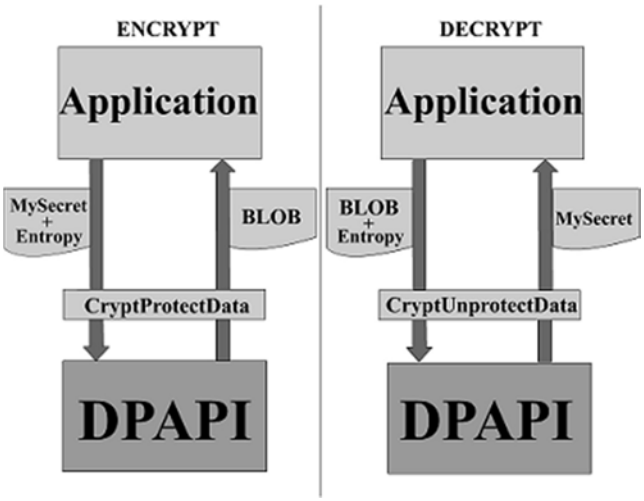


Рис. 3. Схема работы программы с DPAPI

Таким образом, любая программа (в том числе вредоносная), может попросить операционную систему расшифровать ключ EncKey и затем использовать его для получения доступа к паролям [4, 5].

В качестве атаки, использующей данную уязвимость, можно привести тривиальный, но легко реализуемый и практичный пример. Предположим, что работник некого предприятия, следуя злому умыслу и используя служебное положение, получает физический доступ к рабочему компьютеру работника, занимающего высокую руководящую должность. Злоумышленник вставляет в компьютер флешку и запускает с нее скрипт, который, используя функцию CryptUnprotectData, расшифровывает EncKey, а затем с его помощью расшифровывает все пароли, сохраненные в Chrome. Далее программа записывает все полученные данные на флеш-накопитель. Данный скрипт достаточно легко написать, например, используя язык программирования Python.

Рассмотрим решения, которые позволяют устранить данную уязвимость. Конечно, самым простым и действенным способом с точки зрения безопасности будет решение не использовать встроенный в браузер менеджер паролей, и хранить пароли в других, более надежных местах. Однако стоит предположить, что не все пользователи будут готовы пойти на такую жертву удобства в пользу безопасности. Поэтому необходимо предложить более щадящий для пользователя вариант. Такой вариант предлагается в системе хранения паролей Яндекс.Браузера. Данный браузер предлагает пользователю два способа шифрования паролей.

Первый вариант практически полностью аналогичен алгоритму, используемому в Google Chrome – для шифрования используется DPAPI [4]. Это неудивительно, так как Яндекс.Браузер использует тот же движок, что и Chrome.

Второй вариант, который рекомендует выбирать сам Яндекс, – это использование мастер-пароля для шифрования ключа EncKey. Чтобы браузер расшифровал EncKey , пользователь должен ввести мастер-пароль. Мастер-пароль известен только владельцу паролей, он не сохраняется на компьютере, и, следовательно, не может быть с него украден. Сразу после расшифровки EncKey введенный мастер-пароль удаляется из памяти компьютера [4, 5]. Таким образом, пользователю необходимо будет запомнить лишь один только мастер-пароль, что в свою очередь уже значительно повышает уровень защиты, так как теперь даже если вредоносная программа сможет украсть ключ EncKey, она не сможет его расшифровать без наличия мастер-пароля.

В заключение данной работы стоит отметить, что анализ в ней проводился только в рамках операционной системы Windows, и были рассмотрены лишь два наиболее популярных в России браузера. Таким образом,

имеется простор для дальнейших исследований и проведения более глубокого сравнительного анализа.

Список используемых источников

1. Лебеденко А. В., Артеменко М. А., Кушнарев А. А. Исследование уязвимостей в хранении интернет-браузером конфиденциальных данных // Новая наука: Опыт, традиции, инновации. 2016. № 9. С. 78–82.

2. Статистика использования браузеров. URL: https://www.liveinternet.ru/stat/ru/browsers (дата обращения: 20.02.2021).

3. DPAPI на пальцах. URL: https://habr.com/ru/post/148602/ (дата обращения: 18.02.2020)

4. Шифрование паролей в Яндекс.Браузере. URL: https://yandex.ru/support/browser-passwords-crypto/ (дата обращения: 18.02.2021).

5. Как мы создавали менеджер паролей со стойкой криптографией и мастер-паролем. Опыт команды Яндекс.Браузера. URL: https://habr.com/ru/company/yandex/blog/344382/ (дата обращения: 20.02.2021).

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

УДК 004.89
ГРНТИ 28.23.29

СРАВНЕНИЕ МЕТОДОВ ОБУЧЕНИЯ СВЁРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ

Н. А. Косов, Р. С. Тимофеев

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

В данной статье описаны различия методов обучения свёрточной нейронной сети, позволяющая классифицировать изображения. В качестве инструмента разработки использовался язык программирования Python и библиотека Keras, являющаяся API фреймворка TensorFlow. В целях показать результат, наиболее приближенный к реальности, были выбраны метод обучения с учителем (supervised learning) и метод обучения без учителя (unsupervised learning).

нейронная сеть, свёрточная нейронная сеть, нейрон, свёрточный слой.

Гипотеза

Основная гипотеза данной статьи заключается в том, что метод обучения свёрточной нейронной сети с учителем произведёт тренировку нейронной сети быстрее чем метод без учителя. Это обусловлено тем, что в первом

случае свёрточная нейронная сеть на своём выходе знает правильный ответ, она сравнивает его с полученным результатом. Что касается метода обучения без учителя, то при нём свёрточная нейронная сеть сама пытается классифицировать данные по схожим характеристикам.

Введение

Нейронные сети также известные как искусственные нейронные сети или моделируемые нейронные сети, являются подмножеством машинного обучения и лежат в основе алгоритмов глубокого обучения. Их название и структура вдохновлены человеческим мозгом, имитируя способ, которым биологические нейроны передают друг другу сигналы. Благодаря таким сетям, машина обретает способность анализировать и даже запоминать различную информацию.

Свёрточные нейронные сети похожи на сети прямого распространения, но они обычно используются для распознавания изображений, распознавания образов и компьютерного зрения. Эти сети используют принципы линейной алгебры, в частности, матричное умножение, для выявления закономерностей в изображениях.

Описание

В тот момент, когда компьютер на вход получает изображение, он воспринимает его, как некий массив пикселей. Затем, обработав эту матрицу, компьютер выводит числа, которые описывают вероятность класса изображения (например, 0.33456 для утки, 0.0943 для дерева, 0.05894 для здания и так далее).

Нам же нужно, чтобы компьютер был способен различать все изображения, которые ему даны, и распознавать уникальные особенности, делающие утку уткой, а дерево деревом [2]. Всё, что нам необходимо это выделение характеристик базового уровня, к примеру границ и искривлений, и их классификация через группы свёрточных слоев.

Структура свёрточной нейронной сети [2, 3, 5]

1) Свёрточный слой

Основная задача свёрточного слоя - обнаруживать локальные соединения пространственных объектов из предыдущего слоя и отображать их внешний вид на карту признаков. В результате свертки в нейронных сетях изображение разделяется на перцептроны, создавая локальные рецептивные поля и, наконец, сжимая перцептроны в картах признаков размером N×N (рис. 1). Таким образом, эта карта хранит информацию о том, где эта осо-

бенность встречается на изображении и насколько хорошо она соответствует фильтру. Следовательно, каждый фильтр обучается в пространстве относительно положения в объеме, к которому он применяется.

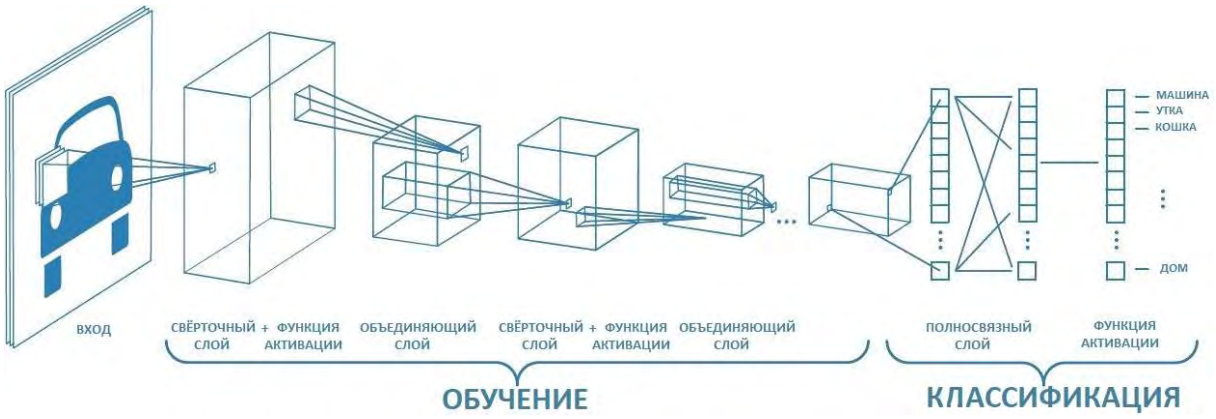


Рис. 1. Схема свёрточной нейронной сети

2) Слой активации ReLU

Выпрямленные линейные блоки (ReLU) – это специальная реализация, которая объединяет уровни нелинейности и исправления в сверточных нейронных сетях. ReLU является кусочно-линейной функцией, которая используется, как функция активации внутри модели (рис. 1).

Выпрямленные линейные блоки обладают тремя значительными преимуществами в сверточных нейронных сетях по сравнению с традиционными функциями активации логистического или гиперболического тангенса:

- Выпрямленные линейные блоки эффективно распространяют градиент и, следовательно, уменьшают вероятность проблемы исчезающего градиента, которая является обычной для глубинных нейронных архитектур.
- Выпрямленные линейные блоки порождают отрицательные значения до нуля и, следовательно, решают проблему отмены, а также приводят к гораздо более разреженному объему активации на его выходе. Редкость полезна по нескольким причинам, но в основном обеспечивает устойчивость к небольшим изменениям входных данных, например к шуму.
- Выпрямленные линейные блоки состоят только из простых операций с точки зрения вычислений (в основном сравнения) и, следовательно, намного более эффективны для реализации в сверточных нейронных сетях.

В результате своих преимуществ и производительности большинство последних архитектур сверточных нейронных сетей используют только слои активации ReLU в качестве слоёв нелинейности вместо традиционных слоёв нелинейности и исправления.

3) Объединяющий слой

Объединяющий слой служит для уменьшения размера карты активации, что приводит к созданию объектов среднего уровня. Он обеспечивает ввод для следующих последующих слоев, если модель состоит из более глубоких слоев.

Объединяющий слой теряет некоторые данные, что, в свою очередь, помогает снизить вероятность переобучения, поскольку сложность модели уменьшается. Предпочтительный размер окна выбирается для перемещения по всему входу, чтобы обеспечить функции среднего уровня на основе надежного подхода подвыборки. Наиболее приемлемым принятым методом подвыборки является метод усреднения или метод максимального значения. В данном исследовании был выбран метод максимальной подвыборки, поскольку он обеспечивает уникальные характеристики производительности.

4) Полносвязный слой

Полносвязный слой – это слой, требующий представления данных в форме вектора для дальнейшей обработки. Именно поэтому значения сжимаются в длинный вектор последовательно упорядоченных чисел.

В наиболее популярных моделях машинного обучения последние несколько слоев являются полносвязными слоями, которые компилируют данные, извлечённые ранее, для формирования окончательного вывода. Это второй по времени слой после слоя свертки.

5) Слой активации SoftMax

Данная функция активации представляет выходные значения в виде вероятностей соответствия тому или иному классу. Сумма всех выходных значений равна 1 (рис. 1).

Данная вероятность получается путём возведения экспоненты в степень входной суммы выходного нейрона и деления на сумму всех сумм выходных нейронов, которые являются степенями экспонент.

Методы обучения

В данной работе для обучения свёрточной нейронной сети используются два самых популярных способа обучения НС [1, 4]:

– с учителем (*supervised learning*);

– без учителя (*unsupervised learning*).

Способ обучения нейронной сети с учителем имеет такое название из-за использования, во время тренировки модели, набора заранее размеченных данных для корректировки получаемых результатов на каждом шаге её создания.

Это означает, что у каждого вектора, поступающего на вход, уже существует целевой вектор, представляющий верный результат, которые должен получиться на выходе. Традиционное такая связь называется обучающей парой и для обучения, обычно, используется определенное количество таких

пар. Данные связи являются основой метода обратного распространения ошибки (*backpropagation*), принцип которого заключается в минимизировании и приведении ошибок вычисления к применимому значению.

Обучение нейронной сети без учителя является более реалистичным способом тренировки с точки зрения применимости в реальной жизни. Потому что, поместив такую модель в условия нашей действительности, она сможет более объективно анализировать результаты из-за наличия у неё данных, полученных не из тепличных условий, что позволит ей быть более эффективной. Такая нейронная сеть не нуждается в целевом векторе для выходных данных. Выборка, на которой происходит всё обучение состоит только из векторов, поступивших на вход сети. Алгоритм, отвечающий за обучение модели, производит регулировку весов таким образом, чтобы представление достаточно близких входных векторов давало одинаковые выходные данные. Благодаря этому, процесс обучения получает статистические свойства обучающей выборки и группирует схожие векторы в классы.

Список используемых источников

1. Обучение нейросети с учителем, без учителя, с подкреплением – в чем отличие? Какой алгоритм лучше? URL: https://neurohive.io/ru/osnovy-data-science/obuchenie-s-uchitelem-bez-uchitelja-s-podkrepleniem/ (дата обращения 20.03.2021).

2. Сверточная нейронная сеть, часть 1: структура, топология, функции активации и обучающее множество. URL: https://habr.com/ru/post/348000/ (дата обращения: 25.12.2020).

3. Распознавание изображений на Python с помощью TensorFlow и Keras. URL: https://evileg.com/ru/post/619/ (дата обращения: 20.12.2020).

4. Особенности машинного обучения средствами CNN в рамках синтеза речи. URL: https://gstou.ru/files/nauka/works_ggntu/29-35-osobennosti-mashinnogo-obucheniya-sredstvami.pdf (дата обращения: 04.03.2021) С. 31–32.

5. Шолле Франсуа Глубокое обучение на Python. Серия Библиотека программиста. СПб. : Изд-во Питер, 2018. С. 151–156.

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

УДК 004.056
ГРНТИ 49.33.35

АНАЛИЗ МЕТОДИК ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

И. В. Котенко, В. В. Пучков

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В работе проводится анализ используемых в настоящее время методик оценивания защищенности киберфизических систем. Рассматриваются достоинства и недостатки существующих методик. Основное внимание уделяется методикам оценки защищенности киберфизических систем на основе анализа графов атак.

киберфизические системы (КФС), методики анализа защищенности, графы атак.

В настоящее время в связи с активным развитием компьютерных иинформационных технологий все большее распространение находят киберфизические системы (КФС), которые являются совокупностью устройств, вычислительный процесс в которых тесно связан с реакцией на физическом уровне и выполняется на некоторой физической платформе. К КФС можно отнести: системы управления предприятиями (АСУ, SCADA-системы); интернет вещей (умный дом, умные вещи); робототехнические системы; беспилотные летательные аппараты и беспилотные автомобили. В целях обеспечения бесперебойного и безопасного функционирования КФС необходимо проводить оценивание защищенности подобных систем. Методики анализа защищенности дают возможность представить уровень защищенности в виде значений набора различных показателей. В этом случае показатель – это мера измерения, которая дает качественную или количественную оценку определенных атрибутов, выведенную на основе аналитической модели, разработанной для определенных информационных потребностей [1, 2, 3, 4].

Используется несколько видов методик оценки безопасности.

Методики, которые используют оценку риска на качественном уровне (например, используется шкала «высокий», «средний», «низкий») называют *качественными*. К ним относятся: FRAAR, COBRA, OCTAVE. Рассмотрим более подробно методику FRAAR.

FRAAR
(*Facilitated Risk Analysis and Assessment Process, Облегченный процесс анализа и оценки рисков*) [5]

Управление рисками при применении данной методики начинается с оценки рисков. Рассмотрим кратко основные этапы оценки рисков по FRAAR. Первый этап – происходит определение защищаемых активов (изучение документации, сканирование сете и т. д.). Второй этап – идентификация угроз. Могут использоваться различные методы (ранее подготовленные чек-листы, анализ статистики происшествий в проверяемой системе и т. д.). Третий этап – после составления списка угроз, оценивается вероятность их возникновения. Из полученных данных оценивается уровень угрозы. Предложена следующая шкала оценки (по вероятности реализации угрозы): высокая (очень вероятно, что угроза реализуется в течении года); средняя (возможно угроза будет реализована в течении года); низкая (маловероятно, что угроза будет реализована в ближайший год). Еще одна используемая оценочная шкала – ущерб, причиняемый активу: высокий (высокий ущерб бизнесу, потеря имиджа); средний (несущественные перерывы в работе систем, могут привести к каким-то финансовым потерям в одной бизнес-единице; низкий (не происходит значимых финансовых потерь). Данные, полученные при оценке риска, оцениваются так: уровень A – действия по безопасности должны быть выполнены немедленно; уровень B – действия должны быть выполнены; уровень C - нужен мониторинг, но срочных действий принимать нет необходимости; уровень D - никаких действий предпринимать не нужно. Четвертый этап - после проведения оценки риска и идентификации угрозы, определяются контрмеры, которые могут снизить риск до приемлемого уровня. Достоинства методики: использование внутренних экспертов, минимальные трудозатраты на выполнение анализа и оценки рисков, простота процесса анализа. Недостатки методики: не производится разработка показателей защищенности для анализа определения вероятности угрозы или годовых потерь, исключая случаи, когда информация для их определения легко доступна; отсутствие средств глубокой декомпозиции и точной оценки рисков не дает возможности точечного применения нужного набора мер и средств защиты, что отрицательно влияет на экономическую эффективность информационной системы безопасности.

Далее рассмотрим *количественные методики* анализа защищенности. В них риск оценивается через какое-то конкретное числовое значение, например, размер ожидаемых годовых финансовых потерь. Ранжируют риски относительно друг друга на основе ценности активов, уязвимостей и защитных мер [5]. К данному классу относят следующие методики: RiskWatch, Microsoft и т. д. [5, 6, 7, 8] Рассмотрим методику RiskWatch.

Методика количественной оценки риска RiskWatch

Данная система была разработана компанией RiskWatch. Также специалистами компании было разработано и семейство программных средств, в которых она реализуется [7]. В основе данной методики находится анализ рисков, который состоит из четырех этапов. Первый этап – определение предмета исследования. Дается описание типа организации, вид системы, требования безопасности. Второй этап – ввод данных, которые описывают конкретные характеристики системы. На этом этапе дается описание потерь и классов инцидентов. Для определения возможных уязвимостей разработан опросник, в котором содержится около 6 000 вопросов. Третий этап – количественная оценка риска. Здесь происходит расчет рисков и выбираются меры безопасности. Риск оценивается как математическое ожидание потерь за год (m = p*v, где m - математическое ожидание, p - вероятность угрозы, v - стоимость ресурса). Четвертый этап – генерация отчетов. Виды отчетов: краткие итоги; отчеты по элементам на первом и втором этапах; отчет по стоимости ресурсов и ожидаемых потерях при реализации угроз; отчет по угрозам и мерам противодействия; отчет по возврату инвестиций; отчет по результатам аудита системы безопасности. Достоинства данной методики: позволяет оценить не только риски, которые существуют в данный момент, также можно определить выгоду, которую принесет внедрение новых механизмов защиты. Итоговые отчеты и графики дают достаточно данных для анализа и принятия решений о модернизации системы безопасности. Недостатки методики: полученный расчетный ущерб в итоге будет выше, чем реальный, т. к. на один и тот же актив может быть направлено несколько угроз. Следовательно, общий ущерб, определенный по угрозам, будет гораздо больше реального.

На практике для проведения анализа защищенности обычно применяются качественно-количественные методы. В этом случае какому-то качественному уровню безопасности соответствуют некоторые диапазоны количественных величин [9].

Качественно-количественная методика оценки рисков CRAMM

Разработана центральным агентством по компьютерам и телекоммуникациям (*Central Computer and Telecommunications Agency*, CCTA) в Великобритании [8]. Методика включает три этапа работы: определение и оценка активов; выявление угроз и уязвимостей; определение адекватных защитных мер. Достоинства данной методики: обширная база данных по контрмерам в области информационной безопасности; гибкость, дающая возможность использовать ее для аудита систем любого уровня сложности. Недостатки методики: требует высокой квалификации аудитора; трудоемкий процесс аудита; возможность внесения изменений в базу данных пользователем недоступна.

Методика анализа защищенности на основе графов атак

В [2, 3, 4, 9] предлагается проводить анализ защищенности сетей, используя реализацию комплекса следующих действий: построение графов атакующих воздействий, которые выполняются из различных точек сети; далее происходит выявление уязвимостей и «узких» мест в защите системы; затем происходит вычисление метрик безопасности и определяется общий уровень защищенности; последний этап – это сопоставление полученных метрик с требованиями и выработка рекомендаций по улучшению защищенности системы. Главная особенность описанного подхода заключается в использовании общего графа атак для определения класса различных метрик защищенности системы, которые используются для анализа защищенности сети и реализуемой в ней политики безопасности.

Проанализировав рассмотренные выше методики анализа защищенности, которые наиболее часто используются специалистами по безопасности информационных систем, и оценивая важность динамического анализа безопасности КФС, можно сделать вывод о перспективности дальнейшей разработки методики анализа защищенности КФС на основе графов атак. Методика анализа защищенности, построенная на основе графов атак, позволит создать систему для анализа состояния защищаемой КФС на всех циклах ее существования, начиная с момента проектирования и обеспечивая ее безопасную работу в процессе настройки и эксплуатации. Используя методику анализа графов атак, возможно определять метрики безопасности, актуальные для данной системы. В таблице приведены показатели защищенности, которые применяются при анализе безопасности с помощью графов атак.

ТАБЛИЦА. Метрики безопасности при использовании графов атак

Название показателя	Описание	Источник	Используемый граф атаки
Показатель уверенности в атаке	Определяет уровень уверенности, что атака выполняется.	[10]	Вероятностный граф
Индекс уверенности в компрометации	Определяет уровень уверенности в том, что узел графа атак был достигнут.	[11]	Вероятностный граф
Вероятность успешного использования уязвимостей	Определяет вероятность успешного использования уязвимостей, соответствующих узлам графа атаки.	[12]	Вероятностный граф
Наиболее критичный компонент системы	Определяет наиболее критичные уязвимости для определения точек внедрения.	[13]	Байесовский граф

Согласно [14] графы атак могут также применяться как для анализа безопасности сети в автономном режиме, так и в режиме онлайн. В автономном режиме, не вмешиваясь в текущую работу целевой сети, они могут быть использованы для определения систем обнаружения/предотвращения вторжений, вычисления показателей оценки безопасности сети, проведения анализа рисков сетевой безопасности. Также графы атак можно использовать для измерения риска, создаваемого эксплойтами в целевой сети. В случае сбора информации из целевой сети в режиме близком к реальному времени, графы атак могут быть использованы для анализа заражения сети и корреляции журналов безопасности.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. М.: Стандартинформ, 2012. 56 с.

2. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science (LNCS). Vol. 8407. Springer. 2014. pp. 462–471.

3. 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, Springer-Verlag. 2005. V. 3685. pp. 311–324.

4. Kotenko I., Stepashkin M., Doynikova E. Security Analysis of Information Systems taking into account Social Engineering Attacks // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). 2011. pp. 611–618.

5. Peltier T. R. Information security risk analysis, Third Edition. CRC Press, 2010. 456 p.

6. Caralli R. A., Stevens J. F., Young L. R., Wilson W. R. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Technical Report. Software Engineering Institute, 2007. 154 p.

7. RiskWatch. URL: http: // www.riskwatch.com

8. Астахов А. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.

9. Котенко И. В., Степашкин М. В. Метрики безопасности для оценки уровня защищенности компьютерных сетей // Защита информации. Инсайд. 2006. № 3 (9). С. 36–45.

10. Stakhanova N., Basu S., Wong J. A cost-sensitive model for preemptive intrusion response systems // Proceedings of the 21st International Conference on Advanced Networking and Applications. 2007.

11. Wu Y.-S., Foo B., Mao Y.-C., Bagchi S., Spafford E. H. Automated adaptive intrusion containment in systems of interacting services // Computer Networks: The International Journal of Computer and Telecommunications Networking. 2007. Vol. 51. pp. 1334–1360.

12. Man D., Yang W., Yang Y., Wang W., Zhang L. A quantitative evaluation model for network security // Proceedings of the 2007 International 159 Conference on Computational Intelligence and Security (15–19 Dec. 2007). pp. 773–777.

13. Chunlu W., Yancheng W., Yingfei D., Tianle Z. A novel comprehensive network security assessment approach // Proceedings of the 2011 IEEE International Conference on Communications (Kyoto). IEEE, 2011. pp. 1–6.

14. Kaynar K. A taxonomy for attack graph generation and usage in network security // Turkish Advanced Research Center (GT-ARC), TU Berlin, Ernst Reuter Platz 7, 10587 Berlin, Germany. 2016.

УДК 004.056
ГРНТИ 49.33.35

АНАЛИЗ АКТУАЛЬНЫХ МЕТОДИК АТРИБУЦИИ НАРУШИТЕЛЕЙ КИБЕРБЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

И. В. Котенко, С. С. Хмыров

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Целевые атаки на критическую инфраструктуру не только наносят серьезный ущерб экономической и национальной безопасности страны, но и в большинстве случаев не позволяют идентифицировать нарушителя кибербезопасности. Разнообразие высокотехнологичного инструментария и анти-криминалистических методик позволяет оставаться безнаказанным и выводит на новый уровень кибертерроризм и киберприступность, которая зачастую поддерживается внешними государственными организациями. Атрибуция нарушителей кибербезопасности является одной из актуальных задач в области обеспечения защиты объектов критической инфраструктуры. В данном исследовании рассматриваются методики атрибуции нарушителей кибербезопасности, выделяются их недостатки и преимущества.

целевые атаки, критическая инфраструктура, атрибуция кибернарушителя, кибербезопасность.

События, связанные с необходимостью атрибуции кибератак, встречаются еще на заре формирования отрасли информационной безопасности, но на новый уровень эта проблематика вышла в 2010 г., когда на комплексе по обогащению урана в иранском Натанзе был обнаружен вредоносный код, позже получивший название «Stuxnet». Именно тогда специалисты всерьез задумались о том, как идентифицировать силы, стоящие за данным вредоносным кодом [1, 2].

Развитая устойчивая угроза или целевая кибератака – это сложная, многоуровневая атака, выполняемая преимущественно на информационно – телекоммуникационную инфраструктуру военных и государственных объектов [3]. Данные объекты в большинстве случаев ведущими государствами мира относятся к объектам критической информационной инфраструктуры (КИИ) [4]. Как правило, кибернарушитель обладает значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения [5, 6, 7]. В проведении целевых кибератак чаще всего подозревали спецслужбы других стран и отряды «правительственных хакеров» [8].

Атрибуция кибератаки, т.е. идентификация происхождения и источника кибератаки, – это киберфизический процесс (на основе интеграции цифровой криминалистики с доказательствами из физического мира) с целью установления злоумышленника или группы злоумышленников [9, 10].

Исследования в данной области направлены на решение политических, правовых и технических проблем [11].

Методика, представленная в [12] и называемая «Q» моделью, предполагает объединение технических и социальных доказательств в процессе атрибуции. «Q» модель (1) описывает атрибуцию как постепенный процесс, переходящий от одного уровня к другому. Атрибуция кибератаки включает в себя несколько уровней: технический (тактический); оперативный (операционный); стратегический. Каждый из уровней позволяет получить ответы на вопросы: «Как? Кто? Зачем?». «Q» модель акцентирует основное внимание на социальных доказательствах, где знания, такие как текущие конфликты между странами или соперничество между корпорациями, очень полезны для выявления мотивов потенциальных нарушителей кибербезопасности. Недостатком этой модели является отсутствие экспериментальных оценок, подтверждающих эффективность данной методики [13].

Представленная [14] модель атрибуции кибератак «Intrusion Kill Chain model» (2), включает семь элементов кибератаки: разведка, вооружение, доставка, эксплуатация, установка, управление и контроль, действия по достижению цели. Каждый из элементов включает описание систематического процесса на данном этапе и применение наиболее популярных векторов атаки для достижения цели. Также в модели существуют индикаторы и жизненные циклы индикатора. Индикатор – это любая информация, объективно описывающая вторжение. Они подразделяются на три типа: атомарные; вычисляемые; поведенческие. Используя концепцию данной модели, аналитики посредством анализа или совместной работы выявляют индикаторы и применяют их в цифровой криминалистике при обнаружении совпадающей

активности. В случае, если индикаторы будут неверно сформированы, аналитики могут ошибочно применить их к легитимной деятельности и пустить расследование по ложному следу.

«Алмазная модель» (The Diamond Model) (3) [15] получила свое название за простую организацию базовых аспектов вредоносной деятельности кибернарушителей. Модель обеспечивает метод интеграции интеллекта для аналитической платформы и осуществляет корреляцию, классификацию и прогноз на основе деятельности злоумышленников. В модели выделяется четыре основные характеристики события: противник, возможности, инфраструктура и жертва. Эти объекты соединены ребрами, представляя основные взаимодействия между ними и расположены в форме алмаза. Также перечислены мета-функции, чтобы выделить их важность в анализе высшего порядка, группировке и функции планирования. Данная модель устанавливает формальный метод, применяющий научные принципы анализа вторжений (принципы измерения, тестируемости и повторяемости) и требует неавтоматизированного (ручного) контроля в процессе атрибуции кибернарушителя.

Анализ данных методик показал, что все модели требуют неавтоматизированного подхода, что делает процесс атрибуции длительным и низкоэффективными процессом.

Архитектурная анонимность сети Интернет является свойством, усложняющим процесс атрибуции [16]. Часто, доказательства, собранные из различных источников, противоречат друг другу. В случаях «обмана», когда либо злоумышленник подбрасывает ложные доказательства, либо доказательства указывают на нескольких действующих лиц, что приводит к неопределенности, корректная атрибуция кибернарушителя имеет очень низкую вероятность. Для повышения точности процесса атрибуции, в ситуациях «обмана» предлагается использовать машинное обучение совместно с моделью аргументированного рассуждения – DeLP (Defeasible Logic Programming) [17], основанной на логическом программировании [18]. Также в [19, 20] разработана формальная логическая основа для рассуждений о кибер-атрибуции, которая исследует конкурирующие гипотезы на основе доказательств «за» и «против» конкретного злоумышленника, чтобы помочь аналитикам принять решение об атрибуции, предоставив перечень аргументов, которые помогли прийти к данному выводу. Argumentation-Based Reasoner (ABR) (4) [19, 20] использует как технические доказательства, так и социальные соображения, которые представлены в модели «Q». ABR состоит из двух основных компонентов - правил рассуждения и фоновых знаний. В частности, ABR может отвечать на такие вопросы, как, например, кто является возможным исполнителем атаки, у кого есть мотивы для ее совершения, каковы возможности, необходимые для совершения нападения или каково сходство с ранее совершенными атаками [21].

Общая характеристика анализируемых методик атрибуции представлена в таблице.

Таким образом, процесс атрибуции нарушителя кибербезопасности является сложной многоцелевой задачей. Основной проблемой является достоверность входных данных, которые формируются в ходе технического анализа кибератаки. Анализ рассмотренных методик показал, что технические причины лежат в основе невозможности простого определения источника кибератак. В этой связи, перспективно выглядит применение методов машинного обучения и искусственного интеллекта (ИИ) совместно с инструментами цифровой криминалистики, предлагаемые в методике (4).

ТАБЛИЦА. Общая характеристика анализируемых методик атрибуции

Модель	Применение	Преимущества	Недостатки
1	Улучшение атрибуции за счет более детального анализа на каждом из уровней модели.	Объединяет социальные и технические данные в процессе атрибуции, позволяя осуществлять атрибуцию на нескольких уровнях.	Является теоретической моделью. Практического доказательства не имеет.
2	Является базовой моделью для большинства подходов при анализе атрибуции кибератак.	Помогает разработать защитные стратегии для каждого из семи элементов, входящих в данную модель.	Не подходит для моделирования внутренней угрозы (злоумышленник, как потенциальный инсайдер).
3	Повышение аналитических показателей с помощью корреляции, классификации и прогнозирования на основе действий кибернарушителей при интеграции модели в платформу анализа инцидентов.	Разработана с целью увеличения стоимости реализации кибератаки и уменьшения стоимости защитных мер.	Требует ручного контроля в процессе атрибуции кибернарушителя.
4	Систематизация криминалистических данных для дальнейшей атрибуции кибернарушителя.	Применяет ИИ и автоматизацию при анализе криминалисти-ческих данных, основывается на множестве доказательных источников.	Большая зависимость от входящих неструктурированных данных.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Лукацкий А. В. Определение источника кибератак // Индекс безопасности. 2015. № 21. С. 73–86.

2. Википедия. Stuxnet. URL: https://en.wikipedia.org/wiki/Stuxnet (дата обращения: 15.02.2021).

3. Steffens T. Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage. Springer-Verlag, Berlin, 2020. 205 p.

4. Котенко И. В., Саенко И. Б., Чечулин А. А. [и др.] Интеллектуальные сервисы защиты информации в критических инфраструктурах. СПб.: БХВ-Петербург, 2019. 400 с.

5. 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, Springer-Verlag. 2005. V. 3685. pp. 311–324.

6. 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. 4 (47). С. 5–27.

7. 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. 4 (47). С. 5–27.

8. Clark R., Hakim S. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. Springer, Cham, 2017. 290 p.

9. Christian R. Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace. 2019, Springer, Cham, 2019. 424 p.

10. Энциклопедия «Касперского». Атрибуция кибератаки. URL: https://encyclopedia.kaspersky.ru/glossary/cyber-attribution/ (дата обращения: 15.02.2021)

11. Hunker J., Hutchinson R., Margulies J. Roles and Challenges for Sufficient Cyber Attack Attribution. Research Report, Institute for Information Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, 2008. pp. 5–10.

12. Thomas R., Buchanan B. Attributing Cyber Attacks // Journal of Strategic Studies, 38:1-2/ 2015. pp. 4–37.

13. Nunes E., Shakarian P., Simari G., Ruef A. Argumentation Models for Cyber Attribution // Proc. 2016 IEEE, ACM Int. Conf. Adv. Soc. Networks Anal. Mining, ASONAM. 2016. pp. 837–844.

14. Hutchins E. M., Cloppert M. J., and Amin R. M. Intelligence – Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains // 6th Annu. Int.Conf. Inf. Warf. Secur., July 2005, 2011. pp. 1–14.

15. Caltagirone S., Pendergast A., Betz C. The diamond model of intrusion analysis // Threat Connect. 2013. Vol. 298. No. 0704. pp. 1– 61.

16. Tran D. The Law of Attribution: Rules for Attribution the Source of a Cyber-Attack // 20 Yale J. L. & Tech, 2017. 76 p.

17. Garcıa A., Simari G. Defeasible logic programming: An argumentative approach // Theory and practice of logic programming. 2004. Vol. 4. Iss. 1-2. pp. 95–138.

18. Shakarian P., Simari G., Moores G., Parsons S. Cyber-deception and attribution in capture-the-flag exercises // Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2015, Paris, France, 2015. pp. 962–965.

19. Shakarian P., Simari G. I., Moores G. and Parsons S. Cyber attribution: An argumentation-based approach // Cyber Warfare: Building the Scientific Foundation, 2015, Springer. pp. 151–171.

20. Shakarian P, Simari G., Moores G., Parsons S., Paulo D., Falappa M., Aleali A. Belief revision in structured probabilistic argumentation // Annals of Mathematics and Artificial Intelligence, 78, (3-4), Springer, Cham, 2016. pp. 1–43.

21. Karafili E., Wang L., Lupu E. C. An Argumentation-Based Reasoner to Assist Digital Investigation and Attribution of Cyber-Attacks // Forensic Science International: Digital Investigation 32. 2020. pp. 1–9.

УДК 004.75
ГРНТИ 49.33.35

АНАЛИЗ УЯЗВИМОСТЕЙ В ПРОТОКОЛАХ ИНТЕРНЕТА ВЕЩЕЙ УМНЫХ ГОРОДОВ

А. В. Красов, А. В. Крылов

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

Интернет вещей (IoT) – это развивающаяся технология, ориентированная на подключение устройств между собой, с сетью Интернет и пользователями. Ожидается, что технология IoT станет необходимым требованием при разработке умных городов, так как предлагает удобство и эффективность горожанам, чтобы они могли добиться лучшего качества жизни. Применение модели IoT в умных городах создает множество новых проблем безопасности с точки зрения конфиденциальность, подлинность и целостности данных. Эти проблемы делают умные города чрезвычайно уязвимыми для различных типов сетевых угроз. Следовательно, необходимо определить возможные риски безопасности, чтобы получить полную оценку состояния безопасности. Эта статья применяет методологию оценки критических угроз, активов и уязвимостей (OCTAVE Allegro), для оценки рисков безопасности умных городов. Метод OCTAVE Allegro фокусируется на информационных активах и рассматривает различные информационные контейнеры, такие как базы данных, физические документы и люди. Ключевые цели этого исследования - выделить различные уязвимости на основе Интернета вещей, чтобы определить риски и предложить подходы к их снижению.

умные города; Интернет вещей (IoT); OCTAVE Allegro; оценка рисков безопасности.

Интернет вещей (IoT) – это парадигма, развивающаяся благодаря обширным разработкам в информационных и коммуникационных технологиях (ИКТ). Инфраструктура Интернета вещей содержит сеть устройств или объектов, таких как встроенные компьютеры, управляемые датчики и радиочастоты идентификационные метки (RFID), а также шлюз IoT и удаленный сервер [1]. Архитектура обычная система IoT разделена на три уровня:

уровень восприятия, сетевой уровень и уровень приложения. Способ группировки компонентов на трех уровнях общей системы Интернета вещей показан на рис. Термин «вещи» в модели IoT включает в себя как кибер-мир (действия, события и услуги) так и физический мир (объекты и физических события) [2].

Рис. Структура IOT

Цель IoT – расширить функции Интернета за счет увеличения возможностей соединения многочисленных объектов. Используя модель Интернета вещей, пользователи могут обмениваться информацией, собранной подключенными объектами в физическом мире [2]. В процессе развертывания Интернета вещей используются различные технологии, такие как беспроводной датчик сети (WSN), RFID, Bluetooth, связь ближнего радиуса действия (NFC), интернет-протокол (IP), электронный код продукта (EPC), стандарт беспроводной связи (Wi-Fi), датчики и исполнительные механизмы [3, 4]. Ключевая цель Интернета вещей состоит в том, чтобы позволить пользователям однозначно идентифицировать и получить доступ к управлению устройствами в любое время и в любом месте через сеть Интернет [5].

Хотя существует несколько определений умных городов, с технической точки зрения общая концепция заключается в подключении датчиков и интеллектуальных устройств через Интернет для удаленного мониторинга, доступа и управления инфраструктурной средой [6]. Умный город так же может определяться как город, который автоматизирован с помощью парадигмы Интернета вещей и способен реагировать на требования его жителей и обеспечивать комфорт и безопасность [7]. Основные цели умного

города - повысить автоматизацию городов, упростить управление энергопотреблением и сократить количество выбросов в окружающую среду [8]. Кроме того, уровень потребление энергии и комфорт горожан являются ключевыми факторами при проектировании любой среды умного города.

Беспроводные интеллектуальные датчики стали очень популярными устройствами для мониторинга и отслеживания перемещений объектов в среде умного города, в следствии этого они стали целью различных атак. Существуют различные атаки, например, связанные с доступностью сервисов (лавинная рассылка, глушение и воспроизведение атаки), сетевая маршрутизация (несанкционированное обновление маршрутизации и атаки через червоточины) и узел аутентификация (атаки с перехватом и подражанием). Человек может напрямую атаковать устройство межсетевого взаимодействия (например, шлюз) или другое устройство, используя свой сетевой или локальный интерфейс связи (т. е. атакуя device) [9], и устройство может быть имитировано с помощью его неисправного сертификата подлинности. Атака на шлюз может немедленно привести к атаке на всю локальную сеть, так как это точка, в которой возможно внешнее подключение. В исследовании [10] сделан вывод о том, что у злоумышленника есть два варианта для получения доступа к устройствам сети IoT: сетевые атаки и атаки на устройства. В сетевых атаках злоумышленник может попытаться перехватывать, манипулировать, подделывать или прерывать передаваемые данные. Атаки на устройства можно классифицировать как программные атаки, физические или атаки по побочным каналам. Кроме того, есть возможность того, что злоумышленник может замаскироваться под внутреннего пользователя через различные сервисы или службы мониторинга.

Методология, принятая для этого исследования, – OCTAVE Allegro. Для оценки рисков была выбрана методология, позволяющая проводить комплексную оценку, приносящую надежные результаты, и фокусируется в основном на информационных активах. Подход OCTAVE Allegro анализирует, как информация используется пользователями или устройствами в системе. Кроме того, он рассматривает информационные контейнеры как места, где существует информация, и как эта информация подвергается рискам. Прочие критические активы могут быть идентифицированы и оценены путем установления связей с первоначально идентифицированным информационным активом.

Результаты исследования представлены в таблицах 1 и 2, которые дают обзор выявленных угроз безопасности и потенциальные риски в среде умного города на основе Интернета вещей. В двух таблицах показаны информационные активы, которые были идентифицированы и использованы в процессе оценки рисков, связанных с ними угроз и последствия в виде конкретных рисков и оценок.

ТАБЛИЦА 1. Угрозы безопасности, обнаруженные при выполнении оценки информационных рисков с точки зрения возможных угроз, связанных с информационными активами

Информационный актив	Возможные угрозы безопасности
Учетные данные пользователя	Выдача себя за другое лицо; Кража личных данных и учетных данных.
Мобильные личные данные и приложения	Вредоносный код внедряется в приложения, установленные на телефоне.
Информация, собираемая устройствами	Модификация информации; Атаки типа отказа в обслуживании (DoS); Взлом устройства или датчика; Раскрытие информации; Прерывание функции.
Инвентарная информация	Получите доступ к инвентарной информации для поиска определенного устройства с известными уязвимостями для атаки;
Информация журнала событий	Получение доступа к данным журнала и информации о включение возможных атак.
Информация, передаваемая через шлюз	Украсть информацию из пакетов, передаваемых через шлюз
Информация о настройке	Модификация информации

ТАБЛИЦА 2. Риски безопасности, выявленные при выполнении оценки информационных рисков с точки зрения возможных угроз

Потеря контроля над системой	41
Злоумышленник может получить доступ к смартфонам	41
Злоумышленник определяет самое слабое устройство с известными уязвимостями	39
Злоумышленник изменяет конфигурацию системы	39
Системные ресурсы истощаются из-за постоянной саморепликации	39
Нарушение конфиденциальности пользователя	34
Потеря информации	23

Список используемых источников

1. King J. Awad A. I. A Distributed Security Mechanism for Resource-Constrained IoT Devices // Informatica (Slovenia). 2016. 40. pp. 133–143.

2. Ning H. Unit and Ubiquitous Internet of Things; CRC Press, Inc.: Boca Raton, FL, USA, 2013.

3. Miller M. The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities are Changing the World; Que Publishing: Indianapolis, Indiana, 2015.

4. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications // IEEE Commun. Surv. Tutor. 2015. 17. pp. 2347–2376.

5. Suryadevara N. K.; Mukhopadhyay S. C. Smart Homes: Design, Implementation and Issues. Springer: Cham, Switzerland, 2015.

6. Савинов Н. В., Токарева К. А., Ушаков И. А., Красов А. В., Сахаров Д. В. Исследование модели сети цод на основе политик Cisco Aci // Защита информации. Инсайд. 2019. № 4 (88). С. 32–43.

7. Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, India, 17–19 December 2012. pp. 257–260.

8. Сахаров Д. В., Красов А. В., Ушаков И. А., Орлов Г. А. Защищенная модель программно-определяемой сети в среде виртуализации Kvm // Электросвязь. 2020. № 3. С. 26–32.

9. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе Ipv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51–57.

10. Khan R.; Khan S. U.; Zaheer R.; Khan S. Future Internet: The Internet of Things Architecture, Possible.

УДК 621.39
ГРНТИ 49.44.33

ПОВЕРКА ОПТИЧЕСКИХ РЕФЛЕКТОМЕТРОВ

В. С. Кузнецов

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

Рефлектометрические измерения являются важнейшей составной частью работ, проводимых при строительстве и эксплуатации волоконно-оптических линий связи. Оптические рефлектометры обладают рядом метрологических характеристик, несоответствие которым может оказать существенное влияние на качество этих линий. В данной статье описывается такая характеристика, как определение основной абсолютной погрешности оптического рефлектометра при измерениях ослабления и предлагается альтернативный вариант ее определения.

ВОЛС, оптический рефлектометр, поверка, ослабление, погрешность.

Согласно действующим методикам поверки, а именно МИ 1907-99 [1] и Р 50.2.071-2009 [2], по которым поверяются большинство оптических рефлектометров (ОР), для определения погрешности при измерении ослабления собирается установка по следующей (рис. 1) блок-схеме:

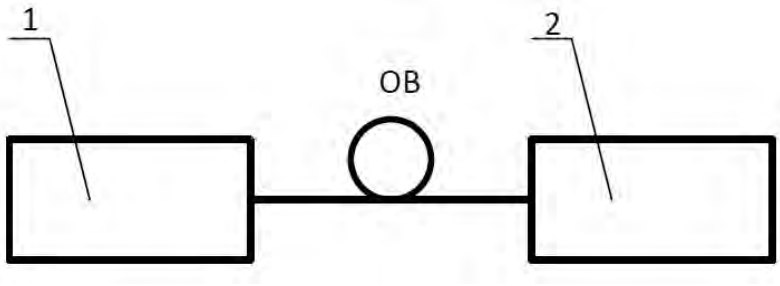


Рис. 1. Блок-схема для определения погрешности при измерении ослабления:
1 – поверяемый ОР; *2* – оптический генератор рабочего эталона (ОГ РЭ);
ОВ – оптическое волокно

Согласно данной блок-схеме, подключают поверяемый рефлектометр к ОГ РЭ с помощью оптического волокна, генератором устанавливают два импульса и поочередно вводят значения ослабления между ними: 1,0; 3,0; 5,0; 10,0; 15,0 дБ (значения могут быть изменены в зависимости от шкалы данного ОР). Далее определяют поочередно значения ослаблений *A* по шкале рефлектометра для каждого из установленных на генераторе значений ослабления для каждой длине волны. Измерения проводят $n = 10$ раз.

Определяют средние значения ослабления по формуле:

$$\bar{A} = \frac{\sum_{i=1}^{n} A_i}{n},$$

где A_i – i-е значение ослабления.

Рассчитывают среднее квадратическое отклонение результата измерений по формуле:

$$S = \sqrt{\frac{\sum_{i=1}^{n}(A_i - \bar{A})^2}{n(n-1)}}$$

Определяют основную абсолютную погрешность ОР Δ при измерениях ослабления по формуле:

$$\Delta = \sqrt{\frac{1}{3}(\Theta^2 + \Delta_0^2) + S^2},$$

где $\Theta = (\bar{A} - A_0)$, где A_0 – значение ослабления, устанавливаемого по ОГ РЭ; Δ^2_0 – погрешность установки ослабления.

Предлагается альтернативный вариант определения абсолютной погрешности при измерении ослабления (рис. 2). В нем полностью исключается использование ОГ РЭ. Контроль ослабления, вносимого аттенюатором,

будет осуществляться с помощью источника оптического излучения и измерителя оптической мощности из состава рабочего эталона средней мощности (РЭСМ).

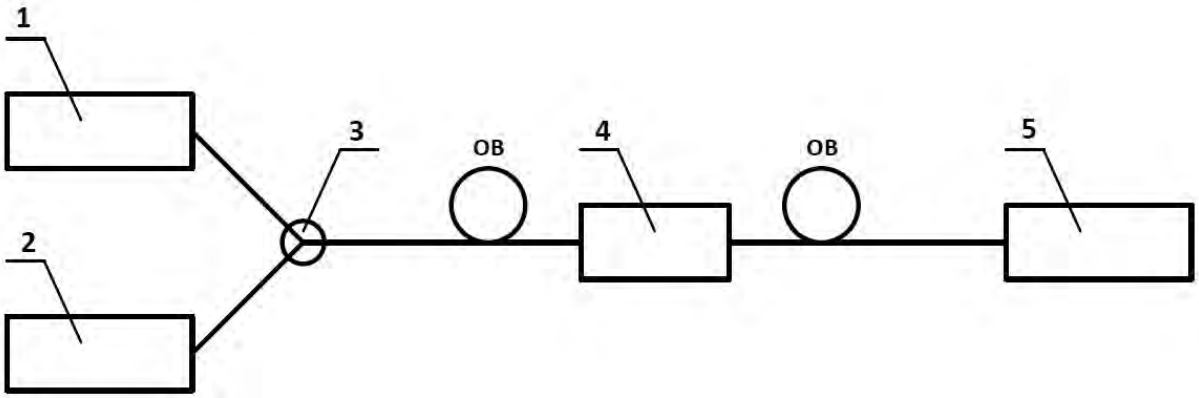


Рис. 2 Новая блок-схема для определения абсолютной погрешности при измерении ослабления: *1* – поверяемый ОР; *2* – источник излучения из состава РЭСМ; *3* – делитель; *4* – оптический аттенюатор; *5* – измеритель из состава РЭСМ; ОВ – оптическое волокно

В данной работе использовался делитель с коэффициентом деления 10/90 (10 % – от источника излучения, 90 % – от ОР). Длины обеих катушек с оптическим волокном – 10 км.

Согласно данной блок-схеме, подключается через одно из плеч делителя источник оптического излучения. Измеренный уровень мощности принимается за относительный ноль (переход в режим относительных измерений), затем источник отключается. Через второе плечо делителя подключают поверяемый ОР, устанавливают параметры СИ согласно методике поверки, проводят измерения в режиме усреднений.

На полученной рефлектограмме необходимо установить курсоры на линейном участке так, чтобы внесенное собственное затухание аттенюатором располагалось между ними (рис. 3). Разница между курсорами в дБ принимается за исходную. Вносится ослабление аттенюатором, снова включается источник и измеряется относительный уровень мощности. Затем измеряется внесенное ослабление ОР, из новой разницы между курсорами вычитается исходная и соотносится с измеренным значением измерителем мощности (рис. 4).

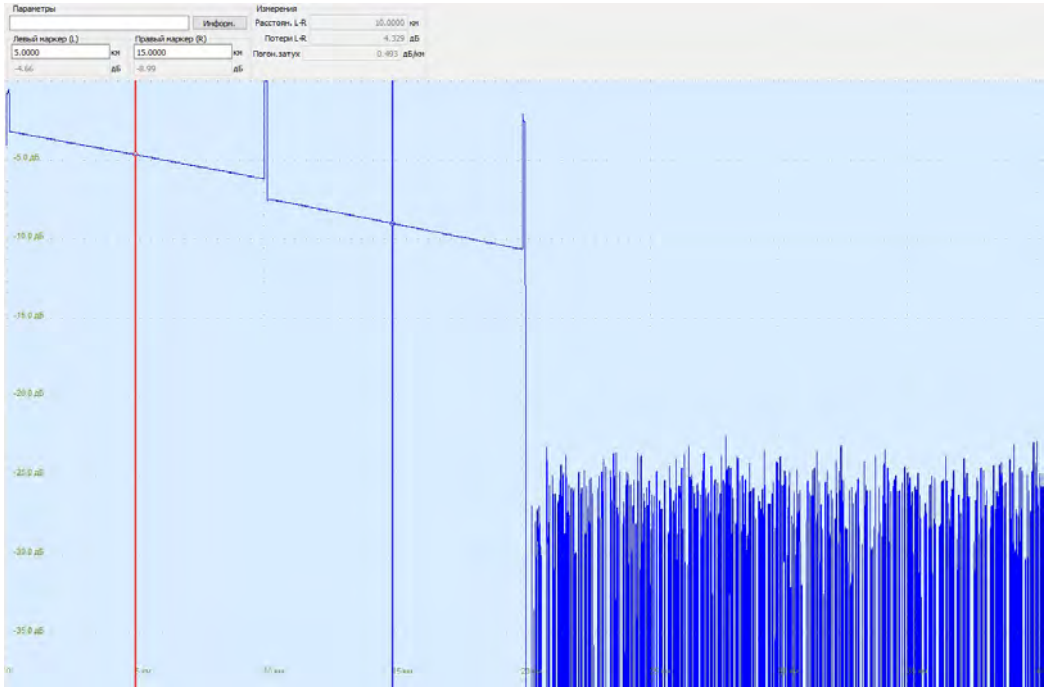


Рис. 3. Исходная рефлектограмма, полученная на длине волны 1310 нм при длительности импульса 1 мкс

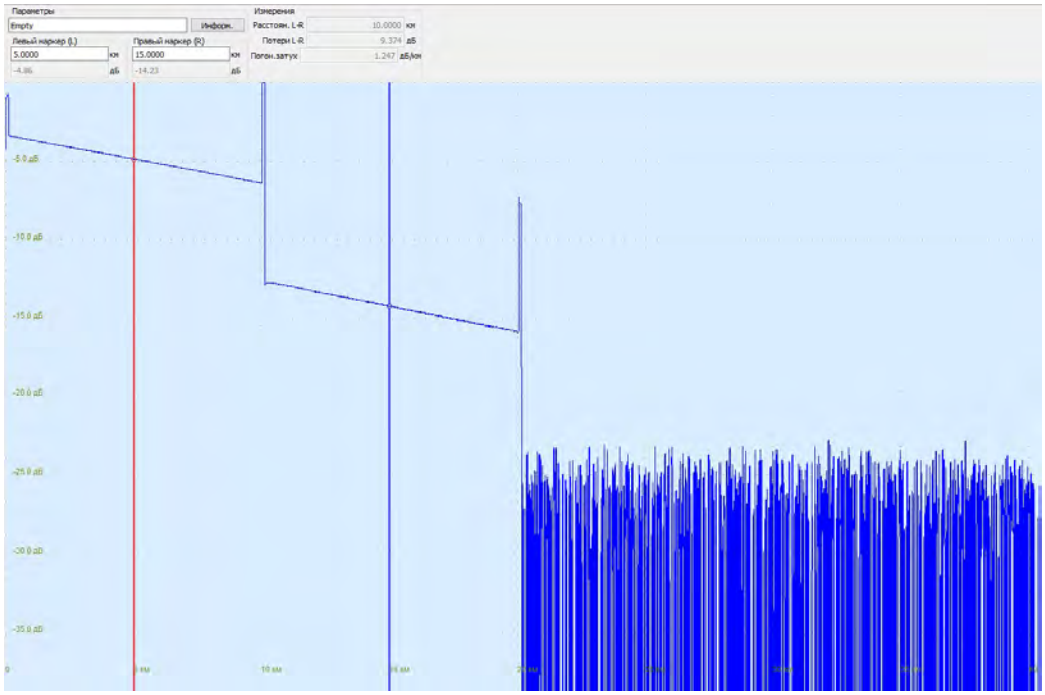


Рис. 4. Рефлектограмма, полученная на длине волны 1310 нм при длительности импульса 1 мкс и внесенном ослаблении 5 дБ

В таблицах 1 и 2 приведены результаты измерений с использованием ОР Топаз-7317ARX [3].

ТАБЛИЦА 1. Результаты измерений на λ = 1310 нм при длительности импульса 1 мкс

Внесенное ослабление, дБ	Измеренное значение ослабления по рефлектограмме, дБ	Измеренное значение ослабления, дБ	Погрешность, дБ	Допуск, дБ
0	4,329	–	–	–
1,077	5,391	1,062	0,029	0,05
3,065	7,366	3,037	0,040	0,15
5,037	9,374	5,045	0,025	0,25
10,023	14,238	9,909	0,134	0,5

ТАБЛИЦА 2. Результаты измерений на λ = 1550 нм при длительности импульса 1 мкс

Внесенное ослабление, дБ	Измеренное значение ослабления по рефлектограмме, дБ	Измеренное значение ослабления, дБ	Погрешность, дБ	Допуск, дБ
0	2,946	–	–	–
1,007	3,948	1,002	0,002	0,05
3,006	5,942	2,996	0,025	0,15
5,036	7,957	5,011	0,036	0,25
10,027	13,257	13,311	0,32	0,5

Таким образом, процесс определения погрешности при измерении ослабления может проходить без использования ОГ РЭ, что позволяет не только снизить стоимость затрат на проведения поверки, так как в процессе поверки необходим будет только РЭСМ, но проводить поверку в условиях реальной работы ОР.

Погрешность измерения относительных уровней мощности рабочего эталона фиксирована и составляет не более 0,5 % [4], что позволяет определять погрешность при измерении вносимого ослабления с высокой точностью, так как погрешность ОГ РЭ сильно зависит от вносимого ослабления [5]:

$$\pm 0{,}02 \times A, \text{ дБ}.$$

Список используемых источников

1. Рекомендация. Государственная система обеспечения единства измерений. Рефлектометры оптические. Методика поверки. МИ 1907-99. Москва, 1999. 11 с.

2. Р 50.2.071-2009. Государственная система обеспечения единства измерений. Рефлектометры оптические. Методика поверки. Москва: Стандартинформ, 2011. 11 с.

3. Описание типа средства измерений (в редакции, утвержденной приказом Росстандарта № 986 от 15.05.2017 г.): Тестеры оптические серии «Топаз 7000»: Федеральное бюджетное учреждение «Государственный региональный центр стандартизации, метрологии и испытаний в г. Санкт-Петербурге и Ленинградской области» (ФБУ «Тест-С.-Петербург»), 2017. 8 с.

4. Описание типа средства измерений: Рабочий эталон средней мощности оптического излучения в волоконно-оптических системах передачи «РЭСМ-В», регистрационный номер 68272-17: Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт оптико-физических измерений», 2017. 7 с.

5. Описание типа средства измерений для государственного реестра Генераторы оптические ОГ-2-1, регистрационный номер 19115-99: Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт оптико-физических измерений», 1999. 4 с.

Статья предоставлена научным руководителем, доцентом кафедры ФиЛС СПбГУТ, кандидатом технических наук, доцентом С. Ф. Глаголевым.

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ УЯЗВИМОСТЕЙ УДАЛЕННОГО ИСПОЛЬЗОВАНИЯ КОДА В ПРИКЛАДНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Д. В. Кушнир, И. М. Нестеров, Д. С. Суханов

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

В статье проводится анализ взаимосвязанных уязвимостей удаленного использования кода. Представлены проблемы информационной безопасности. Приведены результаты экспериментов по выявлению однотипных уязвимостей при различных конфигурациях и особенностях одного и того же установленного прикладного программного обеспечения.

компьютерные уязвимости, программное обеспечение, несанкционированный доступ, удаленное использование кода, безопасность.

В настоящее время важной и серьезной проблемой является наличие уязвимостей в программном обеспечении (ПО). Многие пользователи уверены, что наличия антивирусного ПО на компьютере достаточно, чтобы полностью оградить себя от вредоносных программ и хакерских атак. В действительности же антивирус – лишь один из элементов защиты ПК. Даже при его наличии уязвимости в системе безопасности ОС и программ могут быть использованы для атаки на систему и внедрение различных шпионских или управляющих модулей для получение конфиденциальных данных и использовании их. Основные проблемы информационной безопасности пользователей заключаются в переходе по не проверенным ссылкам Интернет-

ресурсов, скачивании подозрительных файлов и использовании несвоевременно обновляемого ПО [1]. В большей степени на уязвимости в компьютерной системе влияет установка незаконного или «пиратского» ПО.

В компьютерной безопасности термин «уязвимость» используется для обозначения недостатка в системе, используя который, можно намеренно нарушить её целостность и вызвать неправильную работу. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ. ***Атакой называют*** действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на компьютерную систему является реализацией угрозы безопасности информации в ней. Интернет уязвимости, в основном, связаны с отсутствием знаний рядового пользователя о настройках системы. Не стоит забывать и о незнании принципов работы вредоносных программ или пользователей (фишинг, соц. инженерия, back door, шифрование, блокировка и т. д.) [2].

В ходе эксперимента, представленном ниже, можно будет увидеть разницу в уязвимостях на персональных электронно-вычислительных машинах (ПЭВМ) с лицензионным и нелицензионным программным обеспечением и проанализировать полученные данные.

Низкий	3

Для примера были взяты два персональных компьютера с нелицензионным программным пакетом Office 2016 (назовём их ПЭВМ 1 и ПЭВМ 2) и один персональный компьютер с установленным лицензионным пакетом Office 2016 (ПЭВМ 3). Для автоматических проверок наличия уязвимостей программного обеспечения использовалась программа ФСТЭК ScanOVAL и база XML-файлов с OVAL-описаниями уязвимостей, выполненных в соответствии со стандартом «The OVAL Language Specifiation» [3].

Результат выполненного аудита на ПЭВМ 1 представлен в таблице 1.

ТАБЛИЦА 1. Результат сканирования ПЭВМ 1

Уровень угрозы	Количество найденных уязвимостей
Критический	14
Высокий	143
Средний	69

Общее количество найденных уязвимостей на ПЭВМ 1 и ПЭВМ 2 представлено в таблице 2. В результате проверки было найдено большое количество взаимосвязанных уязвимостей на обоих устройствах. Проанализировав отчеты уязвимостей на ПЭВМ 1 и ПЭВМ 2 (пример представлен на рис.

ТАБЛИЦА 2. Количество найденных уязвимостей на ПЭВМ 1 и 2

Устройство	Найдено уязвимостей
ПЭВМ 1	229
ПЭВМ 2	197

1) можно заметить, что большинство угроз связаны с уязвимостью удаленного выполнения кода Office 2016.

Рис. 1. Пример обнаруженных критических уязвимостей на ПЭВМ 1

В программном обеспечении Microsoft существует уязвимость удаленного выполнения кода. Данная уязвимость возникает, когда программа не может должным образом обрабатывать объекты в памяти. Злоумышленник, успешно воспользовавшийся уязвимостью, может запустить произвольный код в контексте текущего пользователя. Если текущий пользователь вошел в систему с правами администратора, преступник может получить контроль над уязвимой системой. После этого он может устанавливать программы, просматривать, изменять или удалять данные, создавать новые учетные записи с полными правами. Пользователи, чьи учетные записи настроены на меньшее количество прав в системе, могут пострадать меньше, чем пользователи, которые работают с правами администратора. Для использования уязвимости необходимо, чтобы абонент открыл специально созданный файл в уязвимой версии Microsoft Office. В сценарии атаки по электронной почте злоумышленник может воспользоваться уязвимостью, отправив специально созданный файл и убедив открыть его. В сценарии атаки через Интернет злоумышленник может разместить веб-сайт (или использовать взломанный веб-сайт, который принимает или размещает предоставленный абонентом контент), содержащий специально созданный файл, предназначенный для использования уязвимости [4].

Далее программа ScanOVAL была запущена на ПЭВМ 3 с установленным лицензионным программным пакетом Office 2016.

В ходе выполнения аудита было обнаружено 58 уязвимостей. Просмотрев отчет на ПЭВМ 3 (рис. 2) можно увидеть, что уязвимости с ПО Office остались, хоть и в гораздо меньшем количестве.

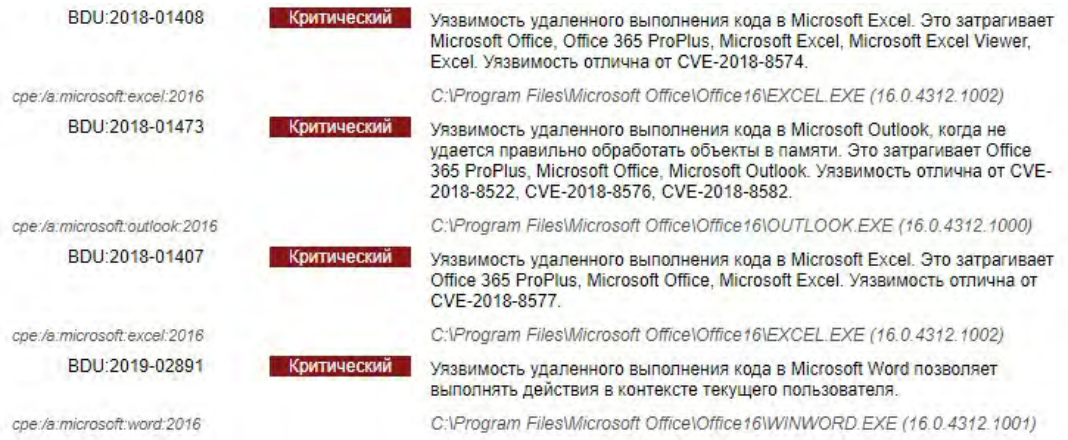


Рис. 2. Пример обнаруженных критических уязвимостей на ПЭВМ 3

Первая уязвимость данного рода появились в 2017-2018 годах под идентификаторами CVE-2017-11882 и CVE-2018-0802, позволяющая злоумышленникам получать доступ к атакуемым персональным устройствам. Они все еще могут быть использованы из-за отключённых обновлений для офисных пакетов на компьютерах, а также использования уже неподдерживаемых версий самого пакета. Способ заражения для хакера довольно прост. Обычно жертва атаки получает зараженный документ, к примеру, Microsoft Word (как уже упоминалось выше через электронную почту либо загрузку с веб-сайта). Чтобы уменьшить вероятность выявления антивирусом, злоумышленник разделяет созданный эксплойт. Эксплойт- это фрагмент программного кода или последовательность команд, способных воспользоваться одной или несколькими уязвимостями в ПО для проведения атаки на локальном или удаленном устройстве. В полученном зараженном файле содержится только загрузчик, который после выполнения сохраняет из сети Интернет HTML-страницу с имеющейся основной частью эксплойта, написанную через Visual Basic Script (VBScript). VBScript – это виртуальный язык сценариев. Данный язык используется и для продуктов Microsoft [4].

На странице Microsoft по данной уязвимости присутствуют рекомендации. Обновление для системы безопасности устраняет уязвимость, изменяя способ обработки Microsoft Office объектами в памяти. Одним из немногих способов исключить возможность взлома – устанавливать все пакеты обновления безопасности Microsoft Office и по возможности использовать последние версии продуктов. Но, как упоминалось ранее, данные рекомендации реализованы не на каждом персональном устройстве, поэтому данные угрозы остаются до сих пор значимыми.

Стоит заметить, что обновления не всегда выходят своевременно, а новые уязвимости данного рода могут быть найдены и использоваться злоумышленником намного раньше, чем выйдет решение данной проблемы.

Основными рекомендациями по защите до выхода решения данной уязвимости могу служить: не переходить по подозрительным или непроверенным ссылкам; отключение Интернет-соединения во время работы.

Исходя из вышесказанного можно сделать вывод, что установка лицензионного программного продукта не обеспечивает защиту в должном объеме. Уязвимости сохраняются, что влечет за собой сохранение возможности их использования в корыстных целях. Также хочется заметить, что данные версии ПО уже устарели. Устранить подавляющее большинство уязвимостей поможет своевременное обновление операционной системы, системы безопасности и установленных приложений. Это невозможно или затруднительно будет сделать в случае, если на компьютере используется нелицензионное ПО. Немаловажной причиной возникновения случаев проникновения является несвоевременная проверка системы безопасности или полное отсутствие таковых проверок. По результатам анализа можно увидеть, что подобные мероприятия, вероятно, не проводились, что влечет к возможности использования данной уязвимости (утечка персональных данный, нарушение целостности файлов, и т. д.) [1].

Список используемых источников

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70–76.

2. Скабцов Н. В. Аудит безопасности информационных систем. СПб.: Питер, 2018. С. 212–220.

3. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.

4. Бирюков А. А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. С. 205–235.

УДК 004.056.55
ГРНТИ 49.03.05

МЕТОДЫ ОРГАНИЗАЦИИ ЗАЩИЩЕННЫХ КАНАЛОВ СВЯЗИ И ВОЗМОЖНЫЕ ФУНКЦИИ ПРОМЕЖУТОЧНЫХ УЗЛОВ В КВАНТОВЫХ СЕТЯХ

Д. В. Кушнир, А. А. Чуриков

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

В статье рассматриваются возможные подходы к организации защищенных каналов связи между абонентами квантовых сетей. Значительные достижения в области квантовой информации, позволяют вплотную подойти к вопросу построения полностью или частично квантовых сетей. В работе выполнен анализ возможных методы построения квантовых сетей и проблемы их масштабирования.

квантовая криптография, квантовые повторители, протоколы квантового распределения ключа, квантовые сети, доверенные узлы.

Квантовая сеть – это система передачи данных, работающая по законам квантовой механики. В таких сетях обмен данными осуществляется при помощи кубитов [1]. Кубиты – это поляризованные фотоны, транслируемые по каналу оптической связи. Для того чтобы развернуть глобальные квантовые сети, покрывающие всю планету, как интернет, требуется решить ряд технических задач. Например, определённую сложность вызывает передача фотонов на большие расстояния из-за их «хрупкости».

Так как квантовая сеть управляется законами квантовой механики, в ней происходят явления, не имеющие аналогов в классических сетях, такие как отсутствие клонирования, квантовое измерение, запутывание и телепортация. Эти неотъемлемые свойства накладывают ограничения на проектирование сети. К примеру, классические сетевые функции - механизмы контроля ошибок, буферизация данных, основаны на предположении, что классическая информация может быть безопасно прочитана и скопирована, однако это предположение не выполняется в квантовой системе. Как следствие, проектирование квантовой сети требует других подходов для использования ключевых особенностей квантовой передачи информации.

За последние несколько десятилетий в области квантовой связи произошел значительный прогресс, особенно в создании систем квантового распределения ключей (КРК, *Quantum key distribution* QKD). Недавние эксперименты [2] распределения ключей по квантовой сети общей протяженностью порядка полутора тысяч километров из участков волокон-

ных сетей и использованием спутниковой линии связи показали, что системы КРК на больших расстояниях возможны. Несмотря на такие значительные экспериментальные достижения, частные возможности двухточечной КРК ограничены фундаментальными ограничениями. Эти ограничения утверждают, что в режиме с высокими потерями скорость передачи ключей масштабируется в основном линейно с коэффициентом пропускания канала, соединяющего конечных пользователей, например, Алису и Боба, то есть она уменьшается экспоненциально с увеличением общей длины канала. Это накладывает строгие практические ограничения на возможность реализации двухточечной системы КРК на произвольных больших расстояниях.

Способ преодолеть это ограничение – использовать один или несколько промежуточных узлов в квантовом канале, соединяющем стороны. На данный момент существует два основных подхода для увеличения дальности передачи квантовых ключей.

Первый способ – использование квантовых повторителей [3]. Они дают полиномиальное масштабирование эффективности связи с расстоянием. Более того, схему квантового повторителя можно произвольно повторять по квантовому каналу, тем самым увеличивая, в принципе, общее расстояние связи между Алисой и Бобом до любой необходимой длины. Идея квантового повторителя заключается в использовании квантовой запутанности фотонов для связи по различным квантовым связям. Квантовая запутанность – ключевой аспект в применении квантовой связи и квантовой информации. Квантовая запутанность подразумевает, что несколько частиц связаны вместе таким образом, что измерение квантового состояния одной частицы определяет возможные квантовые состояния других частиц. Даже когда частицы разделены на большие расстояния, они все равно составляют единую квантовую систему. Верность сцепления – это свойство, используемое для описания того, насколько хорошо сцепление между двумя подсистемами сохраняется в квантовом процессе.

Теоретически, применению запутанных состояний и обмена запутанностью препятствуют два основных фактора. Во-первых, чем больше расстояние между двумя запутанными системами, тем ниже точность. Фактически, достижимая точность квантового состояния экспоненциально уменьшается с расстоянием из-за квантовых каналов с потерями. В этом контексте концепция очистки запутанности может быть использована для повышения точности одного запутанного состояния за счет использования ряда зашумленных запутанных состояний. Однако, это увеличивает количество требуемых ресурсов для передачи каждого кубита через квантовый ретранслятор (то есть количество запутанных состояний). Второе препятствие на пути создания квантового повторителя, заключается в том, что для масштабирования квантовой запутанности требуется использовать квантовую память, реализация которой на сегодняшний день практически недоступна.

Использование квантовых повторителей основано на идее создания «цепочек» запутанных фотонов с помощью техники, называемой перестановкой запутанности, которую очень сложно реализовать на практике с использованием современных технологий: она требует либо квантовой памяти, либо квантовой коррекции ошибок. Таким образом, каждый узел в квантовой сети действует как повторитель и пересылает пакеты или состояния зацепления других узлов, чтобы обеспечить обмен квантовой информацией между конечными узлами. Хотя в текущий условиях такой механизм технически недостижим, но квантовые повторители могут быть реализованы в будущем.

Второй способ – использование доверенных узлов. Доверенный узел представляет собой схему, соединяющую две разнесенные квантовые сети, либо две линии квантовой коммуникации, построенные по принципу «точка-точка», в одну. Для обеспечения требуемых параметров стойкости результирующей системы подобные узлы должны быть защищены от активного и пассивного вмешательства противника, так как между блоками отправителя и получателя такого узла происходит классическая передача информации. Фактически такие узлы должны быть доверенными и их безопасность должна быть реализована на таком же уровне, что и безопасность конечных узлов системы КРК. Как показано на рис. доверенный узел включает в себя два модуля для создания квантового канала с предыдущим и последующим корреспондентом.

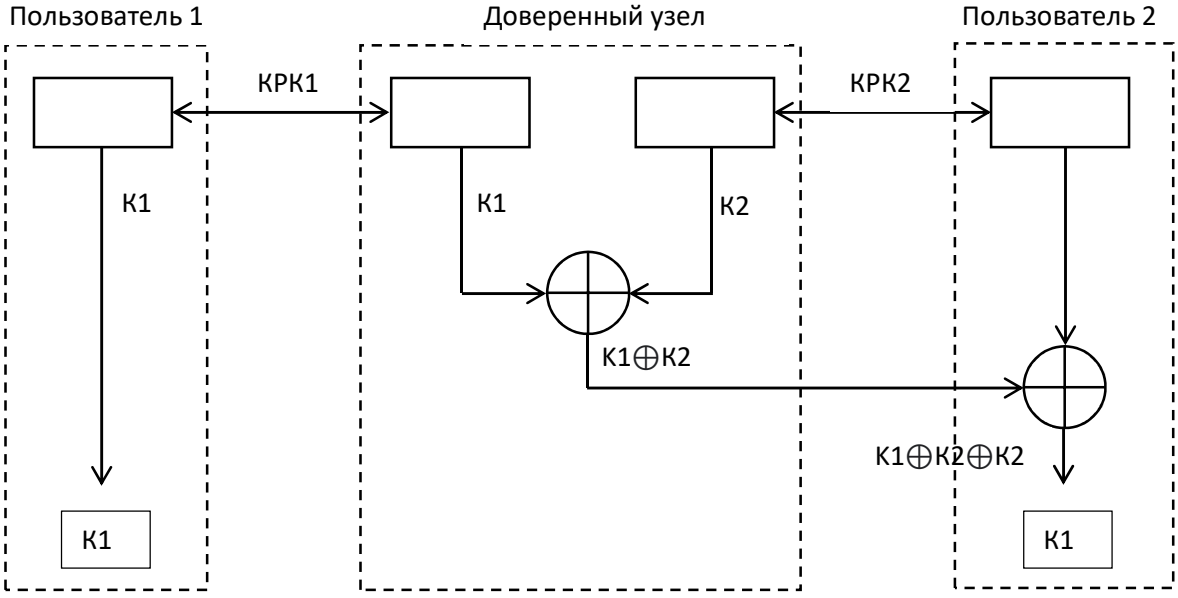


Рис. Схема формирования сквозного ключа через доверенный узел

Квантовые каналы организованы между пользователями и доверенным узлом. Таким образом, в доверенном узле образуются два ключа K_1 и K_2, по

ключу от каждой из сторон. Ключ первого пользователя может быть зашифрован вторым ключом и в зашифрованном виде передан второму пользователю. Далее второй пользователь расшифровывает К1 на своем ключе, что и приводит к формированию общего сквозного ключа между конечными узлами в такой сети. Использование доверенного узла позволяет увеличить дальность передачи ключа и может быть легко масштабировано на произвольное количество промежуточных узлов.

Принимая во внимание отсутствие квантового повторителя, доверенные узлы также отвечают за механизмы маршрутизации и пересылки. Подобная организация сети является ее самым большим недостатком, поскольку безопасность передачи зависит от безопасности всех узлов на пути. Однако сети доверенных повторителей не ограничены расстоянием или номерами узлов и могут состоять из различных устройств КРК, реализующих разные технологии построения квантовых каналов.

Ещё один из вариантов реализации сети квантового распределения ключей – сети КРК с коммутацией. Коммутируемые сети КРК состоят из узлов, подключенных к полностью выделенной оптической сети. Эта сеть содержит механизм коммутации, используемый для установления прямого оптического двухточечного КРК-соединения между любыми двумя узлами в сети КРК. Ограничения на расстояние в двухточечных каналах КРК ограничивают эти сети до городского или регионального масштаба. Поскольку каждый оптический переключатель добавляет потери к фотонному тракту, оптические переключатели могут значительно уменьшить радиус действия сети.

Основным недостатком коммутируемых сетей КРК является потребность в выделенной оптической инфраструктуре для квантовых каналов, что часто экономически нецелесообразно. Напротив, основным преимуществом этого класса сетей является использование оптического коммутатора, который позволяет устанавливать соединение между двумя узлами без активного участия других узлов сети. Другим недостатком коммутируемых сетей КРК является согласованность применяемой техники КРК. Комбинирование различных методов КРК, таких как КРК в свободном пространстве и КРК по оптоволокну, невозможно, поскольку отсутствуют подходящие устройства, которые могли бы выполнять это преобразование в тракте. Первая коммутируемая многоходовая сеть КРК состояла из четырёх узлов, которые были подключены через оптический коммутатор, и каждый из терминалов КРК был спроектирован как приемопередатчик, чтобы они могли установить канал КРК одновременно с одним из трех других узлов [4].

Рассматривая системы квантового распределения ключа необходимо учитывать, что оборудование легитимных пользователей не является идеальным. Поскольку квантовые каналы могут быть «переданы» перехватчику

без ущерба для безопасности КРК, именно узлы могут оказаться потенциально наиболее слабым звеном. Узлы содержат систему управления оптическими устройствами, реализуют выработку итогового ключа и всё это реализуется на обычной компьютерной логике, безопасность результирующей системы будет не лучше, чем безопасность, в том числе физическая, реализованная для классической составляющей узлов в системе КРК.

Одним из подходов к повышению защищенности результирующих квантовых сетей является многолучевая передача, которая обменивает доверие к ретрансляторам на предположение, что некоторая часть промежуточных узлов может быть уязвима для вмешательства, а злоумышленник вынужден анализировать данные с многих промежуточных узлов для выполнения успешной атаки. В самом деле, при отсутствии полностью доверенных узлов множественные маршруты являются теоретической необходимостью. В то же время, избыточность путей также смягчает проблему уязвимости всех реализаций КРК для атак типа «отказ в обслуживании» (злоумышленник может пассивно подслушивать не для получения информации, а для того, чтобы локальные хранилища квантовых ключей иссякли, что принудит конечные точки к необходимости перейти на традиционные методы передачи). Можно использовать расширенные механизмы маршрутизации для обхода линий с обнаруженным вмешательством. В противном случае злоумышленники могут попытаться взломать систему безопасности, используя пассивное подслушивание для перенаправления трафика через уязвимые узлы и, таким образом, завладеть секретным ключом. Было выявлено, что «сквозная безопасность» без обеспечения во всей квантовой сети полностью доверенных узлов (без квантовых повторителей) может быть обеспечена только при наличии относительно небольшой доли уязвимых узлов [4]. Топология квантовой сети обычно оказывает сильное влияние на достижимую безопасность, и, несмотря на теоретический и практический прогресс в построении квантовых сетей, даже без доверенных повторителей, задача обеспечения безопасности для конкретной топологии квантовой сети продолжает оставаться актуальной. Одной из приоритетных задач является уменьшение роли доверенных узлов в построении полноценной квантовой сети.

Квантовые коммуникации являются одной из сфер применения, широко развивающих на сегодняшний день, квантовых технологий. Исследования в области квантовых вычислений подталкивают квантовые коммуникации к необходимости обеспечить надежную связь к моменту построения первых полноценных квантовых компьютеров. Надежная связь будет необходима как для передачи данных для обработки на квантовых компьютерах так и получения итоговых результатов с учетом потенциальной возможности самих квантовых компьютеров изменить представления о безопасности целого ряда подходов к обеспечению информационной безопасности.

Список используемых источников

1. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. Experimental quantum cryptography // Journal of Cryptology. 1992. Vol. 5. No. 1. pp. 3–28.
2. Yin J., Li Y. H., Liao S. K. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres // Nature. 2020. 582. pp. 501–505.
3. Hasegawa Y., Ikuta R., Matsuda N. et al. Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters // Nat Commun. 2019. 10. 378.
4. Глейм А. В., Банник О. И., Гилязов Л., Чистяков В. В., Мельник К., Васильев А. Б., Гайдаш А. А., Козубов А. В., Смирнов С. В., Егоров В. И., Арсланов Н. М., Козлов С. А., Моисеев С. А. Многоузловая квантовая сеть на основе технологии квантовой коммуникации на боковых частотах // XI Международный симпозиум по фотонному эхо и когерентной спектроскопии (ФЭКС – 2017). Сборник тезисов. 2017. С. 43–44.

УДК 004.056.55
ГРНТИ 49.03.05

ОСОБЕННОСТИ ФОРМИРОВАНИЯ КЛЮЧЕВЫХ ДАННЫХ В КВАНТОВОЙ КРИПТОГРАФИЧЕСКОЙ СЕТИ

Д. В. Кушнир, С. Н. Шемякин

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

В статье рассматривается ряд аспектов, влияющих на формирование ключевых данных при формировании квантовой криптографической сети. Авторами анализируются способы формирования ключей между конечными узлами исследуемой сети, технические сложности непосредственного формирования ключевых данных и подходы к решению обозначенных проблем.

квантовая криптография, квантовые повторители, протоколы квантового распределения ключа, квантовые сети.

Значительные достижения в сфере построения квантовых каналов связи, появление квантовых компьютеров и связанных с ними технологий вплотную приблизили необходимость решения задачи построения квантовой криптографической сети. Формирование ключа в квантовой криптографии осуществляется непосредственно в процессе передачи единичных квантов (фотонов) по каналу связи, а надежность формируемого ключа базируется на фундаментальных законах квантовой физики [1]. Первона-

чальные разработки систем квантовой криптографии предполагали обеспечение защищенным каналом связи отдельных пар пользователей. Однако актуальным является разработка и исследование подобных методов для связи неопределенного большого количества пользователей распределенной сети.

Одна из особенностей построения квантовых сетей – это обеспечение работы системы в режиме точка-точка. В случае необходимости построения распределённых систем и невозможностью построения отдельных линий для каждой взаимодействующей пары необходимо прибегать к использованию промежуточных узлов.

Эти узлы могут обеспечивать работу системы на основе каких-либо правил маршрутизации и обеспечивать доставку необходимых данных конкретному адресату. Однако работа квантовой сети предполагает формирование ключевых данных между конечными пользователями системы и промежуточные узлы не должны мешать этому формированию. Кроме того факта, что обеспечить конечных пользователей выделенной линией бывает проблематично организационно/технически, современные протоколы квантового распределения ключей позволяют обеспечить адекватную работу на линиях только ограниченной длины.

Передачу квантовой информации без искажения на большие расстояния могли бы обеспечить квантовые повторители. Исследуемым направлением является построение квантовых повторителей, но на сегодняшний день для их полноценной реализации требуется решить ряд сложных теоретических/технических проблем [2].

Для построения всеохватывающей квантовой сети требуется обеспечить покрытие территорий опорными узлами (рис. 1). Опорными узлами в квантовой сети, могут быть как наземные узлы, так и спутниковые системы [3]. Линии могут быть спутниковыми, использовать волокно или быть построены на основе воздушного оптического канала.

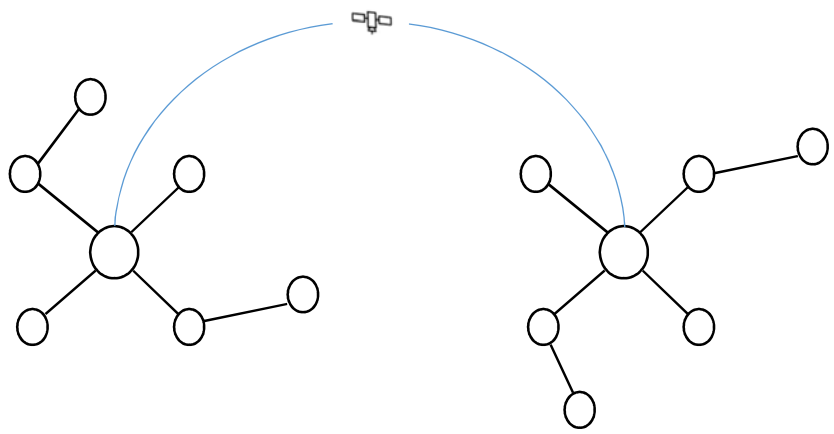


Рис. 1. Схема взаимодействия узлов в квантовой сети

К каждой такой линии предъявляются свои требования и реализуются свои возможности, из которых имеет смысл отметить дальность линий. Так волоконная линия квантового распределения ключа может обеспечить дальность передачи приблизительно от ста до двухсот километров [4]. Квантовая линия до спутника обеспечивает работу на участке длинной порядка тысячи километров при присутствии одной из точек линии на земной поверхности и может покрывать пока неопределенно большие расстояния в открытом космосе. При этом воздушная квантовая линия, которая в некоторых случаях может обеспечить подключение конечных пользователей к базовым узлам квантовой сети, может покрывать лишь несколько километров [5].

Как уже отмечалось раннее одна из проблем для обеспечения квантовой сети – это необходимость обеспечения именно конечных пользователей распределённым квантовым ключом. Из-за ограничения длины непосредственного распределения ключа в квантовом канале предлагаются различные решения, которые бы решили проблему получения общего ключа между пользователями, разделёнными значительным расстоянием. Эта проблема была бы в некоторой мере решена появлением квантовых повторителей, разработка которых активно ведется [2], но необходимо отметить, что встраивание в квантовую линию квантовых повторителей всё равно, фактически приводит к появлению на линии связи некоторого доверенного узла для обеспечения штатной работоспособности подобного устройства.

Другим решением для реализации передачи защищенного сообщения между конечными пользователями по квантовой сети, т. е. сети из узлов, которые связаны между собой квантовыми каналами, является передача защищенных данных на ключах, распределенных между соседними узлами [4]. Варианты реализации квантовой сети могут зависеть от выполняемых задач на таких узлах. Один из возможных вариантов предполагает, что информация, при передаче по сети, на самих узлах будет перешифровываться с ключа одного участка квантовой сети на ключ следующего. Данное решение может потребовать использования дополнительных ключей на самих промежуточных узлах. Такие ключи потребуются для временного хранения принятых данных перед их отправкой по следующему сегменту или для передачи от приемного оборудования до передающего. Другим аспектом может стать необходимость подтверждения подлинности передаваемых данных, что потребует для каждого участка пересчета кода аутентификации передаваемых данных.

Общий вид подобных преобразований на каждом узле может быть представлена следующим образом:

$$f\,(g\,(f\,(\mathrm{M},k_1),k_1)k_2),$$

где $f\,()$ – некоторая функция шифрования в системе,

$g\,()$ – дешифрования,

М – исходное сообщение,

k_i – ключ шифрования на соответствующем участке. К этим действиям может добавляться и преобразования на ключе узла. При требовании к аутентификации данных пересчет кода аутентификации первого участка вида *MAC(M,k')* в код аутентификации второго участка *MAC(M,k")* также потребуется.

Предложенное решение требует наличия полностью доверенных промежуточных узлов как на период выполнения протокола квантового распределения ключа, так и до окончания выполнения процедур перешифрования и отправки информационных сообщений на данном ключе через соответствующий узел.

Более приемлемым представляется все-таки формирование сквозного ключа между конечными пользователями сквозь последовательность узлов (рис. 2). Как и в ранее приведенном варианте, в данном решении нам потребуются полностью доверенные последовательные узлы для формирования ключа, удовлетворяющего традиционному набору требований для ключей, распределенных по квантовым протоколам.

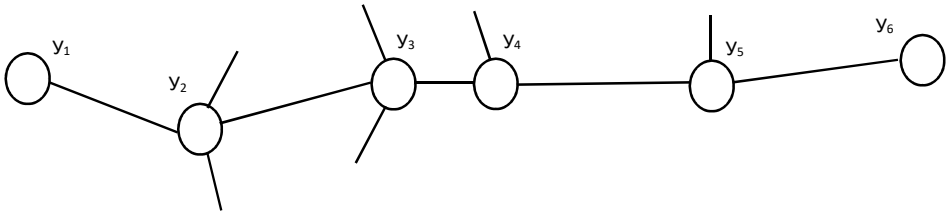


Рис. 2. Последовательные узлы квантовой сети

Предположим, имеется сеть из узлов конечных пользователей $У_1$, $У_n$ и промежуточных узлов: $У_2$, …$У_{n-1}$. В процессе работы сети между каждой парой соседних узлов формируется ключ на основе выполнения квантового криптографического протокола K_{ij}. Для получения итогового сквозного ключа один из законных пользователей формирует ключевую последовательность K_1 и передает по цепочке узлов квантовой сети. На каждом узле происходит перешифрование ключевой последовательности, т. е. выполняются следующие действия: на первом узле вычисляется и передается результат шифрования f (K_1, K_{12}), на втором результат перешифрования: $f(g(K_1, K_{12}), K_{23})$ и т. д. до последнего узла, который расшифровывает итоговую ключевую последовательность g (K_1, $K_{(n-1)n}$). В итоге конечные пользователи получают общий секретный ключ и в дальнейшем никак не зависят от наличия, загруженности и работоспособности тех узлов, через которые распределялся конкретный ключ для сквозного шифрования. Данный факт позволяет оптимизировать работу самой квантовой сети и не загружать её узлы другими задачами, кроме собственно обеспечения участников сети

ключевой информацией. Кроме того, предварительное распределение ключевых данных позволяет отказаться от них в случае последующего обнаружения компрометации распределенных ключевых данных, и, что может быть более важно, обеспечить до момента исчерпания ключевой информации возможность передачи защищенных данных даже при потере доступа к квантовой сети.

Таким образом, квантовая сеть из произвольного количества соединённых квантовыми каналами доверенных узлов может снабдить любых своих пользователей общим секретным ключом. Получение итогового сквозного секретного ключа для произвольной пары абонентов позволяет в дальнейшем использовать любые каналы связи для защищенного обмена информации и обеспечивает независимость обеспечения защищенного взаимодействия до момента полного расходования ключевых данных. Одновременно, следует отметить, что обозначенный подход ставит дополнительные задачи, такие как построение эффективных маршрутов для итогового формирования ключа и необходимость обеспечить требования к секретности ключа при наличии некоторого количества скомпрометированных узлов.

Список используемых источников

1. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on computers, systems and signal processing, Bangalore, India, 1984. pp. 174–175.

2. Hasegawa Y., Ikuta R., Matsuda N. et al. Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters // Nat Commun. 2019. 10. 378.

3. Villoresi P. et al. Experimental verification of the feasibility of a quantum channel between space and Earth // New Journal of Physics. 2008. Vol. 10. No. 3. P. 033038.

4. Глейм А. В., Банник О. И., Гилязов Л., Чистяков В. В., Мельник К., Васильев А. Б., Гайдаш А. А., Козубов А. В., Смирнов С. В., Егоров В. И., Арсланов Н. М., Козлов С. А., Моисеев С. А. Многоузловая квантовая сеть на основе технологии квантовой коммуникации на боковых частотах // XI Международный симпозиум по фотонному эхо и когерентной спектроскопии (ФЭКС – 2017). Сборник тезисов. 2017. С. 43–44.

5. Pugh C. J. et al. Airborne demonstration of a quantum key distribution receiver payload // Quantum Science and Technology. 2017. V. 2. No. 2.

УДК 621.396.82
ГРНТИ 47.05.09

НЕЛИНЕЙНЫЙ ИНВАРИАНТНЫЙ ЭХОКОМПЕНСАТОР ДЛЯ ДУПЛЕКСНОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

В. В. Лебедянцев, И. И. Павлов

Сибирский государственный университет телекоммуникации и информатики

В статье рассматривается применение синтеза дуплексных систем передачи данных нового для теории связи математического аппарата – теории групп преобразований, который открывает возможность разработки эхокомпенсаторов с инвариантными относительно характеристик эхотрактов свойствами. Представлена структурная схема нелинейного инвариантного эхокомпенсатора для дуплексной системы передачи данных.

инвариантный эхокомпенсатор, эхосигнал, эхотракт, проективное преобразование, длины векторов, помехоустойчивость, относительная погрешность.

Одним из возможных способов минимизации взаимного влияния направлений передачи в дуплексном канале является применение оптимизированных сигналов, максимизирующих отношение энергий сигналов на выходе среды направления передачи к энергии эхосигналов. Однако не всегда оптимизацией сигналов возможно обеспечить требуемое уменьшение сигналов эха. В этом случае необходимо применение дополнительной меры уменьшении эхо сигналов посредством эхокомпенсаторов. Реализации этой меры предполагает использование специального четырехполюсника, включенного параллельно эхотракту, создающий копии эхосигналов. Эти копии затем вычитаются из суммы применяемого сигнала и эхосигнала, что и обеспечивает устранение эхосигнала на входе приемника. Очевидно, для полной компенсации эхосигналов характеристики эхотракта и компенсирующего четырехполюсника должны быть идентичны, т. е., с учетом обозначений матриц операторов эхотрактов в тензорной модели дуплексного канала G_{12} и G_{21}, должны быть обеспечены следующие равенства:

$$G_{эк1} = G_{12}, \quad G_{эк2} = G_{21}, \tag{1}$$

где $G_{эк1}$ и $G_{эк2}$ – матрицы операторов эхокомпенсаторов на соответствующих сторонах дуплексного канала передачи данных.

На практике измерение импульсных реакций паразитных эхотрактов дифференциальных систем с целью создания четырехполюсников эхокомпенсаторов с аналогичными импульсными реакциями представляет собой

сложную задачу в виде малых значений амплитуд их импульсных реакций. Задача дополнительно усложняется тем обстоятельством, что при применении активных дифференциальных систем их амплитудная характеристика зачастую бывает нелинейной, вследствие чего форма их импульсных реакций будет зависеть от амплитуды испытательного сигнала. Для преодоления указанных затруднений необходим принципиально другой подход к формированию копий эхосигналов, базирующихся на использовании нового для теории связи математического аппарата – теории группы преобразований [1].

Благодаря наличию инварианта аффинной группы преобразований удалось синтезировать алгоритмы, модифицированной инвариантной амплитудной модуляции, обеспечивающей безыскаженную передачу сообщений по линейным каналам с любыми заранее неизвестными импульсными реакциями. Разумеется, влияние белого шума на вероятность передачи сообщений в силу особых свойств неустранимо в любой системе связи, включая и инвариантные системы, однако инвариантность к свойствам линейного канала является их принципиальным преимуществом.

Поскольку паразитный эхотракт активных дифференциальных систем, как уже отмечалось выше, может обладает нелинейными свойствами, то для описания преобразований сигналов в таком эхотракте группа аффинных преобразований непригодна. В этом случае будет использовать более общую группу проективных преобразований, включающую в себя аффинную группу как частный случай.

Далее рассмотрим элементы теории проективной группы преобразований, с применением которых можно решить задачу компенсации эхосигналов на выходе паразитного эхотракта активной дифференциальной системы с нелинейной амплитудной характеристикой.

Схемы проективного преобразования длин векторов входных сигналов в длины векторов выходных сигналов нелинейной системы

Рассмотрим простейшую схему проективного преобразования из центра z точек a, b, c, d, лежащих на прямой OA, в точки a′, b′, c′, d′, расположенных над другой прямой OA′ (рис. 1).

Для этой схемы проективного преобразования можно построить амплитудную характеристику зависимости длин векторов выходных сигналов от длин векторов входных сигналов (рис. 2).

При размещении центра проектирования z′ за линией длин векторов выходных сигналов получим другую схему преобразования (рис. 3).

Для другого примера схемы проектирования будет соответствовать другая амплитудная характеристика с выпуклой формой (рис. 4).

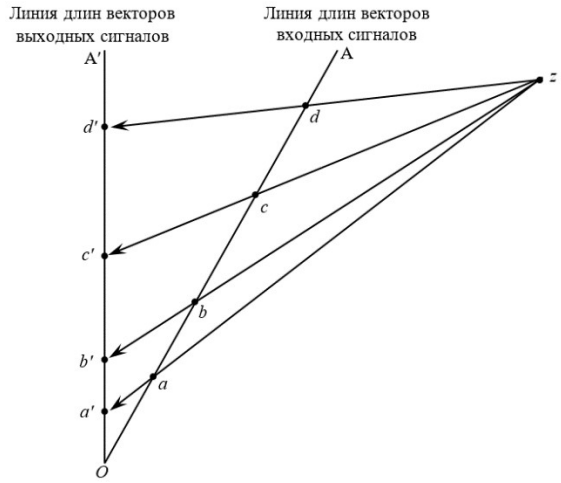


Рис. 1. Схема проективного преобразования точек линий длин векторов входных сигналов в точки линии длин векторов выходных сигналов нелинейной системы

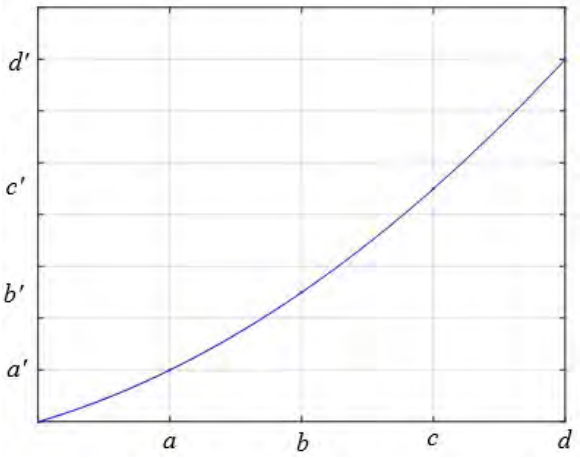


Рис. 2. Амплитудная характеристика для преобразования рис. 1

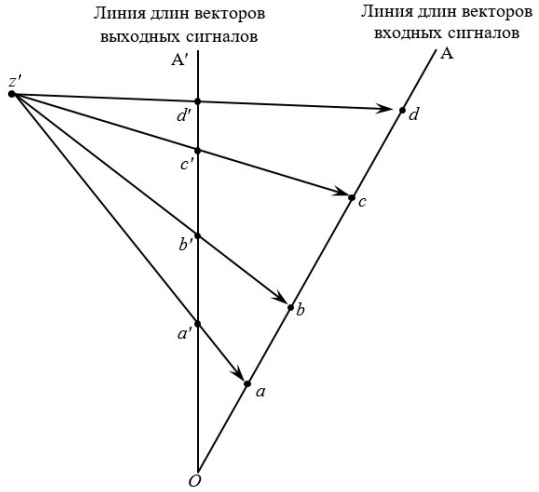


Рис. 3. Другой примет схемы проектирования

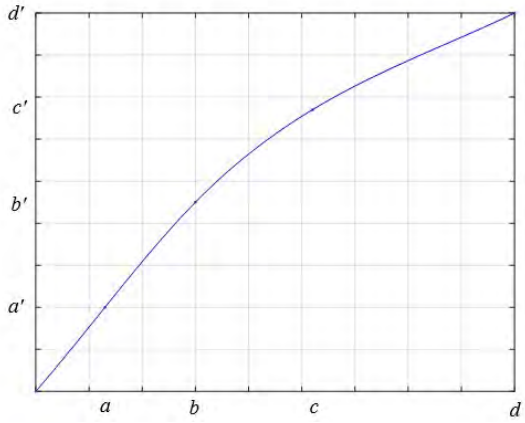


Рис. 4. Амплитудная характеристика другого расположения центра проектирования

Как следует из этих примеров, проективное преобразование может описывать преобразование длин векторов сигналов нелинейными четырехполюсниками. При этом вследствие бесконечного числа вариант взаимного расположения линий OA, OA′ и центров проектирования проективное преобразование может порождать бесконечное число вариантов нелинейных амплитудных характеристик. Поскольку аффинное преобразование является частным случаем проектного преобразования при расположении центра проектирования на бесконечном удалении, то амплитудная характеристика при аффинном преобразовании будет иметь вид прямой линии [2].

Структурной схемы инвариантного эхокомпенсатора

Опишем принцип работы инвариантного эхокомпенсатора (структурная схема представлена на рис. 5) использующего инвариант нелинейного эхотракта, которые характеризуются проективной группой преобразований.

Сигналы передатчика $S_i(t)$ последовательно поступают на вход дифференциальной системы и вследствие неидеальности его работы проходят на вход приемника в виде эхосигналов $S_{i\,эхо}(t)$. Задача эхокомпенсатора, включаемого на входе приемника, состоит в установлении сигнала эха.

Назначение блоков схемы и ее работа в целом состоит в следующем. При этом полагаем, что информационные и опорные сигналы имеют подобные формы, отличающиеся лишь множителем. Последовательность работы схемы состоит из двух этапов – обучения и, собственно, рабочего этапа [5].

На этапе обучения в блоки памяти *БП1* и *БП2* записываются величины модулей векторов первого и второго сигналов $S_{1\,оп}$ и $S_{2\,оп}$, соответственно. Величины модулей рассчитываются блоком вычисления модулей векторов сигналов (БВМВС).

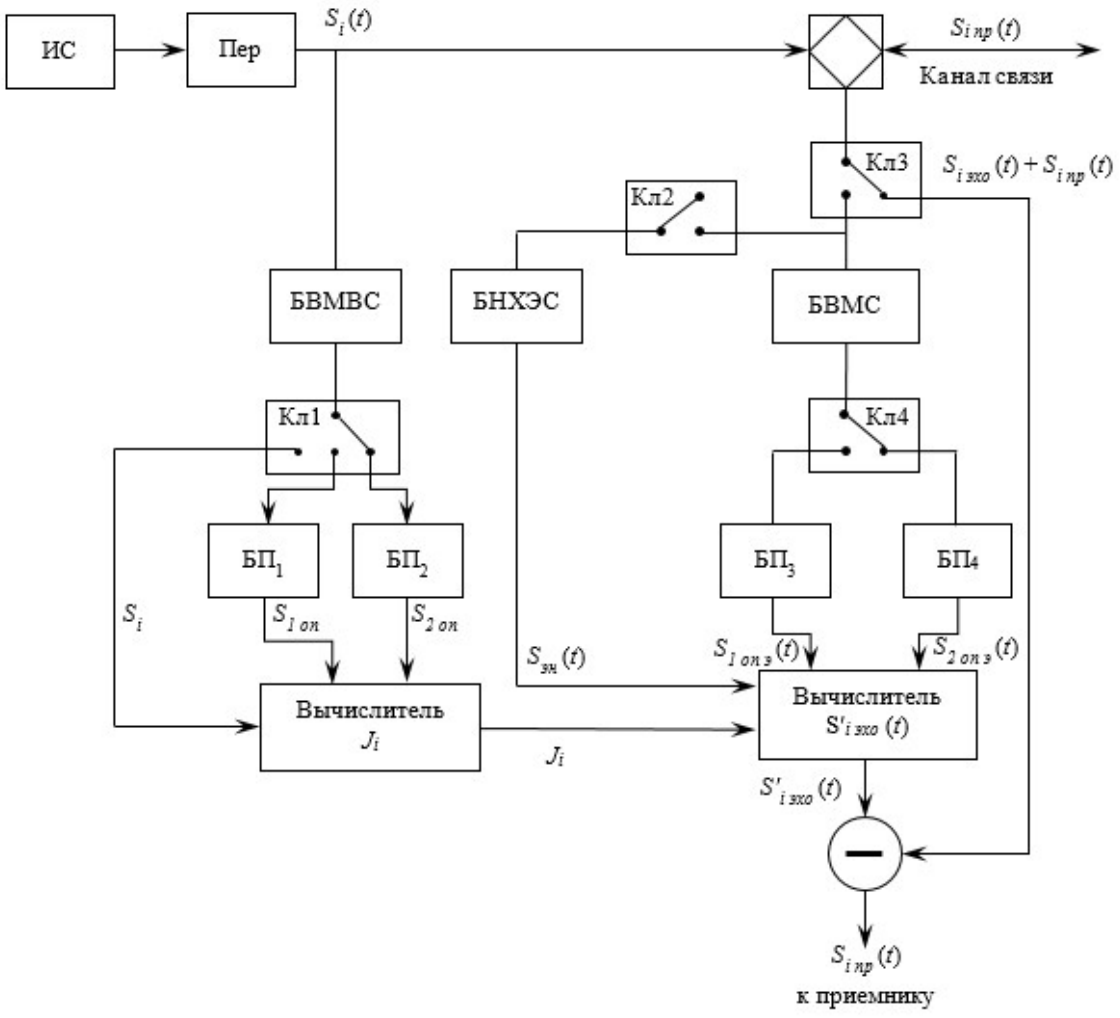


Рис. 5. Структурная схема нелинейного инвариантного эхокомпенсатора

Опорные сигналы $\overline{S}_{1\,on}$ и $\overline{S}_{2\,on}$ вырабатываются последовательно времени передатчиком (*Пер*). При этом эхосигналы, порождаемые опорными сигналами, поступают с выхода эхотракта дифференциальной системы на блок вычисления модулей их векторов (*БМВС*). Вычисленные значения длин векторов прописываются, соответственно, в блоки памяти *БП₃* и *БП₄*. Распределение вычисленных значений модулей векторов опорных сигналов по блокам памяти осуществляется через ключи *Кл1* и *Кл4* с использованием ключа *Кл3*.

На этапе обучения через ключ *Кл2* в блок нормирования и хранения образа эхосигнала (*БНХЭС*) поступают образец формы эхосигнала. После этапа обучения начинается рабочий этап.

В рабочем режиме ключ *Кл1* находится в крайнем левом положении и через него на вычислитель инварианта J_i поступают длины векторов информационных сигналов. Ключ *Кл2* находится в разомкнутом состоянии, а ключ *Кл3* – в крайнем левом положении.

На вычислитель копий сигналов эха $S'_{i\,э}(t)$ подаются величины инварианта J_i, модули векторов сигналов эха $S_{1\,on\,э}$ и $S_{2\,on\,э}$, а также нормированный образец эха с выхода *БНХЭС*. Вычислитель копии сигнала эхо осуществляет следующую математическую операцию

$$S'_{i\,э}(t) = S_{эн}(t) \cdot \left|\overline{S}'_{эi}\right| = \frac{aS_{эн}(t)}{J_i b - \left|\overline{S}'_1\right|}. \qquad (9)$$

Рассчитанная таким образом копия эхосигнала вычитается в вычитателе из суммы принимаемого сигнала и сигнала эха, в результате чего осуществляется компенсация эха. Координация согласованной работы блоков нелинейного инвариантного эхокомпенсатора осуществляется передатчиком.

Выводы

Применение для синтеза дуплексных систем передачи данных нового для теории связи математического аппарата – теории групп преобразований – открывает возможность разработки эхокомпенсаторов с инвариантными относительно характеристик эхотрактов свойствами.

Для повышения помехоустойчивости инвариантных эхокомпенсаторов на этапе обучения возможно использовать как выбор величин длин векторов опорных сигналов, так и процедуру многократного обучения.

Список используемых источников

1. Лебедянцев В. В. Разработка и исследование методов анализа и синтеза инвариантных систем связи: дисс. … док-ра техн. наук: 05.12.02 / Валерий Васильевич Лебедянцев. Новосибирск, 1995.
2. Хорн. Р., Джонсон Ч. Матричный анализ. Перевод с английского языка. М.: Мир, 1989. 656 с.
3. Заездный А. М. Основы расчетов по статической радиотехнике. М.: Связь, 1969. 448 с.

УДК 004.056
ГРНТИ 81.93.25

АРХИТЕКТУРА СИСТЕМЫ АНКЕТИРОВАНИЯ МОЛОДЕЖИ В СОЦИАЛЬНОЙ СЕТИ ВКОНТАКТЕ ДЛЯ ВЫЯВЛЕНИЯ НЕГАТИВНЫХ ЛИЧНОСТНЫХ ТЕНДЕНЦИЙ

Д. С. Левшун

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Система для анкетирования молодежи в социальной сети ВКонтакте представляет собой приложение, разработанное по технологии VK mini app. Процесс взаимодействия пользователя с приложением можно разделить на три этапа: (1) прохождение опросника (имя, фамилия, пол, возраст, университет, факультет и группа); (2) прохождение психологических тестов (Я-структурный тест Аммона, шкала тревоги Спилбергера-Ханина, копинг-тест Лазаруса, опросник уровня субъективного контроля Роттера и опросник САН – самочувствие, активность, настроение); (3) сбор данных о странице пользователя через API социальной сети. Задача опросника – соотнесение личности пользователя с информацией страницы в социальной сети, т.к. для последних характерно заполнение вымышленными данными. Задача психологических тестов – формирование представления о психоэмоциональном состоянии пользователя, выявление негативных личностных тенденций. Задача сбора данных – формирование представления о содержимом страницы пользователя для дальнейшего анализа его взаимосвязи с результатами психологических тестов.

социальные сети, анализ психоэмоционального состояния, выявление негативных личностных тенденций, анкетирование, сбор и анализ данных.

Социальные сети являются неотъемлемой частью жизни современного человека. Неудивительно, что данные площадки также становятся местом распространения воздействий деструктивного характера. При этом под де-

структивными понимаются воздействия, ставящие под сомнение общечеловеческие ценности, а также придающие позитивный окрас подобным процессам [1]. Отметим, что в социальных сетях находятся огромные объемы информации, а потому полностью ручной их анализ представляется неэффективным. Поэтому для выявления негативных личностных тенденций зачастую предлагается использовать обученные нейронные сети [2, 3].

В рамках данного исследования в качестве социальной сети была выбрана крупнейшая русскоязычная социальная сеть – ВКонтакте [4]. Данная социальная сеть позволяет пользователям заводить профили, добавлять друг друга в друзья, вступать в различные сообщества, вести личные и групповые переписки, размещать посты и комментировать их.

Разработанная система для анкетирования молодежи в социальной сети ВКонтакте представляет собой приложение, размещенное в сообществе социальной сети и разработанное по технологии VK mini app [5]. Данное приложение физические размещено на HTTPS хостинге и является встраиваемым в социальную сеть. Работа с API социальной сети осуществляется с помощью библиотеки VK Bridge [6]. Приложение доступно на всех платформах, которые поддерживают социальную сеть. Архитектура приложения представлена на рис.

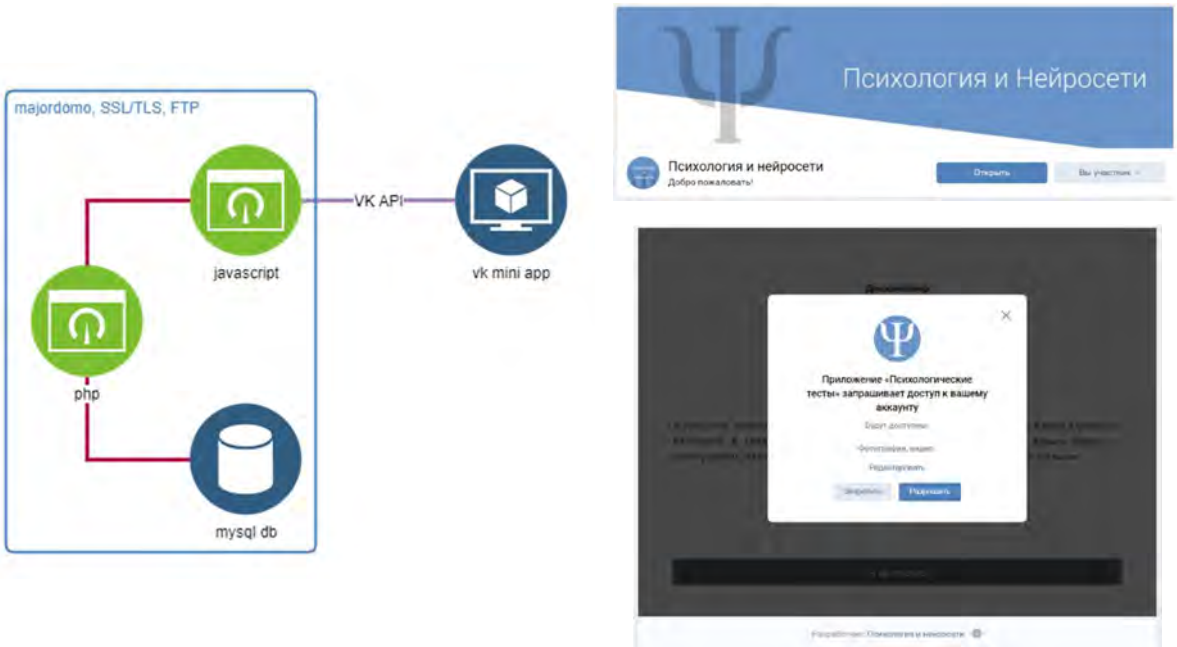


Рис. Архитектура системы анкетирования

Процесс взаимодействия пользователя с приложением можно разделить на три этапа:

1. ***Прохождение опросника:*** пользователю предлагается внести данные о своем имени, фамилии, поле, возрасте, университете, учебном факультете и группе.

2. ***Прохождение психологических тестов:*** пользователю предлагается пройти Я-структурный тест Аммона, шкалу тревоги Спилбергера-Ханина, копинг-тест Лазаруса, опросник уровня субъективного контроля Роттера и опросник САН – самочувствие, активность, настроение.

3. ***Сбор данных о странице пользователя:*** сбор осуществляется через API социальной сети на основе предоставленного пользователем токена доступа.

Отметим, что данные опросника необходимы для соотнесения личности пользователя с информацией его страницы в социальной сети, т. к. для последних характерно заполнение профиля вымышленными данными [7]. При этом данные об университете предоставляют возможность раздельного анализа групп студентов. Анализ результатов прохождения психологических тестов закладывает основу для формирования представления о состоянии пользователей, в то время как сбор данных о страницах пользователей необходим для дальнейшего анализа их взаимосвязи с результатами психологических тестов.

Работа выполнена при финансовой поддержке Гранта РФФИ мк 18-29-22034 в СПб ФИЦ РАН.

Список используемых источников

1. Branitskiy A., Doynikova E., Kotenko I., Krasilnikova N., Levshun D., Tishkov A., Vanchakova N. The Common Approach to Determination of the Destructive Information Impacts and Negative Personal Tendencies of Young Generation Using the Neural Network Methods for the Internet Content Processing // Proceedings of the 13th International Symposium on Intelligent Distributed Computing (IDC 2019), October 7-9, 2019, Saint-Petersburg, Russia. 2020. pp. 302–310. DOI: 10.1007/978-3-030-32258-8_36.

2. Alexander Branitskiy, Dmitry Levshun, Natalia Krasilnikova, Elena Doynikova, Igor Kotenko, Artem Tishkov, Nina Vanchakova, and Andrey Chechulin. Determination of Young Generation's Sensitivity to the Destructive Stimuli based on the Information in Social Networks. Journal of Internet Services and Information Security (JISIS), Vol. 9, No. 3, August 2019. pp. 1–20. DOI: 10.22667/JISIS.2019.08.31.001.

3. Станкевич М. А., Игнатьев Н. А., Смирнов И. В., Кисельникова Н. В. Выявление личностных черт у пользователей социальной сети Вконтакте // Вопросы кибербезопасности. 2019. № 4 (32). С. 80–87. DOI: 10.21681/2311-3456-2019-4-80-87.

4. Социальная сеть ВКонтакте. URL: https://vk.com (дата обращения: 31.03.2021).

5. Платформа VK mini app. URL: https://vk.com/dev/vk_apps_docs (дата обращения: 31.03.2021).

6. Библиотека VK Bridge. URL: https://www.npmjs.com/package/@vkontakte/vk-bridge (дата обращения: 31.03.2021).

7. Соколова Т. В., Чеповский А. М. Проблема восстановления профилей пользователей социальных сетей // Вопросы кибербезопасности. 2019. № 4 (32). С. 88–93. DOI: 10.21681/2311-3456-2019-4-88-93.

Статья представлена заведующим кафедрой,
доктором технических наук, профессором П. К. Смирновым.

УДК 159.9.07
ГРНТИ 15.81.29

ГЕТЕРОХРОННОСТЬ РАЗВИТИЯ AGILE-КОМАНД В ПРОЦЕССЕ ВЫПОЛНЕНИЯ ПРОЕКТНЫХ ЗАДАЧ

Н. Н. Лепехин, С. А. Маничев

Санкт-Петербургский государственный университет

Организация работы проектных agile-команд должна учитывать не только формальные фреймворки agile-методологий, но также стадиальность развития команд, гетерохронность развития сфер командной деятельности, развитие командной ментальной модели и стиль лидерства. Исследование проектной работы 20 agile-команд IT – специалистов подтвердило, что формальные фреймворки (способы работы) задаваемые организацией должны наполняться качественно разным психологическим содержанием в зависимости от стадии развития команды, уровня развития общей ментальной модели, стиля лидерства и проактивности членов команды.

agile-команды, стадии развития, гетерохронность, стиль лидерства, проактивность.

Командный подход как форма организации проектной работы успешно зарекомендовал себя в группах разработчиков программного обеспечения, число которых, по оценкам демографов, насчитывает более 20 млн человек. Ранее проектные команды координировали свою деятельность на основе принципов долгосрочного планирования, а менеджмент проекта строился исходя из «каскадной модели» как последовательного и надежного продвижения от планов к хорошо протестированным продуктам. В настоящее время организации используют гибкие (*agile*) методологии разработки проектов, среди которых выделяются Scrum, Kanban, Lean, XP и другие. Структура этих фреймворков задается со стороны IT-организаций, но при этом мало учитываются социально-психологические закономерности групповой динамики в командах разработчиков [1].

Психологические модели динамики рабочих команд должны учитывать организационный контекст деятельности, характер исполнения задач, временную динамику работы, взаимозависимость при ее выполнении. Анализ концепций, описывающих динамику команд, основанных на интеграции профессиональных знаний, позволяет выделить модель командного развития, релевантную проектной деятельности, которая включает четыре стадии развития: формирование команды, «сборка» команды вокруг задач проекта, «сборка» вокруг диад и триад, «сборка» коммуникативной сети команды [2].

В структуре фреймворков используемых в различных IT-организациях существуют различные практики, опирающиеся на коммуникацию между

членами команды, например, stand up meeting, co-location, retrospective и другие, успех которых очень чувствителен к использованию важных коммуникативных навыков: эмоциональной вербализации, активного слушания, ассертивности, рефлексии, обратной связи и других коммуникативных навыков. Исследования коммуникации в командах свидетельствуют, что использование или неиспользование данных навыков зависит не только от уровня владения ими, но в большей степени от текущего состояния групповой динамики и уровня развития группы [3].

Фреймворки agile-методологий, принятые в организации, задают формальные особенности работы команд и не учитывают психологические процессы групповой динамики, сопровождающие проектную деятельность команд. Закономерности командных процессов на каждой из стадий командного развития детерминируют то, что фреймворки работы agile-команд на каждой стадии наполняются качественно разным психологическим содержанием.

Подход к анализу содержания фреймворков работы agile – команд с учетом психологических возможностей и ограничений каждой стадии командообразования позволяет понять, какую роль различные практики agile – фреймворков играют на отдельных стадиях развития команд и почему «не работают» некоторые предписанные фреймворками способы организации работы. В совокупности это позволяет объяснить широко известный факт, что фреймворки agile никогда не реализуются в полном объеме, как они предписываются в руководствах.

Для проверки данных предположений были выдвинуты следующие гипотезы.

Гипотеза 1. О гетерохронности развития команд: в agile-командах будет одновременно наблюдаться феноменология разных стадий командного развития. Идея гетерохронности развития команд по отношению к разным сферам деятельности заключается в том, что группа может находится на разных модальных стадиях развития, накладывающихся друг на друга. Практика работы с командами показывает постепенное смещения фокуса модальности в профессиональной деятельности команды: от фокуса на индивидуальном выполнении, к фокусу совместной профессиональной деятельности в составе микрогрупп (диад и триад), и далее к фокусу профессионального взаимодействия в командной сети. Модальное изменение в деятельности членов команды в направлении командной сети происходит за счет приобретения социально-психологической компетентности и эмерджентного возникновения профессиональных знаний в совместном взаимодействии для решения новых задач. Создание командной ментальной модели обеспечивается процессами социализации или интеграции членов команды как носителей индивидуальных компетенций сначала в диады (микрогруппы), затем в команду. Возникновение (порождение) командного

знания проходит через ряд уровней усвоения и социальных интеракций: индивидуальный, диадный, групповой, командный – «снизу вверх и интерактивно» [4].

Гипотеза 2. О развитии команды в процессе повторяющихся циклов решения задач (спринтов). В отличие от классических моделей командного развития (Tuckman, 1965, 1977), концепция команды, адаптирующей свою деятельность в соответствии с уложнением командной ментальной модели предполагает повторение циклов профессионального развития. Это связано прежде всего с цикличностью выполнения задач, благодаря чему повторяемые итерации становятся источником приобретения и упорядочивания нового опыта на уровне индивида и группы, что позволяет накапливать и интегрировать познавательный капитал команды (транзактную память – transactive memory) [5].

Гипотеза 3. Гетерохронность в развитии команд обусловлена организационным контекстом и уровнем проактивного усвоения знаний участников проектных команд. Групподинамический подход предполагает, что командные процессы и эмерджентные когнитивные состояния являются медиаторами, оказывающими основное влияние на качество результатов, поскольку сама команда получает полномочия вносить изменения в свою деятельность и проактивно менять дизайн работы на основе собственной экспертной оценки получаемых результатов. Команда профессионалов-экспертов, оперирующая совместным эмерджентным знанием, проактивно вносит изменения в отношении разрабатываемого продукта, чтобы максимально удовлетворить требования заказчика. С нарастанием и расширением областей командного знания происходит рост объема и глубины сопутствующих интеракций, которые на самом высоком уровне развития группы имеют характер командной сети [6].

Эмпирическое исследование протоколов обсуждений на ретроспективах, проводившихся в конце двухнедельных циклов работы agile-команд IT-специалистов, позволило сделать выводы о гетерохронности развития команд. В зависимости от тематики обсуждаемого события члены команд делали высказывания, соответствующие 1, 2 или 3 уровню развития команд. Сдвиги в развитии команд происходили на каждом следующем цикле (спринте) и были следствием командного обсуждения важных событий (макропознания), при этом затруднения в развитии были обусловлены отсутствием навыков рефлексии и предпочтение позитивной обратной связи вместо конструктивной критики, поэтому лидерам команд приходилось использовать инструменты влияния в рамках ролей ментор и инструктор.

Гетерохронность развития команд выражается в том, что в одних аспектах команды достигают третьего уровня развития и начинают приближаться к четвертому, в других – находятся на втором уровне или даже ниже. Выявленные отстающие сферы развития команд позволяют выделить

наиболее важные аспекты командной деятельности, обеспечивающие переход команды на следующую стадию развития.

Подтвердилась необходимость использования гибкого стиля лидерства, соответствующего динамике модального развития группы от стадии «formation» к стадии «team compiliation» [7]. В зависимости от сферы командной работы: организация командной работы, выполнение профессиональных задач, создание видения и стратегии, рефлексия, развивающаяся обратная связь, лидер команды для обеспечения командной результативности и развития процессов макропознания в команде должен менять свой стиль (ментор, инструктор, коуч, фасилитатор) в соответствии с профессиональной и мотивационной готовностью членов команды. Лидеры команд хорошо справлялись с ролями ментора и инструктора (1 и 2 стадия развития команд), но еще слабо освоили роли коуча и фасилитатора (3 и 4 уровень развития команд).

Выводы

1. Подтверждается, что стадии развития проектных команд не отделены друг от друга резкими модальными переходами, но имеется наложение одной стадии на другую.

2. Развитие коммуникации в команде проходит через ряд ступеней освоения социально-психологической компетентности: коммуникация с лидером команды; коммуникация в микрогрупах; коммуникация в командной сети.

3. Основой развития группы в команду являются индивидуальные ментальные модели, которые в процессе выполнения циклов работы над задачами проекта трансформируются в ментальные модели микрогрупп (диад), а затем в командную ментальную модель, что наблюдается при повторении циклов (спринтов) командной работы.

4. В зависимости от аспекта командной деятельности (организация командной работы, выполнение профессиональных задач, создание видения и стратегии, рефлексия – обратная связь) лидер команды для обеспечения командной результативности и развития процессов макропознания в команде должен гибко менять свой стиль (ментор, инструктор, коуч, фасилитатор) в соответствии с профессиональной проактивностью членов команды.

5. Из трех этапов выполнения микроцикла работы над проектом (спринта): подготовка (планирование) – выполнение – рефлексия (ретроспектива) наиболее важным для развития команды является рефлексия командной работы. На ранних стадиях развития команды, вследствие низкого уровня проактивности, проводимая через двухнедельные интервалы ретроспектива не позволяет полностью решить задачи макропознания, рефлексии и обратной связи.

6. Для обеспечения развития команд необходимо проведение специальных тренингов командного взаимодействия в формате «simulation», посвященных развитию макропознания, рефлексии и навыков обратной связи в отношении анализа выполнения тренинговых заданий и умений межличностного взаимодействия как на уровне диад-триад, так и на уровне группы в целом.

Исследование выполнено при финансовой поддержке РФФИ, проект № 19-013-00947 «Проактивное поведение в современном дизайне работы».

Список используемых источников

1. Gren L. Understanding Work Practices of Autonomous Agile Teams: A Social-psychological Review. In: Paasivaara M., Kruchten P. (eds) Agile Processes in Software Engineering and Extreme Programming – Workshops. XP 2020. Lecture Notes in Business Information Processing, Springer, Cham, 2020. V. 396. pp. 227–235.

2. Маничев С. А., Лепехин Н. Н. Групповая динамика и развитие agile-команд // В кн.: Актуальные проблемы психологии труда, инженерной психологии и эргономики. Вып. 9 / Под ред. А. А. Обознова, А. Л. Журавлева. М.: Изд-во «Институт психологии РАН», 2020. 413 с., С. 181–216.

3. Kozlowski S. W. J., Bell B. S. Work groups and teams in organizations: Review update / N. Schmitt & S. Highhouse (Eds). Handbook of psychology. V. 12. Industrial and organizational psychology. 2nd ed. Hoboken, N. J.: Wiley, 2013. P. 412–469.

4. Kozlowski S. W. J., Bell B. S. Advancing Team Learning: Process Mechanisms, Knowledge Outcomes, and Implications / L. Argote, J. M. Levine (Eds). The Oxford Handbook of Group and Organizational Learning. Oxford: Oxford University Press, 2020. pp. 195–232.

5. Kozlowski S. W. J., Watola D., Jensen J. M., Kim B., Botero I. Developing adaptive teams: A theory of dynamic team leadership / E. Salas, G. F. Goodwin, C. S. Burke (Eds). Team effectiveness in complex organizations: Cross-disciplinary perspectives and approaches. N. Y.: Routledge Academic, 2009. pp. 113–155.

6. Grand J. A., Braun M. T., Kuljanin G., Kozlowski S. W. J., Chao G. T. The dynamics of team cognition: A process-oriented theory of knowledge emergence in teams // Journal of Applied Psychology. 2016. V. 101. pp. 1353–1385.

7. Gren L., Lindman M. What an Agile Leader Does: The Group Dynamics Perspective // Innovations in Enterprise Information Systems Management and Engineering. Innovations in Enterprise Information Systems Management and Engineering, 2020. pp. 178–194.

УДК 004.7
ГРНТИ 50.41.23

ИНФОРМАЦИОННЫЙ ПОРТРЕТ АБОНЕНТА

О. М. Лепешкин, А. С. Пермяков, А. С. Шуравин

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

В статье выдвигается гипотеза, что все электронные устройства, окружающие пользователя, а также их совокупность и характер использования создают уникальный информационный портрет (цифровой отпечаток). Для компаний он представляет большую ценность, чем персональные данные человека, поскольку позволяет получить информацию о многих аспектах его жизнедеятельности и использовать ее для продвижения товаров и услуг. В то же время, использование этой информации никак не регламентируется. В статье рассмотрен процесс формирования информационного портрета абонента, его состав, а также формализованное представление.

персональные данные, идентификация, цифровой отпечаток, информационный портрет абонента.

Каждый человек (физическое лицо) имеет свои персональные данные. К ним относятся фамилия, имя, отчество, дата и место рождения, адрес места жительства и регистрации, номер паспорта, телефона и многие другие.

Одновременно с этим практически каждый человек в процессе своей жизнедеятельности окружен электронными устройствами, среди которых:

– мобильный телефон или смартфон;
– фитнес-трекер;
– персональный компьютер или ноутбук;
– пейджер;
– спутниковый телефон;
– радиостанция (радиопередатчик).

Каждое из перечисленных средств имеет индивидуальные идентификационные признаки, также, как и сам человек, использующий их. К ним можно отнести:

– используемые каналы связи;
– сведения о геолокации (местоположение/маршруты перемещения);
– конкретное время/расписание использования устройств;
– адресаты сообщений и звонков (частные лица, организации, государственные органы, отечественные или иностранные);
– аккаунты в социальных сетях, мессенджерах, адреса электронной почты;

– электронная цифровая подпись, верифицированные учетные записи, биометрические данные.

Дополнительно в особые периоды (например, эпидемии) у человека могут появляться дополнительные временные идентификационные признаки (цифровые пропуска для перемещения, разрешения на прогулку, проезд).

Обращение со сведениями, являющимися персональными данными, регламентируется федеральным законом. Использование идентификационных данных, не относящихся к категории персональных, законодательными актами не регулируется.

Согласно [1] создается система, которая формирует цифровой портрет абонента на основании следующих данных:

– персональные данные абонентов, такие как фамилия, имя, отчество, адрес проживания и т. д., вплоть до копии паспорта;

– сведения из биллинговых систем о платежах и оказанных услугах, включая данные по платежам;

– факты о коммуникациях абонента по средствам стационарного и мобильного телефона, сети интернет и месседжеров (с каким абонентом или конечным адресом, сколько раз, каким способом связывался абонент), а также содержимое данных соединений, включая весь переданный или полученный контент, а также запись телефонных разговоров.

В то же время, данная система не учитывает данные, включающие перемещение абонента, а также то, что он может использовать средства связи, зарегистрированные через подставных лиц.

Расширение собираемых данных, а также расчет соответствующих идентификационных векторов позволит выявлять связи между «различными» абонентами, являющимися одним и тем же лицом, а также нетипичное поведение пользователей, основываясь не только на данных о пользовании им различными услугами связи, но и о его перемещении и другой активности.

По устройствам и совокупности идентификационных признаков может быть составлена карта взаимодействия (пространственно-временная матрица) конкретного физического лица (информационный портрет абонента).

Информационный портрет абонента не статичен, он изменяется со временем под влиянием следующих факторов:

– естественный процесс взросления человека;

– покупка новых устройств, в том числе взамен вышедших из строя;

– изменение места проживания, работы;

– появление новых интересов;

– изменение круга знакомств.

В ходе исследования выдвигается следующая гипотеза - каждый абонент имеет свой уникальный информационный портрет, подобно отпечатку

пальца, основанный на совокупности используемых устройств и идентификационных признаков.

Портрет может быть представлен в виде *K*-мерного вектора

$$\vec{p} = \{p_1, p_2, ..., p_k\}, \quad (1)$$

где p – параметр абонента.

Пример различных параметров абонента представлен в таблице 1.

ТАБЛИЦА 1. Параметры абонента

Мобильный телефон / смартфон	Номер UIN Модель MAC-адрес IP-адрес (при выходе в Интернет) GPS-координаты Используемое программное обеспечение
Радиостанция	Модель Частота/режим работы
Персональный компьютер	MAC-адрес сетевого адаптера / Wi-FI IP-адрес–сетевого адаптера / Wi-FI GPS-координаты Модель процессора Системное время Тип операционной системы Используемое программное обеспечение

Также уникальными являются данные о перемещении абонента. Известно, что уже по 4 точкам (базовым станциям), где регистрировался мобильный телефон абонента через определенные промежутки времени (1,5–2 часа) можно идентифицировать человека с точностью более 95 % [2].

В таблице 2 приведена точность определения местоположения абонента в зависимости от используемых технологий и устройств.

ТАБЛИЦА 2. Точность определения местоположения

Способ определения местоположения	Точность
1. GPS/ГОНАСС	2–4 м/3–6 м
2. Считыватели Bluetooth	5/15/100 м в зависимости от класса
3. RFID-метки	0,2/5/100 м в зависимости от класса
4. По сигналам сети сотовой связи	200–500 м/1 500–2 000 м в городе и в сельской местности соответственно
5. По сигналам точек доступа Wi-Fi	150 м
6. По IP-адресу	5–100 км

Ставится задача по отдельным элементарным информационным событиям с определенной долей вероятности определить/идентифицировать абонента [3].

Элементарное информационное событие (ЭИС) – факт передачи информации, включающий совокупность выявленных данных отправителя, получателя, используемые устройства, каналы связи, время передачи/получения. Совокупность данных может быть не полная.

Взаимосвязь абонентов, устройств связи, каналов связи и различных сетей представлена на рис. Оконечными устройствами (ОУ) являются мобильный, спутниковый и другие телефоны, радиостанции, пейджеры, персональные компьютеры и т. п. Возможные пути прохождения информационных потоков обозначены красными стрелками.

В ходе дальнейшего исследования требуется определить зависимость вероятности идентификации абонента от полноты данных отдельного элементарного информационного события, либо от совокупности нескольких элементарных информационных событий с неполными данными [4, 5].

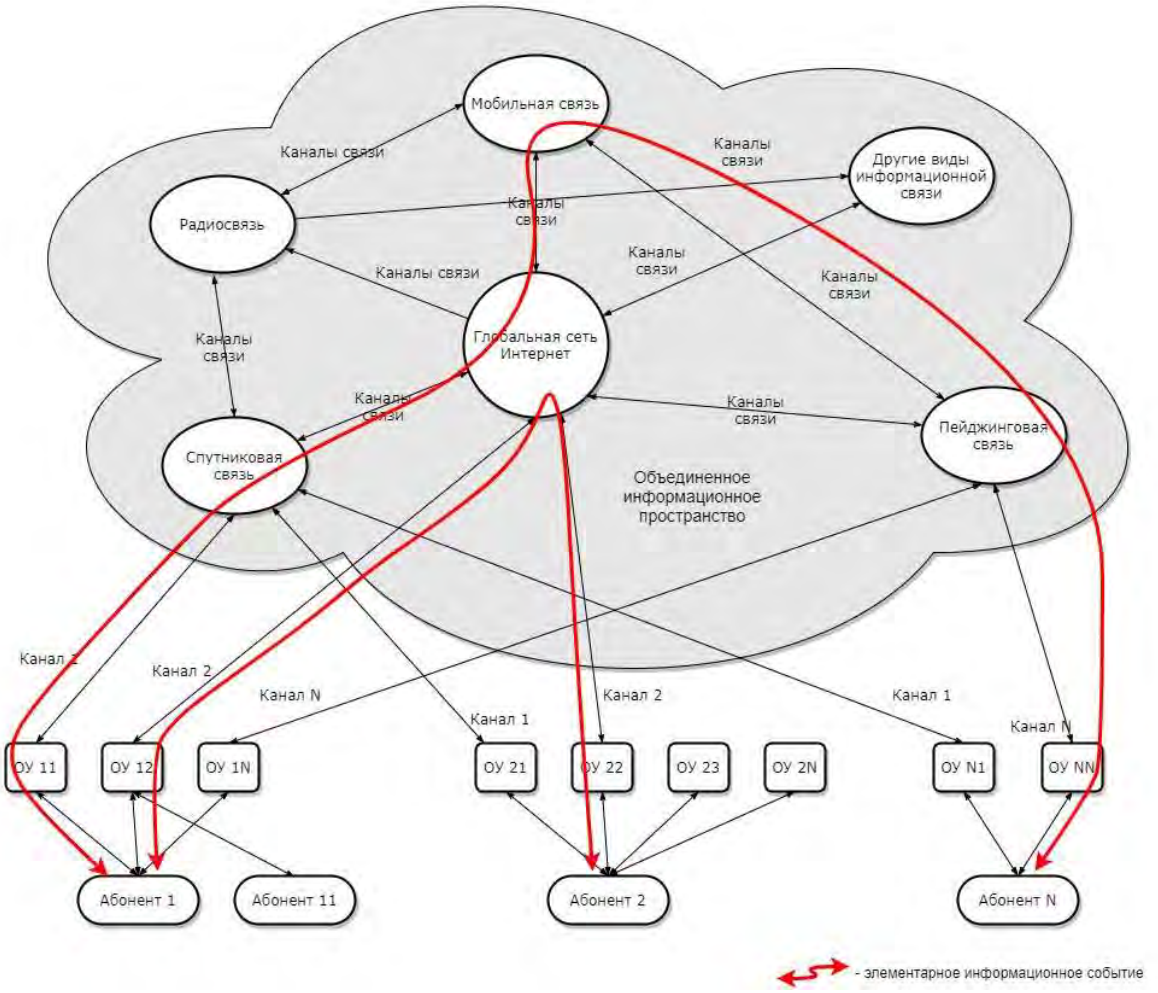


Рис. Схема информационного взаимодействия абонентов

В заключение отметим, что «закон Яровой» создал условия для хранения больших объемов информации об абонентах. Но, в то же время, огромное количество идентификационных данных, которыми они обладают, собирается провайдерами, компаниями, занимающимися таргетированной рекламой и всеми желающими практически бесконтрольно [6].

Список используемых источников

1. Приказ Минкомсвязи РФ от 29.10.2018 N 573. URL: https://minjust.consultant.ru/documents/41292 (дата обращения: 25.01.2021)

2. Лепешкин О. М. Способы определения местоположения устройства сотовой связи // Актуальные проблемы защиты и безопасности. Труды XXIII Всероссийской научно-практической конференции РАРАН. 2020. С. 241–244.

3. Лепешкин О. М., Шуравин А. С., Пермяков А. С., Зройчиков П. С., Шимаров Е. В. Модель контроля информационной безопасности распределенной сети связи // Известия Тульского государственного университета. Технические науки. 2020. № 12. С. 250–255.

4. Стародубцев Ю. И., Иванов С. А., Вершенник Е. В., Вершенник А. В., Закалкин П. В., Шевчук А. Л., Карасенко А. О. Способ определения оптимальной периодичности контроля состояния сложного объекта. Пат. на изобретение RU 2718152 C1, 30.03.2020. Заявка № 2019143358 от 24.12.2019.

5. Лепешкин О. М., Лепешкин М. О., Бурлов В. Г. Синтез модели процесса управления техническими системами на основе теории радикалов // Нейрокомпьютеры и их применение. Тезисы докладов. Под редакцией А. И. Галушкина, А. В. Чечкина, Л. С. Куравского, С. Л. Артеменкова, Г. А. Юрьева, П. А. Мармалюка, А. В. Горбатова, С. Д. Кулика. 2016. С. 18-В.

6. Атнагуллов Т. Н., Никитин В. В. Кибернетические воздействия на нейронные сети // Нейрокомпьютеры и их применение. XVIII Всероссийская научная конференция. Тезисы докладов. 2020. С. 324–325.

УДК 004.421
ГРНТИ 49.33.29

ОСНОВНЫЕ АСПЕКТЫ ОЦЕНКИ НАДЕЖНОСТИ СЕТИ ТАКТОВОЙ СЕТЕВОЙ СИНХРОНИЗАЦИИ

М. В. Лобастова, Е. А. Лыткина, К. М. Понамаренко, И. Д. Шарипова

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

В настоящее время происходит бурное развитие сетей связи. Это приводит не только к возникновению новых услуг связи, но и к ужесточению требований к построению сетей связи, а также к их надежности. Ни одна, даже самая современная услуга

связи не может быть предоставлена, если она не поддерживается транспортной инфраструктурой, одной из компонентов которой является сеть синхронизации. Именно поэтому вопросу надежности сети тактовой синхронизации следует уделять большое внимание.

тактовая сетевая синхронизация, надежность сети, надежность сетевого элемента, генераторное оборудование, режимы работы сети синхронизации, теория матриц, теория графов, марковские цепи.

Сеть тактовой сетевой синхронизации является важнейшей частью современных цифровых сетей связи. Именно от организации работы сети синхронизации зависит надежность сети связи в целом [1]. При этом показателями, непосредственно связанными с организацией сети синхронизации, можно считать частоту рассогласования в канале, частоты согласования указателей в сетях с SDH, скачки и дрожания фазы сигналов, потери пакетов и т. д.

Однако, сеть синхронизации является наложенной сетью и поэтому следует следить за ее надежностью. Для ее устойчивого функционирования необходимо, чтобы был надёжен каждый элемент сети от первичного задающего генератора до генераторов сетевых элементов; отсутствовали петли при передаче сигнала хронирования; маршруты передачи сигнала синхронизации не превышали требований по числу переприемов; были надежны маршруты, по которым осуществляется передача сигнала синхронизации [2].

Сеть синхронизации состоит из генераторного оборудования различных уровней иерархии. В зависимости от уровня иерархии, это может быть первичный задающий генератор (PRC), генератор узла (SSU) или генератор сетевого элемента (SEC). При этом каждый генератор можно рассматривать как одну структурную единицу.

Множество всех состояний, в которых может находиться сетевой элемент можно разделить на два непересекающихся множества: множество работоспособных и множество неработоспособных состояний [1].

К множеству работоспособных состояний относятся:

– состояние S_1 – включение электропитания элемента сети синхронизации;

– состояние S_2 – самотестирование элемента сети;

– состояние S_3 – работа в режиме свободных колебаний;

– состояние S_4 – выбор внешнего источника колебаний по наилучшим характеристикам входного сигнала;

– состояние S_5 – установление режима синхронной работы;

– состояние S_6 – работа в режиме удержания.

К неработоспособным состояниям относится состояние S_7 – отказ элемента и его восстановление. Так как отказ может наступить в любой момент, переход в состояние отказа возможен из любого другого состояния.

Для описания работы элемента сети тактовой синхронизации можно использовать Марковские цепи.

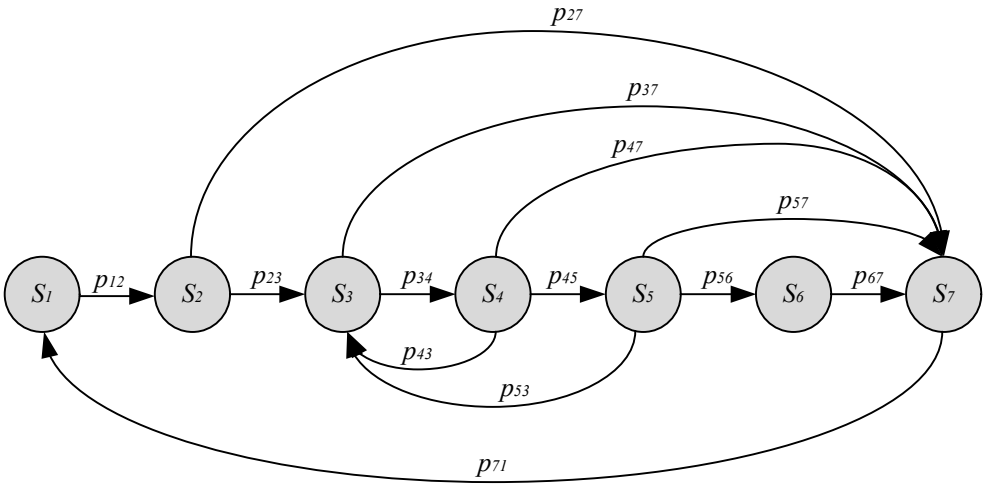


Рис. Марковская цепь,
характеризующая работу элемента сети тактовой синхронизации

С помощью Марковской цепи зададим матрицу переходных вероятностей $П = (p_{ij})$. Матрица переходных вероятностей задается аналогично матрице смежности ориентированного графа с отличием в том, что вместо булевых элементов содержит переходные вероятности из одного возможного состояния в другое [1].

$$П = \begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ S_6 \\ S_7 \end{array} \begin{array}{c} \begin{array}{ccccccc} S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_7 \end{array} \\ \begin{pmatrix} 0 & p_{12} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & p_{23} & 0 & 0 & 0 & p_{27} \\ 0 & 0 & 0 & p_{34} & 0 & 0 & p_{37} \\ 0 & 0 & p_{43} & 0 & p_{45} & 0 & p_{47} \\ 0 & 0 & p_{53} & 0 & 0 & p_{56} & p_{57} \\ 0 & 0 & 0 & 0 & 0 & 0 & p_{67} \\ p_{71} & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Для определения стационарных вероятностей пребывания системы в каждом из семи состояний будем использовать метод миноров и путем определённых математических преобразований и вычислений получим формулу стационарной вероятности пребывания в каждом из состояний:

$$\pi_i = \frac{P_i T_i}{\sum_{j \in S} P_j T_j},$$

где $i, j = 1,\ldots,7$; $i, j \sum_{i \in S} \pi_i = 1$, T_i – математическое ожидание безусловного времени пребывания узла сети в любом из возможных состояний [1].

$$T_i = \sum_{j \in S} p_{ij} T_{ij} \text{ , где } T_{ij}(t) = \int_0^\infty \left[1 - F_{ij}(t) dt\right].$$

Для каждого отдельно взятого элемента сети можно ввести такие понятия как коэффициент готовности и коэффициент простоя, их можно вычислить по следующим формулам:

$$K_\Г = \sum_{i \in S_p} \pi_i ,$$

$$\text{К}_\text{ПР} = \sum_{i \in \overline{S_p}} \pi_i = 1\text{-К}_\Г .$$

Однако, оценивая надежность сети тактовой синхронизации, необходимо учитывать не только безотказную работу генераторного оборудования, но и надежность маршрутов передачи синхросигнала.

Описав сеть синхронизации ориентированным графом, в котором вершины соответствуют сетевым элементам, а дуги – направлениям передачи сигнала, необходимо оценить, насколько надежен каждый путь, по которому происходит передача сигнала синхронизации.

Решая данную задачу, будем считать, что все пути исправны, а также идентичны по надежности. Основным методом поиска исправного маршрута между задающим генератором и некоторым сетевым элементом будет метод прямого перебора.

Для того, чтобы сделать вывод о надежности сети при отсутствии петель синхронизации необходимо, чтобы выполнялись следующие условия:

1. Все сетевые элементы, участвующие в маршруте передачи сигнала хронирования, находились в состоянии готовности.

2. Все линии, по которым осуществляется передача сигнала, были исправны.

Так как в сети синхронизации предусмотрено резервирование источника синхросигнала, то при переключении с основного источника на резервный, могут возникнуть петли. Отсутствие петель в сети является одним из ключевых моментов надежной работы сети синхронизации.

Алгоритм, который позволяет избежать петель еще на этапе проектирования заключается в оценке матрицы смежности, которая соответствует данной сети синхронизации. Если матрица треугольного вида, это значит, что сеть синхронизации не содержит петель. Изначально матрица смежности может быть не треугольной, но приводимой к треугольному виду путем перестановки строк и столбцов.

Однако, петли могут появиться уже при работе сети. Одной из главных задач является мониторинг сети на наличие новых петель после переключения на резервный источник сигнала синхронизации. Существуют несколько методов обнаружения петель в сетях синхронизации.

1. Алгоритм, основанный на вычеркивании нулевых строк и столбцов в матрице смежности графа.

Алгоритм основан на анализе матрицы смежности ориентированного графа, соответствующего сети синхронизации. Наличие в матрице смежности нулевых строк говорит о том, что элемент сети, которому соответствует нулевая строка, не синхронизирует ни один другой генератор. Нулевые столбцы в матрице смежности соответствуют генераторам, не получающим сигнала синхронизации от других источников. Поэтому, элементы сети, соответствующие нулевым строкам или столбцам, не могут участвовать в петлях.

Вычеркивая нулевые строки и столбцы из матрицы смежности, можно исключить генераторы, не входящие в петли. В том случае, если после вычеркивания в матрице останутся элементы, это будет свидетельствовать о том, что они участвуют в петле или в нескольких петлях. Если в матрице смежности вычеркивать те элементы, которым соответствуют нулевые строки и столбцы, то элементы, не участвующие в петле, будут исключаться.

2. Алгоритм, основанный на выделении компонент связности.

Сеть синхронизации может состоять из нескольких компонент связности. Если сеть содержит компоненты размерностью больше или равной двум, это говорит о наличии петель в сети синхронизации [3].

Таким образом, при проектировании и эксплуатации сети синхронизации необходимо помнить о ее надежности. Способы обеспечения и оценки надежности, рассмотренные в данной статье, позволяют сделать обоснованный вывод о том, в каком состоянии находится сеть в рассматриваемый момент времени.

Список используемых источников

1. Лобастова М. В., Матюхин А. Ю. Оценка надежности работы элемента сети тактовой сетевой синхронизации // Радиотехнические и телекоммуникационные системы. 2020. №3. С. 27–36.

2. Лобастова М. В., Матюхин А. Ю. Использование алгоритма Флойда-Уоршалла для поиска маршрута передачи сигнала синхронизации с минимальным числом переприемов // Электросвязь. 2020. № 4. С. 51–54.

3. Lobastova M., Matyukhin A. Method to detect and eliminate loops synchronization in 5G networks // 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2019. pp. 897–970.

Статья представлена доцентом кафедры ССиПД СПбГУТ, кандидатом технических наук А. Ю. Матюхиным.

УДК 65.011.56
ГРНТИ 50.49

ИНФОКОММУНИКАЦИОННАЯ СИСТЕМА ФУНКЦИОНИРОВАНИЯ СКЛАДСКОГО ОТГРУЗОЧНОГО ПУНКТА

Е. А. Матвеева, К. А. Сомов

Поволжский государственный университет телекоммуникаций и информатики

В настоящее время практически не существует организаций, не использующих современные достижения инфокоммуникаций. Говоря о цифровизации бизнес-процессов, подразумевают уже не просто создание автоматизированных систем, а создание инфокоммуникационных систем, использующих все средства коммуникаций, имеющихся в организации. Построение такого рода систем является трудной, дорогостоящей работой, во время выполнения которой специалисту необходимо учесть большое количество нюансов и факторов.

инфокоммуникационная система, аппаратно-программный комплекс, бизнес-процесс, отгрузочный пункт, автоматизация.

Руководителям организаций для повышения эффективности деятельности и конкурентоспособности необходимо развивать IT-технологии, которые позволяют повысить скорость и качество обработки информации, минимизируют влияние человеческого фактора и в конечном результате, становятся важным инструментом на всех этапах работы. Так, логистическим компаниям крайне необходимо проводить оптимизацию и автоматизацию своей деятельности, из-за постоянно возрастающего спроса на доставку различного рода строительных и промышленных материалов, продуктов питания, одежды и т. д. [1, 2].

Актуальность разработки инфокоммуникационной системы для логистической компании заключается в обеспечении складского отгрузочного

пункта программным продуктом, который предоставит возможность перехода от бумажного учета товарооборота к цифровому, позволит хранить и обрабатывать данные используя одну программу, повысит безопасности отгрузочного пункта, автоматизирует процесс отгрузки, таким образом упрощая планирование предстоящих работ и позволяет развиваться организации быстрее благодаря наличию точных, структурированных данных и принимать обоснованные решения в стратегическом планировании по дальнейшему улучшению работы.

Для обеспечения поставленной цели требуется разработать аппаратно-программный комплекс (АПК), входящий в инфокоммуникационную систему и решающий следующие задачи:

– автоматическое распознавание номеров грузовых машин,

– представление оператору информации о типе, количестве материала, номере склада для загрузки и расположении склада покупателя для проверенной грузовой машины,

– фиксация и долговременное хранение результатов взвешивания в базе данных совместно с фотоизображениями взвешиваемых автомашин и распознанными номерами,

– автоматическое или ручное взаимодействие с весами, автоматический расчет массы нетто,

– автозаполнение товарно-транспортных накладных,

– формирование отчетов о прошедших отгрузках.

Для отображения потоков информации и документооборота, протекающих при работе складского отгрузочного пункта, спроектирована диаграммы *DFD* при применении нотации Гейна-Сарсона. Данная диаграмма отражает процесс отгрузки и описывает какая информация обрабатывается и куда записывается с момента создания плана отгрузки до передачи товарно-транспортной накладной водителю. Фрагмент диаграммы представлен на рис. 1.

При проектировании диаграммы идентифицированы и структурированы процессы передающие потоки информации в ходе выполнения отгрузки и определено их взаимодействие в системе. На основании этого выявлено необходимое оборудование для создания АПК.

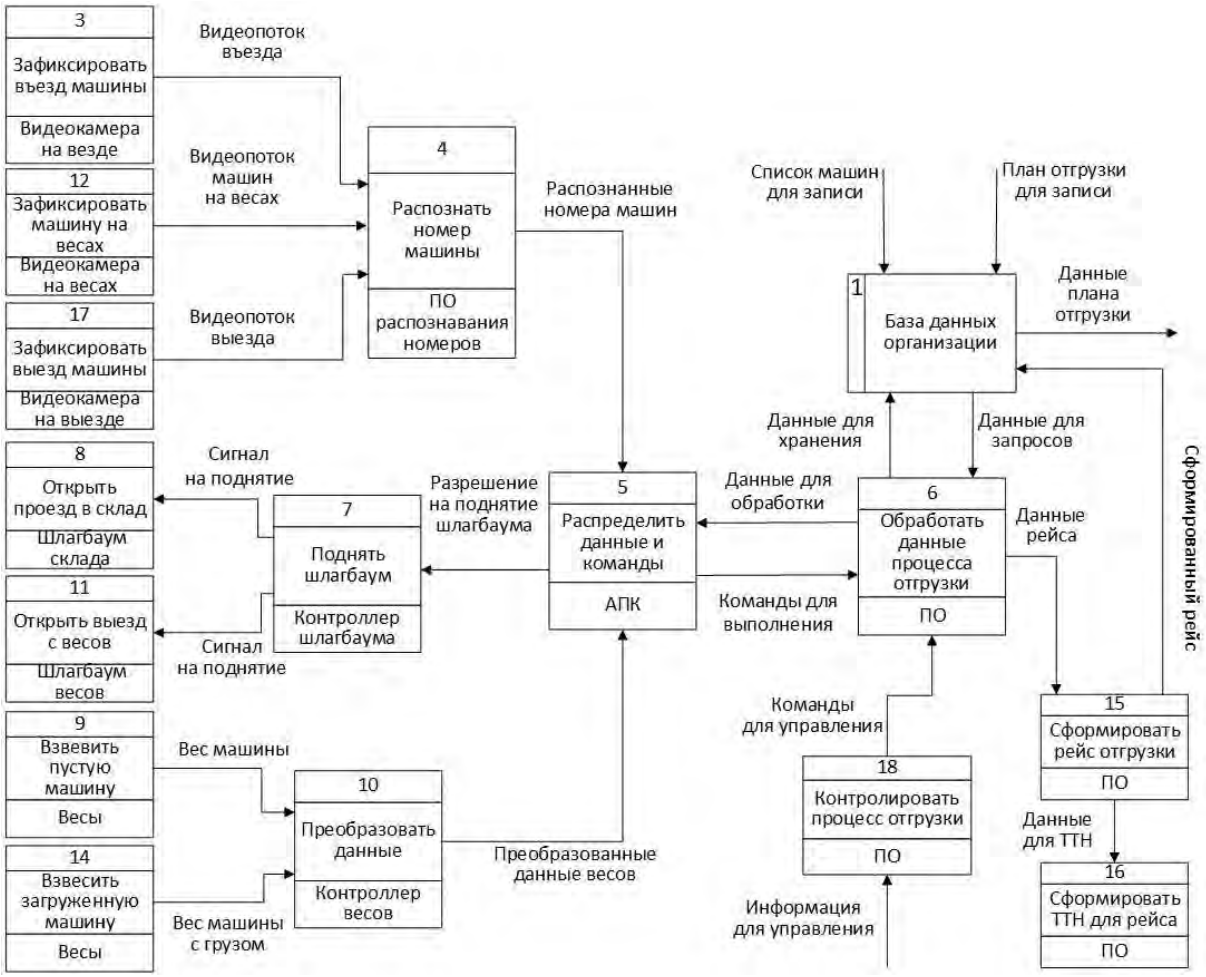


Рис. 1. Фрагмент диаграммы *DFD* процесса отгрузки

Разрабатываемый АПК для выполнения поставленных задач должен содержать перечень оборудования, указанный в таблице 1.

ТАБЛИЦА 1. Перечень оборудования АПК

Оборудование	Количество	Назначение
Компьютер	1	Управление системой, рабочее место оператора отгрузки
Видеокамера	3	Фиксация номеров грузовых машин
Коммутатор	1	Объединение всех видеокамер в единую сеть
Маршрутизатор	1	Объединение в одной сети компьютера, сервера, принтера
Светодиодный прожектор	1	Подсветка грузовых машин на весовой платформе
Шлагбаум	2	Контроль проезда на территорию отгрузочный пункт
Устройство дискретного ввода-вывода	1	Удаленное управление шлагбаумами
Сервер	1	Хранение информации базы данных

Оборудование	Количество	Назначение
Принтер	1	Печать документации

Обобщая информацию, полученную в ходе анализа бизнес-процессов и определения необходимо технического оборудования [3], спроектирована структурная схема размещения и подключения оборудования. Схема представлена на рис. 2 и отображает выше описанное оборудование, его размещение и способы подключения для обеспечения автоматизации процесса отгрузки и работоспособности.

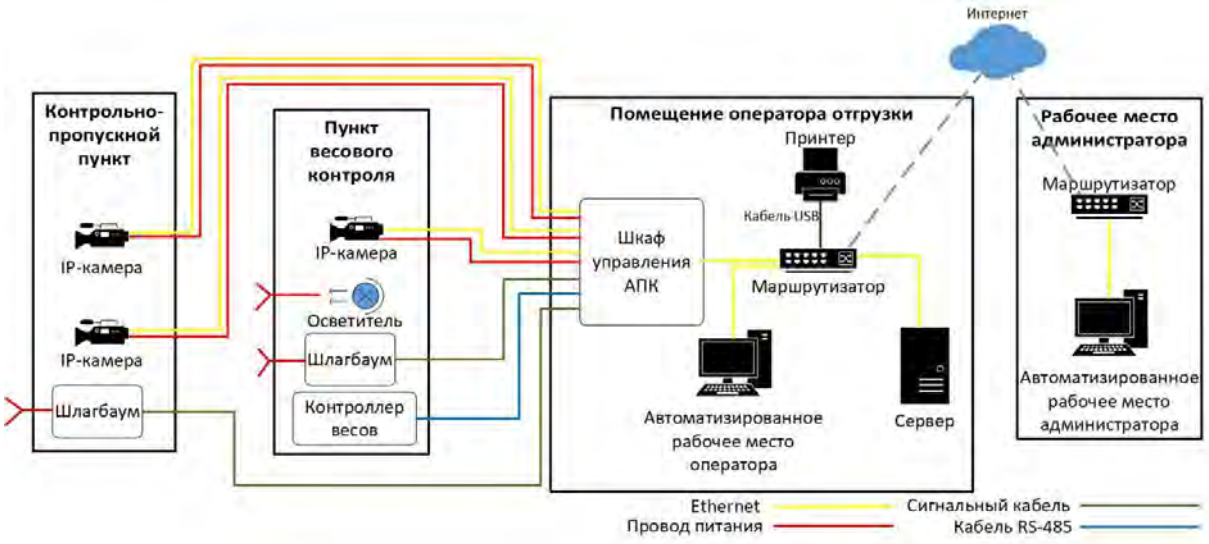


Рис. 2. Схема размещения оборудования

Помещение оператора отгрузки является центром системы, где располагаются управляющее процессом отгрузки оборудование. Помещение разделено на две комнаты: рабочая комната оператора и техническая комната.

В рабочей комнате оператора располагаются компьютер для управления системой, принтер для печати товарно-транспортных накладных и маршрутизатор для прямой связи компьютера, сервера и шкафа управления АПК. На компьютере установлено специализированное программное обеспечение для организации взаимодействия различных компонентов системы, для обеспечения работы с базой данных, и программное обеспечение распознавания номеров.

Для удобства работы оператора сервер и шкаф управления АПК перенесены в отдельную комнату, предназначенную для установки технического оборудования. На сервер устанавливается база данных организации и для обеспечения удаленного доступа организована клиент-серверная архитектура. Шкаф управления АПК предназначен для передачи информации для обработки, полученной от контроллера видеокамер и контроллера весов, и обратной передачи команд управления от программного обеспечения

до контроллеров шлагбаумов. Шкаф управления АПК состоит из: коммутатор IP камер, блоков питания для IP камер, конвертер интерфейсов RS 232/485, модуль дискретного ввода-вывода для управления шлагбаумами.

Контрольно-пропускной пункт оборудован двумя IP камерами, направленными на въезд и выезд с территории склада организации, и шлагбаумом ограничивающий проезд не допущенного к проезду транспорта.

Пункт весового контроля оборудован IP видеокамерой для фиксации взвешиваемой машины, осветителя, шлагбаумом для контроля положения ГМ на весовой платформе и контроллером весов.

Рабочее место администратора находится в другом здании, поэтому для обеспечения удаленного соединения с сервером необходимо обеспечить подключение к интернету при помощи маршрутизатора.

Провода и кабеля необходимые для подключения используемого оборудования представлены в таблице 2.

ТАБЛИЦА 2. Описание необходимых проводов и кабелей

Оборудование	Тип соединения	Назначение
IP камера	Кабель Ethernet FTP 4, категории 5e, до 100 м	Передача видеопотока
	Провод DC12V	Питание камеры
Шлагбаум	Сигнальный кабель 3x0.75	Передача сигнала контроллеру
	Провод питания 220В	Питание шлагбаума
Осветитель	Провод питания 220В	Питание осветителя
Контроллер весов	Кабель RS – 485	Передача данных с весов
Шкаф управления АПК	Кабель Ethernet UTP 4, категории 5e, до 100 м	Передача информации с контроллеров
Сервер	Кабель Ethernet UTP 4, категории 5e, до 100 м	Передача данных
Принтер	Кабель USB A(m) – USB B(m) 2.0	Управление принтером
АРМ оператора/ администратора	Кабель Ethernet UTP 4, категории 5e, до 100 м	Управление системой

Работа с системой происходит при помощи пользовательского интерфейса, ориентированного на оператора отгрузки и администратора компании. Каждый сотрудник имеет собственную учетную запись при помощи которой авторизуется в системе.

Таким образом внедряемая инфокоммукационная система обеспечит компанию многофункциональным программным обеспечением и аппаратно-программным комплексом, которые окажут положительное влияние

на производительность и конкурентоспособность на рынке предоставляемых услуг. Также эффективность от данной системы можно оценить путем сравнения затрачиваемого времени на загрузку одной грузовой машины до внедрения системы и после. Результаты проведенного оценивания представлены в таблице 3.

ТАБЛИЦА 3. Результаты сравнения затрачиваемого времени

Действие	До внедрения АПК	С применением АПК
Проверка грузовой машины на въезде и выписка одноразового пропуска	300 сек	10 сек
Определение номера ангара, типа и количества груза для загрузки	60 сек	5 сек
Взвешивание пустой грузовой машины	90 сек	40 сек
Взвешивание загруженной грузовой машины	90 сек	40 сек
Заполнение товарно-транспортной накладной	120 сек	30 сек
Итог:	660	125

Как видно по результатам проведенной оценки, внедряемая система позволит сократить время обслуживания в 5,28 раз, что в свою очередь уменьшит время простоя грузовых машин в очереди на загрузку и обеспечит увеличение скорости выполняемых поставок, что в конечном итоге позволит выполнять больший объем заказов и как следствие увеличится доход и масштабы компании.

Список используемых источников

1. Величко В. В., Катунин Г. П., Шувалов В. П. Основы инфокоммуникационных технологий. М.: Горячая Линия – Телеком, 2009. 718 с. ISBN 978-5-9912-0055-4.

2. Щербаков В. В., Мерзляк А. В., Коскур-Оглы Е. О. Автоматизация бизнес-процессов в логистике. СПб.: Питер, 2016. 464 с. ISBN 978-5-496-01409-0.

3. Точчи Рональд Дж., Уидмер Нил С. Цифровые системы. Теория и практика: 8ое издание. М.: Вильямся, 2018. 1024 с. ISBN 978-5-8459-0586-4.

УДК 004.021
ГРНТИ 50.41.25

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ДЛЯ ОБЕСПЕЧЕНИЯ КЛИЕНТСКОГО СЕРВИСА ХОСТИНГ-ПРОВАЙДЕРОВ

В. Н. Мельников, Д. В. Окунева

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

В рамках клиентской поддержки важным критерием является скорость реагирования – поэтому предложено внедрение современных интеллектуальных компьютерных технологий с целью повышения качества обслуживания клиентов и ускорения времени реагирования на их запросы. В докладе определены типовые задачи, которые целесообразно осуществлять в автоматическом режиме.

хостинг, поддержка, клиентский сервис, интеллектуальные компьютерные технологии.

Наиболее актуальными проблемами сервисной компании являются необходимость в полном объеме удовлетворять информационные потребности клиента. Согласно современным моделям клиенториентированного бизнеса компании необходимо сформировать ядро потребительской ценности.

Стандартные процедуры по созданию ядра потребительской ценности описаны ниже:

– аккумуляция данных об объемах оказания сервисных услуг;

– анализ ситуации на рынке и поиск незанятых ниш;

– изучение ожиданий потребителей (опросы, анкетирование, фокус-группы, анализ прямых обращений и жалоб клиентов);

– изучение тенденций в потреблении, основных ценностей клиентов;

– приведение полученных сведений в систему ценностей для конкретного потребителя и конкретного продукта [1];

– объединение аналогичных ценностей, определение целевых сегментов;

– формулирование совокупной потребительской ценности как суммы отдельных элементов, которые вместе позволяют наиболее полно удовлетворить потребности клиента благодаря синергетическому эффекту.

– Практика показывает, что основными причинами для смены поставщика услуг хостинга являются [2, 3]:

– участившиеся перебои в работе сайта, вызванные неполадками со стороны хостинг-провайдера;

– медленная работа сайтов – согласно исследованию *Google* [4], 53 % пользователей уходят со страницы, если мобильная версия сайта загружается более чем за 3 секунды;

– низкое качество работы службы поддержки – медленное время реагирования на обращения, недостаточная компетенция операторов, отсутствие помощи по вопросам, непосредственно относящимся к работе хостинга;

– отсутствие у текущего провайдера необходимого объема услуг (дискового пространства на сервере, вычислительных ресурсов, трафика);

– резкое и неоправданное повышение стоимости услуг хостинга;

– недостаточная безопасность серверов – утечка/пропажа данных с ресурсов хостинг-провайдера.

Рассмотрим отдельно такой немаловажный аспект успешного оказания услуг хостинга, как работа службы поддержки. По данным опроса, проведенного подразделением международной компании SAP Hybris, 70 % российских потребителей готовы отказаться от использования сервиса по причине неотзывчивой службы клиентской поддержки [5].

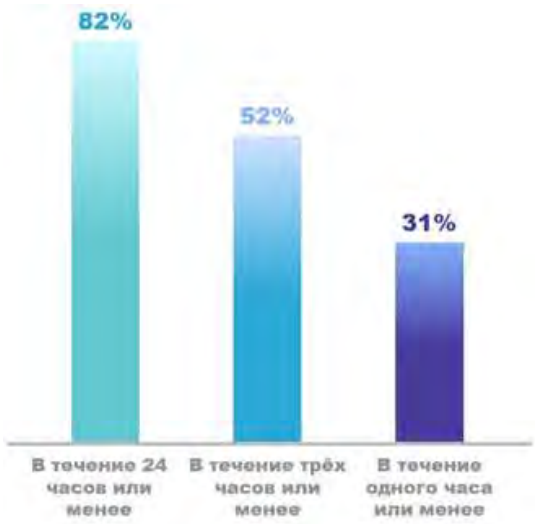


Рис. 1. Процент пользователей и ожидаемое ими время реагирования

52 % пользователей ожидают ответа на свой запрос не позже, чем через 3 часа, а 65 % – не более чем через 12 часов (рис. 1) [5]. Поэтому в целях удержания клиентов необходимо уделять внимание скорости реагирования. Согласно исследованию американской компании Nielsen «Технологические тренды в маркетинге и жизни потребителя», 37 % компаний на момент 2019 года уже используют чат-боты для связи с клиентами, а к 2022 году доля таких компаний должна увеличиться до 51 % (рис. 2).

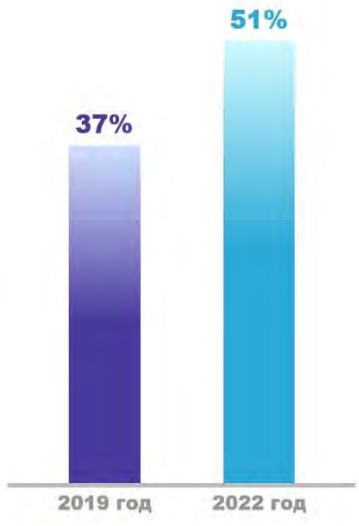


Рис. 2. Ожидаемый рост доли компаний, использующих чат-боты

На текущий момент большинство чат-ботов представляют из себя удобный интерфейс, связывающий покупателя, который пишет через мессенджеры (*VK*, *Telegram*, *Facebook*) с живым человеком – представителем компании [7]. Слабым звеном здесь является тот факт, что отвечает на первичные запросы пользователя все еще человек – это замедляет время ответа. При этом, через чат-боты поддержка оказывается преимущественно консультационная – простые ответы на несложные вопросы, в большинстве случаев с применением т. н. «быстрых ответов (шаблонов)».

Систематизируем перечень вопросов, на которые в рамках переписки в мессенджерах отвечает специалист отдела технической поддержки хостинг-провайдера:

– консультация по осуществлению различных действий в панели управления хостингом – центром управления сервером и размещенными службами;

– консультация по стоимости услуг, особенностям системы биллинга (списания денежных средств);

– уведомление о происходящих/предстоящих технических работах или неполадках в работе сервера и/или служб, непосредственно влияющих на работоспособность сайта/сервера пользователя.

Прочие действия (например, углубленная диагностика работоспособности сайта, осуществление действий в панели управления пользователя) по обращению из мессенджеров не осуществляются, поскольку мессенджеры не являются авторизованным каналом связи – нельзя доподлинно установить, что автором обращения является владелец сайта или лицо, непосредственно связанное с ним. В случае возникновения запроса, который невозможно решить в рамках диалога в мессенджере, оператор направляет пользователя в панель управления хостингом – авторизованный канал связи, в котором можно создать обращение в службу поддержки.

Таким образом, с учетом вышесказанного, оператора поддержки в чат-боте вполне может заменить программа, анализирующая запрос пользователя и оперативно отвечающая ему уже подготовленным заранее ответом из внутренней базы знаний. Помимо этого, для чат-бота в целях улучшения качества обслуживания и решения спорных ситуаций нужно оставить возможность связи с реальным оператором. Это может быть реализовано как автоматически (в случае отсутствия информации в базе знаний), так и по запросу пользователя (реакция на определенные слова в его сообщения, либо отдельная кнопка).

На данный момент чат-боты уже автоматизированы у различных операторов связи, таких как «Вымпелком» («Билайн») и «МТС» [8, 9]. По подсчетам крупнейшего российского телекоммуникационного оператора «МТС», 8 из 10 клиентских запросов через сайт МТС обрабатываются без привлечения специалистов поддержки, то есть роботом [9].

Ожидаемые эффекты от внедрения автоматического оператора в чат-боте:

- сокращение времени ожидания клиентом;
- сокращение времени обслуживания;
- снижение затрат на обслуживание;
- рост удовлетворенности клиентов.

Список используемых источников

1. Пискунова Е. Е., Мельникова И. Ю. Модели клиентоориентированного бизнеса // KANT. 2018. № 3. С. 225–232.

2. Megan Hendrickson. Should I Switch Web Hosts? How to Know When It's Time to Migrate Your Site. URL: https://www.dreamhost.com/blog/how-to-switch-web-hosts-migrate-site/ (19.01.2021).

3. Kaumil Patel. 12 Practical Reasons Why You Should Switch Web Hosts Now. URL: https://www.greengeeks.com/blog/12-practical-reasons-why-you-should-switch-web-hosts-now/ (19.01.2021).

4. Google Consumer Insights: Analytics data from a sample of mWeb sites opted into sharing benchmark data, March 2016. URL: https://www.thinkwithgoogle.com/consumer-insights/consumer-trends/mobile-site-load-time-statistics/ (20.01.2021).

5. SAP Hybris. Анализ предпочтений потребителей // 2017. URL: https://gallery.mailchimp.com/b950402581ac99712c827691c/files/33a27b99-b3a5-4f6f-a865-5e1ffd72bb4f/SAP_Hybris_Consumer_Insights_Survey_Russia_20_03.pdf (дата обращения: 20.01.2021).

6. The Nielsen Company. Технологические тренды в маркетинге и жизни потребителя // Май 2019. URL: https://www.nielsen.com/wp-content/uploads/sites/3/2019/05/technological-trends-in-marketing-and-consumer-life.pdf (дата обращения: 20.01.2021).

7. Джошуа Ганс. В чем важность Facebook Messenger для обслуживания клиентов. // Harvard Business Review, 6 мая 2016 г. URL: https://hbr.org/2016/05/why-facebook-messenger-is-a-big-deal-for-customer-service

8. Билайн. Чат-бот для клиентов Билайн // 2017. URL: https://moscow-beeline.ru/news/chat-bo-dlya-klientov-beeline

9. ПАО «МТС». МТС начала продавать роботов // 03.06.2019. URL: https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2019-06-03/mts-nachala-prodavat-robotov

УДК 004.056.5
ГРНТИ 81.93.29

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

А. А. Миняев

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

Создание комплексной системы защиты информации является сложной, трудно формализуемой и слабо структурированной задачей. Связано это тем, что для решения такого рода задачи необходимо использовать системный подход, позволяющий связывать множество процессов, протекающих в территориально распределенных информационных системах и процессов, протекающих в самой системе защиты информации. В данной статье предложен метод разработки системы защиты информации территориально распределенных информационных систем на основе когнитивного моделирования. Метод позволяет также исследовать проблему разработки системы защиты информации территориально распределенных информационных систем, учесть изменения среды функционирования, определить реакцию информационной системы (ее ИТ-инфраструктуры).

разработка СЗИ, территориально-распределенные ИС, когнитивное моделирование.

В настоящей работе предлагается метод разработки системы защиты информации (СЗИ) территориально-распределенных информационных систем (ИС) на основе когнитивного моделирования ввиду того, что создание комплексной системы защиты информации является сложной, трудно формализуемой и слабо структурированной задачей. Связано это также с тем, что для решения такого рода задачи необходимо использовать системный подход, позволяющий связывать множество процессов, протекающих в территориально-распределенных ИС и процессов, протекающих в самой СЗИ территориально-распределенных ИС [7].

Когнитивное моделирование и анализ позволяет также исследовать проблему разработки СЗИ территориально-распределенных ИС, учесть изменения среды функционирования, определить реакцию ИС (ее ИТ-инфраструктуры).

Для реализации метода разработки СЗИ территориально-распределенных ИС была построена когнитивная карта, представленная на рис. 1.

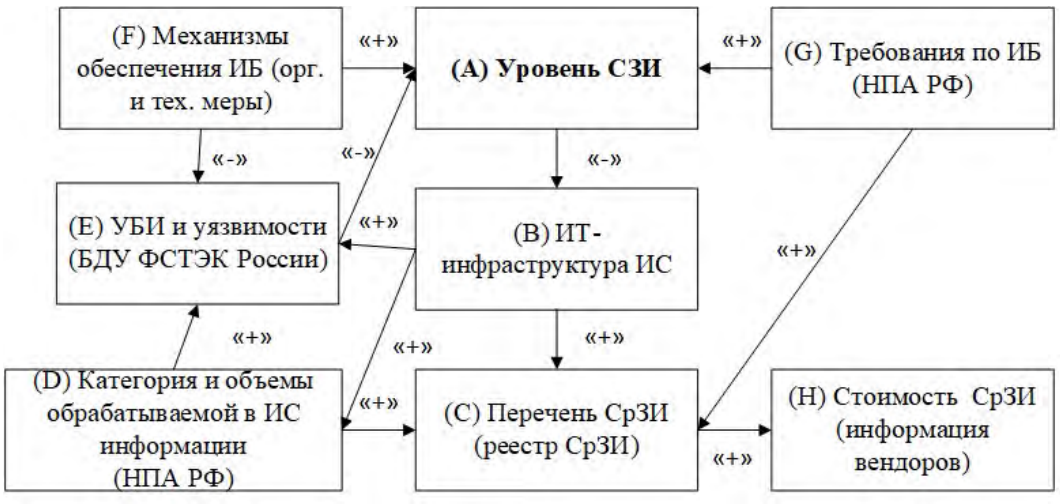


Рис. 1. Когнитивная карта для анализа процесса разработки СЗИ территориально-распределенных ИС

Проблему разработки СЗИ территориально-распределенных ИС можно описать 8 факторами $\{A,B,C,D,E,F,G,H\}$. На рис. 1 дугами отмечены причинно-следственные отношения, при этом считается, что влиянием остальных можно пренебречь. Знак «+» означает, что при увеличении исходного фактора (концепта) зависимый фактор также увеличивается. Знак «-» означает, что эти два фактора изменяются в противоположных направлениях: увеличение исходного концепта ведет к уменьшению значения зависящего от него концепта [2].

Взаимодействие факторов в контуре $\{A-B-D-E-A\}$: масштабы ИТ-инфраструктуры территориально-распределенных ИС значительные с точки зрения используемых средств вычислительной техники, программного обеспечения, каналов связи между площадками и информационных технологий, реализующих ИС, что приводит к увеличению количества обрабатываемой информации и, следовательно, к появлению большего количества угроз безопасности информации (УБИ) и уязвимостей, что, в свою очередь, повлечет снижение уровня информационной безопасности территориально-распределенных ИС.

Получение прогноза развития СЗИ является прямой задачей, а задача нахождения управляющих воздействий – обратная задача. Решению прямой и обратной задач посвящены множество работ [3, 4, 5] и в настоящей статье не рассматриваются. Следует отметить, что специфика когнитивного моделирования заключается в том, что формальные математические методы анализа применяются к моделям, описывающим субъективное видение СЗИ. На каждом этапе формирования модели приходится принимать решения, от совокупности которых, в конечном счете, зависит адекватность построен-

ной модели. Набор моделей и методов анализа влияний в слабоструктурированных ситуациях сам по себе не гарантирует построения адекватной модели.

При формальном выделении факторов и связей между ними неизбежно выявляются ранее неучтенные аспекты СЗИ, связи, казавшиеся несущественными, и формируется система понятий, в терминах которой даже неформальное обсуждение проблемы становится более четким и обоснованным [6]. Главным достоинством аппарата когнитивных карт является возможность систематического качественного учета отдаленных последствий принимаемых решений и выявления побочных эффектов, которые могут помешать реализации очевидных решений и которые трудно оценить интуитивно при большом числе факторов и многообразии многочисленных путей взаимодействия между ними. Данный подход является математической основой для интеллектуальных информационных технологий поддержки принятия решений в слабоструктурированных предметных областях, к каким относится разработка СЗИ территориально-распределенных ИС.

На основании предложенного метода разработки СЗИ территориально-распределенных ИС поэтапно были реализованы подсистемы защиты [6]. Пример логической схемы подсистемы антивирусной защиты на основе предложенного метода представлен на рис. 2.

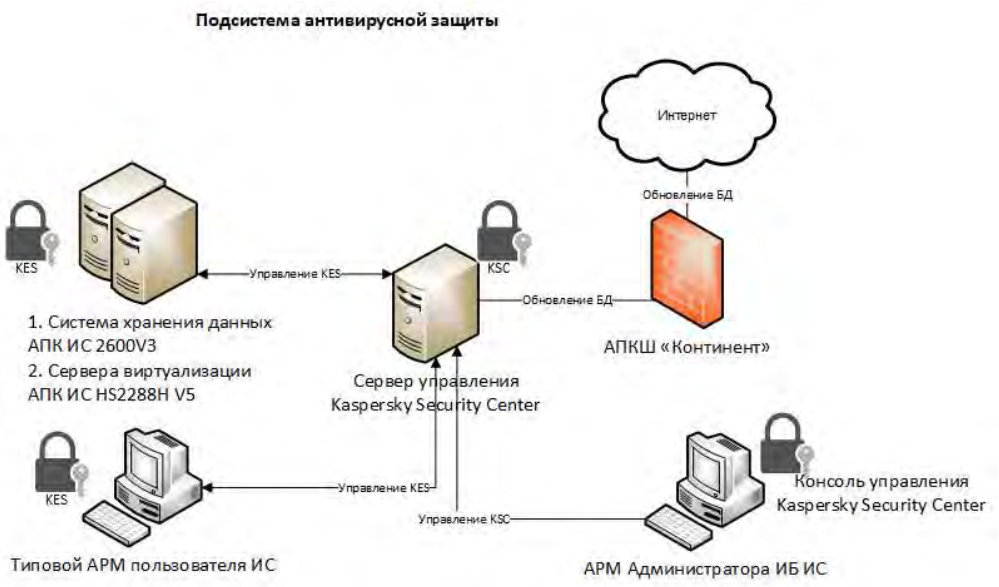


Рис. 2. Логическая схема подсистемы антивирусной защиты

В работе были поставлены задачи по разработке оптимального метода разработке СЗИ территориально-распределенных ИС. В качестве математических моделей и методов были исследованы методы динамического программирования теории управления и теории вычислительных систем. На основе когнитивного моделирования была построена когнитивная карта для

анализа процесса разработки СЗИ территориально-распределенных ИС, учитывающая необходимые аспекты разработки СЗИ, такие как: ИТ-инфраструктура территориально-распределенных ИС, категории обрабатываемой в ИС информации, перечень актуальных УБИ и уязвимостей, перечень требований по ИБ регуляторов РФ в области обеспечения безопасности информации, перечень средств защиты информации и их стоимость [1]. На основе этих факторов доказано, что эффективность СЗИ зависит именно от них.

В работе были сформированы и решены прямая и обратные задачи построения эффективной СЗИ территориально-распределенных ИС. Разработанный метод позволяет наиболее эффективно и рационально проектировать СЗИ, требует минимальных вычислительных ресурсов, что достигается благодаря оптимальной структуре когнитивной карты построения СЗИ территориально-распределенных ИС. Метод предлагается использовать для разработки СЗИ территориально-распределенных ИС различных видов и назначений, для различных категорий и видов обрабатываемой в ИС информации, классов, уровней защищенности, категорий значимости территориально-распределенных ИС. Необходимым условием для реализации метода является формирование требований по ИБ, определения актуальных УБИ и уязвимостей, а также актуального нарушителя.

Список используемых источников

1. Миняев А. А., Красов А. В., Сахаров Д. В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник СПГУТД. 2020. № 1. С. 29–33.

2. Волкова В. Н., Горелова Г. В., Козлов В. Н. [и др.] Моделирование систем и процессов / под ред. В. Н. Волковой, В. Н. Козлова. М.: Издательство Юрайт, 2015. 449 с.

3. Котенко И. В., Саенко И. Б., Чечулин А. А., Полубелова О. В., Новикова Е. С., Дойникова Е. В., Шоров А. В., Десницкий В. А. Интеллектуальные сервисы защиты информации в критических инфраструктурах. Монография / под ред. И. В. Котенко и И. Б. Саенко. СПб.: Изд-во «BHV», 2019. ISBN 978-5-9775-3968-5.

4. Richard Baskerville. Information systems security design methods: implications for information systems development // ACM Computing Surveys. 1993. Vol. 25. № 4. pp. 375–414.

5. Shelupanov Alexander, Evsyutin Oleg, Konev Anton, Kostyuchenko Evgeniy, Kruchinin Dmitry, Nikiforov Dmitry. Information Security Methods // Modern Research Directions, Symmetry. 2019. 11, 150, pp. 33.

6. Jain A. K.; Ross A.; Pankanti S. Biometric: A Tool for Information Security // IEEE Trans. Inf. Forensics Secur. 2006. 1. pp. 125–144.

7. Будько М. Ю., Миняев А. А. Метод оценки эффективности системы защиты персональных данных // Информатизация и связь. 2016. № 2. С. 85–87.

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

УДК 004.77
ГРНТИ 49.33.29

АНАЛИЗ МЕТОДОВ И ПРОБЛЕМ ПРИМЕНЕНИЯ БПЛА В УМНОМ ГОРОДЕ

А. С. А. Мутханна, Н. А Тагандурдыев

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

До начала развития технологий 5G было практически невозможно создать сеть, в котором поддерживались бы идея массовой межмашинной связи с низкими задержками на ультравысоких скоростях. Реализация этих услуг технологиями 5G открыла возможность для развития идей умного города. Умный город, благодаря технологии 5G и использованию беспилотных летательных аппаратов в качестве телекоммуникационных узлов, может помочь в решении задач мониторинга окружающей среды города, дорожного движения и т.д. Это позволит сделать город максимально безопасным и удобным в управлении и контроле городской среды.

В данной статье производится анализ организации беспилотных летательных аппаратов совместно с технологиями MEC и SDN для реализации концепции умного города. Эта статься иллюстрирует функциональные особенности архитектуры городской сети будущего. Также показываются особенности взаимодействия городских узлов связи с сетевой инфраструктурой.

5G, Интернет Вещей, Умный город, Интернет Вещей, БПЛА.

Введение

В эпоху развития сетей 5G на стадии разработки находятся огромное количество проектов и идей не доступных в предыдущих поколениях мобильных сетей. Концепции умного дома, умного города, умного предприятия, тактильного взаимодействия через Интернет были частью исследований давно, но были либо трудно реализуемы, либо изобретениями из части фантастики. Революция, сопровождаемая технологиями 5G, позволила реализовать три услуги:

- создание сверхширокополосной мобильной связи (Embb);
- создание сверхнадежной связи с низкими задержками (URLLC);
- поддержки массовой межмашинной связи (Mmtc) [1].

Эти услуги и стали основным катализатором дальнейших исследований в области «умных» объектов.

Глобальной целью услуг 5G является развитие телекоммуникационной отрасли для повышения качества жизни людей и упрощение управления жизненными процессами общества. Эта цель достигается и на уровне домов, и на уровне предприятий, и на уровне городов.

Умный город является идеей, улучшающая множество процессов городской среды: оптимизация работы транспортной системы, повышение энергоэффективности и экономии используемых ресурсов, повышение безопасности граждан. Умный город – это город, который стремится достичь целей города будущего за счет использования решений и тенденций в области информационных и коммуникационных технологий (ИКТ). Реализация 5G на основе использования беспилотных летательных аппаратов способна решить поставленные задачи. В следующей главе разбирается роль БПЛА в проектировании «умного» города, а также анализируется архитектурная модель сети, поддерживающая приложения БПЛА совместно с услугами 5G.

Основная часть

БПЛА ранее использовались лишь в военных целях, но в настоящее время они стали широко использоваться и в гражданских отраслях. Перспективной областью применения БПЛА является их использование в «умных городах».

Отчет, подготовленный McKinsey and Company, показывает, что мировые расходы на строительство и инфраструктуру городов составляют около 2 триллионов долларов США в год, а расходы на ИКТ составляют от 1,5 до 2 % от этого числа [4]. В течение ближайшего десятилетия ожидается, что прогресс в области облачных вычислений, беспроводных датчиков, сетевых беспилотных систем, больших данных, открытых данных и Интернета вещей продолжится. Следовательно, ожидается скорая возможность использования БПЛА для решения задач города.

Планируется, что БПЛА при использовании для задач умного города будут выполнять следующие функции:

- Управление движением транспорта. Находящиеся в воздухе дроны могут оценивать состояние дорожного трафика в городах и передавать информацию в телекоммуникационные узлы для последующего использования для приложений управления транспортным потоком. Эта функция позволит практически полностью избавиться от проблем управления трафиком.
- Сбор информации с сенсорных узлов. Благодаря функции БПЛА в качестве мобильного шлюза будет обеспечен мониторинг опасных для здоровья и жизни человека объектов городской инфраструктуры.
- Борьба со стихийными бедствиями и мониторинг ситуации. Возможность съемки высокого разрешения вблизи объектов с небольших высот для применения БПЛА в зонах чрезвычайных ситуаций без риска для жизни и здоровья людей.
- Обеспечение общественной безопасности. Благодаря возможности передачи фотографических изображений в реальном времени БПЛА может

использоваться для преследования целей, ведения поисково-спасательных работ и т. д.

- Перевозка грузов. В скором времени БПЛА могут стать одним из способов доставки малогабаритных грузов, корреспонденции и т. д. [2].

Для эффективного использования БПЛА для приложений умного города необходимо создать сеть, которая обеспечит надежную связь с низкими задержками для огромного количества устройств. В силу огромного количества трафика, которые должны обработать БПЛА, необходимо построить архитектуру на основе локальных вычислений для разгрузки трафика с ядра сети. Это поможет для быстрых вычислений локальных задач, а также для разгрузки трафика с ядра сети. Для оптимизации маршрута трафика для облачных данных необходимо развернуть технологию SDN на всем пути прохождения трафика.

На основе вышеописанных суждений была предложена архитектура (рис.) для оптимального использования БПЛА для задач умного города.

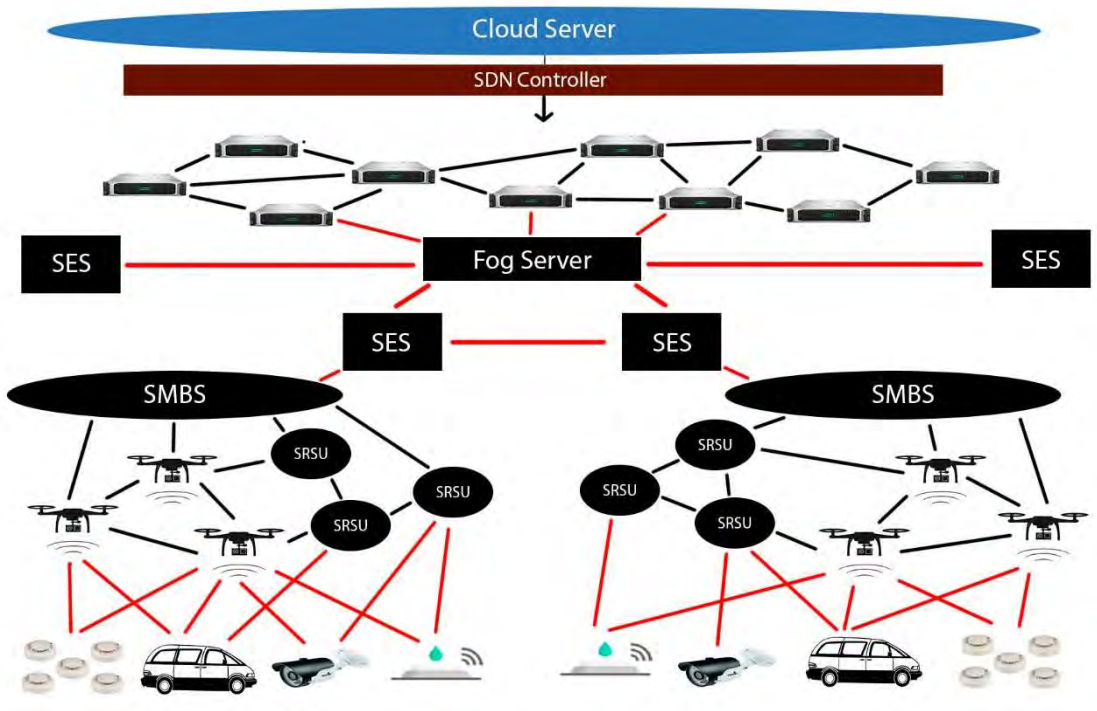


Рис. Архитектура сети умного города на основе БПЛА

Задачи умного города, например, такие как управление движением транспорта, требуют быстрых вычислений с ультранизкими задержками. Эти задачи не смогут быть решены при вычислении всех данных в облачных центрах. Несмотря на огромные вычислительные мощности ЦОД, накладываются большие ограничения на пропускную способность сетей с традиционной архитектурой. Эта проблема становится более актуальной в эпоху развития Интернета Вещей. Поэтому для архитектуры сети умного города

было принято решения использования технологии MEC (*Mobile Edge Computing*), задачей которого является вычисление данных на границе сети. В облаке предлагается обрабатывать данные, не требующие вычислений в реальном времени. Технология MEC организует в предложенной архитектуре 3 уровня вычислений: Cloud Server, Fog Server, Edge Server (SES).

SDN, в свою очередь, благодаря отделению функций управления и физической передачи данных, обеспечивает эффективное распределение нагрузки между узлами сети. SDN применяется в гибридном режиме, то есть реализовывается не только в ядре сети, но и в граничных вычислительных серверах (*Fog Server*, SES, SMBS). При реализации SDN в SMBS и SES, решается задача географической оптимизации БПЛА для разгрузки трафика либо для оперативного применения БПЛА в качестве мобильного шлюза.

Таким образом, исходя из предложенной архитектуры, будет возможно построить сеть, способная решить все задачи умного города.

Конечно, несмотря на огромные преимущества использования БПЛА, существуют огромное количество проблем, препятствующих их реализации. Проблемы БПЛА можно разделить на два направления – юридические и технические проблемы.

К юридическим проблемам относят:

1) Конфиденциальность. БПЛА многими экспертами рассматривается как вторжение в частную жизнь.

2) Стоимость. Развертывание БПЛА – дорогостоящая задача.

3) Лицензирование и законодательство.

К техническим проблемам относят:

1) Промежуточное программное обеспечение БПЛА. ПО необходимое для бесперебойной и правильной работы БПЛА

2) Разработка отказоустойчивых систем. Необходимы системы, гарантирующие высокий уровень безопасности в случае отказа воздушного судна и потери связи между БПЛА и центром управления.

3) Точный полет БПЛА с точки зрения высоты и траектории полета в течение длительных периодов времени при любых погодных условиях, как днем, так и ночью.

4) Разработка механизмов восприятия БПЛА. Эти механизмы необходимы для восприятия окружающей среды, позволяющие БПЛА предпринимать действия по уклонению [3].

Заключение

Умный город является концепцией будущего, которая, бесспорно, улучшит не только качество телекоммуникационных услуг, но и качество жизни в целом. Технологии 5G закладывают огромный потенциал в разнообразие предоставляемых услуг. Конечно, для устойчивого развития таких

услуг требуется пересмотр и поиск более эффективных аналогов к ранее используемым технологиям. Одним из таких аналогов является БПЛА, которое на основе предложенной архитектуры готовы создать основу для безопасного, комфортного и эффективного города будущего.

Список используемых источников

1. Услуги 5G. URL: http://1234g.ru/5g/uslugi-5g, режим доступа: свободный (дата обращения: 25.02.2020).

2. Вырелкин А. Д., Кучерявый А. Е. Использование летательных аппаратов для решения задач «умного города» // Информационные технологии и телекоммуникации. – 2017. Том 5. № 1. С. 105–113.

3. Moohammed, F. UAVs for Smart Cities: Opportunities and Challenges // International Conference on Unmanned Aircraft Systems (ICUAS), Orlando, 2014. pp. 267–273.

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫСОКОЧАСТОТНОЙ СВЯЗИ В СЕТЯХ ЭЛЕКТРОСНАБЖЕНИЯ

М. А. Овчинников

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

Особенности сетей электроснабжения позволяют использовать высокочастотная связь для передачи информации на дальние расстояния напрямую получателям. Однако, физическая незащищённость каналов связи и устаревание техники обеспечения высокочастотной связи снижают защищённость передаваемой безопасность передаваемой информации.

информационная безопасность, высокочастотная связь, сети электроснабжения.

Энергетическая инфраструктура, как один из важнейших компонентов жизнеобеспечения населения, нуждается в постоянной модернизации для соответствия всем современным требованиям к надёжности и безопасности, в том числе и к информационной безопасности.

Для анализа современного состояния системы информационной защиты ВЧ-связи необходимо дать оценки существующих особенностей и уязвимостей, оценки возможностей и целей злоумышленников, а также возможных последствий от действий нарушителей.

Обычно ВЧ-связь организуется по воздушным линиям электропередачи (ЛЭП) с напряжениями от 35 до 1 150 кВ, при этом используются как фазные провода (фазы), так и тросы грозозащиты. Благодаря высокой надежности в сравнении с традиционными системами связи (радиорелейная связь, кабельная связь) ВЧ-связь имеет широкое распространение на территории Российской Федерации. По оценкам ОАО «СО-ЦДУЕЭС РФ» около 20 % информации, необходимой для функционирования систем электропередачи (без учета сигналов РЗ и ПА), передаётся при помощи системы ВЧ-связи [1]. Также несомненным преимуществом данного вида связи можно назвать небольшие материальные затраты на создание и поддержание работоспособности данной системы, что связано с такими факторами как:

– линия электропередачи обычно является кратчайшим путем между точками связи;

– минимизируются затраты на расчистку трассы линии связи, а также на установку передающего оборудования (среды передачи сигналов);

– отсутствие организационных сложностей при создании новых каналов связи, а также при изменении структуры системы передачи.

Тем не менее, данная система связи имеет ряд уникальных особенностей, затрудняющих эксплуатацию системы. К ним можно отнести:

– разветвленность линий;

– постоянное изменение структуры сети;

– зависимость от погодных условий, времени года и суток;

– наличие высокого напряжения низкой частоты.

Разветвленность линий характеризуется наличием ответвлений к другим подстанциям на трассе линии. Такие ответвления поглощают часть энергии сигнала и нарушают равномерность частотной характеристики канала связи, что негативно сказывается на его пропускной способности.

Структура энергоснабжения имеет изменчивую структуру, что связано с подключениями новых потребителей, оптимизацией структуры сети и отключением неактуальных потребителей. В таких условиях очень сложно реализовать высокую степень защищенности передаваемой информации, так как изменчивость сети усложняет контроль за защищённостью информации и затрудняет адресацию информации в системе связи.

Высокая степень разветвлённости имеет негативный характер – сигналы ВЧ-связи распространяются по всей разветвленной линии, что означает возможный доступ к ним из точки, не лежащей на пути прямого прохождения сигнала между пунктами отправки и приёма, что облегчает нарушение безопасности передаваемой информации. Ситуация усугубляется постоянным изменением структуры сети – в условиях постоянного добавления новых точек приёмопередачи информации и удаления неактуальных затрудняется учет действий диспетчеров и автоматических систем

реагирования, а также контроль за обеспечением конфиденциальности передаваемой информации.

Разветвленность также зависит от напряжения линии электропередачи. Так, например, линии с напряжением 35–110 кВ являются основными для передачи электроэнергии на расстояния порядка 80–100 км, а линии с напряжением 330 кВ и более играют роль магистральных ЛЭП. Поэтому, при анализе уязвимостей информационной безопасности ВЧ-связи на каждой конкретной линии электропередачи необходимо учитывать особенности данной линии – напряжение, протяженность по трассе, географическое расположение и т. д.

В связи с тем, что среда передачи в системе ВЧ-связи является совместной со средой передачи электроэнергии в сети энергообеспечения, то она подвержена тем же зависимостям от времени суток, года и от условий погоды на трассе линии. Основным влияющим параметром является температура окружающей среды, которая может колебаться в значительных пределах в небольшие промежутки времени, что сказывается на пропускной способности канала связи. Таким же образом влияют и метеорологические условия – снегопад, град или дождь могут вызвать кратковременные короткие замыкания, которые приводят к мощным импульсным шумам. Вероятность подобных дополнительных помех увеличивается с ростом длины трассы ЛЭП. Дополнительными помехами можно назвать волны помех, возникающие в моменты оперативного переключения оборудования, а также возникновение электрических разрядов в воздухе и на поверхностях изоляторов (помехи типа «корона»). Эти обстоятельства приводят к тому, что каналы связи не обеспечивают постоянной скорости передачи на выделенной частоте.

Обеспечение возможности своевременной передачи информации оконечным оборудованием связи обеспечивается постоянным аудитом качества передачи информации и, при необходимости, агрегацией нескольких каналов передачи в один канал связи для передачи необходимой информации. Для быстрой агрегации каналов при постоянно меняющихся технических характеристиках среды передачи данных на сегодняшний день применяется широкочастотное оборудование, способное перестраиваться в кратчайшие промежутки времени и агрегировать каналы, расположенные в случайном порядке на частотном диапазоне. Также находят применение микропроцессорные системы, основанные на пакетном способе передачи данных. Применение микропроцессорных систем позволяет применять программные методы защиты информации, но, в связи с их небольшой распространённостью, значительная часть информации передается аналоговыми способами, программная защита которых значительно сложнее. Необходимо отметить, что на сегодняшний день в сетях электропередачи можно видеть множество различного оборудования, принципы работы которого

основаны на различных технологиях. Несмотря на то, что в системе ВЧ-связи наблюдается переход к цифровым методам передачи, на большей части России можно наблюдать аналоговое оборудование.

Необходимо заметить, что наличие высокого напряжения повышает требования к оборудованию связи и усложняет его эксплуатацию. Так, например, для ремонта и контроля оборудования необходимо отключение ЛЭП, что в некоторых ситуациях невозможно, что также повышает требования к надежности оборудования ЛЭП, в том числе и оборудования ВЧ-связи.

Таким образом, ВЧ-связь обладает уникальными параметрами, затрудняющих применение ряда средств обеспечения информационной безопасности, например, программные средства или готовые решения, применяемые для обеспечения защиты информации в компьютерных сетях. Исходя из этого выглядит оптимальным разработка нового оборудования и программного обеспечения для работы в системе ВЧ-связи, но основанные на современных достижениях науки и техники.

При анализе системы обеспечения информационной безопасности в сетях ВЧ-связи предполагается, что злоумышленник относится к одной из следующих групп:

– террористические организации;
– службы иностранных разведок;
– коммерческие организации в рамках конкурентной борьбы.

Террористические организации имеют значительные материальные и технические средства для нанесения ущерба. Основной целью нарушения работы системы ВЧ-связи для данной категории является создание аварийных ситуаций, например, введение оборудования в нестандартные режимы функционирования или отключение телеизмерений и телеуправления на удаленном оборудовании. В целом, данную категорию злоумышленников можно характеризовать как одну из самых опасных, так как они преследуют цель разрушения инфраструктуры энергообеспечения.

Службы иностранных разведок также можно охарактеризовать значительными материально-техническими ресурсами. Но, в отличие от террористических организаций, целью иностранных разведок чаще становится сбор информации, то есть в первую очередь подвергается угрозе конфиденциальность информации. Также значительную роль играет нарушение доступности информации как один из методов скрытия присутствия нарушителя в системе связи.

К коммерческим организациям можно отнести российские и иностранные фирмы, интерес нарушения информационной безопасности ВЧ-связи которых состоит в получении технологического и экономического преимущества для приобретения неких прибылей. В целом, данная категория уни-

кальна тем, что целевой информацией для атаки является данные междиспетчерского обмена, а не данные о структуре и состоянии системы энергообеспечения. Также можно утверждать, что данная категория постепенно теряет свою актуальность, поскольку обмен целевыми данными постепенно переходит в другие системы связи (спутниковые системы, ВОЛС, радиорелейная связь).

Таким образом, интерес к нарушения информационной безопасности ВЧ-связи имеют различные группы злоумышленников, каждая из которых имеет свои особенности и возможности, а также свою целевую информацию, на нарушение безопасности которой будет направлена преступная деятельность этой категории.

Для анализа современного состояния ВЧ-системы передачи информации рассмотрим передаваемую в сети ВЧ-связи информацию. На сегодняшний день узлы системы энергопередачи обмениваются следующими видами информации [2]:

- Телефония – для обеспечения диспетчерского оперативного управления и телефонной связи общего пользования.
- Данные телемеханики (телеметрия, телеизмерения, телеуправление).
- Данные систем АСКУЭ, СДКСБ (SCADA), электронная почта.
- Сигналы системы РЗА (Релейной защиты и противоаварийной автоматики).

Вся информация, передаваемая через систему ВЧ-связи, разделена на 2 группы – информация системы РЗА и информация междиспетчерского обмена, включающая в себя все остальные типы передаваемых данных.

Информация системы РЗА характеризуется высочайшим приоритетом в передаче, периодическим обменом сообщениями в нормальном режиме функционирования сети электропередачи, и значительными объёмами передаваемой информации во время срабатывания система автоматической защиты. Информация РЗА представляет собой данные об автоматических противоаварийных действиях оборудования в сети (с целью предотвращения и ликвидации аварийных ситуаций), данные об оптимальном режиме работы сети (автоматический выбор режима генерации электроэнергии и ее передачи) и другие.

Информация междиспетчерского обмена включает в себя всю остальную передаваемую информацию и имеет более низкий приоритет в целом. Эта информация характеризуется постоянно изменяющимися объёмами и маршрутами передачи, а также различными требованиями к надёжности и скорости передачи в канале связи. Данная категория информации включает в себя данные, необходимые для обеспечения работы системы энергообеспечения, и данные, которые могут быть переданы при помощи других систем связи. На сегодняшний день часть междиспетчерских данных передается с помощью иных систем связи (в частности, радиорелейные системы

и ВОЛС), но даже в таком случае информация обычно дублируется в системе ВЧ-связи. То есть переход на иные системы передачи данных не исключает системы ВЧ-связи, которая в таких условиях становится резервно-аварийной.

Таким образом, к критически важной информации можно отнести:

– информация, отражающая состояние устройств и оборудования, принимающего участие в процессе передачи электроэнергии;

– управляющая информация, обеспечивающая управление устройствами и оборудованием;

– техническая информация оборудования и сети электропередачи (структура и характеристики построения, информация о недопустимых режимах функционирования);

– информация диспетчерской телефонии (связь диспетчера с выездными бригадами сотрудников).

Рассмотрим выявленные особенности на примере реальной линии электропередачи. В качестве рассматриваемой линии выбрана линии 500 кВ Звезда-Вятка протяженностью около 325 км. Линия проходит по двум регионам – Кировской и Костромской областям и связывает г. Киров и пос. Мантурово. В целом, данная линия является секцией ЛЭП, связывающей Воткинскую ГЭС (г. Ижевск) и Костромскую ГРЭС (г. Кострома). Линия является самой северной из 4 линий электропередач напряжением 500 кВ и более, связывающей европейскую часть России и Уральский Федеральный округ. На территории обслуживания данного отрезка (Кировская область и восточная часть Костромской области) проживает около 1,6 млн чел. Исходя из этого, обеспечение защиты данной линии является одной из приоритетных задач в области информационной безопасности.

Большая часть трассы линии проходит недалеко от автомобильной дороги, связывающей Киров и Кострому, но тем не менее линия по большей части закрыта лесными массивами от вида с дороги что облегчает подключение к ней злоумышленников с использованием специального оборудования, средств защиты и прочего.

Данный отрезок ЛЭП является частью Единой Энергетической Системы Российской Федерации (ЕЭС РФ), и связывает центральные регионы России (по большей части генерирующие электроэнергию), и регионы Уральского федерального округа (мощные потребители в лице промышленных предприятий). Благодаря такому стратегическому расположению, нарушение работы линии повлечет за собой последствия как на генерирующих электроэнергию предприятиях, так и на производственно-обрабатывающих.

Из-за особенностей передачи информации в системе ВЧ-связи злоумышленники могут получить доступ к конфиденциальной информации и нарушить работу не только на данной линии, но и на других участках ЕЭС

РФ, причем точное местоположение злоумышленника не будет установлено. То есть, данная линия из-за своей большой протяженности по трассе и малым числом просматриваемых участков представляет собой удобное для внедрения злоумышленника структурный элемент.

Данная линия имеет структуру типа «точка-точка», то есть не является разветвленной, также линия является достаточно стабильной с точки зрения добавления новых потребителей, поэтому подключение к данной линии не позволит нарушить работу большого числа оборудования, принадлежащего к данной ЛЭП.

Для террористических организаций нарушение работы данной линии не представляет значимого интереса, так как система электроснабжения России имеет значительный аварийно-резервный потенциал. Но данная ЛЭП может интересовать террористов как место для подключения и нарушения работы других элементов ЕЭС РФ, например, нарушение работы Воткинской ГЭС как ближайшего электрогенерирующего предприятия.

Для иностранных разведок может представлять интерес информация о транзите электроэнергии, о составе и территориальной структуре энергозависимых потребителей. Для данной категории выбранная ЛЭП также представляет собой интерес как место для незаметного подключения к ЕЭС РФ, причем с удобным расположением – злоумышленники получат доступ к энергосетям Центра, Средней Волги и Урала одновременно.

Для конкурирующих фирм данная линия представляет интерес, как один из источников информации о внутренних решениях компании на самом высоком уровне. Поскольку данная информация обычно передается по магистральным сетям связи общего пользования (сети Интернет), а в системе ВЧ-связи носит дублирующий характер, то, учитывая гораздо более слабую защищенность систем ВЧ-связи, атака на данной линии актуальнее атаки на линии связи сети Интернет.

Исходя из анализа особенностей системы передачи данных по ЛЭП можно выявить следующие проблемы обеспечения информационной безопасности:

- Злоумышленники могут получить доступ к информации используя временные точки доступа (например, обеспечение электроэнергией строительства) или на трассе ЛЭП в условиях низкой просматриваемости линии.
- Управляющая информация может передаваться на значительные расстояния и управлять работой оборудования, находящегося на расстоянии в тысячи километров.
- Большое разнообразие применяемого оборудования затрудняет поиск и ликвидацию уязвимостей и программно-аппаратных закладок в нем.
- Большое число устаревшего оборудования, соответствующего техническим требованиям ГОСТ, но не соответствующего требованиям, касающихся информационной безопасности.

•В условиях высоких внутриканальных помех и, как следствие, низкой пропускной способности, затруднено применение классических алгоритмов обеспечения информационной безопасности.

Для устранения выявленных проблем в области информационной безопасности автором статьи предлагаются следующие пути решения:

•Сегментирование сети на логические сектора, разделенные между собой средствами защиты.

•Запрет на удаленное выполнение кода и изменения конфигурации устройств, исходящих из соседних сегментов.

•Обеспечение двусторонней аутентификации на длинных по протяженности линиях электропередачи.

•Разработка специализированных протоколов передачи информации для ВЧ-связи с обеспечением криптографической защиты.

•Создание современного оконечного оборудования связи с применением современных аппаратно-программных решений в области информационной безопасности.

•Физическое разделение сигналов постоянных элементов сети и временных в устройствах связи.

•Отказ от передачи в системе ВЧ-связи информации междиспетчерского обмена, которая может быть передана другими способами с обеспечением более высокого уровня защищенности данных.

Список используемых источников

1. Дубровин В. С., Мариниченко А. А. Модернизация системы передачи данных по ЛЭП на участке «Рузаевка-Арзамас» // Электроника и информационные технологии. 2009. № 2 (7).

2. Глушко С. И., Брауде Л. И., Скитальцев В. С., Шкарин Ю. П. Концепция развития ВЧ-связи в электроэнергетике России // ФСК «ЕЭС» - 2003.

Статья представлена преподавателем кафедры 31 ВАС, кандидатом технических наук Ф. А. Скориком.

УДК 004.021
ГРНТИ 50.41.25

МЕХАНИЗМЫ ОБРАБОТКИ ОШИБОК НА ПЛАТФОРМЕ 1С:ПРЕДПРИЯТИЕ 8

Д. В. Окунева, А. В. Полянская

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

В статье приводятся возможности платформы 1С:Предприятие 8 по поиску, обработке и анализу ошибок.

Во время работы с системой 1С:Предприятие 8 пользователи часто сталкиваются с ошибками, не понимая причин возникновения и способов их решения, обращаются к специалистам технической поддержки и ожидают устранения ошибки. Этот процесс занимает много времени как у специалистов технической поддержки, так и у самих пользователей.

Анализ существующих механизмов обработки ошибок повысит скорость и качество процесса устранения проблемных моментов, существенно сократив время ожидания пользователя, позволит снизить «время простоя» в рабочем графике предприятия.

1С:Предприятия, поиск ошибок, обработка ошибок, анализ ошибок, целевая группа, категории ошибок, обработчик ошибок, отчёт об ошибках.

1С:Предприятие 8 – это универсальная система автоматизации экономической и организационной деятельности предприятия. Система 1С:Предприятие 8 может адаптироваться к особенностям конкретной области деятельности, в которой она применяется [1]. Многопрофильность и индивидуальные решения, открытый программный код – все это делает систему 1С:Предприятие универсальным конструктором, который можно собрать и оптимизировать под деятельность предприятия.

Указанные преимущества программных продуктов, предлагаемых компанией 1С, позволяют пользователям автоматизировать учетный процесс, координировать деятельность сотрудников, структурировать бизнес-процессы и, соответственно, повысить эффективность деятельности предприятия.

Как и в любой сложной системе, иногда при работе с программными продуктами 1С: Предприятие 8 возникают ошибки, с которыми обычный пользователь не может справиться, так как не понимает причины возникновения данной ошибки, это затрудняет работу пользователя с платформой и, как следствие, снижается производительность деятельности предприятия.

Для решения этой проблемы фирма 1С выделила несколько целевых групп, работающих с программными продуктами, и каждой из них предоставила различные возможности для ознакомления и обработки появляющихся ошибок.

Первая целевая группа – конечные пользователи, и они могут получать от системы различные подсказки и рекомендации по исправлению ошибок, если, конечно, пользователь имеет соответствующие права и знания для устранения данных ошибок. Также для первой выделенной целевой группы предусмотрена возможность предоставления пользователю понятного в использовании функционала для сообщения о возникшей ошибке специалистам технической поддержки.

Второй целевой группой являются прикладные разработчики, имеющие возможность пользоваться необходимым функционалом для обработки ошибок, возникающих в системе, и для отображения пользователям различной полезной информации.

ИТ-отделы компаний клиентов и компании, занимающиеся внедрением продуктов, объединяются в третью целевую группу. Для них предусмотрена возможность быстрого получения информации об ошибках, а также возможность информирования пользователей о том, куда именно необходимо обращаться для устранения ошибок.

Стоит отметить, что ошибки были разделены на несколько категорий:

- нарушение прав доступа;
- ошибка доступа к локальному файлу;
- ошибка сети;
- ошибка работы с принтером;
- ошибка компиляции встроенного языка;
- ошибка во время выполнения встроенного языка;
- ошибка использования встроенного языка;
- исключение, вызванное из встроенного языка;
- ошибка системы взаимодействия;
- ошибка настроек компоновки данных;
- ошибка сеанса;
- ошибка хранимых данных;
- прочая ошибка.

Такое разделение на тринадцать категорий может быть полезным для каждой целевой группы. Для конечных пользователей был изменен внешний вид окна, на котором отображается сообщение об ошибке, исходя из категории ошибки, появляется та или иная форма с необходимой информацией.

Для удобства разработки программных модулей в платформу был добавлен новый обработчик «ОбработкаОтображенияОшибки». Данный обработчик будет вызываться перед тем, как пользователю отобразиться окно

ошибки с соответствующей информацией. Одна ошибка может принадлежать сразу к нескольким категориям. У разработчиков появились новые возможности для реализации программных модулей. К примеру, основываясь на категории ошибки, можно изменять текстовую информацию об ошибке и окно, в которой отображается ошибка пользователям системы. Еще одной возможностью платформы можно выделить отправку данных о проблеме на сервис технической поддержки.

Важная особенность системы 1С: Предприятие 8 заключается в том, она является открытой системой и предоставляет возможности для интеграции почти с любым внешним программным продуктом и оборудованием на основе общепризнанных открытых стандартов и протоколов передачи данных. Платформа 1С:Предприятие 8 содержит решения, с помощью которых можно: создавать, обрабатывать и обмениваться данными различных форматов, поддерживать различные протоколы обмена. Решение разработчика об использовании программных средств должно приниматься, исходя из конкретной решаемой задачи. Такой подход обеспечивает гибкость механизмов обмена данными и их применение для решения как можно большего количества задач [2].

Платформа также позволяет сформировать отчёт об ошибке, это можно сделать как программно, а именно путем добавления в отчёт необходимых объектов и вложений, так и интерактивно, нажав на форме ошибки команду «Сформировать отчет для техподдержки». В адрес сервиса регистрации ошибок (на форме «Управление настройками ошибок») можно указать адрес сервиса технической поддержки и отправлять отчеты на заданный сервис. Сервисом регистрации ошибок является внешний компонент, состоящий из набора HTTP-сервисов. В системе также существует функционал, позволяющий сохранить сформированный отчет на жесткий диск.

Помимо этого, можно декларативно, без использования программного кода, настроить текст сообщения об ошибке, исходя из категории данной ошибки. Данную настройку может произвести специалист по внедрению или администратор информационной базы. Также они могут добавить в сообщения об ошибке специальную информацию для определенного внедрения или этапа работы. Такой информацией могут быть номера телефонов, имена сотрудников и другое.

Пользователь, столкнувшись с проблемой, может теперь не формировать заявку в системе технической поддержки, а создать отчёт о проблеме в самой информационной базе и ожидать ответа для дальнейшего самостоятельного устранения ошибки.

Отчет об ошибке, сформированный пользователем, при помощи http-сервиса и сервера IIS или Apache будет отправляться в специально созданную информационную базу для обработки ошибок и хранения готовых решений тех или иных проблем. Отчёт передается в виде файла с расширением

.json. Так же можно воспользоваться web – сервисом и передавать данные при помощи XDTO - пакетов. В эту информационную базу вся необходимая информация будет поступать из отчета, и на его основе будет формироваться ответ пользователю, в котором будут написаны рекомендации по устранению ошибки. Рекомендации будут браться из хранилища готовых решений, которое есть в информационной базе. Ответ отправляется пользователю в ту конфигурацию, в которой произошла ошибка.

Основная трудность в реализации данной системы может состоять лишь в корректном создании внешней информационной базы, обрабатывающей ошибки и хранящей готовые решения для формирования ответа пользователю. От того, насколько верно и быстро анализируется ошибка в этой информационной базе, будет зависеть качество работы всей реализованной системы в целом. Важно правильно выбрать механизмы для вывода необходимого решения пользователю, этими механизмами могут быть как простые запросы, так и обученная нейронная сеть.

Подводя итоги, можно говорить о том, что разделение на целевые группы, выделение тринадцати категорий ошибок и создание нового механизма для оформления отчёта об ошибках дают много возможностей в использовании платформы 1С:Предприятие 8.

Список используемых источников

1. Родченко М. Г., Хрусталева Е. Ю. 1С: Предприятие 8.3 Практическое пособие разработчика. Примеры и типовые приемы. М.: 1С-Паблишинг, 2013. 13 с. ISBN 978-5-9677-2041-3.

2. Габец А. П., Гончаров Д. И., Козырев Д. В., Кухлевский Д. С., Радченко М. Г. Профессиональная разработка в системе 1С: Предприятие 8. М.: 1С-Паблишинг, 2006. 19 с. ISBN 5-9677-0268-7.

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ

И. Б. Паращук[1], **Е. В. Федорченко**[1, 2]

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

В статье представлен обобщенный обзор методов теории нечетких множеств с точки зрения их возможного применения для решения частных задач анализа эффективности системы управления информационной безопасностью индустриального Интернета вещей. Рассмотрено применение нечетких методов, снижающих уровень неопределенности при формулировке целевых интегральных метрик, которые должны отвечать на вопросы оценки защищенности и при выборе защитных мер противодействия угрозам. Даны рекомендации по практическому применению рассмотренных методов.

индустриальный Интернет вещей, нечеткие множества, защищенность, модель, эффективность, информационная безопасность, система управления, метрика.

Киберфизические системы с каждым годом завоевывают все большую популярность в мире. Одним из важных направлений развития киферфизических систем являются современные IT-инфраструктуры, внедряемые в производство и называемые индустриальным Интернетом или индустриальным Интернетом вещей (ИИВ). Это комплексные программно-аппаратные промышленные системы, обеспечивающие эффективное взаимодействие объектов (вещей), машин, компьютеров и человека. Они обеспечивают интеллектуальные производственные процессы с использованием анализа данных для получения новых качественных результатов индустриальных операций [1].

Иными словами, под ИИВ понимается система, которая связывает и интегрирует подсистемы промышленного управления с корпоративными подсистемами, бизнес-процессами и бизнес-аналитикой. Причем такие индустриальные системы являются большими и сложными объектами управления и включают множество сенсоров и исполнительных механизмов.

Сложность, многогранность и большое разнообразие разнородных взаимодействующих компонентов ИИВ обуславливает объективное существование проблем защиты объектов такого класса и проблем разработки систем управления (СУ) информационной безопасностью (ИБ) ИИВ [2].

Эти проблемы решаются путем исследований в рамках ряда частных подзадач: формирование множества объектов анализа эффективности СУ ИБ и характеристик ИИВ; анализ журналов событий объектов ИИВ и существующих средств мониторинга безопасности ИИВ; идентификация источников входных данных безопасности; синтез множества иерархически связанных метрик безопасности (показателей защищенности), позволяющих оценивать эффективность СУ ИБ ИИВ; анализ онтологий метрик безопасности ИИВ в интересах оценивания защищенности системы. Для решения этих подзадач использовался ряд методов (классификации, теоретического и системного анализа, статистического и семантического анализа, логического вывода и интеллектуального анализа данных) [3].

Однако ключевой, объединяющей целевой задачей продолжает оставаться разработка методов и средств достоверного и оперативного анализа эффективности СУ ИБ ИИВ. В общем случае анализ эффективности сложных технологических систем и комплексов, включая СУ ИБ индустриального Интернета вещей, представляет собой процедуру принятия решения о качестве данных объектов и степени (уровне) достижения цели их функционирования. Оценивание эффективности возможно только в замкнутой схеме, когда к показателям качества и эффективности СУ ИБ ИИВ предъявлены требования. При этом наряду с количественным, возможен и качественный анализ эффективности, когда условия оценивания и исходные данные обладают высокой неопределенностью. Под этим обычно понимают процедуру принятия решения по двоичной схеме, когда реализуется процедура выбора одной из двух альтернатив: годен – негоден [4].

Вместе с тем, практический опыт показывает, что такой качественный анализ эффективности сложных управляемых информационно-производственных и высокотехнологичных систем должен быть более гибким и двоичная схема оценивания для этих случаев неприемлема, примитивна и не информативна. В этом случае могут помочь, так называемые, нечеткие оценки качественных показателей эффективности, которые принимают значения в рамках множества лингвистических переменных типа возрастающей последовательности: отвратительный – плохой – удовлетворительный – хороший – отличный. Степень соответствия тому или иному значению лингвистических переменных определяется в рамках методов теории нечетких множеств с помощью функций принадлежности [4].

Очевидно, что за каждой такой лингвистической переменной, за каждой нечеткой качественной оценкой скрыты количественные показатели,

характеризующие эффективность объекта (степень достижения цели). Таким образом, можно исследовать как качественные характеристики количественной меры эффективности сложных систем, так и количественные характеристики качественной меры.

В случаях, подобных нашим исследованиям, когда оцениваемые объекты, в частности СУ ИБ ИИВ, или их характеристики, зачастую субъективны и получить требуемые данные о них путем объективных измерений затруднительно или вовсе невозможно, определение численных значений функций принадлежности нечетких множеств в интересах выбора метрик защищенности и анализа эффективности систем такого класса осуществляется путем экспертного оценивания. Экспертное оценивание представляет собой комплекс организационных, логических и математических процедур, направленных на получение от специалистов-экспертов информации, ее анализ и обобщение с целью выбора рациональных решений.

Рассмотрим некоторые наиболее существенные аспекты анализа эффективности системы управления информационной безопасностью индустриального Интернета вещей с использованием аппарата нечетких множеств. В общем случае по каналам наблюдения, образуемым в интересах СУ ИБ, могут передаваться различные виды информации, необходимой для контроля защищенности ИИВ. Эти каналы диагностики ИБ, каналы сбора данных, как и базовые каналы информационного обмена ИИВ, могут быть подвержены несанкционированному вмешательству, а данные, передаваемые по ним – модификации. Несанкционированное вмешательство в процесс передачи информации в интересах анализа защищенности и, в конечном итоге, в интересах управления ИБ ИИВ, возможно на любом этапе, но в разной степени для каждого конкретного датчика, участка инфраструктуры ИИВ или способа передачи. Причем оценить количественно степень мешающего воздействия при использовании каждого сенсора, элемента инфраструктуры ИИВ или способа передачи информации довольно сложно. Трудность решения этой задачи заключается в том, что возникает неопределенность нестохастического характера, определяемая:

– недостаточной изученностью некоторых явлений, сопровождающих процесс функционирования СУ ИБ ИИВ (природная неопределенность);

– возможным наличием целенаправленного вмешательства со стороны противоборствующей системы (нарушителя), способы действия которой неизвестны исследователю (поведенческая неопределенность);

– зачастую нечеткого представления цели операции (например, целевых интегральных метрик, которые должны отвечать на вопросы оценки защищенности и выбора защитных мер), приводящего к неоднозначной трактовке соответствия реального результата функционирования СУ ИБ ИИВ требуемому (целевая неопределенность).

Эти неопределенности нестохастического характера могут быть аналитически учтены путем задания нечетких соответствий, связывающих метрики, онтологии и показатели защищенности ИИВ, что позволит свести задачу анализа эффективности функционирования СУ ИБ системы к относительно несложным математическим операциям.

Так, представляя нечеткие отношения, связывающие метрики, онтологии и множество показателей защищенности ИИВ в форме нечетких графов, получаем возможность сформулировать и построить адекватные математические модели процесса функционирования СУ ИБ ИИВ. Модели, в которых связь между объектами, средствами и процессами является нечеткой (например, из-за участия в процессе функционирования СУ ИБ ИИВ людей, из-за невозможности учета ряда факторов ввиду большой размерности и сложности процессов).

Важен и потенциально полезен вклад нечетких множеств в процедуры оценивания объектов в частных задачах многокритериального выбора методик оценки защищенности и защитных мер. Нечеткий подход к решению этих задач заключается в выражении общей цели функционирования СУ ИБ ИИВ в виде иерархии подцелей, где на нижнем уровне иерархии находятся частные цели, связываемые с элементарными критериями, которые позволяют оценить объекты из заданного множества. При этом для оценки методик оценки защищенности и защитных мер осуществляется операция свертки над нечеткими множествами, объединяющими частные цели.

В задачах такого типа могут быть применены четыре класса операций свертки, а именно: классы операций пересечения, объединения, осреднения и симметричного суммирования. В результате свертки получаем нечеткое число, тогда среди выбранных объектов (методик оценки защищенности и защитных мер) одни будут более вероятны (заслуживать большего доверия), чем другие. В итоге получим нечеткое множество объектов (методик оценки защищенности и защитных мер), которое при использовании принципа обобщения, обеспечит нечеткие оценки защищенности.

Таким образом, существует ряд конкретных практических задач, где методы теории нечетких множеств позволяют устранить либо корректно учесть неопределенность в вопросах выбора и принятия решений по управлению сложными технологическими процессами и системами. А сочетание методов теории нечетких множеств и методов теории случайных процессов позволит математически описать процессы почти любой сложности и использовать полученные описания при решении разнообразных прикладных задач анализа.

Работа выполнена при финансовой поддержке РФФИ (проект 19-07-01246) в СПИИРАН.

Список используемых источников

1. Страшун Ю. П. Технические средства автоматизации и управления на основе IIoT/IoT. Учебное пособие. М.: Лань, 2020. 76 с.
2. European Union Agency for Cybersecurity (ENISA). Good practices for Security of Internet of Things in the context of Smart Manufacturing. 2018. P. 11.
3. Дойникова Е. В. Классификация и анализ целей кибератак в системах Индустриального Интернета вещей // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2019 г.: Материалы конференции. СПб.: СПОИСУ, 2019. 596 с., С. 116–117.
4. Паращук И. Б., Бобрик И. П. Нечеткие множества в задачах анализа сетей связи. СПб.: ВУС, 2001. 80 с.

УДК 004.056.2
ГРНТИ 20.53.23

АТАКИ НА БЕСПРОВОДНЫЕ СЕТИ И ИХ ОБНАРУЖЕНИЕ

Р. Б. Петрив, Д. Д. Стародубова, Р. Д. Стародубов

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

На сегодняшний день вопросы безопасности беспроводных сетей являются актуальными в силу их повсеместного распространения. Безопасность беспроводных систем заключается в предотвращении несанкционированного доступа или нанесения вреда компьютерам со стороны злоумышленников. Риски, связанные с использованием сетей WLAN, колеблются от прослушивания до нацеленных внутренних атак, а также атак, направленных на внешние сайты.

информационная безопасность, Wi-Fi сети, беспроводные сети.

Беспроводные сети стали неотъемлемой частью нашей деятельности. Они упрощают многие процессы, практичны и быстры, однако, другой стороны, не секрет, что беспроводные сети более уязвимы для атак и злоумышленников. Акты проникновения и вторжения, известные как атаки на беспроводные сети, нацеленные на беспроводные сети, являются серьезными угрозами. В виду перечисленных причин, необходимо знать о видах атак и их последствиях в целях дальнейшего предотвращения и уменьшения их воздействия.

Атаки на беспроводные сети направлены на захват информации, передаваемой по сети, и вторжение в информационный трафик.

В работе [1] представлен обзор протоколов беспроводной безопасности, где подробно рассмотрены типы протоколов безопасности WiFi и уязвимости. В [2] представлены уязвимости беспроводных протоколов и возможности, доступные для в настоящее время хакерам для осуществления атак. Обзор различных подходов к обнаружению аномалий приведен в работах [3-5]. Различные методы и методики, предлагаемые для обнаружения аномалий, указывают на трудности обнаружения аномалий сетевого трафика.

Рассмотрим наиболее популярные атаки.Атаки типа – человек по середине. Как правило, атаки вида «человек посредине» делятся на два вида: подслушивание и манипуляция. Во время прослушивания, злоумышленник прослушивает некий набор передач между различными хостами, важно, чтобы в это время компьютер злоумышленника не являлся одной из сторон в соединения. Атаки манипуляции используют возможность прослушивания, а также захвата данных с целью дальнейшеймодификации его содержимого.

Одними из популярных среди злоумышленников атак сталиспуфинг-атаки. Данный вид атак представляет собой сетевые атаки, где один участник маскируется под другого. Чаще всего спуфинг-атаки нацелены на вынуждение жертвы отправлять трафик не напрямую легитимному получателю, а атакующему, ретранслирущему трафик дальше. В случае IP-спуфинга преследуется цель убедить жертву, что трафик приходит от легитимного отправителя и принять или хотя бы просто пропустить его.

Другим популярным видам атак на беспроводные сети являются атаки вида – отказ в обслуживании. Целью любой атаки данного вида является создание помех для пользователя при подключении к сетевым ресурсам. из-за путей по которым различные уровни OSI стека взаимодействуют между собой. Беспроводные системы особенно восприимчивы к DDoS атакам. Наиболее часто применяемыми способами нападения на канальный уровень является управление разнесенными антеннами. Другой наиболее частой проблемой на канальном уровне беспроводных сетей является спуфинг точек доступа, в том числе с WEP аутентификацией. Сторона клиента как правило настраивается таким образом, чтобы связываться с точкой доступа с наиболее сильным сигналом, в свою очередь атакующий может подделать SSID точки доступа и клиенты подключаться к ней автоматически.

Так же наиболее часто встречающимися атаками являются нападения на нарушение трех главных аспектов информационной безопасности – атаки на конфиденциальность, целостность и доступность.

Атаки на конфиденциальность направлены на перехват личной информации, передающейся по беспроводной сети в открытом или зашифрованном виде, с помощью 802.11 либо протоколов верхнего уровня. Атаки на неприкосновенность (на целостность). Данный вид атак посылает

фреймы ложного контроля, управления или содержащие в себе данные провоцирующие сбои на стороне получателя, или применяются для облегчения проведения другого вида атак. Атаки на аутентификацию осуществляются с целью кражи личных данных, а также полномочий, для дальнейшего доступа к другим сервисам и частным сетям.

Проведя анализ существующих методов обнаружения атак в беспроводных сетях можно отметить, что наиболее актуальными средствами детектирования являются системы обнаружения атак. Однако, в настоящее время в связи с широкими возможностями методов интеллектуального анализа данных, проблему детектирования на предмет наличия признаков атаки можно решить, используя данные методы. В силу того, что системы обнаружения беспроводных атак являются молодым видов средств защиты, функции и подходы к их реализации у довольно серьезно разнятся. Несмотря на это, важно отметить следующие задачи, которые находят решение с их помощью: создание карты беспроводной сети, учет сетевых устройств, диагностика пропускной способности беспроводной сети, контроль политик безопасности, детектирование уязвимостей конфигурации, обнаружение и противодействие атакам в беспроводных сетях и другие.

Методы обнаружения атак делятся на интеллектуальные и поведенческие. Поведенческие методы основаны на информации о поведении сканируемой сети, в свою очередь, в основе интеллектуальных методовзаложенаинформация о самих атаках. Мониторинг системы и последующий анализ ее состояния на наличие аномалий может проводиться как статически в виде «снимка» среды, так и динамически в режиме реального времени. Интеллектуальные системы детектирования атак содержат в себе механизмы выявления популярных атаквместо шаблона о состоянии сети, однако, они могут не справиться с их модификациями, если заранее они не будут добавлены в базу. Довольно часто организацияподобных систем требует внедрения нейронных сетей или машинного обучения. Нейронные сети используют большое количество разных алгоритмов обучения, преобразовывая исходные данные в классификацию аномалий сети. Машинное обучение в свою очередь строится на основе Байесовских сетей со стохастическим аппаратом идеревьев решений.

Определение уязвимостей конфигурации беспроводных сетей и противодействие атакам в беспроводных сетях являются основами для обеспечения конфиденциальности, целостности и доступности информации в сетях WLAN.

Список используемых источников

1. Lashkari A. H. and Danesh M. M. S., Editors, A Survey on Wireless Security Protocols WEP, WPA and WPA2/802.11i // IEEE International Conference on Computer Science and Information Technology, (2009) August 8-11, Beijing.

2. Sabbah E., Majeed A., Kang K. Y.-D., Liu K. and Abu-Ghazaleh N., Editors, An application-driven perspective on wireless sensor network security // ACM international workshop on Quality of service &security for wireless and mobile networks. 2006.

3. Myers S., Musacchio J., Bao N. Intrusion Detection Systems: A Feature and Capability Analysis. Tech. Report UCSC-SOE-10-12. JackBaskinSchoolofEngineering, 2010.

4. Kacha C., Shevade K. A. Comparison of Different Intrusion Detection and Prevention Systems // Intl. Journal of Emerging Technology and Advanced Engineering. Dec. 2012. Vol. 2. Iss. 12. pp. 243–245.

5. Bhuyan M. H., Bhattacharyya D. K., Kalita J. K., Survey on Incremental Approaches for Network Anomaly Detection // Journal of Communication Nteworks and Information Security (IJCNIS). Dec. 2011. Vol. 3. No. 3. pp. 226–239.

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

УДК 004
ГРНТИ 49.33.35

РАЗРАБОТКА РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ХРАНЕНИЯ, ИНДЕКСИРОВАНИЯ И ВЫДАЧИ ЦИФРОВЫХ ДОКУМЕНТОВ

А. В. Помогалова

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

Работа посвящена созданию распределенной системы хранения, учета и выдачи цифровых документов, к которым относится весь спектр документов, включая документы о высшем образовании, сертификаты, документы о профессиональной переквалификации и схожие. Данная тематика является крайне актуальной, так как позволяет провести цифровизацию масштабного сегмента документооборота. В рамках работы рассматриваются архитектурные особенности решения, проблематика выбранной области, а также стек технологий, используемых для его успешной реализации. Разрабатываемая система позволяет хранить документы, подтверждать их актуальность и фиксировать любые изменения, а также повторно перевыпускать документ в случае его утраты в максимально короткое время. Также необходимо отметить возможность формирования необходимого дизайна документа, что делает систему универсальной.

блокчейн, Ethereum, смарт-контракт, умный контракт, децентрализованные приложения, DApp, распределенная система хранения, документооборот.

Сегодня вопрос возможности получения оригинала документа о получении высшего образования стоит достаточно остро. Дистанционное, заочное обучение предполагает возможность удаленного нахождения студента. Но необходимость личной выдачи документов усугубляет ситуацию, лишая гибкости университет. Особенно это чувствуется в условиях глобальной цифровизации.

Система, разрабатываемая авторами работы, предназначена для фиксации информации (с учетом результатов обучения и сдачи экзаменов) об окончании образовательного учреждения, то есть цифровизацию документов об образовании. Одной из функций проекта является хранение документов в неизменяемом виде [2], что позволяет однозначно проверить корректность данных. Также проект позволяет оперативно получать информацию из базы при наличии специальных индексов без необходимости регистрации. Другой функцией проекта является формирование электронного документа в соответствии с шаблоном, характерным для стиля оформления документов того или иного учебного заведения.

Потребителями данного проекта могут быть университеты Санкт-Петербурга и России, школы и лицеи. Это позволит перевести данные о высшем образовании в единый цифровой формат, который обеспечивает возможность не только облегчить доступ к этим данным, но и позволит избежать проблем с утерей данных и документов, поскольку в представляемом проекте будет использован принцип децентрализованного хранения информации. Решение является крайне актуальным и активно внедряется за рубежом.

Целью проекта является разработка продукта для повышения эффективности работы с документами, подтверждающими окончание высшего учебного заведения. Конечный продукт позволяет достичь упрощения и облегчения процесса занесения, хранения, подтверждения и выдачи официальных документов, содержащих информацию об уровне образования, без привязки к единой центральной системе хранения данных. Также целью проекта является упрощение и ускорение процесса получения документов об уровне образования в условиях дистанционного обучения или заочного обучения, так как позволяет получить официальный документ без необходимости личного присутствия в течение короткого промежутка времени.

Также конечный продукт позволит ускорить процесс проверки корректности данных работодателями и другим заинтересованным лицами с полной гарантией [3]. Персонализация системы выдачи цифровых документов посредством генерации различных цифровых шаблоны, используемые при формировании документов, позволяющих сохранить внешний вид официальных документов, характерных для того или иного учебного заведения.

При разработке системы были выделены следующие задачи:

•Разработка смарт-контракта, в рамках которого будет происходить регистрация данных о документах, подтверждающих получение высшего (среднего) образования.

•Интеграция умного контракта с площадкой (веб-сайтом), то есть удобным интерфейсом для комфортного взаимодействия с ним, где также будет разработан личный кабинет и удобная форма для ввода данных.

•Разработка и создание структуры базы данных, где будут сохраняться пользовательские настройки, а также данные авторизации.

•Интеграция open-source проекта, позволяющего создавать собственные дизайны документов, в зависимости от стиля оформления документов того или иного учебного заведения.

•Тестирование проекта.

•Запуск проекта и создание сопровождающей документации и медиаматериала, распространение проекта среди университетов.

Итоговым результатом работы будет являться программный продукт - удобная веб-площадка с личными кабинетами, которая позволит не только вносить информацию университетам, но и проверять ее работодателями без необходимости регистрации за короткий промежуток времени и другими заинтересованными лицами. Информация, введенная университетами на данной площадке будет сохраняться в рамках блокчейн-сети, что позволит гарантировать неизменность данных и их децентрализацию.

При этом можно выделить следующие ключевые факторы:

•Повышение качества (точности, достоверности, своевременности, согласованности) ведения и учета информации о количестве выпустившихся студентов и соответствующих документов.

•Структуризация и унификация хранимых данных и процессов доступа к ним.

•Повышение оперативной доступности данных.

•Персонализация доступа к информации.

•Обеспечение единой системы процедур формирования подтверждающих обучение документов.

•Отсутствие необходимости печати документов и личного вручения.

•Упрощение процедур внутреннего контроля, процесса формирования личных дел студентов.

•Возможность для пользователей использовать систему проверки и подтверждения корректности документа.

•Повышение надежности хранения данных.

Исходя из анализа целей, требований и задач данного проекта, наиболее разумной и подходящей будет являться архитектура, представленная на рис.

Данное решение предполагает разработку следующих единиц:

– веб-интерфейса, для проверки актуальности информации документа об окончании учебного заведения;

– веб-интерфейса для ввода данных в систему и фиксации информации в распределенной базе данных;

– личного кабинета пользователя;

– умного контракта, содержащего логику для фиксации введенной информации в распределенной базе данных;

– базы данных, для хранения пользовательских настроек и данных аутентификации;

– системы генерации электронных документов согласно шаблону учебного заведения.

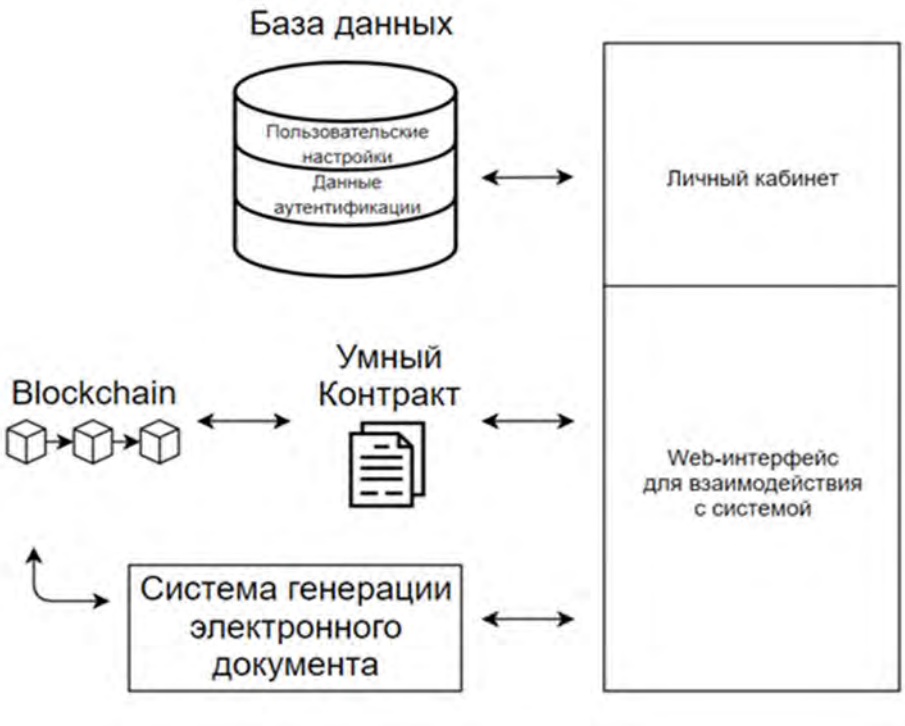


Рис. Архитектура проектируемой системы

Функции, выполняемые продуктом после завершения стадии тестирования и разработки:

– отображение информации в рамках графического интерфейса (веб-страницы);

– внесение данных о документах о получении высшего образования каждого из университетов в рамках специализированных личных кабинетов;

– редактирование данных, при допущении ошибок с идентификацией о непригодности предыдущих внесенных данных и отображении актуальной последней информации;

– генерация электронного документа о высшем образовании со всей информацией, характерной документам такого рода, в рамках персонализированного шаблона с уникальной индексацией;

– проверка актуальности и корректности данных посредством ввода данных уникальной индексации.

Конечная версия проекта также может быть усовершенствована. Если первично она представляет собой единую платформу с личными кабинетами организаций, то также возможна разработка более локального решения для внутренней работы в рамках различных организаций.

Также необходимо выделить узкие области, решение проблем в которых также является ключевым. Так, можно выделить необходимость соответствия стандартам хранения персональной информации, вопросы безопасности [1, 4] и масштабирования системы. Данные вопросы будут проработаны при дальнейшем развитии проекта.

Список используемых источников

1. Елагин В. С., Спиркина А. В., Владыко А. Г., Иванов Е. И., Помогалова А. В., Аптриева Е. А. Основные сетевые характеристики Blockchain трафика и подходы к моделированию // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 39–45.

2. Гойхман В. Ю., Помогалова А. В. Технология Blockchain - новое поколение сети Интернет: Интернет Ценностей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 231–235.

3. Yuan C., Xu M., Si X., Li B. Blockchain with Accountable CP-ABE: How to Effectively Protect the Electronic Documents // 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), Shenzhen, China, 2017. pp. 800–803.

4. Haveri P., Rashmi U. B., Narayan D. G., Nagaratna K., Shivaraj K. EduBlock: Securing Educational Documents using Blockchain Technology // 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020. pp. 1–7.

Статья представлена научным руководителем, начальником УНРПНК, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.912
ГРНТИ 49.33.35

СИСТЕМА ЗАЩИТЫ АВТОРСКОГО ПРАВА НА БАЗЕ ПЛАТФОРМЫ ETHEREUM С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ IPFS

А. В. Помогалова, И. Ф. Тарабанов, Л. А. Тирбах, И. А. Федосеев

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

Работа посвящена созданию системы защиты авторского права на базе платформы Ethereum с применением технологии IPFS. Система позволяет загружать и скачивать работы, хранящиеся в системе, а также производить проверку подлинности работы на основе проверки хеш-функции исходного документа.

облачные технологии, Ethereum, IPFS, Metamask, Ropsten, блокчейн, смарт-контракт, хеш-функция, фреймворк, react.js, web3.js, Ganache CLI, Infura.

Целью работы является создание системы защиты авторского права. Проект предлагает способ решения значимой проблемы подмены, изменения и присвоения ложного авторства документа путем внедрения в процесс технологии блокчейн, в частности, смарт-контракта на основе платформы Ethereum, которая позволяет существенно уменьшить возможность подмены документа. Также в проекте используется система распределенного хранения файлов IPFS, которая позволяет значительно снизить вероятность утери или умышленного изменения документа.

Проект включает в себя три ключевых функциональных части:

- Веб-интерфейс, с помощью которого происходит взаимодействие пользователя и системы;
- Связь интерфейса с распределенным хранилищем IPFS и смарт-контрактом;
- Смарт-контракт, загруженный в рамках блокчейн-сети платформы Ethereum.

Получив данные от пользователя, система отправляет их в IPFS для дальнейшего хранения документа. Сформированный хеш, данные о документе и ссылка на документ в IPFS отправляются в смарт-контракт. При запросе подлинности данных будет сравниваться хеш подлинника и хеш загруженной пользователем работы. При совпадении результатов хеширования загруженный документ считается подлинным. При скачивании пользователь получает ссылку на документ в IPFS. Для разработки приложения были выбраны следующие технологии:

IPFS – это гипермедийный протокол связи с открытым исходным кодом, с помощью которого одноранговые узлы осуществляют хранение и распространение данных в единой распределенной файловой системе. При загрузке информации в IPFS адрес для доступа к объекту, файлу или пользовательским данным в системе формируется с привязкой не к серверу, а к его уникальному криптографическому хешу-идентификатору (*Content Identifier*, CID) [2]. Таким образом CID обеспечивает безопасный доступ к любому загруженному в IPFS файлу. Кроме того, адрес формируется на основе содержимого файла, и самое небольшое изменение в нем приводит к созданию абсолютно другого адреса, что исключает возможность подмены исходного файла. Таким образом, IPFS может считаться подходящим решением для авторской защиты контента [6, 7].

Ethereum – это платформа для создания децентрализованных онлайн-сервисов на основе технологии блокчейн, работающей на базе смарт-контрактов с одноименной внутренней криптовалютой. Платформа реализована как единая децентрализованная виртуальная машина. В качестве «топлива» для произведения сделок и контрактов в рамках виртуальной машины используется криптовалюта эфир (ETH) и понятие газа, как меры оценки реально необходимых вычислительных ресурсов. Данный подход к оценке вычислительных ресурсов, необходимых для произведения сделок в сети, позволяет избавиться от зависимости текущего курса внутренней криптовалюты и объективно оценить фактически необходимые ресурсы.

Смарт-контракт – это приложение (или программа), работающее в блокчейн-сети. Как правило, он выступает в качестве цифрового соглашения, которое подкрепляется определенным набором правил. Эти правила предопределены компьютерным кодом, который реплицируется и выполняется всеми узлами сети [5].

Смарт-контракты позволяют создавать доверительные протоколы и приложения. Это означает, что обе стороны могут взять на себя обязательства через блокчейн, без знания или доверия друг к другу. Участники данного процесса могут не беспокоиться о правильности выполнения обязательств, поскольку, если условия не будут удовлетворены, то контракт аннулируется. Помимо этого, использование смарт-контрактов может устранить необходимость в посредниках, значительно снижая операционные расходы. Таким образом, смарт-контракт позволяет повысить прозрачность и надежность разработанного решения.

Infura – это кластер узлов, который соединяет интерфейс пользователя (UI) DApp (*decentralized applications*, децентрализованного приложения) с IPFS. Провайдер Infura может обрабатывать подключение к сети IPFS без необходимости синхронизации узла сети. Также он может выступать как посредник и для подключений к сети Ethereum [3].

Таким образом, любой пользователь, используя обычный браузер, может пользоваться приложением без необходимости организации IPFS узла на своем устройстве.

Web3.js – официальная библиотека для работы с блокчейном Ethereum. Web3 позволяет абстрагироваться от внутренней механики Ethereum и работать с сетью и смарт-контрактами так, будто это обычные JavaScript-объекты, позволяя создать удобный пользовательский интерфейс для взаимодействия со смарт-контрактом [3, 4].

Metamask – децентрализованный кошелек для Ethereum и токенов ERC20, представленный в виде расширения для браузера. Позволяет пользователю отправлять, получать и обменивать криптовалюту. MetaMask генерирует пароли и ключи непосредственно на устройстве, поэтому только у владельца есть доступ к своим средствам и конфиденциальной информации. Кроме того, кошелек позволяет взаимодействовать с другими DApp.

На веб-странице существует четыре основных блока взаимодействия пользователя с системой:

- Загрузка документа.
- Поиск документа.
- Скачивание документа.
- Проверка документа на подлинность.

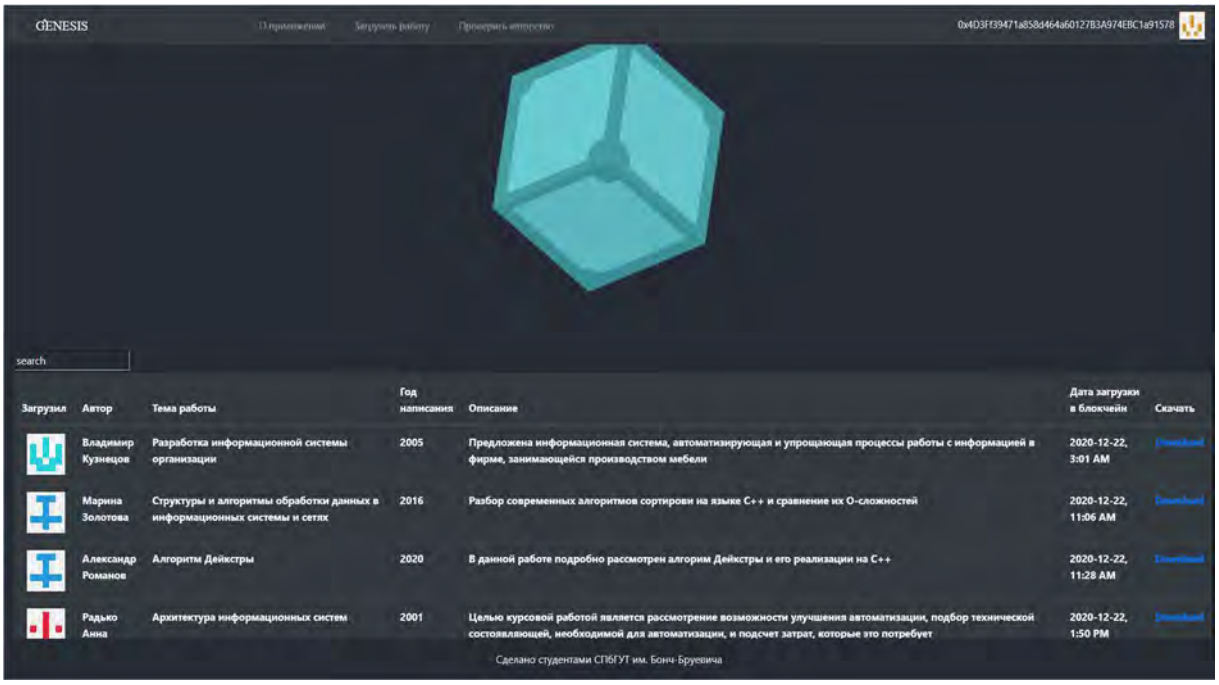


Рис. 1. Интерфейс приложения

Поиск документа осуществляется посредством ввода характерной информации в строку «поиск». Также, на экран выводится список всех работ, когда-либо загруженных в систему, и пользователь может выбрать работу без использования функции поиска.

Архитектура решения представлена на рис. 2, на нем показаны основные элементы взаимодействия системы.

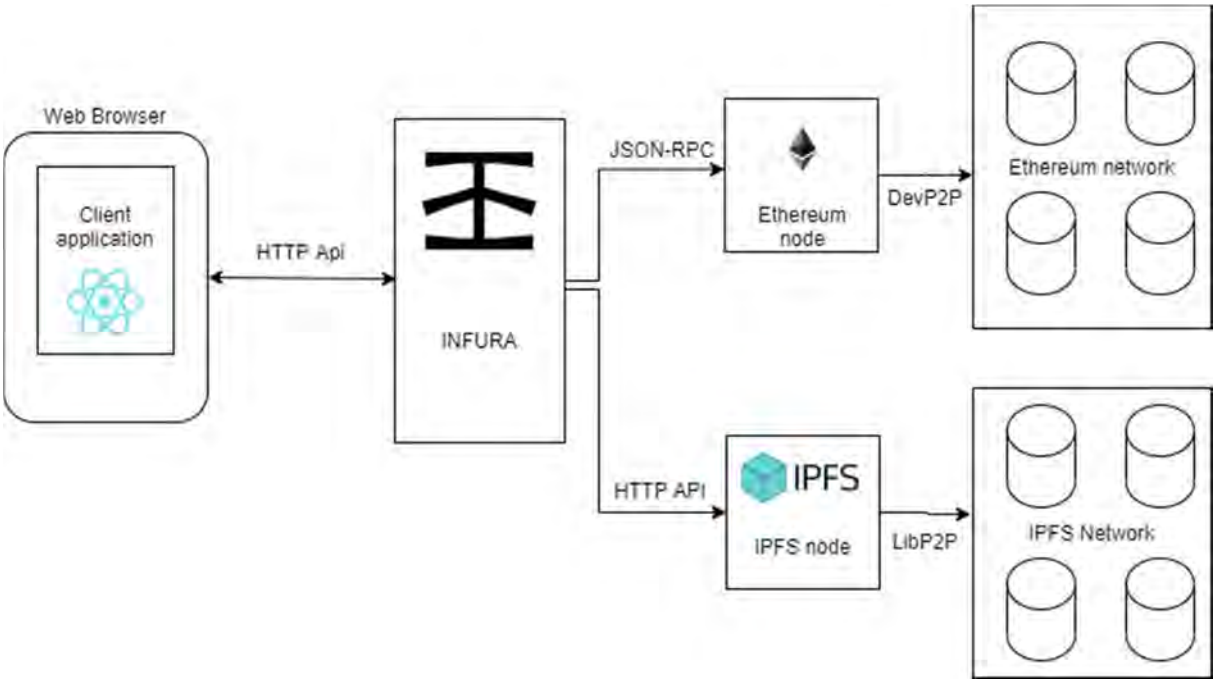


Рис. 2. Архитектура системы

Стоит отметить, что логика самого приложения была полностью реализована на ReactJs, из этого можно сделать вывод о том, что приложением полностью выполняется в браузере и не требуют собственной инфраструктуры в виде сервера. Для хранения информации о работах используется смарт-контракт, загруженный в тестовую сеть платформы Ethereum, точнее в сети Ropsten. Это происходит путем запросов к API кластерной платформы Infura, при принятии запроса Infura отправляет к одной из своих нод запрос, о том, что необходимо произвести действие со смарт-контрактом, и вернуть результат в обратном направлении в браузер пользователя. При загрузке файла в децентрализованную сеть IPFS происходит аналогичный набор, действия, для оптимизации количества запросов скачивания файла происходит не с помощью запроса к Infura, а с помощью запроса к другим шлюзам, как основной было решено выбрать шлюз ipfs.io, он по своему времени ответа, оказался самым быстрым.

Авторами был проведен анализ существующих решений. Аналитика позволила обнаружить, что разработок с аналогичным стеком решений на данный момент на рынке не представлено. В процессе работы была выявлена необходимость создания своего решения для дополнительного хранения файлов в системе, функционально было полностью проверено в сети

Ropsten. В процессе тестирования системы, также было выявлена необходимость в дополнительной обработке файлов до отправки в IPFS, для лучшего распознавания фактов копирования материалов.

Список используемых источников

1. Документация Infura. URL: https://infura.io/docs/gettingStarted/authentication (03.12.2020).
2. Документация IPFS. URL: https://docs.ipfs.io (05.12.2020).
3. Документация Web3.js. URL: https://web3js.readthedocs.io/en/v1.3.0/ (28.11.2020).
4. Документация React.js. URL: https://ru.reactjs.org/docs/getting-started.html (30.11.2020).
5. Определение Solidity. URL:https://docs.soliditylang.org/en/v0.5.1/ (13.12.2020).
6. Kumar R. and Tripathi R. Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain // 2019 Fifth International Conference on Image Information Processing (ICIIP), Shimla, India, 2019. pp. 246–251.
7. Zheng Q., Li Y., Chen P. and Dong X. An Innovative IPFS-Based Storage Model for Blockchain // 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile, 2018. pp. 704–708.

Статья представлена научным руководителем, начальником УНРПНК, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 535.8/654
ГРНТИ 49.31

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ MIMO В ОПТИЧЕСКОЙ СВЯЗИ

Б. К. Резников, А. А. Сивухин

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

В этой статье представлена новая система передачи данных с множеством входов и множеством выходов (MIMO) в области луча для оптической беспроводной связи. Оптическая базовая станция, оснащенная массивными оптическими передатчиками, связывается с рядом пользовательских терминалов через передающую линзу. Сосредоточившись на светодиодных передатчиках, мы анализируем преломление света линзами и устанавливаем модель канала для оптических массивных передач MIMO.

MIMO, оптическая связь, BDMA.

Для большого количества светодиодов векторы каналов разных пользовательских терминалов (User terminal, UT) становятся асимптотически ортогональными. Исследуется максимальное отношение передачи и предварительное кодирование с принудительным обнулением в оптической массивной системе MIMO и предлагаем схему линейного предварительного кодирования для максимизации суммарной скорости.

Далее предусматривается предварительное кодирование, когда количество передатчиков становится асимптотически большим, и показываем, что передача множественного доступа с разделением лучей (BDMA) обеспечивает асимптотически оптимальную производительность для максимизации суммарной скорости.

В отличие от оптического MIMO без передающей линзы, BDMA может увеличивать суммарную скорость пропорционально 2K и K при ограничениях общей мощности и мощности на передатчике, соответственно, где K – количество UT. В неасимптотическом случае мы доказываем условия ортогональности оптимального распределения мощности в области луча и предлагаем эффективные алгоритмы распределения луча. Численные результаты подтверждают значительно улучшенные характеристики предлагаемых нами подходов к оптической массивной MIMO-связи в лучевой области [1].

Оптическая система Massive MIMO на основе линзовой передачи

Рассматривается оптическая систему MIMO, состоящую из базовой станции, оснащенной передатчиками M^2 и передающей линзой UT, каждый из которых имеет один фотодетектор, используемый в качестве приемника. Передатчики могут быть светодиодами или волоконно-оптическими трансиверами. В этой статье мы сосредоточимся на светодиодных передатчиках, и каждый светодиод излучает свет с одинаковой длиной волны. С передающей линзой на BS свет, излучаемый разными светодиодами, проходящими через линзу, преломляется в разных направлениях (рис. 1).

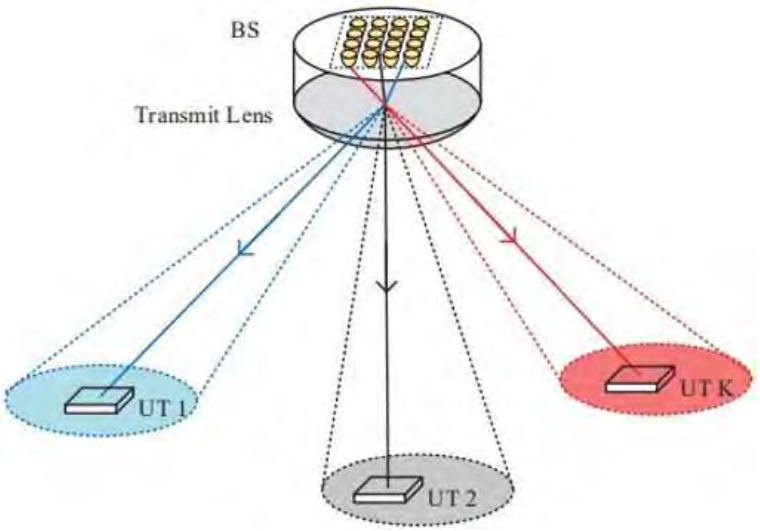


Рис. 1. Оптическая система MIMO с трассировкой

Базовая станция использует квадратную светодиодную матрицу для передачи сигналов на UT. Обозначим $x_k \in R^{m^2*1}$ как сигнал, предназначенный для *k*-го UT, а принятый сигнал в *k*-м UT можно записать как:

$$y_k = \mathbf{h}_k^T x + z_k = \mathbf{h}_k^T x + h_k^T(\sum_{k' \neq k} x_{k'}) + z_k,$$

где $x = \sum_k x_k$ – сумма всех сигналов,

$h_k^T \in R^{1*M^2}$ – вектор канала от светодиодов до *k*-го UT,

z_k – шум на приемнике, который содержит дробовой шум и тепловой шум, и обычно моделируется как действительная аддитивная белая гауссова переменная с нулевым средним и дисперсией σ^2. Здесь, без ограничения общности, мы предполагаем единичную дисперсию шума (т. е. $\sigma^2 = 1$).

Преломление света, проходящего через линзу

Первоначально следует проанализировать преломление света от одного светодиода, проходящего через объектив. Предположим, что (i, j) светодиод в квадратном светодиодном массиве находится в точке *S*, с координатами (x_S, y_S, z_S), как показано на (рис. 2a). Для простоты опускаем подстрочный индекс (i, j). Пусть φ_C обозначит полуугол половинной интенсивности светодиода. Световая интенсивность светодиода, как правило, следует за Ламбертским распределение радиантов. В частности, для света с полярным углом φ, сила света может быть выражено как:

$$I_0(\varphi) = \frac{m_L + 1}{2\pi} \cos^{m_L}(\varphi),$$

где порядок излучения Ламберциана задается $m_L = -\log 2 / \log(\cos(\varphi_C))$.

Используется сферическая линза с индексом преломления n перед светодиодом. Плоская поверхность обращен к светодиоду, а центр сферической поверхности, радиус которой равен *R* (рис. 2).

Рассмотрим свет, излучаемый светодиодом с полярным углом φ и азимутальным углом ζ0. Свет сначала преломляется через плоскость. Поверхность на P1, как показано на (рис. 2b), и преломляется через сферическую поверхность на P2, как показано на (рис. 2c). В P1 угол падения – φ, а угол преломления – ξ. Это следует из закона Снеллиуса: $\sin\varphi / \sin\xi = n$. Преломляющий свет можно рассматривать как свет, излучаемый виртуальным источником света.

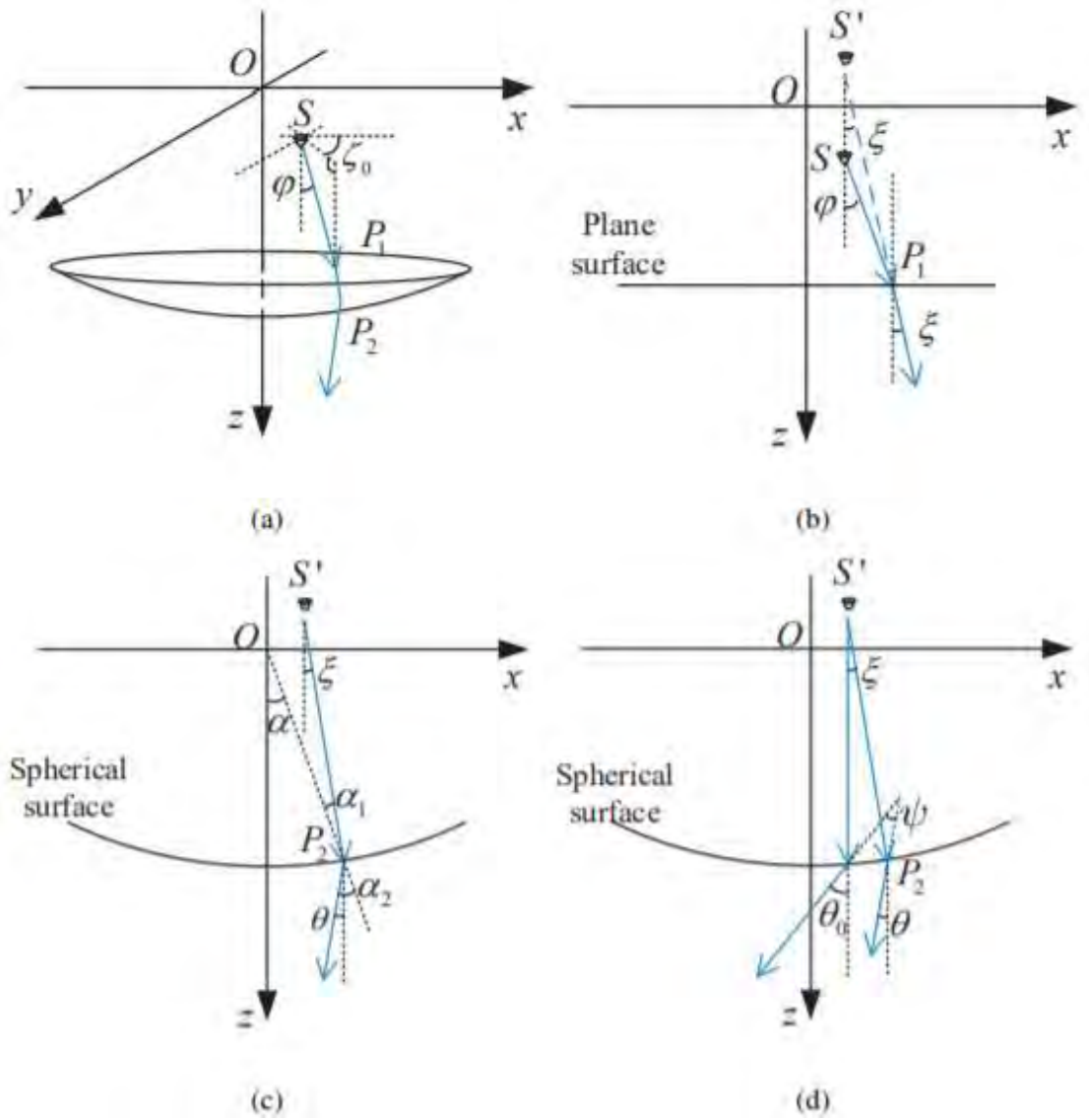


Рис. 2. a) иллюстрация света, проходящего через объектив;
b) преломление на плоской поверхности; c) преломление на сферической поверхности;
d) угол преломления по отношению к центральному свету

Сравнение приблизительной интенсивности с точной интенсивностью для светодиода с $\varphi_C = 30^\circ$. Индекс преломления $n = 1{,}5$, а радиус сферической поверхности $R = 10$ см. Можно заметить, что аппроксимация хорошо подходит к точному распределению интенсивности во всех случаях (рис. 3) [2].

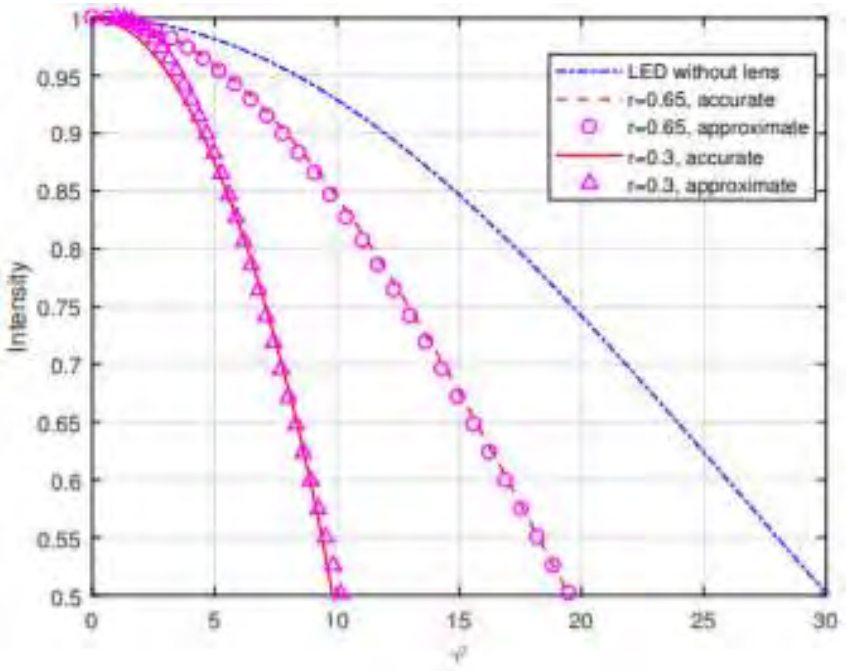


Рис. 3. Сравнение приблизительной и точной интенсивности света

В последнее время лазерные диоды (LD) рассматриваются в качестве потенциальных источников оптических сигналов. Связь благодаря высокой пропускной способности модуляции, эффективности и сходимости пучков. Пользователь терминалы (UT) используют фотоприемники как фотодиоды в качестве оптических приемников для преобразования оптической энергии в электрический ток. Оптическая связь может значительно разгрузить переполненное радио частотного (RF) спектра, обеспечивают высокоскоростную передачу данных, и достигают простой и низко затратной модуляции и демодуляции за счет модуляции интенсивности и прямого детектирования.

Список используемых источников

1. Amirabadi M. A. On the performance of some new Multiuser FSO-MIMO Communication Systems. IET OPT

2. Chen Sun, Xiqi Gao, Jiaheng Wang, Zhi Ding, Xiang-Gen Xia. Beam Domain Massive MIMO for Optical Wireless Communications with Transmit Lens. arXiv:1710.05282v3 [eess.SP] 23 Nov 2018.

Статья представлена заведующим базовой кафедрой ССС СПбГУТ, доктором технических наук, доцентом В. В. Котовым.

УДК 530145(21); 621.3.049.77
ГРНТИ 50.33

КВАНТОВЫЕ ТЕХНОЛОГИИ В ИНФОКОММУНИКАЦИЯХ

С. А. Рогов, А. Р. Салтыков

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

В последние годы значительное внимание уделяется исследованиям и внедрению квантовых технологий в области обработки и передачи информации. Огромный вычислительный потенциал квантовых компьютеров позволяет в перспективе достаточно быстро решать задачи, считавшиеся трудноразрешимыми с помощью обычных вычислительных средств. Это относится, в частности, к задаче расшифровки надежных секретных кодов, используемых при передаче закрытой информации. В то же время на основе квантовых методов был разработан новый способ передачи секретных кодов, принципиально защищенный от взлома законами квантовой механики.

квантовый компьютер, квантовые вычисления, квантовая криптография.

Рассмотрим, чем объясняется высокая вычислительная мощность квантового компьютера [1]. В квантовом компьютере информация хранится не в виде бита, который может иметь только два значения 0 и 1, а в состояниях кубита, в качестве которого могут использоваться разные квантовые объекты, такие например, как ядерный спин с его двумя возможными ориентациями в однородном магнитном поле, электрон с двумя состояниями в одиночном атоме, фотон с двумя возможными поляризациями, состояния сверхпроводимости и др. Принципиальное отличие кубита от бита в том, что он может находиться в суперпозиции своих базовых состояний $|0\rangle$ и $|1\rangle$ в соответствии с формулой:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

где α и β это комплексные коэффициенты, модуль квадрата которых $|\alpha|^2$ и $|\beta|^2$ равен вероятности нахождения кубита в первом и втором базисном состоянии, причем $|\alpha|^2 + |\beta|^2 = 1$. С помощью внешнего воздействия, например, облучения атома электромагнитным полем, можно переводить кубит из состояния $|0\rangle$ в состояние $|1\rangle$ или наоборот. Если время облучения уменьшить, то можно получить кубит в суперпозиции состояний, например, в такой:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

Так как возможных состояний кубита бесконечно много, в нем содержится огромное количество информации. Изменение состояния кубита с помощью внешнего воздействия эквивалентно некоторым математическим или логическим действиям над коэффициентами в кубите. Если увеличить число кубитов, то закодированная в них информация может обрабатываться параллельно, а скорость обработки будет расти экспоненциально. Действительно, состояние суперпозиции из двух кубитов характеризуется четырьмя комплексными числами:

$$|\psi> = \alpha_{00}00|00> + \alpha_{01}|01> + \alpha_{10}|10> + \alpha_{11}|11>,$$

где α_{ij} – амплитуды (комплексные числа). Для n кубитов чистые состояния имеют вид: $|x_1,x_2,\ldots,x_n>$, $x_i \epsilon [0,1]$ и суперпозиция состояний характеризуется уже 2^n амплитудами. При $n = 500$ это больше числа атомов во вселенной. Ни на каком классическом компьютере не сохранить эти комплексные числа, однако лишь несколько сотен атомов оперирует такой информаций. При эволюции системы эта информация изменяется определенным образом. Это означает огромную вычислительную мощность, если воспользоваться сведениями об изменении этой информации.

Как производятся квантовые вычисления? На рис.1 представлена схема идеального квантового компьютера [2]. По существу, квантовый компьютер представляет собой регистр из n кубитов, управляемых внешними (классическими) сигналами. Квантовый компьютер встроен в классическое окружение, состоящее из управляющего классического компьютера и других устройств, управляющих эволюцией кубитов (например, генераторов импульсов), а также средствами измерения состояния кубитов.

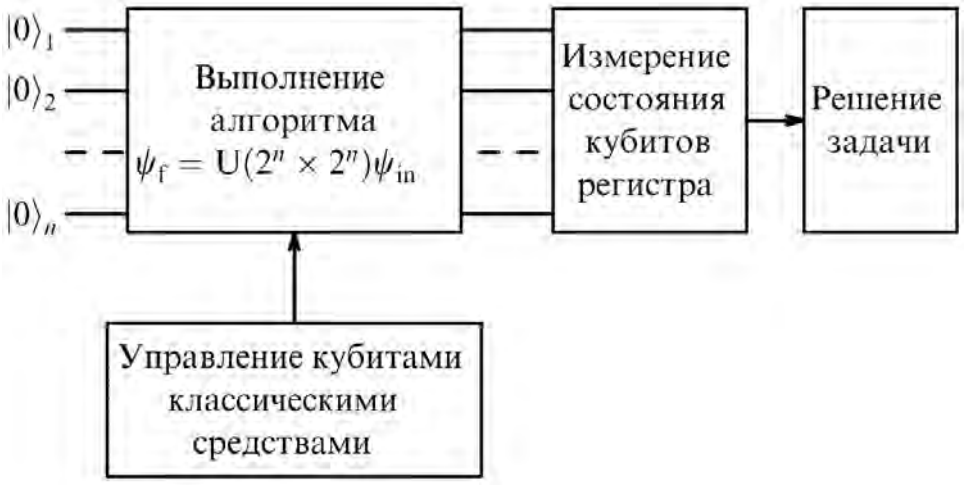


Рис. 1. Схема идеального квантового компьютера

Вектор состояния квантового регистра, из n кубитов, содержит информацию в виде коэффициентов $\alpha_{x_1,\dots,x_n}$ суперпозиции из 2^n базисных состояний этого регистра:

$$|\psi> = \sum_{x_1,\dots,x_n} \alpha_{x_1,\dots,x_n} |x_1 \dots x_n>, \;\; x_1 \dots x_n = \{0,1\}\,.$$

Всё, что можно сделать с системой кубитов – это преобразовать ее начальный вектор $|\psi_{in}>$ в другой вектор $|\psi_f>$ путем умножения входного вектора на матрицу преобразования U размерности $2^n \times 2^n$:

$$|\psi_f> = \mathrm{U}(2^n \times 2^n)|\psi_{in}>.$$

Классическая информация о решении задачи содержится в конечном векторе состояния. Она должна быть получена измерением состояния кубитов.

Было показано, что произвольная матрица изменения состояния многих кубитов может быть реализована с помощью конечного универсального набора простых однокубитовых логических элементов и простейшего двухкубитого элемента, который осуществляет связь между кубитами [1]. Это позволяет сократить общее число элементарных операций в квантовом компьютере по сравнению с классическим аналогом.

Например, дискретное преобразование Фурье набора из $N = 2^n$ комплексных чисел, которое, по существу, представляет умножение вектора на матрицу с известными элементами, требует в квантовом компьютере n^2 однокубитовых операций, тогда как в классическом, даже при его вычислении по быстрому алгоритму (БПФ) требует $N \log N = n2^n$ операций. Отсюда следует, что вычисление на квантовом компьютере преобразования Фурье имеет экспоненциальное преимущество.

Это отличный результат, поскольку преобразование Фурье много где используется, однако регистрация результатов вычислений затруднена, поскольку при измерении состояния кубитов по законам квантовой механики происходит переход каждого кубита в одно из двух базовых состояний, что не позволяет непосредственно узнать амплитуду вероятности, в которой содержится выходная информация. Один из способов преодолеть эту проблему – делать многократные измерения, но при этом вычисления придется повторять. Другой способ – использовать такие алгоритмы, при которых вероятность на выходе была бы большой только у одного базового состояния. Такие алгоритмы и предлагают. В частности, это алгоритм факторизации на основе преобразования Фурье.

Существуют и другие проблемы на пути создания квантового компьютера. Например, кубиты в квантовом компьютере должны быть хорошо изо-

лированы от внешней среды и друг от друга, чтобы их состояние не менялось от нежелательного воздействия, и в то же время ими нужно управлять. Это противоречивое требование.

Несмотря на трудности, работы по созданию квантовых компьютеров активно проводятся в развитых странах. Рассматриваются варианты реализации квантового компьютера на оптических фотонах, на ионных или атомных ловушках, на ядерном магнитном резонансе, на сверхпроводимости, на электрических зарядах в квантовых точках и др. В кампаниях IBM и GOOGL уже были созданы экспериментальные образцы квантового компьютера на сверхпрводимости с числом кубитов около 50. Было продемонстрировано квантовое преимущество при решении вычислительных задач. Так, с помощью китайского квантового компьютера на фотонах за несколько минут была решена задача, потребовавшая бы при использовании классического компьютера 2 млрд лет.

В России в ближайшие годы также планируется создание квантовой вычислительной системы. В рамках программы «Цифровая экономика РФ», которая предусматривает развитие квантовых технологий при финансировании РОСАТОМа, ФПИ и Минобрнауки РФ, был запущен пилотный проект по развитию технологий сверхпроводниковых кубитов.

Если исследования, направленные на создание универсального квантового компьютера, носят пока фундаментальный характер, то в области квантовых коммуникаций и квантовой криптографии удалось достичь гораздо больших успехов.

Влияние измерения на квантовомеханическую систему, затрудняющее регистрацию выходных сигналов квантового компьютера, в системах связи оказывается полезным. Из-за этого влияния любая попытка считывания информации из квантового канала может быть обнаружена, что защищает систему связи от несанкционированного доступа. В качестве квантового объекта в квантовых системах связи используются фотоны.

В настоящее время уже существуют три варианта реализации квантовой коммуникации:

– по оптоволоконному кабелю – серверы связаны по уже существующим каналам коммуникации;

– по открытому пространству – по оборудованию и сетям сотовых операторов;

– через спутниковую связь – обмен квантовым ключом шифрования с наземной станцией и орбитальным спутником.

Несомненным лидером по развитию квантовых коммуникаций является Китай. Китайская квантовая сеть сегодня составляет около 2 тысяч километров в длину и соединяет столицу и несколько крупнейших финансово-промышленных центров. А благодаря квантовой спутниковой станции была установлена связь Пекин-Вена на расстоянии 7 600 километров.

Список используемых источников

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация: Пер. с англ. М.: Мир, 2006. 824 с.
2. Валиев К. А. Квантовые компьютеры и квантовые вычисления // УФН. 2005. Том 175. № 1. С. 3–39.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ МЕТАДАННЫХ СОЦИАЛЬНЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ

И. Б. Саенко[1], А. В. Хинензон[2]

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

Социальные сети могут быть представлены в виде информационной модели, с некоторыми атрибутами и связями. Такие модели позволяют выделить ряд признаков, которые применимы для обнаружения аномального поведения пользователя в социальной сети. В статье под аномальным поведением пользователя понимается отклонение от статистической нормы.

социальные сети, аномальное поведение пользователя в социальной сети, информационная безопасность, обнаружение аномалий.

Введение

Сегодня пространство онлайновых социальных сетей (СС) привлекает внимание ученых-исследователей из разных областей науки, будь-то информационная безопасность, системный анализ, маркетинг или экономика. Для любой из перечисленных областей наук аномалией является отклонение от нормы, однако, само понятие нормы бывает различным. Существует несколько объяснений понятия «норма»: (1) статистическая; (2) идеальная; (3) социальная; (4) субъективная и (5) функциональная [1]. В социальных сетях аномальное поведение представляет собой отклонение от статистической нормы.

Анализ поведения пользователей

Объектом исследования в данной работе является пользователь. Индикация аномального поведения происходит по выявлению отклонений

от усредненного показателя активности аккаунта пользователя. Отдельный пользователь имеет больший вес, если он является лидером мнений [2]. Лидер мнений, имея такие характеристики как активность, авторитетность, уверенность, контактность может оказывать влияние на группы людей с возможностью манипулирования общественным мнением или поведением.

За пользовательским аккаунтом может стоять не только реальный пользователь, но и автоматизированная программа-робот (бот). Его действия могут принести положительный и негативный результат. Положительный результат заключается в пользе автоматизации процессов машинных или повторяющихся действий, например, чат-бот, который оперативно поможет и ответит на необходимые вопросы в режиме реального времени. Негативный результат состоит в том, что боты могут координироваться для нанесения групповых сетевых атак и осуществлению угроз безопасности информации. По данным [3] при правильной работе боты практически невидимы для автоматических механизмов обнаружения. Также некоторые учетные записи могут быть неактивны – они известны как «спящие» боты [4].

С совершенствованием систем обнаружения ботов, прогрессируют и сами автономные программы. Их развитие заключается в том, чтобы максимально приблизить искусственное поведение к реальному. Рассмотрим общую структуру сети для последующего, более подробного анализа признаков и компонентов.

Структура социальной сети

Структура социальной сети имеет форму графа и состоит из следующих элементов: набора групп, пользователей (узлов) и социальных взаимодействий между ними (связей). По структуре данных СС могут быть разделены 3 группы: централизованные, гибридные (частично централизованные) и децентрализованные.

Существуют различные методики для анализа социальных сетей, основывающиеся на изучении зависимостей пользователей и социального графа. Одним из рассматриваемых компонентов анализа является модель поведения.

Разработка модели поведения

Выделим основные атрибуты модели поведения (рис. 1):

– Количество сильных связей (взаимные друзья, подписчики (входящие));

– Количество слабых связей (лайки, комментарии, репосты от несвязанных аккаунтов);

– Показатели активности (лайки, репосты, ретвиты);

– Показатели дискуссий;
– Дискретные признаки (время регистрации, частота входа).

Авторы [5] рассматривают подход к созданию единой модели данных для трех социальных сетей, одна из которых «ВКонтакте», что может послужить важным компонентом для разработки алгоритма обнаружения источника распространения нелегитимной информации.

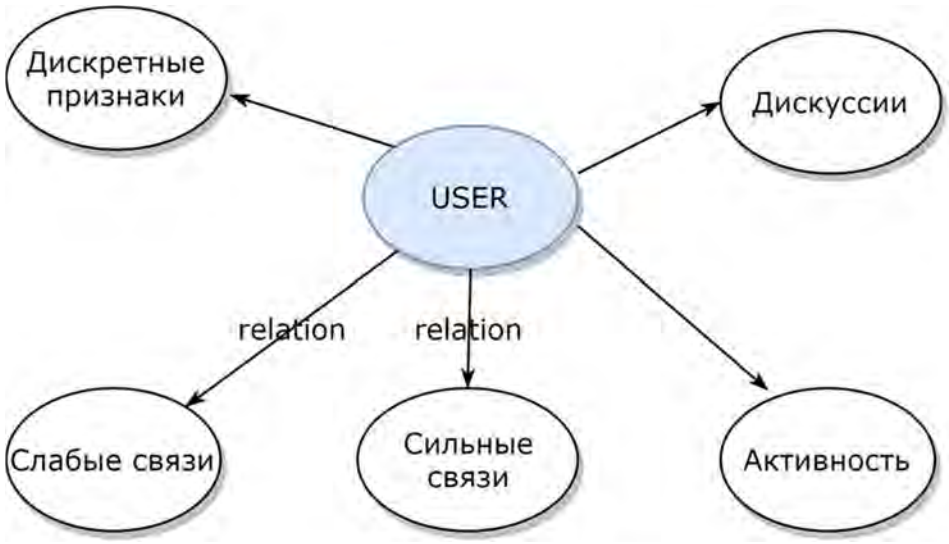


Рис. 1. Модель поведения

Модель поведения позволяет выделить элементы, для которых не требуется анализ отношений между пользователями. Однако пользовательская страница хранит в себе большое количество метаданных. Под метаданными в данной статье понимается средство классификации, упорядочивания и характеристики данных или содержимого страницы. Эта информация может представляться в разном виде: веб-сайт, текстовые сообщения, базы данных, информационные репозитории. Таким образом, метаданные можно назвать описанием вышеперечисленных данных. Авторы [6] предлагают деление по типам:

1. Структурные метаданные – описывают организацию ресурсов (интеллектуальные или физические элементы цифрового объекта; отношение объектов друг к кругу; технические характеристики: формат файла, размер, носитель).

2. Административные метаданные – описывают управление ресурсом (дата создания, право доступа, хранение, удаление).

3. Описательные метаданные – выполняют описательные функции (географическое местоположение, автор).

Авторам [7] удалось идентифицировать направленно созданные автоматизированные учетные записи с использованием метаданных «имя пользователя». В своей разработке они опирались на список ключевых слов [8]. Минусом такого подхода является то, что обработка естественного языка

сильно сокращает возможности обнаружения из-за ограничений на сбор данных от социальных сетей. Авторами [9] была описана и реализована математическая модель нейронной сети, обученная на фотографиях пользователей. Модель показала высокую результативность и скорость, однако же, социальные сети также ограничивают возможность сбора изображений.

На основании проведенного анализа делается вывод о необходимости выбора таких признаков, которые позволят исключать анализ контента.

Эксперимент

В [10] за основу выбран один из показателей метаданных – хештег. При помощи формирования правильно подобранных хештегов появляется возможность быстрого распространения разного рода информации.

Сбор данных может осуществляться при помощи парсинга или через интерфейс API. Данная модель имеет преимущество, так как для выявления аномалий системе необходимы данные открытого типа.

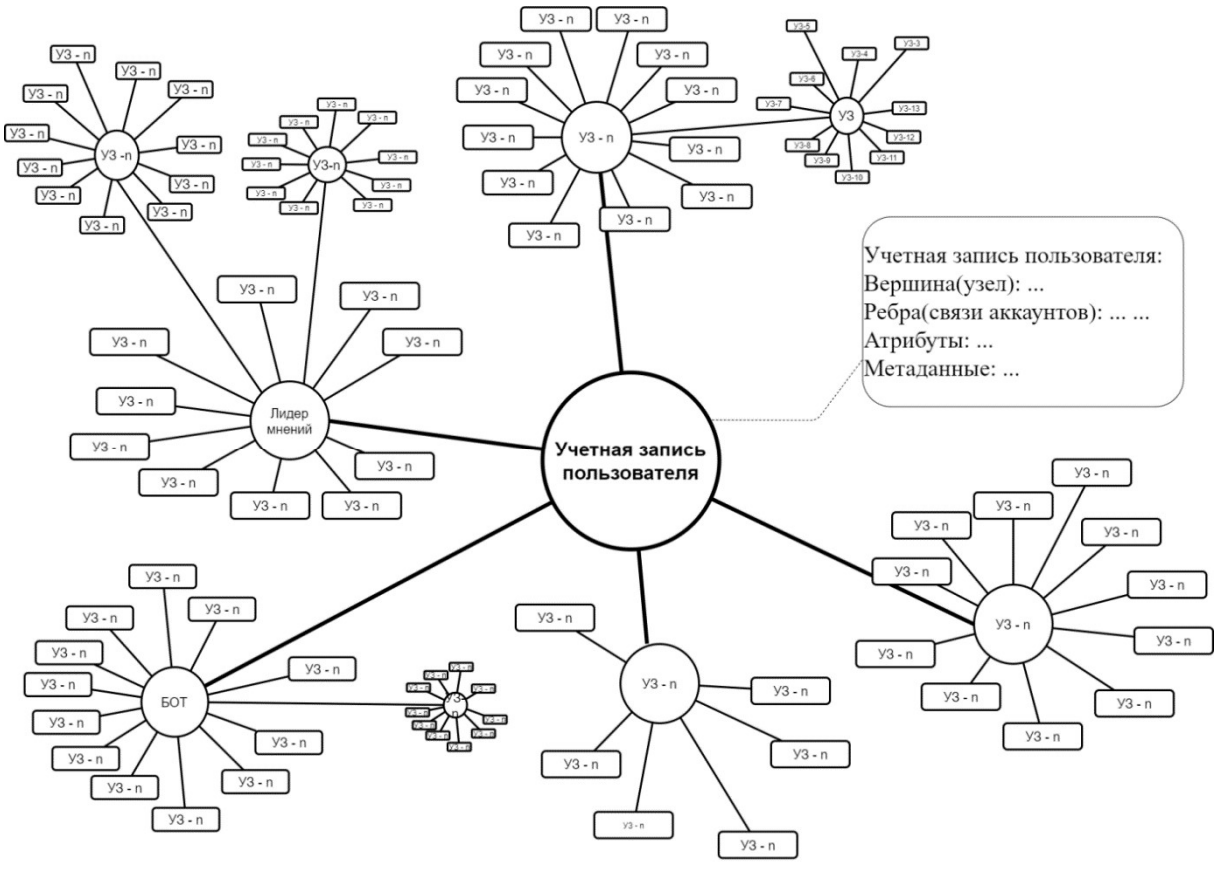


Рис. 2. Социальный граф нескольких учетных записей из группы

На рис. 2 был взят пример части социального графа сети «ВКонтакте», где *УЗ-n* – номер(id) учетной записи, ребра имеют значение «подписан»

и (или) «в друзьях». Участники сообщества «Петербург против коронавируса», с хештегом «#Петербургсвоихнебросает» и общим количеством подписчиков = 21 792. В ходе исследования были выделены признаки учетной записи, канала и способа распространения, скорости передачи, масштабов влияния для последующих разработок выявления и обеспечения контрмер на пользовательские учетные записи, включая потенциальных агентов влияния (лидеров мнений).

Заключение

В рамках данной статьи были рассмотрены признаки пользовательской активности, предложена модель поведения, рассмотрена структура социальной сети. Полученные результатом являются первым шагом на пути исследования, в будущем планируется разработать алгоритмы и методику выявления аномального поведения пользовательской активности для повышения уровня информационной безопасности социальных сетей.

Работа выполнена при финансовой поддержке Гранта РНФ (проект РНФ № 18-71-10094) в СПб ФИЦ РАН.

Список используемых источников

1. Виничук Н. В. Психология аномального поведения // Учебное пособие. Издательство Дальневосточного университета 2004 С. 7. URL: http://window.edu.ru/resource/935/40935/files/dvgu056.pdf (дата обращения: 29.03.2021).

2. Виткова Л. А., Кураева А. М., Проноза А. А., Чечулин А. А. Анализ методов выявления и оценки страниц лидеров мнений в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 233–237.

3. Grimme C., Preuss M., Adam L., and Trautmann H. Social bots: Human-like by means of human control? // Big data. 2017. Vol. 5. No. 4. pp. 279–293.

4. Woolley S. C. and Howard P. N. Computational propaganda worldwide: Executive summary // Working Paper, no. 11. Oxford, UK, p. Projection Computational Propaganda, 2017.

5. Гамидов Т. О., Виткова Л. А., Ковцур М. М. Разработка моделей и алгоритмов анализа данных для исследования хода инцидентов и кризисов в социальных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 3–10.

6. Riley Jenn. Understanding metadata what is metadata, and what is it for? // NISO Publication Date: January 01, 2017. pp. 9–10.

7. Beskow D. M. and Carley K. M. It’s all in a name: detecting and labeling bots by their name // Computational and Mathematical Organization Theory. 2019. pp. 1–12.

8. Stukal D., Sanovich S., Bonneau R. and Tucker J. A. Detecting bots on Russian political Twitter // Big data. 2017. Vol. 5.No. 4. pp. 310–324,

9. Архипкин М. А., Черушева Т. В. Применение нейронных сетей к распознаванию негативного контента в социальных сетях. // Материалы XIV Международной научно-

технической конференции молодых специалистов, аспирантов и студентов Россия, г. Пенза, 1−4 июня 2020 г.

10. Zheng M., Vorobyeva Y., Gabriel A., Qi H., Velasquez N., Manrique P., Johnson D., Restrepo E., Song C., Wuchty S., Johnson N. F. New online ecology of adversarial aggregates: ISIS and beyond // Science 17 Jun 2016. Vol. 352. Iss. 6292. pp. 1459–1463.

УДК 004.41.42
ГРНТИ 81.96

РАЗРАБОТКА МОДИФИЦИРОВАННОГО ПРОТОКОЛА БЕЗОПАСНОГО ОПРЕДЕЛЕНИЯ ТОЧЕК ИНТЕРЕСА ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ВЫСОКОНАГРУЖЕННЫХ СЕТЕЙ

Е. А. Серёжин, В. А. Яковлев

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

Разработаны модификации протокола безопасного определения местоположения точек интереса (POI) пользователей, на основе гомоморфных криптосистем Пэйе и Рабина, адаптированные к работе в высоко нагруженных сетях. Предлагаемые модификации обеспечивают уменьшение нагрузки на сервер и уменьшения времени передачи ответа пользователю. Модификации основываются на трех вариантах сегментации карты местности и применения двухэтапного запроса, что позволяет серверу обработать в десятки раз больше запросов. В связи с развитием и активным использованием беспилотных летательных аппаратов, рассматривается модификация протокола с использованием трехмерной карты. Приведены количественные характеристики эффективности протокола с данными модификациями.

анонимное вычисления, точки интереса, геокарты, гомоморфное шифрование.

В [1, 2] приведено описание, анализ и реализация протокола скрытого определения местоположения точек интереса (*Points of interest* – POI*)* мобильного пользователя. Целью протокола является получение информации о местоположении ближайших *POI* определенного типа без раскрытия серверу и другим пользователям своего местоположения и типа запрашиваемых точек интереса. Для выполнения протокола используется карта местности, разделенная на *nxn* ячеек. В каждой ячейке располагаются точки интереса, закодированными числами *di.*

Протокол состоит из четырех алгоритмов: генерация ключей, формирование запроса пользователя, формирование ответа сервера, получение ответа пользователем. Рассмотрим кратко этот протокол. Пусть пользователь

знает свои координаты своей ячейки и использует их при формировании запроса.

Генерация ключей

Пользователь генерирует две пары (sk_1, pk_1), (sk_2, pk_2) ключей для криптосистем Пэйе и Рабина [1]. Закрытый ключ sk_i состоит из простых чисел $\{p_i, q_i\}$, открытый – из пары чисел $\{g_i, N_i\}$, $i = 1, 2$.

Формирование запроса пользователя

Сначала пользователь, используется алгоритм шифрования Пэйе, вычисляет криптограммы: для *t* типа запрашиваемой точки интереса, используя первый ключ. Для этого для каждого $l \in \{1, 2, \dots, m\}$, где $-$ m число типов точек интереса, пользователь выбирает случайное целое число $r_l \in Z^*_{N_1}$ и вычисляет криптограммы c_l:

$$c_l = \begin{cases} Encrypt\ (1, pk_1) = {g_1}^1 {r_l}^{N_1} \left(mod\ {N_1}^2\right), \text{если } l = t \\ Encrypt\ (0, pk_1) = {g_1}^0 {r_l}^{N_1} \left(mod\ {N_1}^2\right), \text{если } l \neq t. \end{cases} \quad (1)$$

Далее пользователь вычисляет криптограммы для первой своей координаты, используя второй ключ. Криптограмма c'_l вычислется так же как в формуле (1), но $l' \in \{1, 2, \dots, n\}$, где *n*-размер карты и вместо *t* используем первую координату пользователя. Далее шифрует вторую координату вторым ключем по схеме Пэйе, тем самым формируем криптограмму *c*. Пользователь отправляет открытые ключи $(g_1\ N_1, g_2\ N_2)$ и запрос $(c_l\ c'_l\ c)$ серверу.

Формирование ответа сервером.

Сервер, получив запрос вместе с открытыми ключами, используя шифрование Рабина и Пэйе, вычисляет $C_{\alpha,\beta}$ на первом открытом ключе,

$$C_{\alpha,\beta} = \prod_{l=1}^{m} {c_l}^{{d_{\alpha,\beta,l}}^2} (mod\ {N_1}^2)\ . \quad (2)$$

где $\alpha \in \{1, 2, \dots, n\}$, $\beta \in \{1, 2, \dots, n\}$, $d_{\alpha,\beta,l}$ – число, которым закодированы координаты *POI* и типа *POI.*

Далее сервер осуществляет повторное шифрование второй координаты *j* на втором открытом ключе. Для каждого $\beta = \{1,2, \dots, n\}$ выбирается ω_β – целое число из множества $Z^*_{N_2}$ и вычисляется ответ $R = \{C_1, C_2, \dots, C_n\}$:

$$C_\beta = \left(\frac{c}{g^\beta}\right)^{\omega_\beta} \prod_{\alpha=1}^{n} {c'}_\alpha^{\,C_{\alpha,\beta}{}^2} \left(mod\ {N_2}^2\right). \quad (3)$$

Сервер отправляет вычисленные криптограммы $R = \{C_1, C_2, \dots, C_n\}$ пользователю.

Получение ответа пользователем

Пользователь выбирает только криптограмму C_j, которая соответствует его запросу и расшифровывает ее в следующем порядке.

$$C'_j = PallierDecrypt\left(C_j, sk_2\right), \quad (4)$$

$$C''_j = RabinDecrypt\left(C'_j, sk_2\right), \quad (5)$$

$$C'''_j = PallierDecrypt\left(C''_j, sk_1\right), \quad (6)$$

$$d = RabinDecrypt\left(C'''_j, sk_1\right), \quad (7)$$

где *sk* – секретный ключ,

d – информация запрашиваемая информация о точке интереса.

Анализ протокола показывает, что наиболее сложная часть это алгоритм формирования ответа сервером, временная сложность которого $O(n^2)$. Это объясняется тем, что используются все ячейки на карте, что может привести к перегрузке сервера.

Потребность повышения эффективности использования ресурсов является главной задачей в эксплуатации серверов сетей. Особенно остро это проявляется в высоконагруженных сетях, когда нет возможности увеличить вычислительные мощности. Возможность сохранения качества обслуживания пользователей может быть достигнута путем совершенствования сервисов или протоколов обслуживания пользователей.

В [4] были предложено три варианта модификации протокола на основе разных подходов к сегментации карты.

Первая модификация. Карта разделяется на сегменты, каждый из которых содержит *m x m (m<n)* в том числе ячейку в которой находится пользователь. Пользователь формирует криптограмму номера своего сегмента. Сервер получив запрос, расшифровывает номер сегмента, использует данный сегмент для формирования ответа. Поскольку в сегменте существенно меньше ячеек, это снижает объем вычислений.

Вторая модификация. Пользователь сам создает сегмент *m x m* со случайным центром, внутри которого он находится. По сравнению с первым вариантом длина запроса будет такой же.

Третья модификация. Пользователь создает сегмент из случайных малых сегментов и среди них одна, интересующая пользователя. Далее он

шифрует открытым ключом сервера созданный сегмент и отправляет криптограмму вместе с запросом.

Во всех модификациях уменьшается длина криптограммы запроса c'_l, так как пользователю требуется информация только по интересующему его сегменту, поэтому уменьшается время на обработку запроса и длина ответа, формируемого сервером.

Для проверки эффективности модификаций было проведено моделирование модификаций протокола на карте, содержащей $N = 500\,000$ ячеек, для пары ключей длиной 502 и 1024 бит и 50 типов POI. [5].

Как видно из таблицы 1, модифицированный протокол позволяет сократить длину запроса и ответа почти 50 раз и соответственно требуется меньше резервирования памяти для вычислений. Это позволяет обработать большее запросов за тоже время.

ТАБЛИЦА 1. Размеры криптограмм в оригинальном и модифицированном протоколах

Параметр	Размер одной криптограммы, бит	Размер запроса в оригинальном протоколе, бит	Размер запроса в модифицированном протоколе, бит
c_l	2 008	100 400	100 400
c'_l	4 096	2 048 000 000	40 960 000
c	4 096	4 096	4 096
Общий размер запроса		2 048 104 496	41 064 496
$C_{\alpha,\beta}$	1 004	502 000 000	10 040 000
Размер ответа C_β	4 096	2 048 000 000	40 960 000

В современных картах: Яндекс, 2gis, google и т. д. количество типов POI постоянно растет за счет поступления информации от пользователей. Поэтому был проведен анализ протокола с постоянным увеличением количества типов POI. Расчеты показывают, что это может привести к формированию криптограммы c_l недопустимо большой длины (табл. 2).

ТАБЛИЦА 2. Размеры криптограммы в зависимости от количества типов POI

Количество типов POI	Размер криптограммы в запросе, бит	Кбайт
50	100 400	12,25585938
100	200 800	24,51171875
200	401 600	49,0234375
500	1 004 000	122,5585938
1 000	2 008 000	245,1171875

Для уменьшения длины криптограммы предлагается разделение типов POI по диапазонам, например по 100 типов в каждом. Тогда в запросе вместе с криптограммой указывается диапазон. Это существенно уменьшает размер криптограммы, что в итоге уменьшает нагрузку на сервер.

В связи с широким использованием беспилотных дронов, а также началом активной разработки авиатакси, ховеров и прочих летательных аппаратов возникла потребность в использовании трехмерных карт. Поэтому актуальна адаптация разработанных модифицированных протоколов скрытного определения POI для трехмерных карт. Прямой перенос протокола для этих условий не эффективен. Действительно, если использовать протокол для трехмерной карты, то нужно будет проверять все ячейки, без учета того, что большая часть POI находиться на земле, а все что выше, находится в скоплениях. Примеры: торговый центр, многоэтажная парковка, офисное здание и т. д. То есть фактически имеет место множество пустых ячеек, которые замедлят процесс формирования ответа и увеличат размер криптограмм ответа. Временную сложность формирования/выполнения запроса можно оценить в этом случае как $O(h * n^2)$, где h – или количество уровней карты. Следовательно, количество криптограмм в ответе может увеличиться в h раз. Поэтому предлагается при формировании криптограммы добавлять дополнительную метку с указанием диапазона высот или уровня h[.], например, h[2-5] или h[3]. При расчете ответа нужно использовать алгоритм формирования ответа (2) и (3) h раз, то есть для каждой высоты используется свой слой карты:

$$C_{\alpha,\beta}(Map_h, c_l, pk_1) = \prod_{l=1}^{m} {c_l}^{d_{\alpha,\beta,l}{}^2} (mod\ {N_1}^2)\ . \quad (9)$$

$$C_{\beta}(Map_h, {c'}_l, c, pk_2, C_{\alpha,\beta}) = \left(\frac{c}{g^{\beta}}\right)^{\omega_{\beta}} \prod_{\alpha=1}^{n} {c'}_{\alpha}{}^{C_{\alpha,\beta}{}^2} \left(mod\ {N_2}^2\right). \quad (10)$$

Для i-го уровня карты ответ имеет вид $R_i = \{C_1,\ C_2, \dots,\ C_n\}$. А ответ со всеми слоями карты $R = \{R_1,\ R_2, \dots,\ R_h\}$. В таблице 3 приведено сравнение вариантов использования протокола непосредственно для трехмерной карты и с разбиением параметра высоты на уровни. При расчете использовались ключи длиной 502 бит и 1 024 бит.

ТАБЛИЦА 3. Сравнение вариантов использования протокола для трехмерных карт

Варианты карты	Трехмерной	Многоуровневой
Достоинства	Позволяет размешать POI с высокой точностью по высоте.	Требует намного меньше ресурсов.

Варианты карты	Трехмерной	Многоуровневой
Недостатки	Требует много ресурсов для запроса и ответа.	Недостаток точности координат по высоте.
Размер ответа сервера, бит	1 228 800 000	409 600 000

Таким образом, все модификации позволяют уменьшить потребление ресурсов и повысить количество обрабатываемых запросов в несколько раз, что важно для высоконагруженных сетей. Модификация с разделением типов POI по диапазонам позволяет уменьшить в несколько раз длину криптограммы и быстрее передать запрос. Также модификации протокола дают возможность его применения и для трехмерных карт, а для повышения эффективности необходима многоуровневая сегментация карты.

Список используемых источников

1. Yi X. et al. Practical k nearest neighbor queries with location privacy // 2014 IEEE 30th International Conference on Data Engineering. IEEE, 2014. pp. 640–651.

2. Rohilla A., Khurana M., Singh L. Location privacy using homomorphic encryption over cloud // International Journal of Computer Network and Information Security. 2017. Vol. 11. Iss. 8. P. 32.

3. Bilogrevic I. et al. Privacy-preserving optimal meeting location determination on mobile devices // IEEE transactions on information forensics and security. 2014. Vol. 9. Iss. 7. pp. 1141–1156.

4. Серёжин Е. А., Яковлев В. А. Анализ протокола анонимного вычисления точек интереса пользователя на основе сегментации карты привязки // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т.СПб.: СПбГУТ, 2020. С. 787–792.

5. Серёжин Е. А., Яковлев В. А. Сравнение модификаций протокола конфиденциального вычисления точек интереса пользователя // Методы и технические средства обеспечения безопасности информации. – 2020. – №. 29. – С. 83–85.

УДК 004.056
ГРНТИ 81.93.29

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ

В. С. Синельщиков, А. Ю. Цветков

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

Конфиденциальность является главной проблемой в современном информационном обществе. Чтобы защитить частную жизнь отдельных лиц, предприятия должны следовать определенным правилам конфиденциальности, собирая и обрабатывая в процессе персональные данные. В данной работе мы рассматриваем два наиболее часто встречающихся подхода к персональным данным внутри предприятия – E-P3P и аудит.

защита персональных данных, E-P3P, аудит персональных данных, информационная безопасность.

E-P3P

Во многих странах законодательство регулирует сбор и использование персональных данных. Это требует от предприятий соблюдения политик конфиденциальности, которые предписывают, например, время хранения некоторых данных, ограничение доступа, а также цели их использования. Платформа корпоративных политик конфиденциальности (E-P3P), описанная в 2002 году Karjoth, решает именно эту проблему [1]. E-P3P предоставляет XML-ориентированный язык для выражения политик конфиденциальности, а также структуру с особыми функциями конфиденциальности для обеспечения соблюдения этих политик. Прежде чем дать практический пример того, как работает E-P3P, мы дадим обзор основных компонентов E-P3P систем.

В архитектуре E-P3P предприятие собирает персональные данные в так называемых точках сбора. Клиенты предоставляют персональные данные на предприятие, соглашаясь с заявлениями о конфиденциальности предприятия. Каждая точка сбора имеет форму, которая связывает персональные данные со своим объектом, объявляет его тип, например, медицинскую запись или почтовый адрес, а также выбранные вопросы. Эта связь остается неповрежденной внутри предприятия и может даже отправиться на другое. В E-P3P это называется парадигмой «липкой политики» (“*the sticky policy*”) [1]. Липкая политика не относится к политикам предприятия, а относится к заявлениям о конфиденциальности и заполненным вариантам согласия в точках сбора данных, которые связываются с персональными данными.

Защитник конфиденциальности предприятия объявляет, используя язык политик E-P3P, политику конфиденциальности, указав, кто может получить доступ к определённому типу данных и для каких целей. Политика конфиденциальности также может относиться к выбору субъекта и к определенным обязательствам по конфиденциальности, например, удаление данные в течение 30 дней. Затем операции над ПО предприятия сопоставляются с терминологией политики конфиденциальности, а в обратном направлении конфиденциальные обязательства, используемые в политиках конфиденциальности, сопоставляются с операциями в ПО. Например, операция «отправить» системы массовой рассылки, используемой в отделе маркетинга, сопоставляется с указаниями о маркетинге в политике конфиденциальности. И наоборот, термин, определяющий тему в политике конфиденциальности, реализуется как операция «отмены подписки» системы списка адресов.

Доступ к персональным данным субъекта предоставляется в два этапа. Доступ к ПО предприятия оценивается системой контроля доступа, например, с учетом ролей сотрудников, которая не зависит от системы E-P3P. Затем ПО делает запрос доступа к личным данным субъекта к системе обеспечения конфиденциальности. Система обеспечения конфиденциальности решает, какой доступ должен быть предоставлен, путем оценки политики предприятия и сопоставления с выбором согласия субъекта. Если доступ предоставляется, система обеспечения конфиденциальности также выполняет возможные обязанности конфиденциальности, указанные в политике предприятия.

Пример 1. Рассмотрим это на примере интернет-магазина. Предприятие, которому он принадлежит, должно разместить политику безопасности конфиденциальных данных на странице оплаты. С помощью E-P3P внутренние механизмы предприятия действуют согласно этой политике.

Пусть Вова использует этот сайт. Условия политики конфиденциальности указывают, что имя и номер кредитной карты будут доступны работникам расчётного отдела, с учётом того, что данные удаляются сразу после обработки. Помимо этого, работники могут использовать адрес электронной почты Вовы для рекламы, если он дал на это согласие. Код этой политики указан ниже (листинг).

```
<ep3pPolicy
version = '1.2'
issuer = 'Store'
vocabulary-ref = 'http://www.Store.com/Voc'
default-ruling='deny'>
<rule>
<dataCategory>allData.creditCardData</dataCategory>
<purpose>business.billing</purpose>
<userCategory>employees.billing</userCategory>
```

```
<ruling>ALLOW</ruling>
<action>read</action>
<obligation action=deleteWithIn(30)</obligation></rule>
<condition/>
<rule>
<dataCategory>allData.contactData</dataCategory>
<purpose>business.marketing</purpose>
<userCategory>employees</userCategory>
<ruling>ALLOW</ruling>
<action>read</action>
<obligation\>
<condition>OptInToMarketing=True</condition>
</ruleset>
</ep3pPolicy>
```

Листинг. Простейшая политика конфиденциальности

Допустим, что наше предприятие использует массовую рассылку, чтобы отправлять рекламные предложения. Система массового оповещения, после проверки, что рассылка осуществляется авторизованным лицом, оправляет запрос к системе защиты конфиденциальности для проверки того, что доступ должен быть предоставлен, основываясь на политике конфиденциальности предприятия. Этот запрос выглядит так:

```
<ep3pQuery>
Privacy in an Ambient World 7
<userCategory>employees</userCategory>
<dataCategory>allData.contactData</dataCategory>
<purpose>business.marketing</purpose>
<action>Read</action>
</ep3pQuery>
```

Запрос проверяется системами защиты E-P3P. Политика безопасности предписывает проверку того, что Вова дал согласие на использование его адреса электронной почты для рекламных предложений. Если да, система защиты предоставляет доступ, иначе – запрещает его. Кроме того, запрет доступа – значение по умолчанию.

Ключевые элементы политики E-P3P: создание словаря для обращения к данным, данные по умолчания и правила предоставления доступа. Правила предоставления доступа указывают, какие пользователи могут совершать определённые действия с определённым типом данных с определёнными целями. Словарь определяет иерархию типов данных, целей использования и пользователей, что позволяет представить политику безопасности предприятия в виде иерархии.

Полный язык и семантика на основе XML для политик E-P3P была определена в работе Ashley [2]. EPAL [3], язык, очень похожий на (и созданный из) E-P3P, был представлен IBM в W3C для стандартизации, но на момент написания он не был одобрен. IBM также внедрила EPAL в IBM

TivoliPrivacy Manager, систему, обеспечивающую автоматическое управление персональными данными с целью снижения затрат предприятия на управление конфиденциальностью и рисков утечек данных.

Как мы уже упоминали, E-P3P также позволяет перемещать данные из одного предприятия в другое вместе с формой, которая использовалась для ее сбора; «липкая политика». Таким образом, предприятие получает персональные данные с политикой конфиденциальности, выполнение которых может потребовать составления политик или проверки того, что одна политика является уточнением другой. Точное определение операций составления и уточнения для политик E-P3P дано в работе Backes [4].

Аудит

Когда E-P3P предлагает методы для определения политик конфиденциальности и обеспечения соблюдения этих политик в организации, вопрос о том, как защитить конфиденциальность, когда данные могут быть модифицированы и/или перемещаться по разным компаниям, остается открытым. В этом разделе мы описываем метод аудита персональных данных [5], который предоставляет альтернативный подход к защите конфиденциальности. Аудит решает проблему соответствия политикам данных, которые перемещаются в разных доменах безопасности.

Когда данные покидают домен безопасности, контроля доступа недостаточно для защиты данных, поскольку контроль доступа перемещается вместе с данными. С другой стороны, методы управления цифровыми правами (DRM) [6] предназначены для обеспечения соответствия политик для данных, которые перемещаются по доменам безопасности. Лицензии и ключи необходимы для доступа к данным и описания политики для этих данных.

Несмотря на то, что подход к использованию лицензий, ориентированный на данные, можно использовать для предоставления политик конфиденциальности, методы DRM часто недостаточно гибки или имеют требования (такие как необходимость специального (надежного) оборудования) которые не реалистичны в нашем сценарии корпоративного сотрудничества. Чтобы механизм защиты персональных данных был жизнеспособным, он не должен чрезмерно увеличивать затраты или требуемые усилия для вовлеченных компаний.

Аудит персональных данных использует методы, ориентированные на данные, когда соблюдение политик не выполняется априорно, но вместо этого действия пользователей, возможно, должны быть просто обработаны апостериори, то есть пользователи могут быть подвергнуты аудиту. Таким образом, поддерживается подотчётность пользователей и их действий. Подход аудита старается препятствовать, а не предотвращать нарушение правил.

Таким образом, аудит формализует контрольный журнал, который уже присутствует во многих компаниях и позволяет использовать его для защиты конфиденциальности. В некоторых случаях, возможно, это необходимо для защиты аудиторского следа, например, с использованием методов из протоколов, защищенных от несанкционированного доступа.

В подходе аудита неправильное использование не предотвращается, а сдерживается: у органов, осуществляющих аудит, есть мандат на проверку того, использовались ли данные в соответствии с политиками. В такой ситуации пользователи должны быть подвергнуты аудиту, и аудиторам должны быть доступны достаточные аудиторские журналы. Это хорошо подходит, например, в больницах или компаниях, где пользователи могут нести ответственность за свои действия, а контрольные журналы часто уже являются частью требований безопасности. Реализовать эти требования может быть трудно в определенных условиях, таких как большие открытые сети (например, P2P). Впрочем, это может измениться; например, законодательство ЕС требует, чтобы интернет-провайдеры сохраняли записи IP-трафика всех своих пользователей.

Список используемых источников

1. Karjoth G., Schunter M., Waidner M. Platform for enterprise privacy practices: Privacy-enabled management of customer data / In Dingledine, R., Syverson, P.F., eds. // Proc. International Workshop on Privacy Enhancing Technologies (PET). Lectures in Computer Science, Springer. 2002. pp. 69–84.

2. Ashley P., Hada S., Karjoth G., Schunter M.: E-P3P privacy policies and privacy authorization / In Samarati, P., ed. // Proc. Workshop on Privacy in the Electronic Society (WPES), ACM Press (2002). pp. 103–109.

3. Ashley P., Hada S., Karjoth G., Schunter M. Enterprise privacy authorization language (EPAL 1.2) // W3C member submission 10 november 2003.

4. Backes M., Pfitzmann, B., Schunter, M.: A toolkit for managing enterprise privacy policies / In Gollmann, D., Snekkenes, E., eds. // Proc. European Symposium on Research in Computer Security (ESORICS), Springer. 2003. pp. 162–180.

5. Скабцов Н. Аудит безопасности информационных систем: учебник. СПб.: Питер, 2018. 272 с. ISBN: 978-5-4461-0662-2

6. Жарова А. К., Мальцева С. В. Защита интеллектуальной собственности. Изд. 2, пер. и доп. СПб.: Юрайт, 2015. 427 с.

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

УДК 004.056.57
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ ФРЕЙМВОРКА ZEEK И ELK-СТЕКА ДЛЯ АНАЛИЗА РАССЫЛОК ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

М. А. Скорых

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

В настоящее время существует множество видов компьютерных атак. Одним из видов компьютерных атак является рассылка вредоносного программного обеспечения посредством электронной почты. Комплексный анализ таких рассылок является нетривиальной задачей для специалистов по информационной безопасности. В данной статье рассматривается подход к анализу рассылок вредоносного программного обеспечения при помощи фреймворка для анализа сетевого трафика Zeek и ELK-стека.

обнаружение компьютерных атак, вредоносное программное обеспечение, Zeek, ELK-стек.

Рассылка электронных почтовых писем, содержащих вредоносное программное обеспечение (далее – ВПО) на данный момент является одним из основных видов компьютерных атак. Так, согласно данным лаборатории Касперского, средняя доля спама за второй квартал 2020 года в мировом почтовом трафике составила 50,18 % [1]. Анализ массовых рассылок ВПО, позволяет специалистам в области информационной безопасности выявлять общие черты таких рассылок, определять их источник, составлять «черные» списки адресов отправителей писем, узнавать о возможной компрометации учетных записей отправителей электронных писем. В данной статье рассмотрен вариант анализа рассылок ВПО с использованием фреймворка для анализа сетевого трафика Zeek и ELK-стека.

Zeek – это бесплатный пассивный фреймворк для анализа сетевого трафика с открытым исходным кодом [2]. Zeek представляет собой монитор безопасности, проверяющий сетевой трафик на предмет наличия в нем признаков подозрительной активности. После обработки входящего трафика, Zeek генерирует множество журнальных файлов, описывающих зафиксированную сетевую активность. Zeek может «разбирать» основные протоколы прикладного уровня, в том числе такие протоколы как HTTP, DHCP, DNS, FTP, IMAP, POP3, SMTP, NTLM, RADIUS, SIP, SNMP, SSH [2].

В журнальном файле протокола SMTP фиксируется следующая информация: метка времени, идентификатор сессии, 4-х элементный кортеж, состоящий из IP-адресов и портов источника и назначения, почтовые адреса находящиеся в заголовках письма “Helo”, “From”, “Rcpt”, содержание почтовых заголовков “Date”, “From”, “To”, “CC”, “ReplyTo”, “MsgID”, “In-Reply-To”, “Subject”, “X-Originating-IP”, “first Received”, “second Received”, список IP-адресов, через которые прошло письмо (извлекается из служебных заголовков письма). Также фреймворк Zeek имеет возможность извлекать файлы из сетевого трафика, вычислять их энтропию и хэш-суммы, используя алгоритмы MD5 и SHA1, определять MIME тип.

Используя исчерпывающую информацию, предоставляемую фреймворком Zeek, появляется возможность осуществлять некоторые функции в контексте информационной безопасности:

1. Проверять почтовые адреса отправителей писем, IP-адреса инициаторов отправки электронного письма, хэш-суммы извлеченных файлов на предмет их нахождения в различных базах репутации.

2. Основываясь на MIME типе передаваемого файла осуществлять его отправку в систему автоматического исследования ВПО.

3. Агрегировать по определённым признакам однотипные рассылки электронных сообщений, например, по теме, типу вложения, автономной системе IP-адреса инициатора отправки письма.

4. Проверять составление служебных заголовков электронного письма на предмет аномалий, например, нахождение различных адресов электронной почты в заголовках письма “From” и “ReplyTo”.

5. Накопление и хранение информации о SMTP трафике для возможности осуществления ретроспективного анализа.

Для реализации функций 1, 3, 5, а также для централизованного хранения всей информации из журнальных файлов Zeek и дополнительных источников можно применить ELK-стек. Основными программными компонентами стека являются: Elasticsearch – поисковое и аналитическое ядро системы; Logstash – программный конвейер обработки данных; Kibana – средство визуализации и навигации по системе; Beats – набор программ, необходимых для сбора и транспортировки системных журналов и файлов [3].

Для отправки информации из журнальных файлов Zeek на программный конвейер Logstash можно использовать коллектор Filebeat.

Стоит отметить, что источником данных может служить несколько телекоммуникационных сетей или организаций. Для удобства анализа и обеспечения возможности горизонтального масштабирования системы анализа рассылок ВПО предлагается использовать отдельные сенсора Zeek. Сенсор Zeek представляет собой физический или виртуальный сервер, находящийся в отдельной телекоммуникационной сети, с установленным на нем фреймворком Zeek и коллектором Filebeat.

В плагине фильтрации Logstash “translate” удобно реализовать проверку почтовых адресов, IP-адресов и хэш-сумм на предмет их нахождения в различных базах репутации, в простейшем случае для этого достаточно составить текстовые файлы с перечнем вредоносных индикаторов компрометации и указать их параметре “dictionary” вышеупомянутого плагина. Плагин фильтрации Logstash “geoip” позволяет определить местоположение IP-адресов, входящих в цепочку пересылки электронного письма.

Далее обогащенные данные индексируются в Elasticsearch. При необходимости в шаблоне индекса Elasticsearch можно указать алгоритм сжатия данных, а также настроить ротацию индексов при помощи программного обеспечения Curator [4]. Elasticsearch предоставляет возможность создания вычисляемых полей, данную возможность можно использовать для вычисления общего «уровня угрозы» электронного письма, зависящего от репутаций IP-адресов, адресов отправителей электронных писем, хэш-сумм пересылаемых файлов и других пользовательских показателей.

Для визуализации и аналитической обработки информации в составе ELK-стека используется Kibana. С помощью возможностей программного средства Kibana можно создавать пользовательские дашборды, визуализировать на географической карте путь электронного письма, определять источники рассылки, выявлять статистические свойства рассылки, выгружать списки интересующих полей электронных писем, агрегировать документы в индексах по заданным полям.

Структурная схема варианта применения фреймворка Zeek и ELK-стека для анализа рассылок ВПО в сети нескольких организаций представлена на рис.

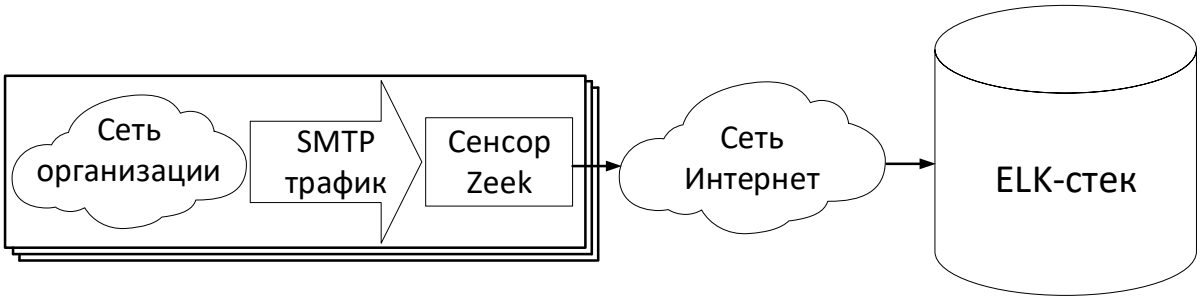


Рис. Структурная схема применения фреймворка Zeek и ELK-стека для анализа рассылок вредоносного программного обеспечения

Преимуществами данного решения являются:

1. Отсутствие затрат на покупку программного обеспечения.

2. Возможность охвата нескольких удаленных организаций при мониторинге почтового трафика, горизонтальная масштабируемость.

3. Хранение исчерпывающей информации о почтовых соединениях.

4. Возможность проведения ретроспективного анализа почтовых рассылок.

5. Возможность реализации автоматического анализа в песочницах приложений электронных почтовых сообщений.

6. Встроенные в ELK-стек возможности обеспечения отказоустойчивости и доступности данных.

К недостаткам данного решения можно отнести:

1. Отсутствие активного воздействия (блокировке входящего электронного письма) при обнаружении вредоносной рассылки.

2. Отсутствие возможности анализа шифрованного трафика.

3. Необходимость выделения относительно высоких мощностей под функционирование ELK-стека.

4. Необходимость доступа к актуальным базам репутации IP-адресов, хэш-сумм и электронных почтовых адресов.

Список используемых источников

1. Спам и фишинг во II квартале 2020 года. URL: https://securelist.ru/spam-and-phishing-in-q2-2020/97655/.

2. Zeek Manual. URL: https://docs.zeek.org.

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

4. Curator Reference. URL: https://www.elastic.co/guide/en/elasticsearch/client/curator/current/index.html

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

УДК 004.7
ГРНТИ 81.93.29

МОДЕЛЬ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА

Д. Д. Стародубова, Р. Д. Стародубов, И. А. Ушаков

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

Обнаружение сетевых аномалий является важной и динамично развивающейся областью исследований. В настоящее время, несмотря на интенсивное развитие в области сетевых технологий, злоумышленники постоянно увеличивают количество атак на сетевую инфраструктуру. Системы обнаружения сетевых аномалий играют важную

роль в обеспечении сетевой безопасности. Из-за динамического изменения вредоносного программного обеспечения в данных сетевого трафика традиционные инструменты и методы не в состоянии защитить сети от проникновения атак. В работе предложена модель обнаружения аномалий. Описываются структура и алгоритмы функционирования системы обнаружения аномалий.

сетевые аномалии, сетевой трафик, обнаружение аномалий, анализ сетевого трафика, нейронные сети.

Учитывая возрастающие с каждым годом достижения в области сетевых технологий, злоумышленники активно увеличивают количество атак на сетевую инфраструктуру. Специалисты пытаются предотвратить такие атаки с помощью средств и систем обнаружения вторжений. Системы обнаружения, в большинстве своем не имеют возможности обнаруживать новые или ранее неизвестные атаки. Особый тип систем обнаружения - системы обнаружения аномалий, разрабатывают модели, основанные на нормальном поведении системы или сети с целью обнаружения как известных, так и неизвестных атак. Системы обнаружения аномалий сталкиваются со многими проблемами, включая высокую частоту ложных срабатываний, возможность работы в режиме онлайн и масштабируемость.

В связи с широким распространением передовых сетевых технологий также возрастает угроза со стороны спамеров и злоумышленников. Системы обнаружения вторжений и технологии брандмауэра могут предотвратить только некоторые из этих угроз. Исследование [1] оценивает количество попыток вторжения порядка 25 миллиардов в день и продолжает увеличиваться. Макхью [2] утверждает, что атаки становятся все более сложными и более автоматизированными, и, таким образом, навыки, необходимые для их запуска, сокращаются. Существует два типа систем обнаружения: сигнатурные и аномальные. Сигнатурные используют сигнатуры уже известных атак. Такие системы требуют частого обновления сигнатур и не могут обнаружить неизвестные атаки или аномалии, для которых сигнатуры отсутствуют в базе данных. Системы обнаружения на основе аномалий являются особенно эффективными в обнаружении и предотвращении известных, а также неизвестных атак или атак нулевого дня [3]. Однако система обнаружения на основе аномалий имеет много недостатков, таких как высокая частота ложных срабатываний и невозможность масштабирования до гигабитных скоростей.

Вторжения или атаки могут быть обнаружены на основе сбора информации из сети или хоста, а именно на основе входящего и исходящего трафика. Эта проблема была сформулирована в [5] с точки зрения распознавания образов. Инкрементные подходы используются для ускорения работы системы с точки зрения обучения, а также тестирования примеров.

Совершенствование методов интеллектуального анализа данных и информационных технологий позволяет изучать алгоритмы интеллектуального анализа данных с точки зрения сохранения конфиденциальности. В качестве алгоритмов интеллектуального анализа могут выступать методы интеллектуального анализа, такие как статистические методы, байесовские сети, алгоритмы неконтролируемой кластеризации и другие.

В сетевых системах обнаружения вторжений предполагается, что вторжение будет проявляться в качестве следа. Согласно принципам обнаружения, обнаружение вторжений классифицируется на следующие категории. ***Обнаружение аномалий:*** этот метод имеет два этапа: этап обучения и этап обнаружения. На первом этапе, алгоритмы машинного обучения обучаются в отсутствие атаки генерировать профиль для нормального поведения, на втором этапе, обнаружения, при отклонении от нормального поведения, события помечаются как атака. На рис. показана общая модель обнаружения сетевых аномалий. Входные данные нуждаются в обработке, однако методы обработки варьируются от метода к методу. Категории обнаружения аномалий являются контролируемыми и неконтролируемыми. Результат обнаружения аномалии оценивается баллом или меткой.

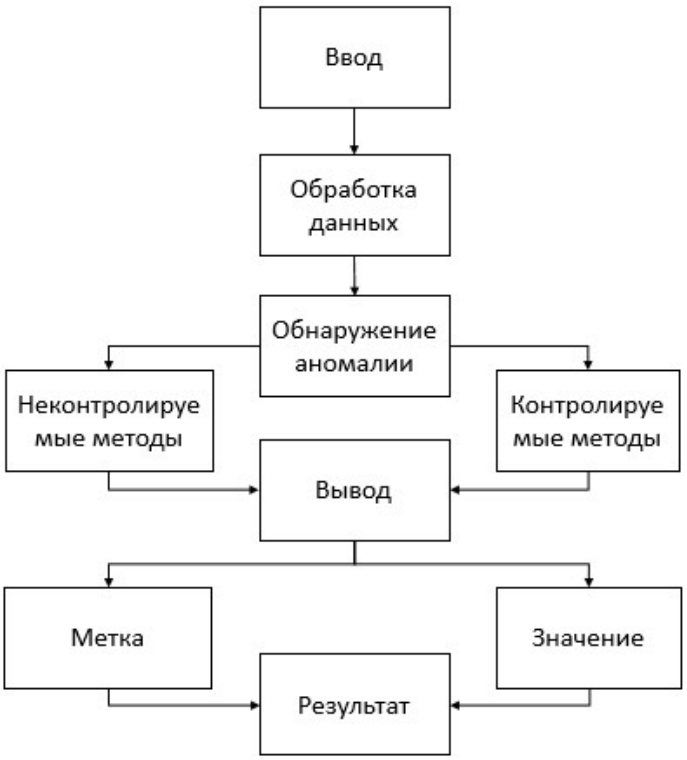


Рис. Обобщенная модель обнаружения аномалий сетевого трафика

Гибридное обнаружение: как метод обнаружения злонамеренного использования, так и метод обнаружения аномалий имеют недостатки, так как метод злонамеренного использования не способен обрабатывать неизвестные атаки, а метод обнаружения аномалий обычно вызывает ложные тревоги. Для нивелирования недостатков предлагается совместное использование.

Обнаружение сканирования: обнаружение сканирования генерирует оповещения, если злоумышленники сканируют систему перед началом атаки [3].

Профилирующие Модули: Он группирует сходные сетевые соединения и ищет доминирующее поведение с помощью алгоритмов кластеризации [3].

Интеллектуальный анализ данных постоянно пытается улучшить процесс обнаружения знаний, он использует статистические модели, искусственный интеллект, математические модели и алгоритмы машинного обучения для извлечения ранее неизвестных поведений из данных. Извлеченный паттерн поведения важен для различения аномального поведения от нормального поведения в данных. Интеллектуальный анализ данных имеет два основных метода: контролируемый и неконтролируемый, контролируемые методы используют помеченные данные, а неконтролируемые методы используют не помеченные данные в качестве обучающего набора. Примерами контролируемыми методами являются классификация и регрессия, а примерами неконтролируемых методов являются ассоциация и кластеризация [3].

Машинное обучение. Процесс построения научной модели, основанный на знаниях, полученных из выборочного набора обучающих данных, называется обучением. Машинное обучение-это сложный вычислительный процесс, который автоматически распознает поведения и делает их интеллектуальными. Решение принимается на основе выборочных данных. Методы машинного обучения можно разделить на четыре категории: основанные на соединениях, основанные на символах, основанные на поведении и основанные на иммунной системе. В зависимости от наличия обучающих данных машинное обучение делится в основном на контролируемые и неконтролируемые. Контролируемый метод в свою очередь делится на структурный и объективный, примерами контролируемого метода являются искусственная нейронная сеть, опорные вектора и дерево решений. В неконтролируемом методе в выборке данных нет цели или метки, некоторые из наиболее известных-иерархическая кластеризация, *k*-среднее и карта самоорганизации [3, 4].

Таким образом, прогнозирование поведения трафика применимо как при проектировании, так и во время обеспечения безопасности. Анализ трафика важен для эффективного управления сетью и своевременного обнаружения аномалий. Главным требованием к любым методам обнаружения вторжений является возможность обнаружения произвольных типов аномалий, в том числе, распределенных во времени.

Список используемых источников

1. Ahmed M., Mahmood A. N., and Hu J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. 2016. Vol. 60. pp. 19–31.

2. Ullah F. and Babar M. A. Architectural tactics for big data cybersecurity analytic systems: A review. arXiv preprint arXiv:1802.03178, 2018.

3. Dua S. and Du X. Data mining and machine learning in cybersecurity. Auerbach Publications, 2016.

4. Buczak A. L. and Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection // IEEE Communications Surveys & Tutorials. 2016. Vol. 18. No. 2. pp. 1153–1176.

5. Moustafa N. and Slay J. The evaluation of network anomaly detection systems: Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set // Information Security Journal: A Global Perspective. 2016. Vol. 25. No. 1-3. pp. 18– 31.

Статья представлена научным руководителем, доцент кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом В. Н. Волкогоновым.

УДК 654.078
ГРНТИ 49.33.35

СИСТЕМА КОНТРОЛЯ СОЕДИНЕНИЙ В КОРПОРАТИВНЫХ СЕТЯХ

А. А. Суюндукова, В. В. Фицов

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

В статье описывается система контроля соединений, принимающая решения на основе данных систем OSS/BSS. Предполагается, что сетевые соединения осуществляются объектами, которые являются источниками потока информации. В роли объектов выступают IoT-устройства или пользователи. Помимо других задач, система OSS/BSS определяет перечень разрешенных и запрещенных взаимодействий объектов. Более эффективная работа системы контроля соединений достигается при использовании технологии OSS/BSS, SDN и DPI. Контроллер сети SDN используется для управления сетевыми соединениями, после принятия решения о их допустимость системой контроля. Инспекция трафика за счет технологии DPI осуществляется для выявления передаваемого контента, либо для определения используемых приложений. Система контроля соединений определяет допустимость сетевых взаимодействий объектов друг с другом. Для упрощения работ по внедрению системы контроля соединений разработан и представлен алгоритм работы системы контроля соединения при взаимодействии перечисленных выше технологий.

система контроля соединений, технология OSS/BSS, технология DPI, программно-конфигурируемая сеть, бизнес процессы, информационная безопасность, алгоритм работы.

Не ослабевает направление по описанию бизнес процессов с целью последующего внедрения программного обеспечения мониторинга и управле-

ния составляющими этих процессов. Такой подход может повысить качество предоставляемых услуг пользователям и помочь в организации взаимодействия между множеством устройств интернета вещей. В [1, 2] дается поверхностное описание возможности применить систему поддержки операций и бизнеса (OSS/BSS, *Operation Support System* / *Business Support System*) для управления возможностью осуществить соединение в сети передачи данных. Однако, отсутствует описание алгоритма взаимодействия устройств и технологий для использования такого типа управления. Основная цель такого применения заключается в повышении информационной безопасности на сети связи или в организации. Далее в данной статье система, обеспечивающая управление возможностью установить сетевое подключение (в том числе к конкретному объекту), будет называться системой контроля соединений.

Обычно, защита сети осуществляется на шлюзах безопасности или системах обнаружения вторжения. В случае применения системы контроля доступа часть соединений, которые нужны для сетевых атак, не будут установлены сетью, т. к. изначально не разрешены с точки зрения бизнес-процесса. Использование системы контроля соединений сможет обеспечить защиту от сетевых атак и утечек информации через сеть, решая одну из самых злободневных проблем информационной безопасности. Применение такого рода защиты сети особенно актуально в корпоративных сетях, где несмотря на множество предпринимаемых мер, не удается обеспечить полный контроль за обменом информацией в сети. С помощью системы контроля соединений весь передаваемый поток данных может быть проверен соответствующими устройствами.

Для работы системы контроля соединений необходимо: иметь сведения о допустимых (или запрещенных) взаимодействиях между сетевыми объектами (или пользователями, которые их используют); получать данные об осуществляемых сетевых соединениях; осуществлять разрешение или запрещение соединений. Таким образом, основная идея системы контроля соединений состоит в управлении потоками сетевого трафика, по заранее имеющимся данным о взаимодействиях сетевых объектов (пользователей) [4].

Очевидно, что для обеспечения функционирования системы контроля соединений на традиционной пакетной сети необходимо наладить взаимодействие между системой OSS/BSS (обладающей сведениями о разрешенных взаимодействиях) и сетевым устройством (маршрутизатором или коммутатором), которое может разрешить или запретить осуществление сетевого соединения внутри себя. Такой подход теоретически осуществим, но практически не очень удобен по ряду причин.

Более интересным выглядит использование системы контроля соединений на программно конфигурируемых сетях (SDN, *Software-Defined Networking*), где проще организовать взаимодействие между контроллером

SDN-сети и системой OSS/BSS. Кроме того, SDN-контроллер позволяет обеспечивать управление сетевыми соединениями на сегменте IP-сети. При этом в SDN-сети поток данных выделяется из общего трафика по таким отличительным чертам, как MAC и IP-адреса, транспортные порты и тип протокола. SDN-коммутатор (уровень данных) осуществляет пересылку потоков трафика согласно правилам, полученным от SDN-контроллера (уровень управления трафиком). Контроллер SDN-сети, запрашивает у системы OSS/BSS разрешено ли осуществлять взаимодействие между сетевыми устройствами (пользователями). Система OSS/BSS также смогла бы фиксировать факт такого взаимодействия, и его параметры такие как время передачи, объем переданного трафика и прочие, связывая их с реализацией того или иного бизнес процесса. Проверка такого рода исполнима благодаря набору правил FlowTable [5].

Описанный выше способ технической реализации системы контроля соединений позволяет осуществить управление над создаваемыми в сети соединениями. Однако, такой способ не позволяет контролировать соединения с точки зрения передаваемой в них информации. Для этого в случае использования системы контроля соединений на традиционной пакетной сети передачи данных или на SDN-сети, может быть задействована технология глубокой инспекции пакетов (DPI, *Deep Packet Inspection*). Технология DPI представляет собой не только проверку заголовков передаваемого трафика, но и передаваемых данных.

Если наладить взаимодействие между системами OSS/BSS и DPI, то последняя позволит осуществлять пропуск или блокировку соединений в точке на сети, где она установлена.

Когда система OSS/BSS разрешает все виды взаимодействий между сетевыми устройствами (пользователями), а сетевые устройства традиционной или SDN-сети пропускают трафик согласно этому разрешению, нужды в системе DPI нет. В случае, когда система OSS/BSS разрешает только часть типов взаимодействий между объектами (например, ограниченный набор сетевых приложений), то поток трафика передается на систему DPI для определения конкретного приложения. После чего принимается решение о допустимости такого взаимодействия.

Кроме того, в компетенции технологии DPI входит проверка передаваемого трафика на факт передачи вредоносного контента. Однако, оборудование DPI является дорогостоящим и поэтому не целесообразно применять DPI на каждой системе контроля соединений. Следует обратить внимание на решения использования оборудования DPI несколькими системами контроля соединениями. А также использовать предоставление DPI как услуги (DPI *as Service*), облачную DPI или DPI на основе системы виртуализации, как более перспективный и экономичный подход.

В качестве примера на рис. 1 продемонстрирована схема системы контроля соединений, использующая технологии OSS/BSS, SDN и DPI.

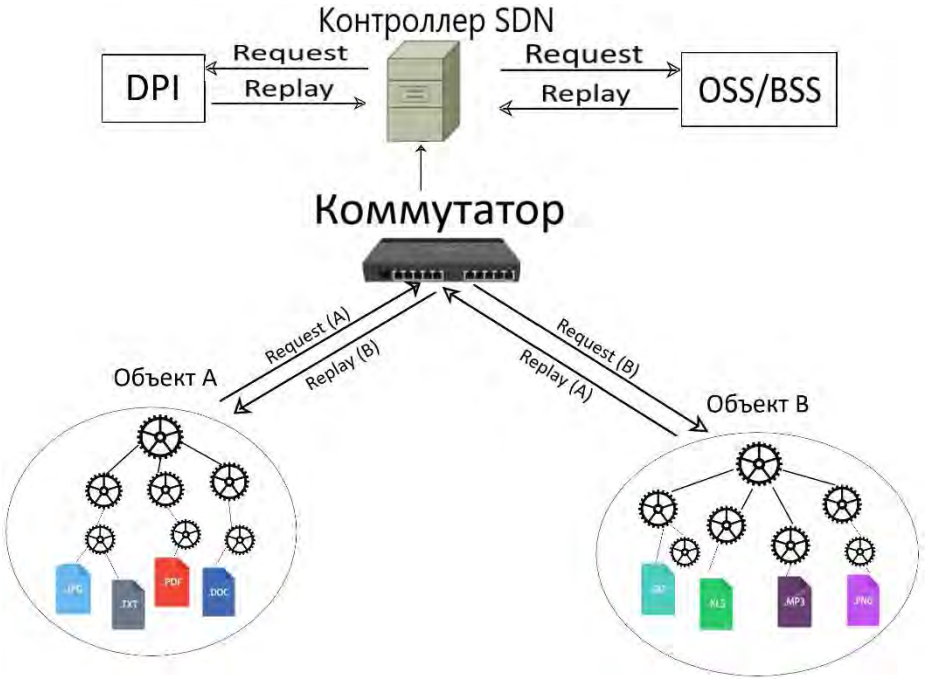


Рис. 1. Схема системы контроля соединений программно-конфигурируемой сети.

На рис. 1 отображены два оконечных сетевых устройства (*A* и *B*), находящихся в SDN-сети. Каждое из оконечных устройств, имеет ряд сетевых приложений и файлов. В [3] оконечные устройства, их приложения и файлы предлагается представить в виде дерева. Корни дерева *A*, *B* – данные информационных преобразований (задачи).

Оконечное устройство *A* отправляет по сети запрос данных оконечного устройства *B*. В случае SDN-сети, SDN-коммутатор обнаруживает новый поток трафика, и запрашивает правила по его обработке у SDN-контроллера. Последний проверяет, разрешено ли такое взаимодействие, отправляя запрос к системе OSS/BSS. Затем оконечное устройство *A*, через сетевое устройство отправляет оконечному устройству *B* подтверждение запроса.

На рис. 2 представлен алгоритм описания совокупности используемых технологий и механизмов системой контроля соединений.

В зависимости от выбранной политики безопасности, взаимодействие оконечных устройств *A* и *B* допустимо лишь после подтверждения системой OSS/BSS разрешения на осуществляемое взаимодействие.

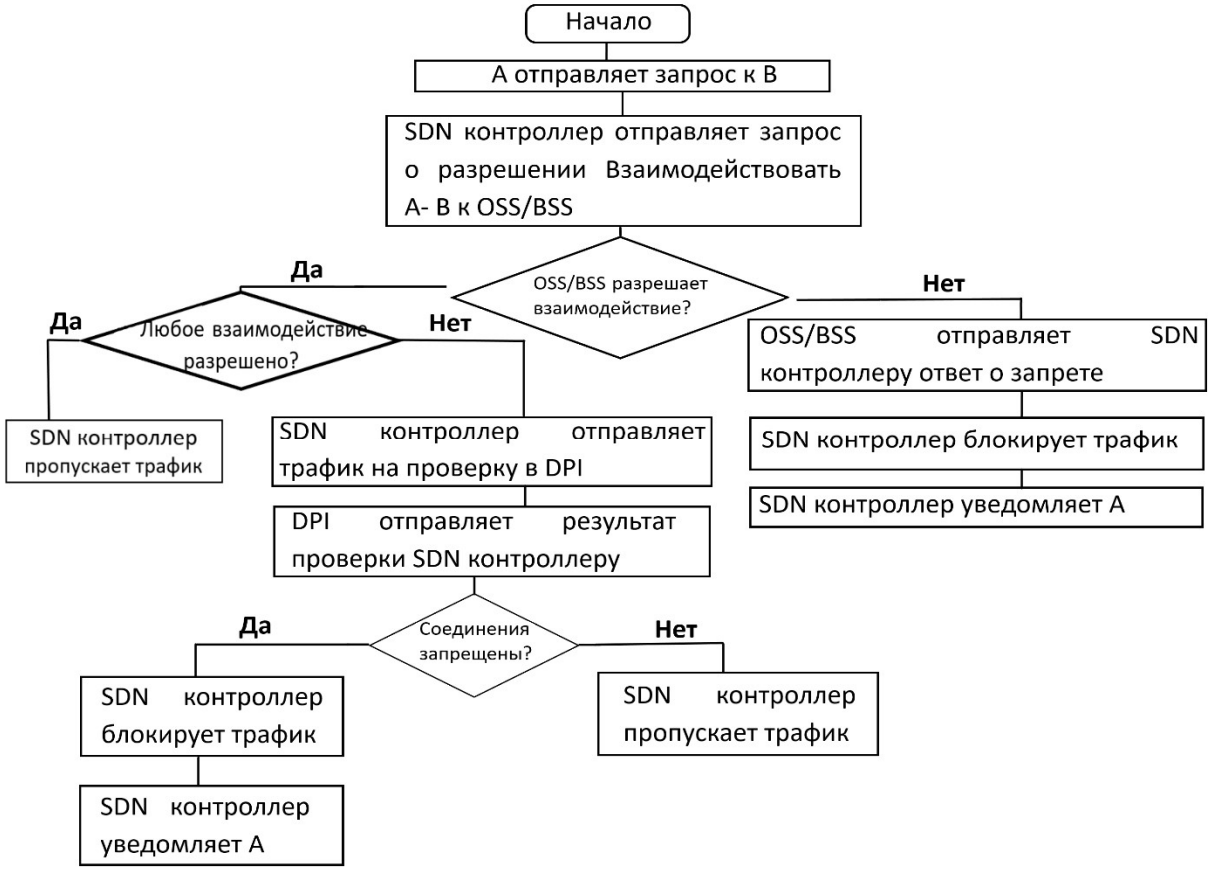


Рис. 2. Алгоритм системы контроля соединений

Рассмотрим ситуации алгоритма более подробно для SDN-сети. Пусть оконечное устройство *A* решает отправить некие данные оконечному устройству B. SDN-контроллер обнаруживает новое взаимодействие, и отправляет запрос к системе OSS/BSS. Последняя на основе имеющихся данных разрешает или запрещает взаимодействие, и сообщает результат контроллеру сети SDN. Когда взаимодействие разрешено, следует уточнение о том, любое взаимодействие между *A* и *B* разрешено или строго определенное. SDN-контроллер разрешает SDN-коммутатору пропустить поток трафика или дает указания его блокировать. Когда разрешается ограниченный перечень взаимодействий, поток трафика передается на проверку системе DPI. Результаты глубокой инспекции пакетов передаются на контроллер сети SDN, который, уже пропускает или запрещает данное взаимодействие. Если взаимодействие разрешено, то об этом уведомляется оконечное устройство *B*. Если – запрещено, то – оконечное устройство *A*.

Не исключено осуществление запроса к системе OSS/BSS, уже после проверки потока трафика оборудованием DPI, когда уже можно дать ответ о допустимости передачи трафика конкретного приложения или с определенным содержимым. Таким образом, становится возможным разрешить передачу всего контента, либо лишь определенной его части.

Система контроля соединений может использовать совокупность технологий для обеспечения информационной безопасности в корпоративной сети. Нами был впервые разработан алгоритм, наглядно описывающий работу так называемой системы контроля соединений. Мы надеемся, что представленный на рис. 2 алгоритм, может быть использован для создания прототипа системы контроля соединений.

Список используемых источников

1. Гольдштейн А. Б., Зимин А. В. Специфика сертифицированных испытаний OSS/BSS // Вестник связи. 2020. № 12. С. 37–44.

2. Фицов В. В. Методы построения сетевых архитектур систем DPI // Вестник связи. 2020. № 12. С. 32–37.

3. Грушо А. А., Забежайло М. И., Грушо Н. А., Тимонина Е. Е. Информационная безопасность на основе метаданных в компонентно-интеграционных архитектурах информационных систем // Система и средства информатики. 2018. Т. 28. Вып. 2. С. 34–41.

4. Грушо А. А., Тимонина Е. Е., Шоргин С. Я. Иерархический метод порождения метаданных для управления сетевыми соединениями // Информатика и ее применения. 2018. Т. 12. Вып. 2. С. 44–49.

5. Елагин В. С., Пупцев Р. И. Проблемы развития OSS-систем при миграции сетей NGN/IMS в направлении SDN/NFV // Технологии и средства связи. 2017. № 2. С. 18–22.

Статья представлена профессором кафедры ИКС СПбГУТ доктором технических наук, профессором Б. С. Гольдштейном.

УДК 004.052.42
ГРНТИ 50.43.19

ОЦЕНКА ПОДХОДОВ К АНАЛИЗУ ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ УЗЛОВ ГИПЕРКОНВЕРГЕНТНОЙ ИНФРАСТРУКТУРЫ

И. Ф. Тарабанов, А. А. Швидкий

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

В статьи приведены основные способы сбора и анализы диагностической информации и проведено сравнение нескольких реализация для решения таких задач. По результатам анализа была выбрана наиболее подходящие решения для такого типа задач, в гиперконвергентной инфраструктуре.

облачные технологии, гиперконвергентная инфраструктура, диагностическая информация.

В настоящие время всю большую популярность получает не классическая, а гиперконвергентная инфраструктура. Гиперконвергентной называют инфраструктуру, состоящую из узлов, содержащих вычислительные ресурсы, средства хранения, технологии сетевого взаимодействия и виртуализации, объединение и предоставление которых происходит на программном уровне.

Одним из главных свойств гиперконвергентных систем, заключается в том, что такие системы объединяют в одном решении, те системы, которые раньше были разрознены и имели различное управление, такие как:

1) Системы хранения.
2) Сетевые функции.
3) Вычислительные ресурсы.
4) Средства управления.

Преимущества таких систем заключается в том, что они имеют единый программный интерфейс управления, и легкость масштабирования таких систем по сравнению с классической инфраструктурой [1].

Но у таких систем есть и минусы, для настройки и обслуживания таких систем необходим более квалифицированный персонал. Такие системы обычно состоят из нескольких программных продуктов, которые имеют интеграцию между собой. Для того, чтобы лучше понимать в каком состояние находится система, или почему происходит сбой в той или иной части системы, необходимо читать диагностическую информацию, генерируемую программными продуктами, но одного чтения в таком случае мало, и может понадобится узнать, что происходило с системой до этого или параллельно текущему событию в другой части системы, в больших системах поиск такой информации может оказаться очень сложным технически и время затратно. Поэтому и придумываются различные способы сбора и анализа такой информации, далее мы расскажем о том какие методы существуют на текущий момент и какие в них есть преимущества и недостатки.

Как один из методов решения таких проблем стоит отметить такой протокол SYSLOG, в настоящие время такой формат отправки диагностической информации поддерживает большой спектр сетевых операционных систем, его начало было заложено еще в 80-ых годах прошлого века Эриком Оллманом. Но хоть это старый и устойчивый протокол в нем стандартизировано не все, но можно отметить основные пункты, которые важны были для обработки диагностической информации, так были заложены поля уровня серьезности сообщения, отправляемого на хранения, они представлены в таблице 1 [2].

ТАБЛИЦА 1. Уровни серьезности, заложенные в Syslog

Уровень	Название	Описание типа проблемы
0	Emergency	Система не работоспособна

Уровень	Название	Описание типа проблемы
1	Alert	Система требует немедленного вмешательства
2	Critical	Состояние системы критическое
3	Error	Сообщения об ошибках
4	Warning	Предупреждения о возможных проблемах
5	Notice	Сообщения о нормальных, но важных событиях
6	Informational	Информационные сообщения
7	Debug	Отладочные сообщения

У этой системы есть несколько отрицательных свойств из-за которых использование такой системы в чистом виде является не совсем эффективным, можно выделить несколько из них.

1) Пакеты в данной системе будут передаваться с помощью UDP в качестве транспорта из-за чего в процессе передачи пакетов могут случаться потери и теряться необходимые сообщения, что может быть недопустимо.

2) Проблема форматирования файлов, создаваемых таким образом, это увеличивает время обработки сообщения получаемых из систем написанных, разными разработчиками, так-как у них нет общего стиля их написания.

3) Отсутствие аутентификации пользователя для передачи информации, в такой системе возможно генерация поддельной логистической информации, которая введет в заблуждения администратора такой системы.

4) Плохое масштабирование, в классическом виде такую систему можно разделить на клиент и сервер, где клиентов может быть множество, а сервер один и он собирает информацию, сервер в данном случае сервер может стать «бутылочным горлышком» системы и не справляться с обработкой большого потока сообщений, поступающих в систему. Такую систему трудно быстро масштабировать.

5) В системах, основанных на таких принципах, осуществляется только накопление информации, но не ее обработка и какое-либо уведомления администратора системы для оповещения о каком-либо сбое в системе.

Как решения проблем Syslog было уже создано, как минимум два продукта, основанного на нем, такие как rsyslog и syslog-ng, мы рассмотрим, как наиболее зрелый вариант syslog-ng, он решает проблемы протокола за счет того, что, в нем уже используется протокол TCP, поддерживает установления TLS соединения с сервером, и уже имеет в себе встроенную возможность фильтрации логов по категориям и отправку уже в другие системы для последующего анализа. В таких продуктах происходит, только агрегирования информации для последующего анализа уже в других системах, или ручного поиска такой информации с помощью просмотра файлов с накопленными сообщениями.

Часто вместе с syslog сообщениями используется графический интерфейс в виде graylog в котором можно более простым образом взаимодействовать с файлами, генерируемыми с помощью протокола syslog [3].

Как оптимальный способ решить все поставленные проблемы был создан программный комплекс, состоящий из Elasticsearch, Logstash, Kibana, кратко называемый ELK [4].

Они разделили между собой три логические функции сбор и фильтрация, анализ и обработка, и визуализация данных, полученных системой. У такой системы есть плюсы, она не становится слишком большой и каждый элемент выполняет в себе только те функции, которые на нее возложены.

Для начала рассмотрим Logstash. Logstash – это инструмент, основанный сборе информации из различных каналов, обработки и генерации журналов или событий. Это помогает в централизации и в режиме реального времени анализ журналов и событий из разных источников. Также плюсом можно отметить то, что он умеет обрабатывать не только обычный syslog, но и любые другие методы хранение диагностической информации, так он в базовой конфигурации умеет обрабатывать журналы Apache, Windows. С помощью встроенных в него фильтров настраивать производить обработку приходящих файлов для вида требуемого для облегчения дальнейшего анализа. Также стоит отметить то, что это программное обеспечение является открытым и распространяется под лицензией Apache 2.0. В работе с ним обработку входного потока можно разделить на три этапа: получения потока, обработка, вывод.

На выводе Logstash сообщение генерируется сообщение в виде JSON с обработанной информацией, и подается на вход Elasticsearch [2].

Elasticsearch используется для хранения, анализа, и поиска по логам. Она является основной системой, которая работает с логами, при запросе пользователя, она основана на библиотеке Apache Lucene, по сути он является поисковой системой, и он это делает это очень хорошо, также стоит отметить, что данная система проектировалась с мыслей о высокой отказоустойчивости и легкой масштабируемости, если к примеру из сети исчезнет один из серверов, то система в автоматическом системе перераспределит запросы по системе и сделает незаметным пропажу одного из серверов в сети, а при появление в своей сети нового узла сам добавить его в сеть и направит нагрузку одинаково по всей сети и будет происходить репликация данных по настройке пользователя и распределятся по всей сети, чтобы отказ одного из узлов, не стал причиной отказа сети.

И самой главной для пользователя данной системы может стать третья часть системы в виде Kibana, это инструмент для визуализации данных в браузере и работы с Elasticsearch через удобную панель, а не путем неудобных запросов в консоль.

Для сравнения двух решений приведена таблица 2.

ТАБЛИЦА 2. Сравнение различных методов сбора и обработки информации

Функции	ELK	Syslog + Graylog
Масштабируемость	Поддерживает масштабирование	Не поддерживает масштабирования
Принимаемые форматы диагностической информации	Возможен прием любого вида диагностической информации	Поддерживает только Syslog сообщения
Отказоустойчивость	Поддерживается, увеличивается с помощью добавления новых нод	Не поддерживается из-за особенностей сбора Syslog
Количество плагинов	Большое количество	Небольшое количество
Графический интерфейс	Гибкий в настройке, есть множество настроек	Малое количество настроек
Модель распространения	Open source, с платным функционалом	Open source, с платным функционалом
Тип лицензии	Apache 2.0	SSPL

Таким образом мы можем увидеть, что стек ELK является наиболее подходящим для решения проблем в гиперконвергентной инфраструктуре, за счет того, что он лучше подходит для систем, где возможно быстрое масштабирования, диагностическая информация собирается не только в формате Syslog, а также с помощью менее распространённых и возможно специфичных для определенных компаний форматы диагностической информации. Решения, основанные на Syslog, больше подходят для систем, в которых есть возможность заранее проектировать систему сбора диагностической информации, исходя из рассчитанных объемов такой информации и нет необходимости сбора информации с иным видом файлов диагностической информации, кроме как Syslog.

Список используемых источников

1. Швидкий А. А., Спиркина А. В., Савельева А. А., Тарлыков А. В. Evaluation of the impact the hyper-converged infrastructure storage subsystem synchronization on the overall performance // 12TH International congress on ultra modern telecommunications and control systems and workshops (ICUMT). 2020. pp. 248–252/

2. The Syslog Protocol. 2021. URL: https://tools.ietf.org/html/rfc5424 (дата обращения: 01.03.2021).

3. Техническая документация Graylog. 2021. URL: https://docs.graylog.org/ en/ 4.0/ index.html (дата обращения: 01.03.2021).

4. Техническая документация Elasticksearch. 2021. URL: https://www.elastic.co/ guide/index.html/ (дата обращения: 01.03.2021).

Статья предоставлена директором НИИ ТС СПбГУТ, кандидатом технических наук, доцентом А. Г. Владыко.

УДК 004.451.87
ГРНТИ 50.41.15

МОДУЛИ ЯДРА LINUX

О. В. Фёдорова, А. Ю. Цветков

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

Все (или почти все) процессоры, которыми когда-либо интересовались производители Unix-подобных ОС, имеют аппаратную поддержку разделения привилегий. Речь идет о «режиме ядра» (kernel land) и «режиме пользователя» (user land). Различные архитектуры ядер ОС различаются прежде всего подходом к тому: какие части кода ОС должны выполняться в kernel land, а какие – в user land? Этот вопрос является важным так как у подавляющего большинства процессоров переключение между двумя режимами занимает существенное время. Модули ядра имеют непосредственный доступ к памяти и функциям ядра. Для программ в пространстве пользователя этот доступ ограничен библиотечными интерфейсами компилятора. Модуль по своей сути примерно то же, что и обычная программа. Модуль так же имеет точку входа и выхода и находится в своем бинарном файле. Рассмотрим особенности использования того или иного вида ядра и опишем уязвимости, связанные с модульным ядром.

модульное ядро, монолитное ядро, операционная система Linux, уязвимость, RootKit.

Введение

В самом начале почти все ОС были реализованы как единое огромное ядро со всеми драйверами устройств, являющимися частью ядра. Данный метод компоновки системы является рациональным, так как почти все драйверы устройств требуют доступа к аппаратному обеспечению/ресурсам, и эти доступы предоставляются частью кода ядра, работающего в режиме ядра/супервизора. Иначе такой доступ к оборудованию/ресурсам не может быть получен [10]. С точки зрения реализации, добавить их в составе ядра будет намного проще, потому что эти драйверы будут иметь полный доступ к структурам данных и другим подпрограммам в ядре и, следовательно, будут легко использовать их [1, 13]. Однако такой подход требует перестройки ядра для включения/удаления драйверов устройств. Такая конструкция вместе с плохо написанным кодом разработчиками ядра может привести к очень связному программному компоненту [3]. Это может затруднить обслуживание и отладку кода.

Виды модулей ядра

В настоящий момент выделяют три вида ядра системы: монолитное ядро, модульное ядро и гибридная архитектура. Рассмотри подробнее каждое из них.

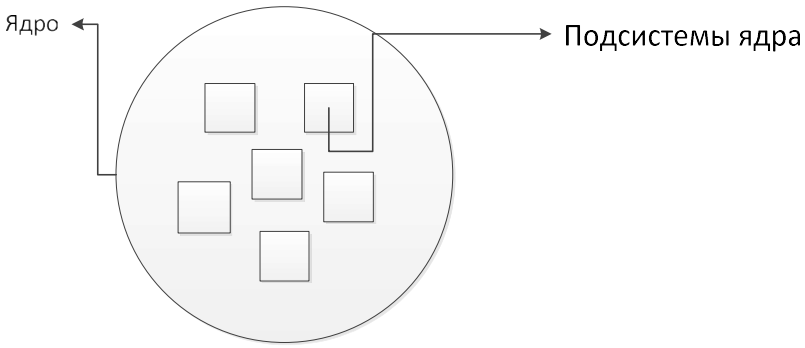


Рис. 1. Монолитное ядро

На рис. 1 представлено монолитное ядро. Достоинствами данной архитектуры является единое адресное пространство, производительность и скорость работы [11]. К недостаткам можно отнести необходимость перекомпиляции ядра при расширении функциональности и избыточная трата памяти ядра для хранения неиспользуемых компонентов.

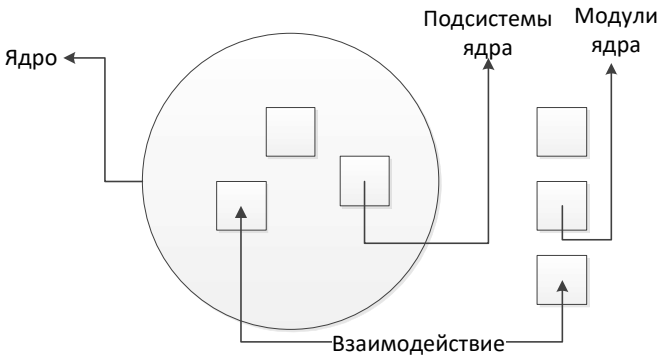


Рис. 2. Модульное ядро

Второй тип архитектуры ядра системы – модульное ядро. Его схематичное изображения представлено на рис. 2. Достоинствами данной архитектуры являются: возможность добавления дополнительного функционала в случае необходимости и небольшое время требующееся для загрузки модулей. Главным недостатком такой системы является то, что не все функции ядра могут быть реализованы в качестве модуля, так как необходимо постоянно обращаться к ним [12].

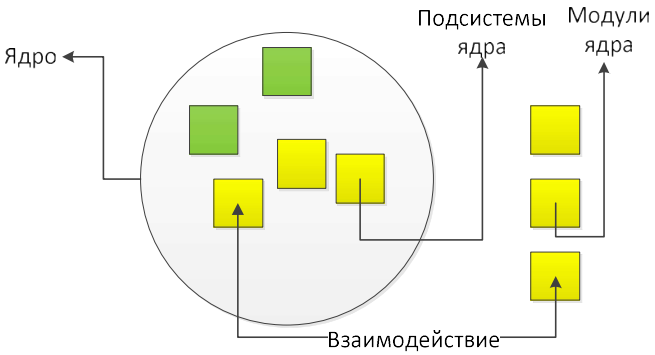


Рис. 3. Гибридное ядро

Третьим вариантом является гибридное ядро. Его структурная схема показана на рис. 3. Система, построенная на базе данного модуля, обладает высокой степенью масштабируемостью, но и высокой сложность.

Структура модуля ядра

Рассмотрим подробнее структуру модуля ядра. Схематично она показана на рис. 4. Модуль может имеет несколько точек входа, исполняемых

при установке и удалении модуля из ядра, а также при обработке поступающих, от пользователя, запросов. Так, точка входа *init_module()* исполняется при загрузке модуля в ядро. Функция *cleanup_module()* исполняется при выгрузке модуля.

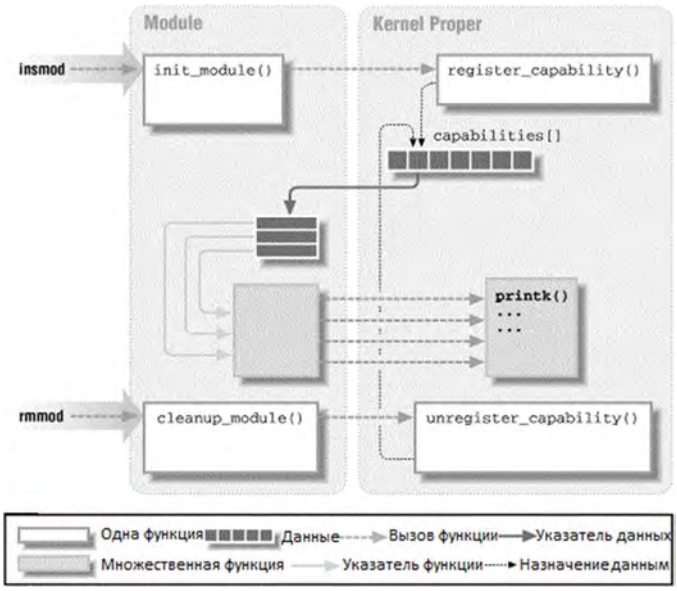


Рис. 4. Структура модуля ядра

Уязвимости модульного ядра

Использование модульного ядра делает систему более уязвимой так как встраиваемые модули работают на уровне ядра, а не пользователя [5]. Данную возможность используют злоумышленники для получения доступа к системе и содержащимся в ней файлах [2].

Потенциальные угрозы безопасности:

Механизмы, которые могут использоваться вредоносными модулями ядра Linux для скрытия своего присутствия в системе:

– перехват таблицы системных вызовов;

– перехват таблицы прерываний (позволяет добавлять собственные обработчики исключений);

– модификация VFS (подменяя функции-обработчики можно получить доступ к любому файлу системы) [9];

– DKOM (*Direct Kernel Object Manipulation*) – механизм, основанный на манипуляции с внутренней структурой ядра, что дает возможность маскировка загруженных модулей, модификацию трафика, скрытие соединений [6, 7].

Заключение

Все рассмотренные механизмы в статье могут быть использованы при реализации Руткитов (*RootKit*). Руткит – это набор утилит или специальный

модуль ядра, который злоумышленник устанавливает на взломанный им компьютер после получения прав суперпользователя. После чего они дают возможность доступа к системе путем открытия портов, создания процессов уровня ядра, что позволяет злоумышленнику полностью контролировать систему, не имея при этом физического доступа к ней, то есть через Интернет.

В связи с этим очень важным вопросом является исследование механизмов работы ядра операционных систем для выявления методов выявления и предотвращения атак с использованием вредоносного программного обеспечения повышения привилегий в системе [4, 8].

Список используемых источников

1. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернбородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 525–527.

2. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. № 1 (7). С. 19–24.

3. Построение доверенной вычислительной среды: монография / Красов А. В., Гельфанд А. М., Коржик В. И., Котенко И. В., Петрив Р. Б., Сахаров Д. В., Ушаков И. А., Шариков П. И., Юркин Д. В. СПб.: Индивидуальный предприниматель Петрив Р. Б., 2019. 108 с.

4. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 321–326.

5. Гельфанд А. М., Лансере Н. Н., Ложкина А. А., Фадеев И. И. Организация концептуальной модели критической информационной инфраструктуры // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 39–40.

6. Кушнир Д. В., Шемякин С. Н., Орлов Г. А. Представление некоторых аспектов отсеивания составных чисел для криптографических приложений // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 25–28.

7. Шемякин С. Н., Орлов Г. А., Холоденко В. Ю., Егорова А. Л. Оценка расстояния единственности... Для некоторых блочных шифров // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 34–38.

8. Волкогонов В. Н., Казанцев А. А., Катасонов А. И., Орлов Г. А. Анализ безопасности wi-fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 270–275.

9. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и

научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 329–334.

10. Гераськина В. С., Сахаров Д. В., Пестов И. Е., Виткова Л. А. Методы и стратегии оповещения населения об угрозах возникновения кризисных ситуаций // Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 507–509.

11. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Материалы XVI Санкт-Петербургской международной конференции "Региональная информатика "РИ-2018" (Санкт-Петербург, 24-26 октября 2018 г.). СПб., 2018. С. 570–571.

12. Sharikov P. I., Krasov A. V., Gelfand A. M., Kosov N. A. Research of the Possibility of Hidden Embedding of a Digital Watermark Using Practical Methods of Channel Steganography // Proc. Int. Symp. on Intelligent and Distributed Computing (Berlin, Germany: Springer), pp. 203-209, 2019.

13. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 2. С. 262–266.

Статья представлена научным руководителем заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.421, 004.942, 681.5.01
ГРНТИ 28.19.23, 49.13

МОДИФИКАЦИЯ МЕТОДА ХУКА-ДЖИВСА ДЛЯ ПОИСКА ПО УБЫВАЮЩЕЙ ФУНКЦИИ ПРИ ЗАДАННЫХ ОГРАНИЧЕНИЯХ

В. В. Фицов

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

В данной статье рассказывается об алгоритме поиска значений функции, соответствующих заданным критериям, с помощью модифицированного метода Хука-Дживса. При расчете систем глубокой инспекции пакетов имеет место убывающая функция времени обработки потоков трафика от числа аппаратных ресурсов системы. При этом имеются определенные ограничения, связанные с максимально допустимым временем анализа и стоимостью оборудования. Для такой функции классический метод Хука-Дживса требует большое число шагов поиска. Поэтому потребовалась его модификация для работы с убывающей функцией. В работе предпринята попытка уменьшить число шагов поиска для нахождения искомого значения и повысить точность полученных значений. В результате были определены условия, при которых целесообразно использование модифицированного метода Хука-Дживса.

программный поиск, метод максимального элемента, метод Хука-Дживса, deep packet inspection (DPI).

Введение

Зачастую встречается задача по нахождению подходящего под заданные ограничения решения. При наличии математической модели такую задачу можно решить классическим образом (математическим путем), не классическим (математическое программирование) или методами поиска. К сожалению, не для всех случаев может быть найдено решение с помощью классического подхода. Чаще решение может быть найдено с помощью математического программирования или случайного поиска.

Значительный интерес представляет выделение достаточных аппаратных ресурсов для использования в системах массового обслуживания, на основе данных математической модели. Так в [1] был разработан программный код на языке python с применением метода максимального элемента (ММЭ) для автоматизации процесса нахождения числа аппаратных ресурсов для системы глубокой инспекции пакетов (*deep packet inspection,* DPI) подходящего под заданные условия. При этом требовалось иметь время распознавания потока и применения к нему соответствующих правил по обработке трафика системой глубокой инспекции пакетов не более максимально допустимого и, одновременно с тем, не использовать слишком много дорогостоящих аппаратных ресурсов системы DPI. Для этого в [1] была приведена функция стоимости, не претендующая на серьезный экономический подход, но демонстрирующая практичность её использования.

Используя математическую модель DPI представленную в [2] проводится программный поиск подходящего решения с использованием ММЭ. В некоторых случаях, а именно, при высокой нагрузке на систему *DPI* или при потребности в большей точности решения для систем с виртуализацией, где имеется возможность распределения долей процессорного времени аппаратного устройства, может понадобиться несколько десятков шагов поиска. Математические расчеты, представленные на рисунке в [6], подтвердили логичное предположение о том, что с ростом числа обслуживающих устройств функция времени обслуживания будет монотонно убывать. Когда ММЭ требует большого числа шагов, можно применить другие методы программного поиска. В том числе случайный поиск, метод Нелдера-Мида, метод Хука-Дживса.

В данной работе описывается применение метода Хука-Дживса для программного поиска. Метод Хука-Дживса использует поиск по образцу, что позволит сократить число шагов поиска.

Метод Хука-Дживса

В 1961 году в [3] был представлен метод Хука-Дживса. Этот метод активно используется по сей день. Он состоит из последовательности шагов исследующего поиска вокруг базисной точки, за которой в случае успеха следует поиск по образцу [4, 5].

Сперва необходимо выбрать величину первой базисной точки для (b_0) для начала расчетов. Например, базисную точку можно выбрать используя соотношение интенсивности поступающих заявок (λ) к интенсивности обработки заявок (μ) системы с учетом предполагаемого коэффициента загрузки системы (ρ_b), согласно (1).

$$b_0 = \frac{\lambda}{\mu \times \rho_b} . \quad (1)$$

Затем рассчитывается значение искомой величины для базисной точки. Для проведения исследования значений в окрестности базисной точки, рассчитывается размер шага поиска (*St*), который задает точность полученного результата поиска. *St* для монотонно убывающих функций может быть задана по (2). Тогда величина шага будет снижаться по мере удаления значения времени нахождения заявки в системе (*Tdpi*) от своего максимально допустимого значения (*Tmax*).

$$St = b_0 \times \frac{Tdpi}{Tmax} \quad (2)$$

Если в точке, находящейся от базисной в стороне на величину сделанного шага изменение функции оказалось полезным, то делается еще один шаг в данном направлении. Если изменение не произошло или оно было негативным, то делается шаг в противоположную сторону. Если шаги не приводят к успеху - это означает что было найдено предварительное решение с точностью соответствующей величине шага. В таком случае результат поиска уточняется, для чего производится снижение величины шага (например, вдвое) вплоть до 10 кратного уменьшения величины шага. Если процедура была успешна после выполнения одного или двух шагов, то наиболее подходящая точка принимается за новую базисную точку и начинается поиск по образцу.

Согласно методу Хука-Дживса, следующее значение для поиска (P_j) определяется согласно (3), как об этом говорится в [5]. Т. е. делается шаг величиной в удвоенную разницу последней базисной точки (b_{j+1}) и предпоследней базисной точки (b_j).

$$P_j = b_j + 2 \times (b_{j+1} - b_j). \quad (3)$$

Однако, при череде успешных шагов по образцу, число шагов исследования в точке поиска и этапов уменьшения величины шага может оказаться достаточно большим. И резко возрастает в случаях, при которых решение оказывается в области более 50 обслуживающих устройств.

Модернизированный метод Хука-Дживса

Эмпирическим путем был разработан модернизированный метод Хука-Дживса, путем его упрощения. За шаг принимается десятикратное значение минимально допустимого шага ($St = 10 \times St_{min}$). Как и в [1] применяется понятие минимально целесообразного изменения функции. В случае, когда за удельный шаг (St/St_{min}) изменение функции менее минимально целесообразного, следует уменьшить величину шага вдвое. А для нахождения более точных решений, следует осуществлять возврат к предпоследней базисной точке.

В таблице показано сравнение по числу необходимых шагов следующих методов программного поиска: ММЭ, Хука-Дживса, модернизированного Хука-Дживса. Для проведения расчетов и поиска использовались исходные данные представленные в [2].

ТАБЛИЦА. Число шагов поиска ММЭ и методами Хука-Дживса при различной точности поиска

Метод	ММЭ	Хука-Дживса	Хука-Дживса	мод. Хука-Дживса
При точности шага, 1 шт.				
Шаг (St), шт.	1	1	10	10
Число шагов	19	12	28	12
При точности шага, 0.01 шт.				
Шаг (St), шт.	1	1	-	10
Число шагов	59	40	-	16

Представленный модернизированный метод Хука-Дживса становится более эффективен с возрастанием числа шагов поиска. В случаях когда требуется более 10 шагов методом максимального элемента, модернизированный метод Хука-Дживса позволит найти решение меньшим числом шагов поиска.

Помимо приведенного в данной статье способа использования метода Хука-Дживса, в ряде работ [7, 8, 9, 10] были предложены улучшения этого метода в рамках прикладных задач.

Многомерный поиск решения для серверов DPI методом Хука-Дживса

Метод Хука-Дживса предполагает возможность многомерного поиска, алгоритм которого дан в [5]. Для распределения числа аппаратных ресурсов

между специализированными серверами DPI, вместо проведения отдельного поиска по каждому из специализированных серверов, можно было бы использовать процедуру многомерного поиска.

Многомерный поиск должен выполнять поочередные шаги поиска то для одного специализированного сервера системы, то для другого. Сначала проводится исследующий поиск вокруг первой базисной точки, а затем он повторяется для другого сервера системы. Делается сравнение степени изменения времени обработки заявки в системе DPI для найденных точек. Наиболее подходящая из них принимается в качестве новой базисной точки.

После исследующего поиска, проводится поиск по образцу, согласно (3), для первого и для следующего из специализированных серверов системы. Для проведения исследующего поиска выбирается то направление поиска (P_j), которое подходит лучше. И повторяется исследующий поиск. Когда значимые изменения времени обработки заявки системой DPI перестают наблюдаться, проводится снижение размера шага. Когда величина шага становится минимальной, поиск завершается.

Заключение

Был разработан программный код на языке python с применением ММЭ и модернизированного метода Хука-Дживса для нахождения подходящего решения по распределению аппаратных ресурсов по серверам системы DPI. Приведенные в данной статье и в [1] методы программного поиска решений по распределению аппаратных ресурсов по серверам системы DPI, использующие для проведения расчетов математическую модель, представленную в [2], упрощают процесс проектирования и выявления необходимости в модернизации системы глубокой инспекции пакетов.
Использование модернизированного метода Хука-Дживса позволит повысить быстродействие процесса распределения аппаратных ресурсов для систем DPI применяемых с технологией виртуализации.

Список используемых источников

1. Фицов В. В. Применение программного кода для оптимизации числа серверов DPI методом максимального элемента // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 650–656.

2. Goldstein B., Fitsov V. Dual mathematical model for calculating of deep packet inspection // Proceedings of the FRUCT’28. 2021. pp. 127−133.

3. Hooke R., Jeeves T. A. Direct Search Solution of Numerical and Statistical Problems // J. ACM. NY, USA, 1961. Vol. 8, No. 2. pp. 212−229.

4. Банди Б. Методы оптимизации. Вводный курс. М.: Радио и связь, 1988. 128 с.

5. Кононюк А. Основы теории оптимизации. Безусловная оптимизация. Кн. 2. ч. 1. Киев: Освита Украины, 2011. С. 359–363. 544 с.

6. Фицов В. Математическая модель DPI: исследование вероятностно временных характеристик // IV науч. форум ТТТ-2020. Материалы 22 научно-технической конференции проблемы техники и технологий телекоммуникаций (ПТиТТ-2020). 2020. С. 126–127.

7. Сулимов В., Шкапов П., Носачев С. Локальный поиск методом Хука-Дживса в гибридном алгоритме глобальной оптимизации // Машиностроение и компьютерные технологии. 2014. № 6. С. 107–123.

8. Мамаев Д., Кобзев А. Параметрическая оптимизация крановых коробчатых конструкций с применением модифицированного метода Хука-Дживса // Мир транспорта и технологических машин. 2011. № 4. С. 38–42.

9. Ивашко А., Цыганова М., Карякин И. Модифицированный метод Хука-Дживса для нахождения параметров модели фазовых превращений // Вестник Тюменского государственного университета. 2009. № 6. С. 197–202.

10. Баранов А., Губанова Л. Определение оптических постоянных интерференционного слоя путем обратного проектирования на основе модифицированного метода Хука-Дживса // Модели, системы, сети в экономике, технике, природе и обществе. 2016. № 2. С. 106–111.

Статья представлена профессором кафедры ИКС СПбГУТ доктором технических наук, профессором Б. С. Гольдштейном.

УДК 004.056
ГРНТИ 81.96

ПОИСК УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

А. Ю. Цветков, Ю. Б. Эллауи

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

В данной статье описаны методы поиска уязвимостей в программном обеспечении, а также рассматриваются современные подходы к его анализу. Целью данной работы является повышение безопасности приложений путем поиска в них уязвимостей.

поиск уязвимостей, статический анализ, динамический анализ.

С повсеместной интеграцией информационных технологий во все сферы общественной жизни растут требования к безопасности применяемого программного обеспечения. Одним из эффективных методов предотвращения угроз информационной безопасности является своевременный поиск и устранение уязвимостей в программном обеспечении. В настоящий момент выделяют три подхода к анализу программного обеспечения: статический анализ, динамический анализ и гибридный анализ.

Статический анализ – это метод поиска уязвимостей в коде приложения без его запуска. Благодаря этому, он может проводиться на всех этапах разработки программного обеспечения, а также легко автоматизируется. Недостатком данного метода является большое количество ложноположительных результатов [1]. Далее рассмотрим пять методов статического анализа.

Первый метод – лексический анализ. Он выполняется следующим образом: программа разделяется на поток токенов (объектов, создаваемых из лексем в процессе лексического анализа), а затем на основе полученных данных осуществляется поиск предопределенных наборов уязвимых функций или шаблонов. Используя лексический анализ можно находить, в том числе, использование небезопасных конструкций, например, применение устаревших функций или языковых конструкций.

Вторым методом рассмотрим анализ потока управления. Принцип данного метода – создание графа, который описывает множество всех возможных путей исполнения программы. Узлы графа представляют собой блоки кода, связи между узлами – зависимости между этими блоками (вызовы функций, передача управления и т. д.). Начинается граф в точке старта программы и заканчивается в конечной точке функционирования программы. Главное назначение данного метода – определить, какие действия пользователя могут привести к вызову уязвимых функций, непредсказуемому поведению программы и т. д. Также данный анализ позволяет находить недостижимые точки программы и бесконечные циклы.

Третий метод – анализ потока данных, тесно связан с методом анализа потока управления. Используя лексический анализ для сбора информации о создаваемых переменных, используемых формулах и передаваемых в функции данных, а также граф потока управления для отслеживания вызываемых функций, строится граф потока данных, который отображает состояние данных в разных точках программы.

Четвертый метод – метод верификации модели. Программу представляют с помощью модели с конечным числом состояний. Чаще всего для этого выбирают модель Крипке [2]. Затем для полученной модели задаются требования, которым она должна соответствовать. Для этого используют темпоральную логику, т. к в разные моменты времени модель находится в разных состояниях. После этого осуществляется верификация модели.

Последним рассмотренным методом будет статический *taint* анализ. Он сосредоточен на анализе потоков данных, проходящих через программу. В первую очередь, данные разделяются на две категории – надежные и ненадежные. Например, данные, полученные от пользователя, помечаются как ненадежные, а данные, полученные из локальной базы данных – как надежные. Целью анализа является определение того, попадают ли ненадежные данные в критически важные участки программы – базу данных, системные вызовы и пр. без предварительной обработки. Принцип анализа следующий.

Данные, которые поступают из ненадежных источников помечаются специальной меткой. Таким образом они «загрязняются». Далее прослеживается жизненный путь этих данных. Если в момент попадания данных в критически важную часть программы данные все еще содержат в себе метку, то это считается уязвимостью. Если же данные в какой-то момент были обработаны программой, то метка должна пропасть, соответственно данные больше не «загрязнены» и их можно безопасно использовать. В статическом *taint* анализе применяется граф потока данных. На его основе и делаются предположения о тех или иных действиях, происходящих с данными.

Динамический анализ – это метод поиска уязвимостей в работающем приложении. На вход приложения подается определенный набор данных, затем анализируется поведение программы, наличие или отсутствие выходных данных, их содержание. Имеет меньшее число ложноположительных срабатываний по сравнению со статическим анализом [3], но требует наличие работающей версии тестируемой программы, что не всегда возможно на ранних стадиях разработки. Рассмотрим три основных метода динамического анализа.

Первым является фаззинг. Это метод поиска уязвимостей, который заключается в подаче на вход программы случайных данных с последующим анализом реакции программы на них. Процесс фаззинга делится на три стадии:

1. Стадия генерирования/модифицирования данных. Осуществляется случайная генерация данных, либо они будут модифицироваться таким образом, чтобы быть заведомо некорректными.

2. Стадия отправки данных на вход программы. Набор данных подается на один или несколько входов программы.

3. Анализ результатов. В зависимости от поведения приложения, наличия или отсутствия ответа, его содержания, фаззер делает вывод о наличии или отсутствии уязвимости.

Например, фаззер может генерировать данные различного объема, чтобы обнаружить переполнение буфера, что в свою очередь может означать наличие уязвимости (рис.).

Вторым рассмотрим метод внедрения неисправностей. Этот метод предполагает внесение неисправностей в окружение приложения для проверки отказоустойчивости программного обеспечения. Целью внедрения может быть любой компонент окружения: регистры процессора, оперативная память, сторонние устройства и т. д. [4].

Третьим методом является динамический *taint* анализ. Этот метод по принципу действия практически идентичен статическому *taint* анализу. Главное отличие заключается в том, что он работает с работающим приложением.

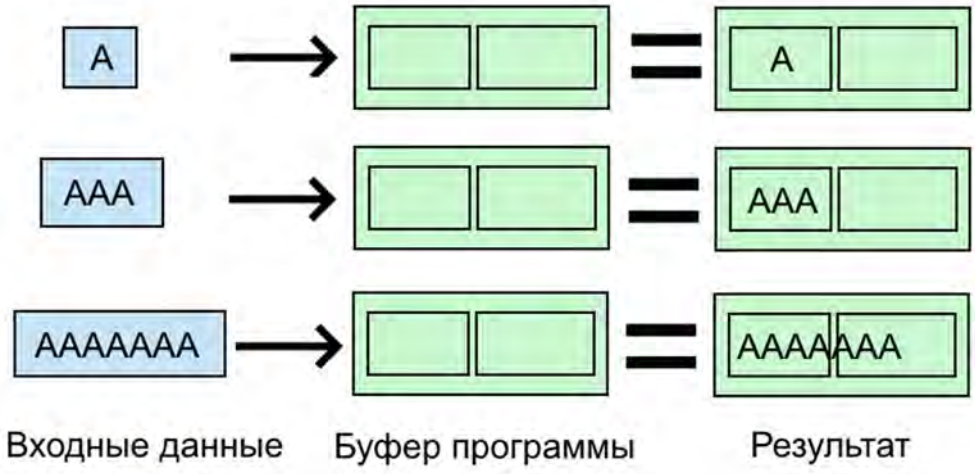


Рис. Пример работы фаззера

Гибридный анализ – это метод поиска уязвимостей, который включает в себя элементы статического и динамического анализа. При гибридном анализе инструменты тестирования интегрируются в приложение, благодаря чему во время выполнения приложения можно наблюдать код приложения, процессы, происходящие с данными, работу внутренних библиотек и компонентов и др. В связи с этим точность поиска уязвимостей в программном обеспечении возрастает. Нужно отметить, что для проведения гибридного анализа все еще необходимо подготовленное окружение для работы приложение и само работающее приложение, в которое будут интегрироваться инструменты для тестирования.

В заключение следует отметить, что для эффективного поиска уязвимостей стоит комбинировать разные методы поиска уязвимостей, поскольку они имеют различные преимущества и недостатки.

Список используемых источников

1. Yunfei S., Mengjun L., Chaojing T., Rongjun S. An Overview of Software Vulnerability Detection // IJCST. 2016. No. 7. pp. 72–76.

2. Zhioua Z., Short S., Roudier Y. Static Code Analysis for Software Security Verification: Problems and Approaches // IEEE 38th International Computer Software and Applications Conference Workshops. 2014. pp. 102–109.

3. Zhidong S., Si C. A Survey of Automatic Software Vulnerability Detection, Program Repair, and Defect Prediction Techniques // Security and Communication Networks. 2020. No. 1. pp. 1–16.

4. Benso A., Di Carlo S. The Art of Fault Injection // CEAI. 2011. No. 13. pp. 9–18.

5. Сахаров Д. В., Ковцур М. М., Бахтин Д. В. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов // Наукоемкие технологии в космических исследованиях земли. 2019. № 5. С. 22–31.

6. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернбородов И.С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст в 4-х т. СПб.: СПбГУТ, 2017 Т. 2. С. 525–527.

7. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования ЭВМ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 343–348.

8. Minyaev A. A., Livshitz I. I., Yurkin D. V. Method of assessment of efficiency of the system of protection of personal data // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь. 2017. С. 552–555.

9. Левшун Д. С., Чечулин А. А., Котенко И. В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 113–122.

10. Doynikova E., Fedorchenko A., Kotenko I. A semantic model for security evaluation of information systems // Journal of Cyber Security and Mobility. 2020. No. 2. pp. 301–330.

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

УДК 004.7
ГРНТИ 49.33.01

АНАЛИЗ ОСОБЕННОСТЕЙ ГОЛОГРАФИЧЕСКИХ СЕТЕВЫХ ПРИЛОЖЕНИЙ

Н. А. Шыпота

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

Актуальность темы исследования обусловлена необходимостью теоретического изучения голографических коммуникаций. В настоящее время, активно реализуются проекты, использующие технологии голографического звонка, визуализацию голограмм, наблюдаемая тенденция к увеличению голографического контента актуализирует изучаемую проблему. В статье рассмотрены перспективы развития голографической коммуникации. Обозначены основные проблемные точки разработки сетевых приложений. Проанализированы особенности голографических сетевых приложений. Представлен план исследования трафика голографических копий. Обозначены подходы к разработке модели трафика голографических приложений.

сетевые приложения, модели сетевого трафика, голографическая коммуникация, голографический звонок, голографические сетевые приложения.

Эволюция технологий коммуникации позволяет выделить несколько этапов ее развития. Первоначально, перед исследователями стояла задача обеспечить передачу речи в реальном времени. Далее осуществлялись разработки по передачи в реальном времени видео-потока. Современное разви-

тие технологий связи дает возможность работать над проблемой обеспечения эффекта присутствия собеседника. Следовательно, изучение процессов передачи данных при использовании технологии голографических копий становится актуальным и перспективным направлением исследований.

Целью данного исследования стало изучение необходимых требований к сетям передачи данных для голографической коммуникации. Предпринята попытка определить необходимые параметры сети и соответствующие характеристики трафика для передачи голографических копий. На первом этапе изучены теоретические и экспериментальные работы, определяющие параметры сети для обеспечения необходимого уровня обслуживания (QoS). На втором этапе проведен сравнительный анализ параметров сети и QoS для передачи речи с параметрами сети и QoS для видео потока в реальном времени. На третьем этапе были обозначены предполагаемые параметры сети и характеристики трафика голографических сетевых приложений.

На наш взгляд, следующим необходимым этапом будет разработка модели трафика передачи голографических копий для экспериментальной проверки соответствия предложенных параметров.

Анализ современных научных публикаций показал, что был проведен ряд научных исследований, направленных на переосмысление потенциала связи. Определены перспективы конструирования и внедрения коммуникационных инноваций на основе развития голографической коммуникации.

Голографическая коммуникация подразумевает создание голограммы собеседника – объемного изображения человека, позволяющего не только увидеть его образ, но и точно передавать его эмоции и жестикуляцию. По сути, голографический звонок можно описать, как встречу собеседников в виртуальной реальности. Во время голографического звонка вы видите оцифрованное трехмерное изображение своего собеседника и можете общаться с ним в режиме реального времени.

Для создания такого оцифрованного трехмерного изображения необходимо пройти несколько этапов. На первом этапе делают несколько цифровых фотографий абонента при помощи 3D-камеры. Затем, используя специальное программное обеспечение, изображение превращают в трехмерный голографический образ. На третьем этапе, созданная образ-голограмма поступает на экраны специальных устройств либо на MR-очки (*Mixed Reality*).

Разрабатывая проблематику голографической коммуникации, компании проводили тестирования технологии голографического звонка. При демонстрации голографического звонка, скорость передачи данных на одно абонентское устройство 5G CPE превысила 2 Гбит/с. На следующем этапе тестирования голографических звонков компании поставили рекорд по скорости на уровне 3,7 гигабит в секунду (тест проводился на смартфоне).

Активно реализовать проекты голографической коммуникационной деятельности возможно только на основе использования современных голографических сетевых приложений в условиях внедрения сетей нового поколения. Исследователи объясняют это тем, что трафик голографических сетевых приложений чрезвычайно чувствителен к задержкам передачи данных. Голографическая коммуникация требует высокой пропускной способности и низкого уровня задержки передачи данных. Максимальное время задержки не должно превышать 1 мс. Термин «задержка передачи данных» мы трактуем как определенный промежуток времени, который можно зафиксировать с момента передачи пакета данных, до момента его приема. Задержка при кодировании информации может быть уменьшена путем совершенствования алгоритмов обработки и преобразования голографических копий. Задержка, которую вносит сеть передачи данных, может быть скорректирована путем разработки новой архитектуры сети с оптимальной инфраструктурой.

Основными показателями качества обслуживания являются пропускная способность сети и задержка передачи данных. Так, в стандартах 3GPP представлены такие требования к задержкам следующих видов сетевых приложений: видеозвонки – 150 мс, VoIP – 100 мс, видеоигры в реальном времени – 50 мс.

Кроме того, необходимо выделить такие характеристики, как готовность сети и ее надежность, которые можно оценить по результатам контроля уровня обслуживания в течении определенного периода времени или определить коэффициент использования.

Парамонов А. И. подчеркивает, что появляется и становится все более актуальным новый показатель качества обслуживания. Так, в частности, он отмечает, что «в дополнение к имеющейся метрике QoS добавилась еще одна – качество восприятия QoE (*Quality of Experience*), определяющая субъективную оценку пользователем, например, качества видео [4, с. 178].

При массовом внедрении голографических звонков, необходимо обеспечить передачу сверхбольших объемов данных, которые будут генерировать голограммы. Таким образом, успешная реализация голографической коммуникации потенциально возможна только в условиях активного внедрения новых поколений сетей связи – 5 G и 6 G.

Заслуживает внимание позиция авторов Водопьянова С. В. и Дрововозова В. И., которые настаивают на необходимости выбирать такие значения параметров сети, чтобы показатели ее эффективности, как минимум, были не ниже предельно допустимых, задаваемых при выборе глобального уровня качества сервиса QoS [2, с. 30].

В цивилизационной перспективе голографический метод записи и восстановления волнового поля, который применим к волнам разнообразной

природы, будет развиваться по экспоненте. На данном этапе активно ведутся разработки использования технологии оптической голографии в сфере медицины, киноиндустрии, бизнеса – для предоставления разнообразных услуг. Потребность в дистанционном обучении вызовет необходимые исследования для организации этого процесса на новом уровне, уровне голографической коммуникации с психофизиологическим эффектом присутствия преподавателя.

Соответственно, исследователи будут создавать все более сложные виды трафика, разрабатывать инновационные приложения, использующие несколько видов трафика, так как необходимо не только изобретать все новые технологии создания голографических копий, но решать проблемы передачи данных и оптимизации трафика.

Братченко Н. Ю. отмечает, что «изучение основных методов теории телетрафика позволяет исследовать характеристики качества обслуживания в телекоммуникационных системах, осуществлять управление основными параметрами качества обслуживания реальных сетей и систем и измерять их, а также предложить оптимальные с точки зрения качества обслуживания технические решения при проектировании новых сетей и систем» [1, с. 8].

Текстовые, видео, графические, голографические приложения образуют поток данных современного трафика с комбинированной структурой. Интересен подход группы ученых (Schwarzmann S., Breitbach P., Zinner T. & Rost M.) к рассмотрению влияния различных параметров на показатели производительности, они характеризуют проблему следующим образом: поскольку до сих пор не существует целостной методологии оценки, мы имеем лишь ограниченное представление о влиянии различных параметров на показатели производительности адаптивной потоковой передачи видео в различных операционных условиях. В этом контексте параметры включают внутренние факторы влияния, такие как количество уровней качества, пороги переключения качества или длительность сегмента, в то время как рабочие настройки относятся к внешним факторам влияния, таким как характеристики сети или видеоконтент [7].

Выводы

Для успешного развития технологии голографической коммуникации необходимым условием является внедрение новых поколений сетей связи 5G и 6G. Так как, для сетей пятого поколения определена максимальная скорость передачи данных в 20 Гбит/с и 5G-системы могут обеспечить минимальные задержки. Такие характеристики сетей связи сделают голографические звонки реальностью. Благодаря высокой скорости передачи данных и минимальным задержкам в сетях 6G рынок сможет создавать иммерсивные диалоговые платформы для обучения и развлечений за счет смешения цифровой и физической действительности.

Меняющаяся ситуация на рынке ИТ-технологий требует новых разработок в сфере визуализации голограмм – оборудования для создания оцифрованных трехмерных изображений.

Новые поколения сетей связи актуализируют проблему разработки сетевой архитектуры, инновационных подходов к её организации.

В нашем исследовании, следующим необходимым этапом будет разработка модели трафика передачи голографических копий для экспериментальной проверки соответствующих параметров.

Список используемых источников

1. Братченко Н. Ю. Теория телетрафика: учебное пособие / авт.-сост. –Ставрополь: Изд-во СКФУ, 2014. 177 с.

2. Водопьянов С. В., Дрововозов В. И., Применение моделей трафика данных для мониторинга компьютерных сетей системы управления воздушным движением // Проблеми інформатизації та управління. 2012. № 1(37). С. 30–35.

3. Кучерявый А. Е., Бородин А. С., Киричек Р. В. Сети связи 2030 // Электросвязь. 2018. № 11. С. 52–56.

4. Парамонов А. И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования: дисс. … д-ра техн. наук: 05.12.13 / Александр Иванович Парамонов. Санкт-Петербург, 2014.

5. Bailey M. L., Gopal B., Pagels M. A., Peterson L. L., and Sarkar P., PathFinder: A pattern-based packet classifier // Proceedings of the First Symposium on Operating Systems Design and Implementation, November 1994. pp. 115–123.

6. Gupta P. and McKeown N. Algorithms for packet classification // IEEE Network Magazine. 2001. Vol. 15. No. 2. pp. 24–32.

7. Schwarzmann S., Breitbach P., Zinner T. & Rost M. Modeling Adaptive Video Streaming Using Discrete-Time Analysis // 31th International Teletraffic Congress (ITC 31). 2019. Budapest, Hungary.

8. Volkov A., Muthanna A., Koucheryavy A. Fifth generation communication networks: on the way to networks 2030 // Telecom IT. 2020. Vol. 8. Iss. 2. pp. 32–43 (in Russian). DOI 10.31854/2307-1303-2020-8-2-32-43.

Статья представлена научным руководителем, доцентом кафедры ССиПД СПбГУТ, доктором технических наук, доцентом М. А. Маколкиной.

УДК 004.056
ГРНТИ 81.96

СПОСОБ АУТЕНТИФИКАЦИИ ЗНАЧЕНИЙ ДИФФИ–ХЕЛЛМАНА НА ОСНОВЕ ПРЕДВАРИТЕЛЬНО РАСПРЕДЕЛЕННЫХ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И ХЭШИРУЮЩИХ ФУНКЦИЙ

В. А. Яковлев

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

Предложен способ аутентификации значений Диффи–Хеллмана между двумя корреспондентами с использованием предварительно распределенных случайных аутентифицирующих последовательностей и алгоритма аутентификации Вегмана-Картера. Получены соотношения для оценивания вероятности ложного отклонения DH-значения (из-за несовпадения бит в распределенных цепочках) и вероятности навязывания ложного DH-значения злоумышленником.

Аутентификация, распределение ключей, метод Диффи-Хеллмана, атака человек-посередине; универсальные хэш-функции.

Метод Диффи-Хеллмана [1] позволяет использовать незащищенный от перехвата канал связи для формирования общего ключа шифрования с целью создания безопасного соединения между двумя корреспондентами. Суть метода следующая. Пользователи сети Алиса (*A)* и Боб (*B)*, согласуют параметры: p и g, где p – просто число, а g – элемент конечного поля $GF(p)$, порождающий группу, имеющую большой порядок и выполняют следующий протокол.

1. Алиса генерирует элемент поля $x \in (1, p-1)$, вычисляет $X = g^x \pmod p$ и посылает его Бобу.

2. Боб генерирует элемент $y \in (1, p-1)$, вычисляет $Y = g^y \pmod p$ и посылает его Алисе.

3. Алиса вычисляет ключ $K = Y^x \pmod p$.

4. Боб вычисляет ключ $K = X^y \pmod p$.

Легко видеть, что ключи, вычисленные Алисой и Бобом, равны между собой $K = g^{yx} \pmod p = g^{xy} \pmod p$.

Будем далее величины *X,Y,* которые передаются по открытым каналам, называть значениями Диффи-Хеллмана (*DH*-значениями).

Однако известно, что данный метод подвержен к атаке «человек посередине».

Перспективным подходом к решению задачи аутентификации ключа, распределяемого по методу Диффи-Хеллмана, является использование для аутентификации предварительно распределенных между пользователями двоичных последовательностей [2, 3].

Одним из способов создания корреспондентами *A* и *B* случайных последовательностей является способ на основе измерения корреспондентами магнитного поля Земли с помощью магнитометров, встроенных в смартфоны. Этот способ получил название MagPairing [2]. Согласно MagPairing, пользователям необходимо удерживать два устройства вблизи друг к другу несколько секунд. Устройства считывают показания датчиков магнитометра. Из этих данных формируется случайные последовательности. В [4] подробно описан процесс сбора и коррекции данных магнитометров. Вероятность совпадения бит двух последовательностей от разных устройств в наших экспериментах составила 0,94.

Пусть пользователи сети (*A* и *B*) имеют двоичные предварительно распределенные последовательности $\boldsymbol{a}$ и $\boldsymbol{b}$ соответственно. Символы в последовательностях равновероятны и взаимно независимы. Обозначим $p_m = P(a_i \neq b_i)$, где $i = 1,2...L$ – номер символа в последовательностях, – вероятность несовпадения бит в последовательностях $\boldsymbol{a}$ и $\boldsymbol{b}$.

Предполагаем, что злоумышленник *E* во время процедуры получения (выработки) аутентифицирующих последовательностей легальными пользователями удален от них, поэтому вероятность совпадения бит в последовательности, которую может сформировать нарушитель, и последовательности бит законного пользователя равна $p_e = P(a_i = e_i) = 1/2$, $i = 1,2...L$.

Для защиты от атаки человек-посередине пользователи *A* и *B* используют следующую схему аутентификации, основанную на использовании класса строго универсальных хэш-функций [5].

Пользователь *A* разделяет *DH*-значение *X* на *N* блоков длиной *m* бит. Для каждого блок $\boldsymbol{u_i}$ вычисляется аутентификатор $\boldsymbol{w_i}$ длиной *v* бит $(i = 1,2,\ldots,N)$ на основе универсального класса хэш-функций и использования последовательности $\boldsymbol{a}$. Для аутентификации каждого следующего блока выбираются новые блоки в последовательности $\boldsymbol{a}$.

Корреспондент *B* проводит аутентификацию значения DH следующим образом. Для каждого принятого блока $\boldsymbol{u_i}$ вычисляется аутентификатор $\boldsymbol{w_i'}$, который сравнивается с аутентификатором $\boldsymbol{w}_i$, полученным по каналу связи. Если $\boldsymbol{w = w_i'}$, то блок $\boldsymbol{u_i}$ аутентифицирован. Если $w_i \neq w_i'$, то блок $\boldsymbol{u_i}$ не аутентифицирован $(i = 1,2,\ldots,N)$. *DH*-значение считается аутентифицированным в целом, если среди *N* принятых блоков окажутся не аутентифицированными не более Δ блоков $1 \leq \Delta \leq N$.

Аутентификатор для каждого блока вычисляется согласно алгоритму Вегмана-Картера [5]. Представим подблок $\boldsymbol{u}$, как элемент поля Галуа

GF(2^m). Тогда аутентификатор $w = [u \times k_0 + k_1]_v$, где $k_0,\ k_1 \in GF(2^m)$ – ключ аутентификации. Знаки $\times, +$ обозначают соответственно умножение и сложение в конечном поле $GF(2^m)$, а $\lfloor \square \rfloor_v$ – «усечение», то есть выбор v левых или правых элементов последовательности в квадратных скобках. Блоки $k_0, k_1 \in GF(2^m)$ длиной m бит, выбираются поочередно из последовательности ***a***. Для каждого очередного блока $\boldsymbol{u_i}$ формируется новый аутентификатор $\boldsymbol{w_i}$ с использованием новой пары ключей $k_0,\ k_1 \in GF(2^m)$. Вероятность навязывания ложного блока при известных ***u*** и ***w*** для данного способа аутентификации определяется соотношением $P_s = 1/2^v$ [5].

Длина ключа аутентификации (минимальная длина последовательности ***a),*** необходимая для аутентификации DH-значения: $L = 2mN$.

Будем считать, что нарушитель Ева, реализуя атаку человек посередине, придерживается следующих стратегий.

Атака *имперсонализации.* Ложное DH-значение $X' = g^{x'}$ создается нарушителем без предварительного приема истинного DH-значения от корреспондента А.

Атака *подмены.* Нарушитель перехватывает DH-значение $X = g^x$ длиной n_0 бит, передаваемое в виде подблоков u_i и аутентификаторов w_i, $i = 1, 2, ..., N$. Генерирует ложное сообщение $X' = g^{x'}$, отличающееся от исходного в D блоках и формирует аутентификаторы к нему по следующему правилу:

– если блоки u_i в исходном и ложном сообщении совпали, он использует перехваченные аутентификаторы;

– если блоки не совпали, нарушитель формирует аутентификаторы случайным образом.

Оценку эффективности аутентификации DH-значения будем осуществлять по следующим параметрам:

P_f – вероятность ложного отклонения DH-значения в отсутствие навязывания. Событие наступает, когда число неправильно аутентифицированных блоков равно Δ и более из-за несогласованности аутентифицирующих последовательностей ***a*** и ***b***.

P_i – вероятность имперсонализации. Событие наступает, когда ложное DH-значение создается без предварительного приема истинного DH-значения и принимается как истинное.

P_s – вероятность подмены DH-значения. Событие можно рассматривать как поледовательное наступление двух событий: создание нарушителем ложного DH-значения, отличающегося от истинного в D блоках размерности m (обозначим вероятность этого события – $P_g(D)$) и события,

состоящего в навязывании этого сообщения путем формировании аутентификаторов для блоков, отличающихся в ложном DH-значении от блоков истинного DH-значения (вероятность навязывания такого DH-значения – $P_r(D)$). Поскольку величина D определяется злоумышленником, то в худшем случае

$$P_s = \max_D P_g(D) P_r(D) . \quad (1)$$

P_d – вероятность навязывания ложного DH-значения. $P_d = \max(P_i, P_s)$.

L – длина ключа аутентификации (длина последовательностей ***a*** и ***b***), необходимая для аутентификации DH-значения длиной n_0 с заданными значениями P_f, P_d.

$W = vN$ – суммарная длина аутентификаторов DH-значения.

P_f – может быть оценена, как вероятность суммы событий, состоящих в том, что в принятой последовательности X из-за ошибок в аутентифицирующих последовательностях окажется не аутентифицированными $\Delta + 1$ и более блоков.

$$P_f(\Delta) = \sum_{i=\Delta+1}^{N} C_N^i p_b^i (1-p_b)^{N-i}, \quad (2)$$

где p_b – вероятность несовпадения ключей (k_0, k_1) равна вероятности несовпадения блоков длиной *2m* бит, выбранных их последовательностей ***a*** и ***b*** и равна $p_b = 1-(1-p_m)^{2m}$ в предположении, что ошибки в битах распределены по закону Бернулли.

Вероятность успешной атаки имперсонализации можно получить, как оценку количества обнаруженных и необнаруженных ложных аутентификаторов в N блоках, при их случайном генерировании. Учитывая, что вероятность успешного навязывания ложного аутентификатора длиной v символов при использовании универсальных хэш-функций равна $1/2^v$, можно записать.

$$P_i(\Delta) = \sum_{i=0}^{\Delta} C_N^i \left(\frac{1}{2^v}\right)^{(N-i)} \left(1-\frac{1}{2^v}\right)^i . \quad (3)$$

Для оценки вероятности подмены P_s рассмотрим сомножители в (1).

Очевидно, что чем меньше отличаются X и X', тем легче нарушителю реализовать атаку «человек посередине». Заметим, что непосредственно значение X' нарушитель выбрать не может. Сначала он выбирает x', затем находит значение экспоненты $X' = g^{x'} \bmod p$. Если x' выбирать случайно из множества чисел от 0 до $p-1$, то число X', будет также случайным числом из

множества чисел от 0 до *p-1*. При большой величине модуля p ($p \approx 2^{256}$) нахождение отображения $x' \Leftrightarrow X'$ требует необозримо больших вычислительных затрат. Поэтому разумной стратегией для нарушителя будет случайный выбор числа *x'*, что равносильно случайному выбору *X'*.

Вероятность случайного формирования нарушителем ложного DH-значения *X'*, отличающегося от перехваченного значения *X* в *D* блоках, может на основе комбинаторных рассуждений о выпадений одинаковых значений двух 2^m-гранных игральных костей, при *N* бросаниях записана как:

$$P_g(D) = C_N^D \left(\frac{1}{2^m}\right)^{N-D} \left(1-\frac{1}{2^m}\right)^D. \quad (4)$$

Вероятность навязывания сформированного ложного DH-значения в зависимости от порога принятия решения Δ, можно оценить

$$P_r(\Delta) \le \sum_{i=0}^{\Delta} C_D^i \left(\frac{1}{2^v}\right)^{(D-i)} \left(1-\frac{1}{2^v}\right)^i \sum_{j=0}^{t} C_{(N-D)}^j p_b^j (1-p_b)^{(N-D-j)}, \text{ где } t = \begin{cases} N-D, \text{если } \Delta - i \ge N-D. \\ \Delta - i, \text{если } \Delta - i < N-D \end{cases} \quad (5)$$

Первая сумма в (4) характеризует вероятность фиксации на приеме *i* ложных аутентификаторов ($0 \le i \le \Delta$), которые обнаруживаются и *D-i* ложных аутентификаторов, которые не обнаруживаются. Вторая сумма – вероятность несовпадения *j* $(0 \le j \le t)$ из *N-D* аутентификаторов исходного сообщения, которые нарушителем были переданы без изменений, а несовпадение произошло за счет несовпадения ключей в аутентифицирующих последовательностях ***a*** и ***b***.

Выбор параметров (длины блока *m* длины аутентификатора *v*), при которых выполняются заданные требования к вероятностям P_f, P_i, P_s, P_d, представляет отдельную оптимизационную задачу, решение которой возможно на основе методики, представленной в статье «Методика оптимизации параметров способа аутентификации значений диффи-хеллмана на основе предварительно распределенных двоичных последовательностей и строго-универсальных хэш-функций» настоящегосборника (см. стр. 698–703).

Список используемых источников

1. Diffe M., Hellman M. New directions in cryptography // IEEE Trans. Inf. Theory. 1976. Vol. 22. No. 6. pp. 644–654.

2. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. No. 6. pp. 1304–1319.

3. Яковлев В. А. Аутентификация ключей, распределяемых методом Диффи-Хеллмана, для мобильных устройств на основе аутентифицирующих помехоустойчивых кодов и магнитометрических данных // Труды СПИИРАН. 2019. Т. 18. № 3. С. 705–740.

4. Яковлев В. А, Ольховой О. О., Корпусов В. Д. Исследование датчика случайных чисел на основе магнитометра // Актуальные проблемы инфотелекоммуникаций в науке

и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. научн. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 488–493.

5. Wegman M., Carter L. New Hash Functions and their Use in Authentication and Set Equality // Journal of Computer and System Sciences. 1981. Vol. 22. pp. 265–279.

УДК 004.056
ГРНТИ 81.96

МЕТОДИКА ОПТИМИЗАЦИИ ПАРАМЕТРОВ СПОСОБА АУТЕНТИФИКАЦИИ ЗНАЧЕНИЙ ДИФФИ-ХЕЛЛМАНА НА ОСНОВЕ ПРЕДВАРИТЕЛЬНО РАСПРЕДЕЛЕННЫХ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И СТРОГО-УНИВЕРСАЛЬНЫХ ХЭШ-ФУНКЦИЙ

В. А. Яковлев

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

Предложена методика оптимизации параметров способа аутентификации значений Диффи-Хеллмана на основе предварительно распределенных между пользователями двоичных последовательностей (аутентифицирующих последовательностей). Аутентификация осуществляется путем разделения значения Диффи-Хеллмана на N блоков и формирования для каждого блока аутентификатора длиной v бит с использованием строго универсальных хэш-функций, ключем для которых являются блоки аутентифицирующих последовательностей. Методика включает этапы: оценку вероятности ложного отклонения ключа и определение допустимых порогов принятия решения для различных длин аутентифицируемых блоков; расчет вероятности навязывания для выбранных длин блоков и отбор только тех длин блоков, которые удовлетворяют требованиям по вероятности навязывания и вероятности ложного отклонения DH-значения и минимизируют суммарную длину аутентификаторов. Приведен пример применения методики для аутентификации значения Диффи-Хеллмана длиной 256 бит.

аутентификация ключей, метод Диффи-Хеллмана, атака человек посередине, универсальные хэш-функции.

Исследуется способ аутентификации ключей формируемых методом Диффи-Хеллмана в условиях применения злоумышленником атаки «человек-посередине». Предполагается, что мобильные пользователи *A* и *B*, формирующие ключ, имеют предварительно распределенные случайные цепочки бит ***a*** и ***b*** соответственно, сгенерированные ими самими на основе

данных, полученных от магнитометров или акселерометров из состава мобильных устройств во время лих личной встречи. Злоумышленник не имеет доступа к этим цепочкам. С целью аутентификации DH-значения пользователем *A* разделяется на *N* блоков длиной *m* бит каждый. Для каждого блока вычисляется аутентификатор с использованием строго универсального класса хеш-функций согласно алгоритму Вегмана-Картера [1]. Длина аутентификатора *v* бит. Хэш-функция задается ключем, который является подблоком случайных цепочек ***a*** или ***b***. DH-значение и аутентификаторы передаются по каналу пользователю *B*. На приемной стороне вычисляются аутентификаторы от принятого DH-значения, которые сравниваются с аутентификаторами, принятыми из канала. Если число не аутентифицированных блоков не превышает порог Δ, установленный в системе аутентификация, то аутентификация DH-значения считается успешной. Для оценки эффективности предложенного способа аутентификации используются следующие параметры.

P_f – вероятность ложного отклонения DH-значения в отсутствие навязывания. Событие наступает, когда число неправильно аутентифицированных блоков равно Δ + 1 и более из-за несогласованности аутентифицирующих последовательностей ***a*** и ***b***.

P_i – вероятность имперсонализации. В этом случае ложное DH-значение создается без предварительного приема истинного DH-значения и принимается как истинное.

P_s – вероятность подмены DH-значения. Событие можно рассматривать, как последовательное наступление двух событий. Первое – создание нарушителем ложного DH-значения, отличающегося от истинного в *D* блоках. Вероятность этого события – $P_g(D)$. Второе – навязывание ложного сообщения путем формировании аутентификаторов для тех блоков, в которых ложное DH-значение отличается от блоков истинного (вероятность навязывания такого DH-значения – $P_r(D)$). Поскольку величина *D*, определяется злоумышленником, то в худшем случае

$$P_s = \max_D P_g(D) P_r(D) .$$

$P_d = \max(P_i, P_s)$ – вероятность навязывания ложного DH-значения.

L – длина ключа аутентификации (длина последовательностей ***a*** и ***b***), необходимая для аутентификации DH-значения длиной n_0 с заданными значениями P_f , P_d .

$W = vN$ – суммарная длина аутентификаторов для аутентификации DH-значения.

В статье «Способ аутентификации значений Диффи-Хеллмана на основе предварительно распределенных случайных последовательностей и хэширующих функций» настоящего сборника (с. 693–698) получены соотношения для оценивания вероятностей ложного отклонения DH-значения, подмены и навязывания ложного DH-значения.

Предлагаемая методика предназначена для обоснования параметров данной системы аутентификации и заключается в нахождении оптимального сочетания параметров (*m,v*), для которых при заданной вероятности несовпадения p_m аутентифицирующих последовательностей ***a*** и ***b,*** выполняются требования по вероятности ложного отклонения и вероятности навязывания ложного DH-значения, то есть $P_f \le \tilde{P}_f$, $P_d \le \tilde{P}_d$, где $\tilde{P}_f, \tilde{P}_d$ заданные пороговые значения и при этом суммарная длина всех аутентификаторов минимальна – $W \to min$.

Методика состоит из следующих этапов:

1. Построение зависимости $P_f(\Delta)$ для заданной вероятности ошибки p_m и разных длин блока аутентификации $1 \le m \le n_0$ (для удобства расчетов целесообразно выбрать *m* делителем n_0). Длину аутентификатора *v* задаем первоначально *v* = *m*.

2. Определение минимальных значений порога $\Delta_{min} = min\,\Delta,$ при котором $P_f = \tilde{P}_f$ для каждой длины блока *m*.

3. Построение зависимости $P_s(D)$ для выбранных значений Δ_{min}, для всех значений *m* и *v,* удовлетворяющих условию $P_f \le \tilde{P}_f$.

4. Отбор пар (*m, v),* для которых выполняется условие $P_s \le \tilde{P}_d$.

5. Нахождение вероятности имперсонализации $P_i(\Delta)$ для всех пар (*m* и *v*), отобранных на предыдущем шаге.

6. Отбор подмножества пар (*m* и *v)*, удовлетворяющих условию $P_f \le \tilde{P}_f$ и $P_d \le \tilde{P}_d$.

7. Выбор из подмножества пары (*m, v)* такой, что $W \to min$.

Найденная пара (длина блока *m* и длина аутентификатора *v*) являются оптимальными для построения системы аутентификации, поскольку при заданной длине DH-значения n_0 выполняются требования $P_f \le \tilde{P}_f$, $P_d \le \tilde{P}_d$ и минимизируется суммарная длина всех аутентификаторов.

Рассмотрим пример применения методики. Пусть DH-значение, которое необходимо аутентифицировать, имеет длину n_0 = 256 бит, вероятность несовпадения аутентифицирующих последовательностей p_m = 0,05. К системе аутентификации предъявлены требования: $\tilde{P}_f = 10^{-6}$, $\tilde{P}_d = 10^{-6}$.

Выберем несколько длин аутентифицируемых блоков *m* = 1, 2, 4, 8, 16, 32, среди которых будем искать, удовлетворяющие заданным требованиям.

Используя соотношение (2) в статье «Способ аутентификации значений Диффи-Хеллмана на основе предварительно распределенных случайных последовательностей и хэширующих функций» настоящего сборника (с. 693–698), построим зависимость $P_f(\Delta)$ для выбранных длин блока аутентификации (рис. 1). На пересечении кривых $P_f(\Delta, m)$ и прямой $P_f = 10^{-6}$ находим значения порогов ($\Delta_{\min}$ = 50, 46, 40, 30 для m = 1, 2, 4, 8 соответственно), при которых выполняется неравенство $P_f \le \tilde{P}_f$. Для m = 16 и 32 такие условия не выполняются, поэтому дальше оставляем блоки с длинами 1, 2, 4, 8.

Используя найденные значения $\Delta_{\min}$, построим зависимости $P_s(D) = P_g(D)P_r(D)$, для выбранных блоков длины m и всех аутентифика-торов длины $v \le m$. Зависимости $P_g(D)$ и $P_r(D)$ рассчитываются согласно (4), (5) в [2] (рис. 2). По полученным зависимостям находим значения $P_s = \max_D P_g(D)P_r(D)$.

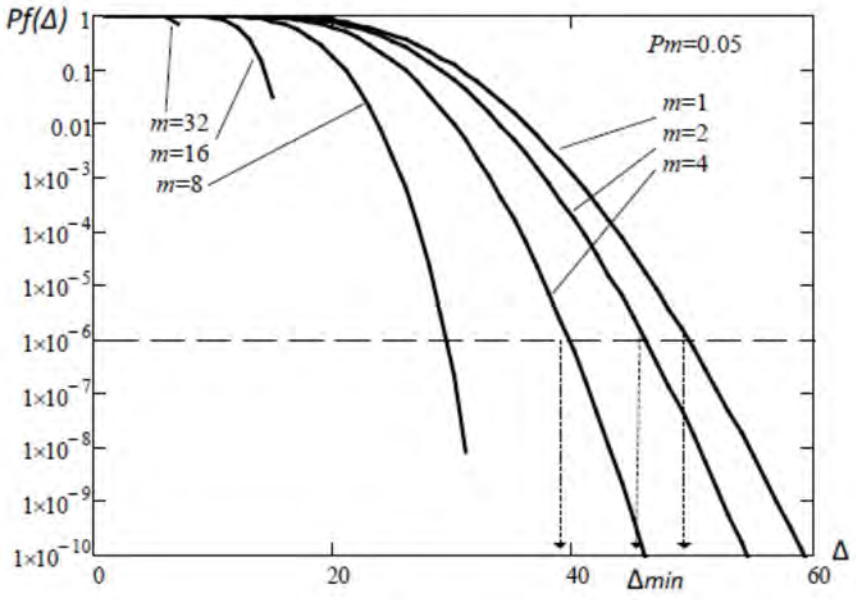


Рис. 1. Зависимость вероятности ложного отклонения DH-значения от порога Δ для разны длин аутентифицируемых блоков

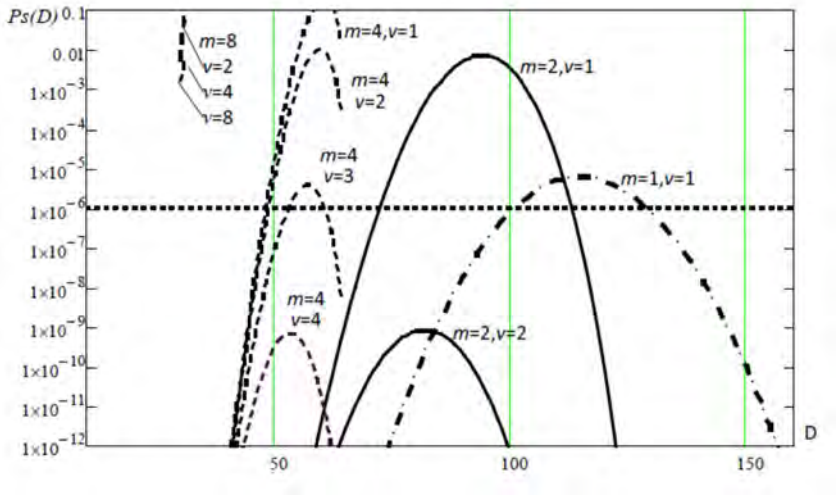


Рис. 2. Зависимость вероятности подмены от значения *D*
(количество блоков в которых различаются истинное и ложное DH-значения)
для отобранных пар (*m, v)*

Значения (*m, v)* и рассчитанные вероятности ложного отклонения, подмены, имперсонализации, навязывания записываем в таблицу. (Вероятность имперсонализации, рассчитывается в соответствии с соотношением (3) в статье «Способ аутентификации значений Диффи-Хеллмана на основе предварительно распределенных случайных последовательностей и хэширующих функций» настоящего сборника (с. 693–698)).

ТАБЛИЦА. Значения вероятности ложного отклонения, подмены, имперсонализации, навязывания для пар (*m,v*)

(*m,v*)	P_f	P_s	P_i	$P_d = \max(P_s', P_i)$
(1,1)	7.1×10^{-7} (+)	6.2×10^{-6} (-)	5.7×10^{-24} (+)	6.2×10^{-6} (-)
(2,2)	**1×10^{-6} (+)**	**8.1×10^{-10} (+)**	**1.4×10^{-20} (+)**	**8.1×10^{-10} (+)**
(2,1)	1×10^{-6} (+)	7.4×10^{-3} (-)	9.3×10^{-4} (-)	7.4×10^{-3} (-)
(4,4)	**6.5×10^{-7} (+)**	**6.8×10^{-10} (+)**	**2.7×10^{-13} (+)**	**6.8×10^{-10} (+)**
(4,3)	6.5×10^{-7} (+)	3.8×10^{-6} (-)	3.3×10^{-7} (+)	3.8×10^{-6} (-)
(4,2)	6.5×10^{-7} (+)	1×10^{-2} (-)	1.8×10^{-2} (-)	1×10^{-2} (-)
(4,1)	6.5×10^{-7} (+)	1.4×10^{-1} (-)	9.8×10^{-1} (-)	1.4×10^{-1} (-)

Проводим анализ таблицы и определяем, что условию $\tilde{P}_f = 10^{-6}$, $\tilde{P}_d = 10^{-6}$ удовлетворяют только две пары (*m, v*). Это (2,2) и (4,4).

Поскольку в данном примере значение вероятности подмены, удовлетворяющее требованию $P_f \le 10^{-6}$, выполняется только при $m = v$, то минимальная длина всех аутентификаторов равна длине DH-значения и равна 256 бит. Длина ключа равна 512 бит.

Таким образом, разработанная методика позволяет оптимизировать параметры системы аутентификации на основе предварительно распределенных цепочек бит и алгоритма аутентификации Вегмана-Картера. Дальнейшее совершенствование методики состоит в создании программы для ЭВМ, позволяющей автоматически рассчитывать параметры системы аутентификации для разных длин DH-значения, разных вероятностей несовпадения бит в аутентифицирующих последовательностях и разных требованиях, предъявляемых к системе аутентификации.

Список используемых источников

1. Wegman M. Carter L. New Hash Functions and their Use in Authentication and Set Equality //Journal of Computer and System Sciences. 1981. 22. pp. 265–279.

ANNOTATIONS

PLENARY MEETING

Gogol A., Osichev I., Petrov B. Problems of Training Technical Specialists in the Television field. Change of Priorities. – PP. 5–8.
This work reviews the changes in the current tech specialists training. Setting of the main television field development trends is presented on the example of JSC "GART" ("Saint-Petersburg" TV-channel).
Key words: virtual studios, augmented reality, information systems, 3D-graphics, artificial intelligence.

Koucheryavy A., Borodin A., Muthanna A., Abdellah A. R., Volkov A. Artificial Intelligence for Telecommunication Networks. – PP. 9–18.
The article sets out research tasks in the field of artificial intelligence for communication networks. We consider solutions for predicting delays and traffic for communication networks of the fifth and subsequent generations based on the use of machine learning and deep learning. Recommendations are given on the application of robust maximum likelihood estimates for VANETs (Vehicular Ad Hoc Networks).
Key words: artificial intelligence, machine learning, deep learning, forecasting, delays, IoT traffic, robust estimates.

INFORMATION AND COMMUNICATION NETWORKS AND SYSTEMS

Abbasov E., Ibrahimov B., Namazov M. Analysis Performance Indicators Multiservice Communication Networks Based on Distributed Communication Network Construction Technology. – PP. 19–24.
Performance indicators multi-service communication networks built in accordance with the architectural concept of NGN (Next Generation Network) and FN (Future Network) based on the technology building distributed communication networks are analyzed. The performance multiservice communication networks using SDN (Software Defined Networking) and NFV (Network Functions Virtualization) technologies is chosen as a criterion for system performance. Analytical expressions for estimation probabilistic-time characteristics communication network are obtained on the basis of model.

Key words: network performance, SDN, distributed communications technologies, NFV, physical resource.

Abramenko G., Minyaev A., Khramtsov D. Research of Attacks and Methods of Protection of Wireless Networks During Authentication Using the 802.1x Protocol. – PP. 25–29.
This article discusses the principles of operation of the IEEE 802.1x standard, as well as possible DoS attacks: EAPOL-Start, EAPOL-Logoff, EAP-Failure, EAP-Success, which can be implemented by an active intruder described in regulatory legal acts. Methods of protection against the presented attacks are determined and methods of their implementation on equipment from various manufacturers, such as TP-LINK, ASUS, are investigated.
Key words: wireless networks, wireless attacks, WPA2-Enterprise, Radius, 802.1x, DoS, denial of service, security methods.

Abramov S., Abramova E., Pavlov I., Pavlova M. Overview of the Basic Concepts of Invariance in Data Transmission Systems. – PP. 29–34.
The article presents the basic concepts of invariance. The forms of invariance in automatic control systems, which differ in the conditions and methods of achieving invariance, are considered. An invariant data transmission system is described. The role and significance of invariant systems in modern systems, devices and telecommunication networks are outlined.
Key words: invariant, invariance, invariant system, noise immunity, error probability.

Alennikov E., Vasin N., Subbotskaya A. The Impact of VPN Connection Encryption Types on the Data Transfer Rate Over the Physical Channel. – PP. 34–39.
Since the organization of a VPN tunnel is the creation of a logical channel between two or more parts of the network on top of a physical communication channel, this creates an additional load on the routers, which reduces their throughput. In this paper, a study was carried out on how a VPN tunnel strongly affects network bandwidth.
Key words: Virtual Private Network, GNS3, VirtualBox, IPSec, Custom VPN.

Alieva A., Ibrahimov B., Mammadova F. Analysis Capacity Indicators Multiservice Telecommunication Networks Based on Innovative Technologies. – PP. 40–44.
Performance indicators multiservice telecommunication networks built in accordance with the architectural concepts of NGN (Next Generation Networks) and FN (Future Networks) are analyzed. Based on the study, a new approach to the construction of a mathematical model taking into account the property of the self-similarity transmitted traffic is proposed to estimate the capacity indicators multiservice telecommunication networks based on innovative technologies. Based on the model, analytical expressions are obtained for analysis probabilistic-temporal characteristics communication networks in the provision multimedia services.
Key words: capacity, SDN, traffic self-similarity, multimedia services, NFV, multi-service network, channel resources, traffic management.

Andreeva E., Kalashnikov A. Features of Video Transmission Fiber-Optic Network with Different Single Mode Fibers. – PP. 45–49.
Comparison of the protection from the traffic interception in fiber optic video network for different fibers is studied.
Key words: fiber optic networks, fiber optic fiber, traffic interception, bending losses.

Antonenko A., Dunaytsev R. A Study of Apple Smartphones Operation in Wi-Fi Networks. – PP. 49–52.
According to recent surveys, one of the most popular smartphones are Apple iPhones running the iOS operating system. In addition to cellular networks, these smartphones are often used to connect to Wi-Fi networks. This paper discusses an algorithm used by Apple iPhones for scanning Wi-Fi channels and choosing an access point for association, as well as an algorithm responsible for roaming between access points.
Key words: Wi-Fi, Apple, iPhone, smartphone, roaming, access point.

Akhmetshina M., Borisenko N., Yakovlev V. Investigation of Affine Equivalence in Substitution-Boxes of Dimension 3x3. – PP. 52–57.
A study of substitution-boxes (S-boxes) that perform nonlinear transformations in the construction of cryptographic systems was carried out in order to determine the number and composition of affine-equivalent classes. Using the developed program using an exhaustive search algorithm, a complete calculation of affine-equivalent sets has been performed. Four affine-equivalent classes were found and their composition was fully determined. This result can be used to identify relationships within classes and serves as the basis for finding an algorithm for finding affine-equivalent classes of S-boxes of large dimensions.
Key words: cryptographic transformations, S-box, Boolean functions, affine-equivalence transformations.

Akhrameeva K., Voroshnin G., Kovtsur M. Investigation of Vulnerabilities of MikroTik Equipment to Attacks on Wireless Networks. – PP. 57–63.
Simultaneously with the growing popularity of the Internet, the number of network equipment manufacturers is growing. As shown in the paper, the network equipment of the company MikroTik is popular because it isn't expensive, while it has a fairly wide functionality. The equipment of this company is the choice for small corporate networks, in particular, for creating a Wi-Fi network. This technology becomes widespread due to convenience, but due to the widespread use of wireless networks, wireless attacks become more common. Some attacks can be implemented quite easily, and the attacked equipment has a large number of vulnerabilities. Huge number of scientific papers and reports are devoted to the topic of wireless attacks and protection against them. But despite this, the impact of wireless attacks on the equipment of specific vendor is not studied well. In the paper, the impact of attacks on wireless networks is studied on the equipment of the manufacturer MikroTik, and methods for detecting attacks are proposed.
Key words: information security, wireless network security, MikroTik.

Ahrameeva K., Gerling E. Use Steganography in Social Networks and Messengers. – PP. 63–67.

Social networks and messengers have firmly entered our lives. They offer great opportunities to communicate with people in various parts of the world. To exchange information through social networks and messengers, you can use, in addition to the text itself, files of various formats. Which, in turn, allows you to use not just files, but files with hidden message steganography methods attached to them. In this work, the possibility of using steganography to exchange hidden information through modern social networks and messengers is considered.

Key words: steganography, social networks, messengers, embedding information, extracting information.

Akhrameeva K., Gerling E., Kulikov I. Review of Genres of Computer Games for Creating Steganographic Systems. – PP. 67–72.

The article presents the results of a study, the purpose of which is to analyze the main genres of computer games, classified according to the methods of obtaining information during the game, according to the type of actions performed, the use of the game environment, movement around the game world, by the type of control and management of game entities (information games, action games and game of control). The possibilities and features of creating steganographic systems in games of certain genres are considered. Methods for creating steganographic systems for popular game genres are proposed. A comparison of the possibilities of creating steganographic systems using gameplay elements of genres and various combinations of these elements in hybrid game genres is given.

Key words: steganography, content-aware steganography, steganalysis, computer games, genres of computer games.

Babkov I. Analysis of the Effectiveness of SIEM-systems in the Organization. – PP. 72–77.

The use of SIEM-class systems significantly improves the level of information resource protection and the effectiveness of information security monitoring in organizations. The article analyzes the main tasks, advantages and disadvantages of such systems. Particular attention is paid to selecting the most effective systems based on criteria that take into account the characteristics of organizations. Ways to improve the efficiency of SIEM systems in the organization are being considered.

Key words: Security Information and Event Management, SIEM, information security.

Balina A., Bylina M. The Possibility of Unauthorized Access to fibers in Passive Optical Network. – PP. 78–83.

The paper investigates the possibility of unauthorized access to optical fibers in passive optical network by creating an acousto-optic leakage channel. The physical reasons for the formation of acousto-optic leakage channels in fiber-optic communication systems are considered. The effectiveness of this leakage channel is estimated. The depth of modulation of the optical signal subjected to acoustic influence chosen as the efficiency criterion.

Key words: passive optical network (PON), acoustic modulation, acousto-optic leakage channel, optical connector, Fresnel reflection, modulation depth.

Batenkov K. Analysis of the Time Spent on the Formation of Sections by Sequentially Iterating Through all Combinations of Vertex Sections. – PP. 83–86.
We consider an approach to the formation of cross-sections based on a method that uses a matrix of connections as a basis, and, in fact, involves a sequential search of all combinations of vertex sections, starting from the source and drain. It is shown that the execution time of such calculations is not too long and did not exceed ten seconds for the test network.
Key words: communication network, cross-section, time costs, two-pole network, graph.

Belov A., Lipatnikov V., Fedorov I. Model of a Cognitive Radio Network Based on the Theory of Stochastic Network Calculation. – PP. 86–90.
The available spectrum resources suitable for wireless transmissions are becoming more limited. The cognitive radio proposal offers a solution to use the limited spectrum in a more efficient way. The stochastic model of the network calculus is able, according to the obtained probabilistic characteristics, to adjust the parameters for effective transmission and reception in a cognitive radio network.
Key words: cognitive radio network, stochastic, network calculus, probabilistic boundary characteristics.

Berezina E., Vitkova L. Development of a Database for Selecting Countermeasures for Malicious Information Detection Systems. – PP. 90–95.
Information technology and online interaction are a part of our lives today. The question of developing a system to detect and counteract malicious information seems to be topical. In this article, the authors offers the structure of the malicious information countermeasures database and the methodology of building the database. It is suppose that the database can interacts with the countermeasure selection and supporting decision-making module in systems for monitoring and counteraction malicious information.
Key words: malicious information, countermeasures databases, monitoring and counteraction systems, decision support system (DSS).

Bogdanova L., Vitkova L. The Development of a Traffic Sequence Diagram in IoT Networks. – PP. 95–99.
The Internet of Things (IoT) becomes more popular in many areas of life, opening up new forms of communication between people and things. The information is transmitted using sensors integrated into smart devices. The growing popularity of IoT implies the development of solutions and algorithms to ensure the information security of the Internet of Things and, in particular, the protection of user data transmitted in communication networks. The design of information security methods requires a clear understanding of the system operating in normal mode. The development of IoT network security algorithms implies a preliminary description of the normal traffic flow. For a visual representation of the exchange of data packets, a sequence diagram is created that displays the elements of the communication network. The report provides a description of the diagram, describes the network nodes involved in the data transfer process, and indicates the messages exchanged during the traffic flow.
Key words: IoT networks, IoT security questions, IoT security threats, traffic analysis, sequence diagram.

Branitskiy A., Kotenko I., Fedorchenko E. Technique for Classification of Social Network Communities Using Neural Networks. – PP. 100–103.
The paper describes a technique for classifying communities in a social network according to the degree of their destructive impact on users belonging to the socio-demographic group "youth", using text classifiers, classifiers built on the basis of artificial neural networks, as well as their ensembles. The classification of communities in social networks is based on the data obtained as a result of the Ammon test among members of these communities. The experimental results demonstrate the applicability of the proposed technique for identifying destructive influences in a social network.
Key words: destructive impact, social network, Ammon's test, neural network, classification.

Buzyukov L., Guseynov N. Protection of Personal Data in Medical Information Systems. – PP. 103–107.
In connection with the pandemic of coronavirus infection in 2020, in all spheres of human life, there is an urgent need to switch to remote services, which has not spared the field of medical services. Therefore, the demand for medical information systems (MIS) has increased. With the growing demand of medical institutions for MIS, there is a need to improve the security of such services.
Key words: digital healthcare, medical information systems, database, electronic medical records, web service.

Buzyukov L., Klochkov M. Analysis of the Problems of Remote Customer Service in the Field of Medicine. – PP. 108–112.
In 2020, due to the COVID-19 pandemic, many service sectors were forced to switch to a remote service format. For this reason, the demand for medical information systems (MIS), especially for integrated systems (KMIS), has increased among medical organizations. Their main advantage is the ability to control cost optimization and improve the quality of patient care.
Key words: digital healthcare, electronic medical records, telemedicine, integrated medical information systems, database, electronic medical records, medical and preventive institutions, web service.

Buzyukov L., Sudarev A. Problem Analysis and the Concept of a System of Employee Monitoring. – PP. 113–116.
Currently, many companies are implementing time-keeping systems. The main goal of the economic is to improve efficiency of work. But the side effect is often the dissatisfaction of employees. Because they perceive the attempt at control as a clear distrust on the part of the leadership, and even as a desire to "tighten the nuts". How to avoid deterioration of relations and not to be left without employees?
Key words: employee tracking, management, WinAPI, C++, Winsock, Database.

Bukshin I., Korzhik V. Elaboration of the Method Using Digital Watermarking Technology Against Paper Certificates Attacks Cloning. – PP. 117–122.
Paper certificates are a popular technology to provide an originality of products and copy right for their owners. Both bar codes and data matrices are examples of such certificates. However, such approach is not sufficient copy-past cloning attacks on paper covers even in the case of digital watermark execution. Algorithm of cloning attack detection is suggested and

investigated performance at the proposed method in them at the probability of errors is consider defending on system parameters.
Key words: paper certificate, cloning, digital watermarking, probability of cloning detection.

Bourdine A., Burdin V., Dashkov M., Nizhgorodov A. Potential Possibilities of Optical Fiber Strength Control by Estimates of Nonlinear Acoustic Emission when Using Test Fibers as an Acoustic Sensor. – PP. 122–125.
The presented work presents experimental results demonstrating the possibility of controlling the strength of optical fibers based on the use of the tested optical fiber as an acoustic sensor for measuring the spectral characteristics of nonlinear acoustic emission signals formed when testing an optical fiber with microcracks on the surface of fiber cladding under the action of an acoustic signal of one frequency.
Key words: optical fiber, optical fiber strength, fiber optic acoustic sensor, nonlinear acoustic emission, microcrack.

Burmistrov M., Tsvetkov A. Implementation of SSH Connection Tunneling Using WebSocket Protocol. – PP. 125–130.
With cloud technologies growth, number of devices within service infrastructure growing rapidly. In this regard, there is a need for centralized management of them. Meanwhile, modern web technologies enable to implement access to network nodes through unified graphical user interface which is accessible via any user device that connected to network.
Key words: web development, tunneling, connectivity, remote management, information security.

Busarov Y., Redrugina N., Shvidkiy A. Analysis of Ways to Improve the Quality of Service for E-Commerce Applications. – PP. 131–135.
The purpose of the article is to model an e-commerce service to calculate the quality characteristics of the system. Approaches to improve the quality of user service are formed, including forecasting the increasing load and the possibility of manipulating the volume of server equipment.
Key words: queuing system, quality of service, QoS, infocommunication services, simulation, server resource allocation.

Buharin V., Kazachkin A. Detection of Unauthorized Information Flows in Information and Telecommunication Networks. – PP. 135–139.
The article considers an approach to identify unauthorized information flows in the information and telecommunications network using identifiers formed by destructive software capabilities or undeclared software capabilities from network nodes.
Key words: unauthorized information flows, undeclared capabilities, protection of information and telecommunications networks.

Bystrov I., Kotenko I. Analysis of User Behavior Models for Malicious Insiders Detection. – PP. 139–143.
The paper analyzes the user behavior models for malicious insiders detection. Detecting malicious insiders is complicated by the fact that the insider, being an employee and being

inside the protected network, is performing official duties. This circumstance makes it difficult to identify malicious insiders. The key factor in solving a problem is the choice of user behavior models.
Key words: user behavioral models, user behavior analytics, insider threat detection.

Bystrov I., Fedorchenko A., Fedorchenko E. An Architecture of Security Assessment and Countermeasure Selection System Based on the Semantic Model of Data and Metrics. – PP. 143–146.
The paper describes the proposed architecture of security assessment and countermeasure selection system. The system is based on the security assessment and countermeasure selection techniques using the semantic model of data and metrics. The developed semantic model incorporates the data sources for security assessment and countermeasure selection, data and metrics. It is designed to construct integral security metrics based on primary metrics calculated using raw data. The developed techniques include the stage of semantic model generation based on the static information on the analysed information system, the stage of dynamic semantic model generation based on the processing of data obtained while analysed information system operation, and the stage of metrics calculation using the formed questions of security assessment and countermeasure selection. The algorithms of integration of the developed system with information security management systems based on the big data processing methods are proposed.
Key words: security assessment, cyber attack, countermeasure, semantic model, metrics, data.

Vershennik E., Teslya S. An Approach to Modeling the Topological Placement of Subscribers of Information and Telecommunications Networks. – PP. 146–151.
The article describes a solution that can be used to model a communication network during its design, modernization, and operation, in particular, to form an optimal variant of the topological placement of a set of information-interconnected subscribers on a given fragment of a public communication network.
Key words: communication network model, modeling of information and telecommunications networks, adequacy of modeling.

Vershinina X., Saltykov A. Application of modified BB84-DS protocol in Quantum Key Distribution. – PP. 151–155.
One of ingenious solution to protect access networks from possible attacks is the application of quantum key distribution technology, one allows users to exchange secret keys with absolute security guaranteed by the quantum mechanics laws.
The problem of attack protection on the photons number splitting is relevant in the QKD networks. The standard QKD-BB84 protocol guarantees security only for signals from single photon impulses. Is proposed a more advanced version of the protocol – BB84-DS, enhanced with decoy-states to resist the photon number splitting attack. The research considers the possibility of improving the security of quantum networks by using the BB84-DS protocol.
The article also considers the prospects of the BB84-DS protocol in the context of global quantum communication networks
Key words: quantum key distribution, QKD, protocol BB84, BB84-DS, decoy-states, PNS-attack, photon polarization.

Vikulova A., Volostnykh V., Kononov P., Parfirov V. Protection of Personal Data of Geographically Distributed Enterprises. – PP. 155–160.
Currently, a significant number of enterprises are located in different territories and telecommunications systems are used to exchange information between separate structural divisions. At the same time, in order to ensure management processes, it is necessary to exchange confidential information, including personal data. The article discusses ways to protect personal data when they are transferred from between structural divisions of a geographically distributed enterprise. The main approaches to the choice of means of cryptographic protection of information for the protection of personal data are given. The article may be useful for specialists of technical information security departments.
Key words: personal data protection, electronic document management, information security tools, cryptographic information security tools, unauthorized access to information, geographically distributed enterprise.

Vitkova L. Analysis of Data Models of Popular Social Networks. – PP. 160–163.
The existing approaches to building models of social networks can be divided into three concepts: models of data representation, models of information exchange in social networks, models of information dissemination. Each concept is unique in its own way and allows you to describe different characteristics. The analysis and synthesis of data structures of popular social networks is based on the concept of data representation.
Key words: IPTV, caching, TV, time-shifted, the proxy.

Vitkova L., Goluzina D. K-Block Cross Validation in Machine Learning Problems. – PP. 163–167.
Machine learning algorithms are widely used today. They are used in business processes, to improve efficiency and accuracy, in the scientific field, to process large amounts of data and change the approach to existing problems, and also just for fun. Since the use of machine learning algorithms allows faster and more efficient processing of large amounts of text, they can be a good tool for solving information security problems. This article discusses a way to improve the quality of machine learning models in the problem of processing test messages from a social network using k-block cross validation.
Key words: neural networks, word processing, machine learning, cross-validation.

Vitkova L., Koptelova V. Classification of E-Commerce Bots and Their Behavior. – PP. 168–173.
The article raises the issue of electronic fraud in the modern information community. The subject of the research is the most widespread tool of fraudsters - special automated programs known as "bots". Research includes consideration of the consequences of using such programs. The main goal is to classify the aforementioned bots in terms of information security.
Key words: automated program, bots, e-commerce, fraud, intelligent bots, trading bots, shopping bots, ad-bots, chatbots, bot behavior.

Vladimirov S., Fomin A. Model Network for Network Coding Based Multicast Transmission Research. – PP. 173–178.
The paper presents the structure of a laboratory model network for the study of multicast transmission by network coding methods in data transmission networks based on TCP/IP

protocols. A structural scheme of a model network has been developed and options for its implementation based on software and hardware platforms have been proposed. Taking into account the peculiarities of the research, the choice of the software and hardware platform of the testbed equipment was made. The principles of implementation of the software of terminal and routing nodes of the network intended for research are considered. The directions of further development of the testbed and the functions of the model network are presented.
Key words: model network, network coding, multicast transmission, TCP/IP networks.

Volkogonov V., Getman E., Salita A. Approaches and Methods of Creating Steganographic Attachments in Network Packages. – PP. 178–183.
The issue of confidentiality of information is very acute in the modern world. Unlike cryptography, when using steganography, there is no need for licensing and coordination. Steganography also allows you to keep the participants in the exchange of information secret, and vice versa – to track the participants in the illegal dissemination of data. This article describes the main approaches and methods of constructing steganographic channels, discusses libraries and software utilities for constructing steganographic channels, as well as practical implementation in the global Internet.
Key words: steganography; network; steganography; security; IPv4; channel steganography; information concealment; information protection; data networks, channel capacity.

Volkogonov V., Getman E., Salita A. Hiding Information in RTP, RTCP Protocols. – PP. 183–188.
Due to the growing popularity of IP telephony and the increase in other delay-sensitive media traffic, the popularity of such protocols as RTP, RTCP has increased. This article discusses the possibility of creating steganographic channels based on the RTP, RTCP protocols, examines the header fields that can be used as stego containers.
Key words: steganography; network; steganography; security; IPv4; channel steganography; information concealment; information protection; data networks, channel capacity.

Voronina K., Muthanna A. Design and Development of an Information System for Automating Household Waste Collection. – PP. 188–193.
The article deals with current issues of digitalization of the economy. It presents ways of solving the environmental problem by installing, in the interior of garbage cans, sensors to monitor the filling of household waste. The experience of foreign countries, which has shown how effective waste management systems are, is studied. For effective control over the fullness of the information system is developed, with the help of which the dispatcher monitors the household containers.
Key words: automation, sensors, household waste collection, system, business process.

Voronov A., Tsvetkov A. Development of Plugins in the Labgen Web Application. – PP. 194–201.
The year 2020 showed that educational institutions cannot do without specialized systems for automating the educational process. Due to the constant increase in the information flow, as well as the need to organize education from anywhere in the world. Automated training platforms are most often organized according to the client-server application model. Due to

this specificity, it is necessary at the development stage to provide mechanisms for ensuring the security of the client-server application to prevent various types of attacks.
Key words: spring MVC, plugins, TLS, obfuscation, access rights, java.

Gavrilenko E., Dokshin A., Kovtsur M., Mislivsky B. Study of the Effectiveness of VPN Tunnels for Remote Access. – PP. 201–205.
Currently, there are urgent problems associated with the organization of remote workstations and gaining access to the work network via the Internet. Traffic tunneling protocols are used to solve these problems. Such protocols provide remote access to corporate network and protect data during transmission over the public channels. The article analyzes popular solutions for tunneling Internet traffic, such as IPSec, L2TP, PPTP, and OpenVPN. The indicators of efficiency, scalability, performance and security of tunnels have been investigated. Considered the features of the implementation of a VPN gateway based on open operating systems
Key words: VPN, IPSec, OpenVPN, Remote Access, efficiency.

Gaifulina D., Kotenko I. Analysis of Criteria for the Classification of Approaches to Security Events Correlation. – PP. 206–210.
Currently, cyber defense systems process a huge amount of data for security analytics and alerts reporting. At the same time, various methods of analyzing security events are used, among which correlation occupies an important place, which makes it possible to identify the relationship between dissimilar events and alerts. The systematization of existing approaches to the security events correlation can be carried out on the basis of various criteria: by the level of events correlation, the methods, the number of information sources, etc. This paper analyzes the criteria for the classification of approaches to the security events correlation. Based on the analysis performed, we propose the most extensive taxonomy of the considered approaches.
Key words: security event correlation, alert correlation, security management.

Gaponenko V., Tcvetkov A. Algorithms for the Search, Use and Elimination of Industrial Radio Interference. – PP. 211–215.
Industrial radio interference-electromagnetic disturbances created unintentionally during the operation of various technical devices, means, devices and apparatuses, as well as, in some cases, created by a person intentionally using special technical components, or neglecting state standards in the field of combating radio interference. Industrial interference interferes quite strongly with radio reception, manifesting itself, for example, as crackles and noises in telephone sets, audio output and output devices, as well as distorting the signal at a frequency similar to the interference frequency. The article will discuss the causes of interference, their impact on the operation of other devices, ways to deal with them, as well as the technical possibility of using interference by an attacker for selfish purposes.
Key words: industrial interference, fighting, interference use, interference effect, listening devices, interference frequency, electromagnetic disturbances, noise, signal distortion.

Gelfand A., Kazantsev A., Krasov A., Ulyasheva V. The Internet of Things (IoT): Security and Confidentiality Threats. – PP. 215–220.
The Internet of Things (IoT) is used to enable communication between multiple devices. It is a system in which objects embedded in sensor technology interact with other objects through a wireless communication medium to exchange and transmit information without human

interaction. The purpose of this article is to bring forward the various security and privacy issues that the Internet of Things environment faces, as well as the existing mechanisms used to protect it.
Key words: privacy, security threats, RFID, WSN, Internet of Things.

Geraskin V., Elagin V., Ermolaev E., Fedotov I. Research of Modern Neuro-headsets: Methods of Signal Processing and Relevance of Technology. – PP. 220–223.
Currently, due to the reduction in the cost of manufacturing microelectronics and the increase in the accuracy of measuring instruments, it is becoming easier and cheaper to conduct scientific experiments that were previously considered unattainable for laboratories and civilian researchers with a modest budget.
This article examines the modern market of neurointerfaces, the range of their application, and also methods of signal analysis will be touched upon.
Key words: Neuro-interfaces, EEG, FFT, brain activity.

Gerling E., Fyodorova A., Kovzur M., Development of a Web Interface for a Monitoring System for IEEE 802.11 Wireless Networks. – PP. 224–228.
Web applications are widely used in the life of the modern person. The main advantage of such applications is the ability to use them without the need to install additional software. Other positive qualities are the absence of updates at the user's workplace and the storage of the main configuration files on the server. Web interfaces are used to work with various online services, as well as for configuration of network devices such as routers, modems, video cameras. This article focuses on the implementation features of the web interface for an embedded device with extremely limited resources.
Key words: web interface, wireless networks, monitoring system.

Glagolev S., Gorskov V., Dotsenko S. The Use of Raman Amplifiers to Maintain the Quasi-soliton Regime in Dispersion-Shifted Single-Mode Fibers. – PP. 228–234.
This paper considers a method for maintaining the quasi-soliton mode in dispersion-shifted single-mode optical fibers using Raman distributed optical amplifiers (OA), which are also called stimulated Raman scattering (SRS) amplifiers. Theoretical calculations and simulations were carried out for amplifiers with counterpropagating and bidirectional pumping. It is shown that the use of an SRS OA makes it possible to increase the length of the amplifying section in quasi-soliton fiber-optic communication systems in comparison with systems using discrete OA. The advantages of bi-directional pumping are also shown. Formulas are obtained for the selection of technical solutions in the design of quasi-soliton fiber-optic communication systems.
Key words: dispersion-shifted single-mode optical fiber, chromatic dispersion, self-phase modulation, soliton, quasi-soliton mode, optical amplifier.

Glagolev S., Gorskov V., Dotsenko S. Use of EDFA Optical Amplifiers to Maintain the Quasi-soliton Signal Propagation Through Dispersion-Shifted Single-Mode Fibers. – PP. 234–240.
The paper considers a method for maintaining the quasi-soliton regime in dispersion-shifted single-mode fibers using erbium optical amplifiers (EDFA). Theoretical calculations and modeling have shown that there is a limitation on the length of the amplifying section. Formulas

are obtained for the selection of technical solutions in the design of quasi-soliton fiber-optic communication systems.
Key words: dispersion-shifted single-mode optical fiber, chromatic dispersion, self-phase modulation, soliton, quasi-soliton mode, optical amplifier.

Golovanov E., Kulikov D., Shvidkiy A. Methods for Organizing Online-Meeting Recordings Storage in Educational Institutions Analysis. – PP. 240–244.
This article describes possible ways for organizing online-meeting recordings storage in educational institutions. The article also presents a solution for improving one of the featured methods along with its functional specification.
Key words: integrating videocalls into educational infrastructure, recording videocalls, saving videocalls to cloud storage, Jibri, Nextcloud.

Golovkova E., Terebenina Yu., Reznikov B. Home Networks. Development of HomePNA Technology. – PP. 245–248.
Now for each of us, the personal computer has become a powerful and even necessary home tool that we use for entertainment, education, work and communication. The Internet has long become a means of obtaining all kinds of information, so there is a need to increase the speed of digital data transmission not only outside the home, but also within the same apartment or office. In this case, the deployment of a local network will turn out to be unprofitable, due to the special difficulties of a technical nature. The solution to this problem is HomePNA (Home Phoneline Alliance) home network technology, which is based on the use of a telephone line and provides a simple, high-speed and low-cost home network.
Key words: HomePNA, Access Networks, Telecommunications.

Gololobov N., Izrailov K. Investigating a Way to Call an Insecure Kernel API on Windows. – PP. 248–252.
Windows is one of the most popular operating systems in the modern world. Its functioning is based on the division of the execution space into user programs available for operation and for the operation of the system kernel. The article discusses one of the mechanisms for attacking the operating system by bypassing security mechanisms when checking calls from custom applications to kernel functions. A hypothetical example and procedure for such a protection bypass are presented. In the interests of countering this type of attacks, the main corresponding approaches are proposed.
Key words: kernel mode, system calls, kernel API, system security.

Golubov N., Kosov N. Research Algorithm for Searching Insiders in the Internal Network. – PP. 252–256.
This article will consider the concept of an insider and their varieties, auxiliary methods for catching, as well as an algorithm for finding them in the internal network. This problem is relevant, since today insiders represent the most serious danger for organizations of all levels, regardless of their activity. Due to their own knowledge and legal access to information systems, they safely bypass physical and electronic controls to achieve their own selfish goals. The intervention of these individuals is difficult during the attack, and it will take a lot of time and money to repair the huge damage. The damage can be not only reputational and financial, internal violators can also harm the health and life of people.

Key words: insider, DLP-systems, honey-pot, UEBA-systems.

Gorlina A., Yakovlev V. Development of Approaches to the Creation of the Secret Remote Voting System in the Dissertation Council of the University. – PP. 257–262.
The paper proposes an approach to creating a system of secret voting, which can be carried out remotely by members of the dissertation council while maintaining the confidentiality and anonymity of their votes, which is relevant during a pandemic. The composition of the voting system, its parameters and the algorithm of functioning have been determined. The voting system is based on the Paillier homomorphic encryption cryptographic system.
Key words: electronic voting, encryption, dissertation council, homomorphic encryption, Paillier cryptosystem.

Gofman M., Kornienko A. About a Multichannel Audio Stego System Based on Watermarked Digital Audio Signals. – PP. 262–265.
A multichannel audio stego system is being developed based on watermarking digital audio signals, focused on noiseproof data transmission in an airborne audio channel. This system makes it possible to embed elements of watermark in arbitrary frequency components of a digital audio signal, considering the provision of the watermark auditory transparency and the possibility of blind reception. The developed audio stego system provides a sufficient degree of noiseproof during the transmission of the watermarked audio signal through the airborne audio channel even with low embedding strengths of the elements of watermark.
Key words: steganography, audio watermarking, covert data transmission.

Grebenshchikova A., Elagin V. The Auto Regressive Integrated Moving Average (ARIMA) Model for Prediction the Network Traffic. – PP. 266–271.
The predictability of network traffic is a significant interest in many domains such as congestion control, admission control, and network management. The predictability of network traffic is a significant interest in many domains such as congestion control, admission control, and network management. The most popular model for prediction is used autoregressive integrated moving average – ARIMA, but this model often fails to perform correct prediction. ARIMA model is a linear time series model that the mean is conditional changed but the variance is constant. The Auto Regressive Integrated Moving Average (ARIMA) with Generalized Auto Regressive Conditional Heteroscedasticity (GARCH) model is a nonlinear time series model which combined the linear ARIMA with conditional variance GARCH. ARIMA/GARCH model provides flexibility when it is applied to model the network traffic
Key words: forecasting the network traffic, data traffic models, ARIMA models, GARCH models, self-similarity, multifractal.

Grishin I., Mikheeva S., Podgornaya K. Overview of Prototype Filters for Multicarrier Technologies. – PP. 271–277.
Orthogonal frequency division multiplexing (OFDM) has become one of the most widely used in broadband wireless communications. This was due to such advantages of the method as: high noise immunity to frequency selective fading and additive interference, as well as the simplicity of signal generation and processing. At the same time, OFDM technology has a number of disadvantages, such as sensitivity to frequency shifts and slow attenuation of the signal spectrum outside the frequency band allocated for transmission, which leads to out-of-

band emissions. In this regard, the OFDM technology has been upgraded to the F-OFDM technology (filtered OFDM), which implies filtering out-of-band emissions. The report contains a comparative analysis of prototype filters used in this technology.
Key words: OFDM, F-OFDM, RC, SRRC.

Gulevich V., Elagin V., Loshakova A., Pomogalova A. Development of an Electronic Voting Information System Based on Blockchain Technology. – PP. 278–282.
The purpose of this work is to develop an information system for electronic voting based on Blockchain technology, which automates the process of conducting voting procedures, as well as ensures transparency, accessibility, anonymity and the impossibility of vote fraud. The relevance of the developed system lies in the possibility of conducting the voting procedure remotely using a computer or phone, which will significantly save the time of voting participants, as well as reduce contacts with other people, which is particularly important during quarantine measures. The result of the work is a developed decentralized information system based on the Ethereum platform, within which users can express their opinions by voting on topics of interest to them. The paper discusses the features of the implementation of the information system, the developed functionality and issues related to the security of the voting procedure using the developed system.
Key words: blockchain, voting system, Smart Contract, Smart Contract, Secure Voting System, Ethereum.

Gurbatov G., Panichev A., Ushakov I. Kubernetes Basic Security. – PP. 282–286.
Containerization technologies have greatly simplified the work with applications, and also made it possible to use computing resources more efficiently by running a set of only the necessary libraries in a container. Convenient container deployment and management systems such as Kubernetes have appeared. But along with the convenience and speed of working with new technologies, new vulnerabilities have appeared that need to be eliminated by security tools to ensure data safety and correct operation.
Key words: Kubernetes, Docker, containers, cluster, security, attack, encryption.

Davydov V., Dmitrieva D. Remote Fiber-Optic Sensor for Controlling γ-Radiation of Various Power. – PP. 286–289.
In the article the necessity of improvement of metrological specifications and functional capabilities of fiber-optic sensors for long distance measurements (more than 10 km) is substantiated. New method of building of communication lines with fiber-optic sources for controlling exposure dose of γ-radiation in the large range of changes (several orders of magnitude) at the remote mode is suggested. Functional capabilities of fiber-optic sensor are identified. The switching diagram and the limits of measurements are developed. The received experimental results are presented.
Key words: fiber-optic sensor, γ-radiation, optical fiber, laser radiation, exposure dose of radiation, radiation-induced losses.

Davydov V., Pilipova V. Fiber-Optic Emergency Simulator for Checking the Operation of Control Systems of Shipboard Nuclear Power Plants. – PP. 289–292.
The necessity of testing the equipment for monitoring the operation of nuclear power plants is justified. It is proposed to use optical fiber and pulsed laser radiation for these purposes.

It is established that optical fiber is more resistant to radiation than other communication systems. The design of a fiber-optic emergency simulator is developed. The calculation of its characteristics is carried out. Their experimental research was carried out. It was found that with an optical signal delay of 98.6 microseconds, the loss is – 26 dB with an uneven frequency response of ± 2 dB. This makes it possible to test the entire set of equipment that uses optical signals used to control a nuclear power plant.
Key words: nuclear power plants, control system, fiber-optic simulator, laser radiation, delay time.

Dedukhova A., Shvidkiy A. Comparative Evaluation of Cloud Infrastructure Component Monitoring Systems. – PP. 292–296.
The article presents the most popular multifunctional component monitoring systems for cloud infrastructures and their comparative evaluation according to specific criteria. These systems currently represent the functionality and performance at a high level, and have proved the importance and convenience of a unified approach to monitoring systems.
Key words: monitoring system, cloud technology, servers, GUI.

Desnitsky V., Parashchuk I. Formal Description of the Features of the Intruder Model and Criticality of Attacking Actions on Wireless Sensor Networks. – PP. 297–301.
An approach to the formal description of the intruder model is considered in the interests of analyzing the security of wireless sensor networks from attacking influences. This approach is based on the classification characteristics of an intruder capable of applying multi-step attacks, both physical and software-informational in nature. At the same time, the use of classification features of the violator allows us to specify the indicators of criticality of the attacking effects on networks of this class.
Key words: wireless sensor network, attacking actions, security, model, criticality, intruder, feature, indicator.

Dmitrieva V., Reznikov B. Use of Antenna Arrays Principles in Optical Signal Processing. – PP. 301–304.
The article describes the principles of operation of antenna arrays, discusses the possibilities of their use in optical signal processing. An example of such use is the ability to determine the angle of arrival of a radio signal to an antenna array using the Fourier transform capabilities of an optical processor.
Key words: antenna arrays, optical processors, diffraction gratings.

Dmitrieva Y., Elagin V. Approaches to Modeling SDN Resources. – PP. 305–309.
A model of a fragment of an SDN-network is proposed, developed on the basis of the queuing theory and allowing one to find the main probabilistic-temporal characteristics of the processes of interaction between switches and an SDN controller. For the stationary mode of operation, on the basis of Erlang's formulas and Laplace transformations, a method is proposed for calculating the parameters of a fragment of an SDN network, expressions are obtained that allow one to determine the average fractions of packet losses at each of the phases of their processing by the switch. A number of assumptions were made that made it possible to consider a three-phase switch as single-phase with three independent flows. Using the presented SDN model, network administrators and planners can formalize the functioning of the elements of a

network fragment, predict the likely performance changes resulting from changes in traffic. The research results can be used in the design and operation of computer networks that implement the SDN concept.
Key words: SDN (software defined networking), the OpenFlow Protocol, Controller, OpenFlow Switch.

Dombrowski J., Malofeev V., Parashchuk I. Analysis of Modern Software Tools for Protecting Infocommunications from Network Attacks. – PP. 310–314.
A comparative analysis of modern software tools for protecting infocommunications from network attacks is carried out. The data obtained in the course of the study can help in assessing the potential effectiveness of the use of various means of detecting malicious influences, taking into account the advantages and disadvantages of the software tools considered. The results of the analysis will increase the validity of decision-making when choosing attack detection systems in the interests of ensuring data protection in an infocommunication network or system.
Key words: infocommunication network, system, detection, network attack, impact, blocking, threat, resource.

Donskov E., Kotenko I. Analysis of Adversarial Attacks on Machine Learning Components of Intrusion Detection Systems. – PP. 315–319.
Today, machine learning is increasingly being used to solve intrusion detection problems. Although highly effective, machine learning models (components) are susceptible to adversarial attacks by malicious attacks designed to mislead the machine learning components. This study analyzes existing adversarial attacks on intrusion detection systems and how to counter them.
Key words: machine learning, adversarial attack, intrusion detection system.

Dunaytsev R., Lebedeva N. On the Impact of MAC Address Randomization on Passenger Traffic Analysis. – PP. 320–324.
In addition to traditional use for wireless Internet access, Wi-Fi has got another application area in the form of Wi-Fi analytics and geotargeting in geomarketing and advertising. To protect users from being spied on, manufacturers of mobile operating systems have developed a technology for randomizing MAC addresses. This paper describes the fundamentals of MAC address randomization and provides an assessment of the possibility of using collected MAC addresses for monitoring passenger traffic.
Key words: MAC address, randomization, smartphone, Wi-Fi.

Dunaytsev R., Lobach D. An Overview of Indoor Positioning Systems. – PP. 325–329.
Positioning and navigation systems play an important role in the life of modern society, penetrating into all areas of science and technology. In recent years, indoor positioning technologies, also known as local positioning, have evolved rapidly and become one of the hot research topics. This paper compares main indoor positioning systems, including their accuracy, benefits and pitfalls, and describes the effects of indoor radio propagation due to the rich presence of obstacles.
Key words: indoor positioning, Bluetooth, RFID, Wi-Fi.

Dyubov A., Reznikov B., Samoilov G. Overview of Spatial Light Modulation Technology. – PP. 329–333.
We are still using spatial light modulation despite that it became part of our lives long ago in the second part of the 19th century. Moreover, if technologies based on spatial light modulation have any analogs, they surpass them. Today we intersect with spatial light modulation every day – many devices that we deal with every day use it as their basis.
Key words: spatial modulators, LCD, DMD, LCoS.

Dyubov A., Khrichkov V. Laboratory Facility for the Study of Fiber-Optic Sensors Based on Bragg Gratings. – PP. 333–337.
Fiber-optic sensors based on Bragg gratings can be used to measure pressure, strain, temperature and other physical parameters. A laboratory setup has been developed to demonstrate and study the operation of measuring systems and sensors based on fiber Bragg gratings. To determine the reflection and transmission specter of a fiber Bragg grating in a laboratory setup, a wavelength-tunable narrow-band laser is used. The designs of pressure, temperature and deformation sensors have been implemented.
Key words: fiber Bragg grating, fiber optic sensor, temperature measurement, strain measurement, fiber optic measurement system, laboratory setup.

Elagin V., Ermolaev E., Pomogalova A., Fedotov I. Analysis of the Possibility of Using the TON Blockchain Platform for PCS. – PP. 338–341.
Modern SDNs and their controllers offer flexible choices for network configuration, management and customization of configuration rules.
The result of the work is an imitation infocommunication system built on the following technologies: Telegram Open Network and Open Network Operating System as an APCS controller. The simulated nodes of the SDN cluster will be the simulated nodes created with mininet.
Key words: blockchain, SDN, ONOS, TON, network simulation.

Elagin V., Murashkin N., Ogoreltsev P., Pomogalova A. Creation of Decentralized Trading Platform Using Escrow Smart Contract Based on Ethereum. Part 1. – PP. 341–346.
This paper focuses on the development of a decentralized smart contract escrow solution for the sale and purchase of goods. The relevance of the work is justified by the security issues of remote payment transactions. This paper proposes a decentralized solution based on the Ethereum blockchain platform, which aims to address the security of remote transactions and guarantee the delivery of goods. The paper discusses the features of creating a secure payment platform using the escrow smart contract on the Ethereum platform. The features of the platform's structure are presented, the potential problems of the platform and its operation are analyzed, and the feasibility of using decentralized technologies and smart contracts in solving similar problems is analyzed.
Key words: blockchain, Ethereum, smart contract, decentralized app, DApp.

Elagin V., Gromov A., Bakatov V., Pomogalova A. Creation of Decentralized Trading Platform Using Escrow Smart contract Based on Ethereum. Part 2. – PP. 346–351.
This paper focuses on the Development of a decentralized smart contract escrow solution for the sale and purchase of goods. The relevance of the work is justified by the security issues of

remote payment transactions. This paper proposes a decentralized solution based on the Ethereum blockchain platform, which aims to address the security of remote transactions and guarantee the delivery of goods.The present part of the work discusses the implementation of the secure payment platform using the Ethereum Escrow smart contract. As an example, an Internet store has been developed in which a smart contract is an intermediary, acting as a store of the buyer's funds until the specified conditions, that is, receipt of the purchased goods. The work contains features of development of a smart-contract, as well as realization of connection between a smart-contract and front-end part of the site.
Key words: Blockchain, Ethereum, smart contract, decentralized app, DApp.

Elagin S., Spirkina A., Fitsov V. Fundamental of Modeling Traffic Heterogeneous Communication Networks, with the Prospective Channel Identification of Individual Services and Forecasting the Network State. – PP. 351–356.
Modern heterogeneous communication networks in comparison with circuit switching networks are insufficiently studied from the point of view of modeling. Complicating the situation is the presence of heterogeneous applications and devices that generate traffic flows with different characteristics. The article will consider some of the existing approaches to modeling traffic in packet communication networks. Namely, the use of fractiona Brownian motion and Levy motion to describe the aggregated packet traffic, as well as the method of network calculus.
Key words: modeling, fractional Brownian motion, network calculus.

Eremenko V., Reznikov B., Shutova L. Fiber Optic Cable Examination. – PP. 356–360.
The article analyzes the ability to transmit the light flux by a fiber-optic bundle depending on the change in the angle of rotation of the central axis of the bundle relative to the radiation source. The main stages of the formation of a binary discrete optical signal with two-dimensional spatial modulation are considered in practice. Conclusions are drawn regarding the input and output signals in the investigated optical bundle.
Key words: optical harness, fiber, optical signal, endoscope.

Esalov K., Kislyakov S., Shalyapin S. Analysis of Tools for Building Corporate Networks Using Cardano. – PP. 360–366.
The Proof of Stake consensus algorithm is a powerful alternative to the Proof of Work one. The developers of the Cardano network have proposed, in addition to the newest blockchain network, a new "Proof of Stake" algorithm. To help third-party researchers, the developers offered a toolkit for studying and analyzing the work of their Cordano-based new network. The research findings presented here are practical in nature. The main purpose of the research is to show the practical aspects of launching, configuring nodes, wallets and tools for building Cardano network.
Key words: blockchain, Cardano, Proof of Stake.

Esalov K., Kulikov E., Onishuk A. Investigation of the Possibilities of Using deep Machine learning Algorithms in the field of Audio Signal Processing. – PP. 367–375.
Machine learning and deep learning algorithms are penetrating deeper and deeper into every area of our life, from complex raw materials production to the service sector. Also, algorithms of this type are widely used in communication networks, for example, for filtering network traffic or detecting problems in switching networks. This article describes deep machine

learning algorithms used in modern voice verification and user identification systems. This work will describe the features of data preparation for training algorithms based on convolutional neural networks, the architectures of the developed systems are given, and the results of the work are shown.
Key words: neural networks, classification, biometrics, speech technologies.

Esalov K., Marochkina A., Poponin A. Development of a Natural Speech Processing System Based on Neurocognitive Architectures for the Implementation of AI Services of Information and Communication Services. – PP. 375–379.
This article provides one of the ways to implement a natural language processing system, namely: Automatic recognition of Russian speech. This article describes the collection of a BigData dataset that meets the training criteria, how the model was trained, how to improve the model results, for example, using neural models at the stage of postprocessing the results of a speech recognition model or preprocessing the input data. This speech recognition system can be used to implement AI services of infocommunication services.
Key words: AI, neural networks, natural speech processing, neurocognitive architectures.

Esalov K., Pomogalova A., Tyan A. Concept of Building an Information and Computer Environment for Remote Research. – PP. 379–383.
The work is devoted to the study of the concept of building an information computer environment for conducting scientific research and educational processes in a remote format. The issue of remote research remains topical, especially in the context of COVID-19. Testing of high-load networks, studying the architecture and infrastructure of networks 2030 in a remote format allows optimization of research processes. The concept considered in this work allows to conduct all types of network research as well as educational processes using real high-performance equipment and virtualization technologies.
Key words: COVID-19, remote research, computer environment, platform, education.

Zhernova K. Methodology for Designing Human-Computer Interfaces for Information Security Applications. – PP. 384–387.
Taking into account the increasing complexity and increase in the total amount of data transmitted over the network, as well as the increase in the number of devices connected to it, the importance of ensuring information security is growing. However, with prolonged work with information and computer security systems, the operator's reliability decreases, the speed of decision-making and work efficiency decrease. This paper presents a methodology for designing human-computer interfaces based on the use of touch screens, which will increase the operator's reliability when working with information security applications.
Key words: human-machine interaction, information security, user interfaces, data visualization, touch screens.

Zhernova K., Kolomeets M. Vulnerabilities of "Operator – Artificial Intelligence" Interfaces in an Unmanned Transport Environment. – PP. 387–390.
Self-driving vehicles are an integral part of a smart city. This technology is constantly developing, the infrastructure of a smart city is being improved, which allows you to interact with unmanned vehicles. However, as smart city technologies develop, the relevance of ensuring the safety of unmanned transport environments increases, as well as the need to

develop measures to counter emerging threats. This work gives a brief description of the operator-artificial intelligence interface of an unmanned transport environment, describes the main vulnerabilities of this system and possible attacks aimed at these vulnerabilities.
Key words: human-machine interaction, information security, user interfaces, data visualization, machine vision.

Zadorozhnyaya A., Kirichek R. Functional Elements of the Network Support System for Autonomous Vehicles. – PP. 391–396.
One of the most relevant technologies in the world is unmanned vehicles. It is expected that this technology will be widely used in the implementation of networks 2030. Despite the fact that the algorithms and scenarios of interaction of self-driving cars with the surrounding infrastructure and with each other are developing and improving every day, it is too early for self-driving vehicles to enter public roads. Today, the work of algorithms for recognizing objects and matching with objects of the surrounding world is far from ideal. For the correct operation of all elements of the network support system of an unmanned vehicle, it is necessary to develop a single uniform functional architecture of such a system.
Key words: unmanned vehicle, autonomous vehicle, self-driving vehicle, functional architecture, lidars.

Zarubin A., Redrugina N., Savelieva A. Digital Quality: Development of Models and Methods for Comparative Assessment of the Quality of Digital Services. – PP. 396–400.
This article discusses the approach of automated assessment of the quality of services provided by software-defined applications of infocommunication networks using a comparative approach and semantic-ontological analysis and assessment of the quality of perception. This approach is considered as a possible complement to the existing recommendations.
Key words: quality of service, QoS, infocommunication services, comparative approach, semantic and ontological analysis.

Zelichenok I., Kotenko I. Analysis of Methods for Multi-Step Attack Detection. – PP. 400–405.
Multi-step attacks are the main threat to information security today. Differences from other types of attacks: the focus of attacks on different nodes of the information environment, the focus on the largest number of breaches of the information security system at the same time. The danger of multi-step attacks is that a few minor actions can disrupt the information environment. To detect such attacks, several network protection methods have been formed. The report presents an analysis of some of them: based on similarity, correlation, structured approach, based on precedents and mixed. A description of each method is provided, with the pros and cons of each method. For the analysis, relevant studies of various methods of detecting multi-step attacks were collected and studied.
Key words: information security, cyberattacks, multi-step attacks, attack detection.

Ibrahimov B., Ismaylova S., Jafarova E. Research Line Performance Fiber-Optical Transmission Systems on base WDM and DWDM Technologies. – PP. 406–410.
Quality of indicators functioning optical telecommunication systems made on the basis fibre-optic transmission systems using modern optical technologies spectral wavelength multiplexing have been analyzed. On the basis of the analysis existing criteria of efficiency

functioning the fiber-optical systems transfer (FOST), indicators of performance of the fiber-optic communication links (FOCL) when rendering multimedia services on optical transport communication networks are chosen. This paper examines the performance FOCL-based FOST lines using spectral WDM (Wavelength Division Multiplexing) and DWDM (Dense WDM) technologies.
Key words: link capacity, WDM, fiber optic link, CWDM, fiber optic transmission system, wavelength, DWDM, line performance.

Ibrahimov B., Tahirova K. Analysis Information Security Indicators on the Basis Network Steganography Technology. – PP. 411–416.
The analysis information security indicators based on network steganography technology in the transmission of useful and service traffic in multiservice telecommunication networks. In order to study the informative characteristics of network steganography, a structural diagram of the physical process transmitting a secret message using a container file is presented. On the basis of the study, important parameters of the informative characteristics of the steganographic system were selected.
Key words: steganography, useful and service traffic, file-container, hidden package, digital steganography

Ivanov V., Nikitin B., Sergeev A. Influence of Some Characteristics of the Medium in the Transmission of Optical Signals in the Fiber-Optic Transmission System. – PP. 417–422.
The increase in the volume of transmitted information leads to the need to take into account the characteristics of the optical transmission medium, which plays a major role in signal translation. Such accounting becomes especially important when increasing the power of individual transmitted channels and, accordingly, the total power of the group signal. The article deals with the influence of the refractive index on the signal transmitted in an optical medium.
Key words: refractive index, nonlinear refractive index, phase self-modulation, phase cross-modulation, group velocity dispersion.

Ivanov K., Shvidkiy A. Analysis of Methods for Load Balancing the Networking Subsystem of Cloud Infrastructure. – PP. 422–428.
The information technology industry in the direction of cloud technology is actively developing, and the number of applications and users is growing every day. In view of this development, the issue of load balancing in cloud infrastructure becomes relevant. This article aims to review current approaches to traffic balancing at different levels and compare popular software solutions for implementation in cloud infrastructure.
Key words: load balancing, software load balancing, cloud infrastructure.

Ignatova I., Parfenova A., Kirichek R. Remote Monitoring of Covid-19 Patients Using Wearable Electronics. – PP. 428–433.
The article discusses the application of the method of collecting data from wearable electronics, which is used for further analysis and prediction of possible diseases for medical applications. The processing of the received data will allow predicting diseases such as COVID-19.
Key words: internet of things, remote monitoring.

Karelskii P., Kovzur M., Minyaev A. Features of Deploying Security Operations Center when Organizing Remote Access to Company Infrastructure. – PP. 433–437.
With the development of technologies, threats to the information security of organizations appear when creating remote access to its infrastructure. The requirements for systems that ensure the company's information security are growing more and more, in this regard, the issue of creating an effective Security Operations Center is especially acute. The article discusses the advantages and disadvantages of SOC when organizing remote access to the company's infrastructure.
Key words: security operations center, information security, remote access.

Katasonov A., Krasov A., Tcvetkov A. Development of a Universal Algorithm for Creating the Simplest Kernel Modules for Different Versions of the Linux Kernel. – PP. 438–442.
Nowadays, with the application of data security, the requirements for ensuring data security are growing. Hackers are using ever new methods of gaining unauthorized access to operating systems in order to obtain, inflict secret information or create a backdoor. One such way is the kernel-level Rootkit. To understand the specifics of this method, it is necessary to understand what the kernel is, how it functions, how it works with kernel modules and knowledge about how kernel modules are created and how they function. This article has developed an algorithm that is used to implement lkm modules on various versions of the Linux kernel.
Key words: GNU/Linux, Rootkit, kernel modules, security.

Katunin R., Shvidkiy A. Evaluation of Cloud Infrastructure Private Network Tunneling Approaches. – PP. 443–448.
The article discusses three approaches to networking between virtual machines, taking into account security requirements, describes the advantages and disadvantages of each approach, and gives examples. A definition of the concept of tunneling is given and existing tunneling protocols are presented, of which three are the most used for comparison and analysis. After comparing the protocols, a conclusion is made describing the most unified protocol.
Key words: virtual machines, tunneling protocols, GRE, VXLAN, Geneve.

Kilicheva K., Muthanna A. Research and Development of the Architecture for a Data Monitoring System of Medical Institution Based on Edge Computing. – PP. 448–453.
The article is devoted to the research and development of the architecture for a data monitoring system of medical institutions based on edge computing. Edge computing is a paradigm of distributed computing performed within the reach of end devices. This type of calculation is used to reduce network response time, as well as to make more efficient use of network bandwidth. In the course of the work, a conceptual description of the architecture of infocommunication access to the environment was presented. The object of the study was the use of the access channel scheduler, in particular, one of the management methods - CSMA/CA, as the basis of the proposed network. In computer and network technology terminology, collisions are defined as the overlap of two or more frames from stations attempting to transmit a frame at the same time. The article also discusses the role of the chosen technology in network components, analyzes the features of the data transmission and retransmission framework. The experiment has a high practical value due to the importance of the health sector and the rapid progress of wireless network technologies. The created model can be integrated for further application in the design and implementation of application services in the Internet of things.

Key words: Internet of things, IoT, Edge computing, E-health, RFID, MEC.

Kirillov D., Kovtsur M., Mikhailova A., Potemkin P. Investigation of Wireless Network Traffic Analysis Approaches Using the Pandas Library. – PP. 453–456.
This article will present an approach to analyzing wireless network traffic, implemented using the tools of the Python programming language, in particular the Pandas library. The main goal of the work is to optimize the traffic analysis of the IEEE 802.11 family networks. To ensure the availability of wireless networks, constant monitoring of the network is necessary to identify threats, therefore the relevance of this work is to increase the performance of tracking abnormal activities when analyzing traffic dumps.
Key words: Python modules, namely NumPY, Pandas, StatsModels, MatPlotLib, math, and Sciypy.

Kirilova K., Krasov A., Tsvetkov A. Development of a Method for Detecting Kernel-Level Rootkits in Running Linux Systems. – PP. 457–460.
With information technologies evolving and spreading all over the world, cyber threats are widely spreading as well. Users and administrators of computers systems often face different malware, such as viruses, trojans, rootkits, etc. UNIX kernel-mode rootkits have much more privilege than user-mode ones, therefore they can use their own effective methods to hide in the system.
Key words: linux, kernel modules, malware analysis, rootkits.

Kirichek R., Kruglova A. Development of the Hotel Industry by Implementing Information Technologies. – PP. 461–465.
The article deals with the introduction of the intellectual solutions in hotel rooms and hotels. Automated rooms will provide visitors with a more comfortable stay. The article also examines data transfer technologies in "smart buildings" system. Presented information technologies can be introduced in equipping of hotel rooms.
Key words: hotel, hotel industry, smart solutions, internet of things.

Kirichek R., Kuznetsova E. Hardware and Software Complex for Testing a Network Fragment that Using Augmented Reality Applications. – PP. 465–470.
Augmented reality every year becomes more popular and in demand in various fields, from entertainment to the medical field. Services using augmented reality are more demanding on the network parameters, which raises the question of the quality of the communication network. To provide a high-quality augmented reality service, it is required to test the network for compliance of the network parameters with the requirements under which the network will work stably and satisfy the user. The article discusses existing hardware and software systems for network testing.
Key words: testing network, SLA, QoS, augmented reality.

Kirichek R., Rozhkov M. 5th Generation O-RAN Architecture Overview. – PP. 471–474.
The development of fifth generation (5G) mobile networks has led to the emergence of requirements from operators, which are the main consumers of 5G network equipment, regarding interoperability and interoperability between solutions from different developers.

The article discusses the principles and problems of standardization of elements and interfaces of fifth-generation networks; as a solution, it is proposed to use the O-RAN architecture when building networks of current and future generations.
Key words: fifth generation networks, radio access, wireless networks, virtualization, standard.

Kirichek R., Filin E. Analysis of Long-Range Narrow-Band Wireless Communication Network Technologies: LoRaWAN, NB-Fi and OpenUNB. – PP. 475–479.
With the growing use and increasing importance of Internet of Things projects based on the use of Long-power Wide-area Network (LPWAN), the importance of ensuring the information security of the technologies used, namely, such key principles as confidentiality, integrity and availability of information transmitted between devices, increases. In this paper, we will review and compare LPWAN technologies operating in the unlicensed frequency range, as well as analyze the features in the context of ensuring the protection of information transmitted over wireless communication channels.
Key words: Internet of Things, Long-power Wide-area Network.

Kislyakov S., Mordvinov E. Analysis of Machine Learning Methods for Forecasting Computing Resources Utilization of Container Applications in a Cluster. – PP. 480–484.
When deploying applications using containerization technologies in a cluster, there is a need for further continuous monitoring of utilized resources. The article proposes to use machine learning methods to analyze and forecast CPU/RAM resources utilization. The article discusses the creation of a test environment with an application, the use of a monitoring system and third-party modules to collect the necessary data from the system. As a result of the study, the application of the selected forecasting methods is assessed and the most suitable for solving the problem are selected.
Key words: machine learning, monitoring, DevOps.

Kistruga A., Kovcur M., Oganesyan A. Investigation of the Stability of Access Points in PSK Mode to DoS Attacks on a Wireless Network. – PP. 485–489.
Wireless access point is the one of the basic elements underlying the IEEE 802.11 network. Attacks targeted to access points can be divided into three groups, in accordance with the principles of information security principles: attacks on violation of confidentiality, integrity and availability. The purpose of attacks to availability is to block user access to the network services. Availability attacks are often represented by various DoS attacks. The article is devoted to the study of mechanisms of attacks on wireless access points operating in PSK mode.
Key words: access point, PSK, DoS, Wi-Fi.

Kovalev I., Kosov N. Adverse Attacks in Neural Networks. – PP. 490–492.
The article reviews the well-known methods of adversarial attacks on machine learning models, in particular, on neural networks, their possible implementation options, methods of protection against such attacks, and provides examples of existing practices of these methods. The possibility of their application is evaluated. The definition and practical evaluation of the use of methods of adversarial attacks are given
Key words: adversarial attacks, neural network, model, machine learning, white box, black box.

Kovtsur M., Minyaev A., Petrov V., Targonskaya A. How to Organize Distributed Security Software Development. – PP. 493–497.
One of the most important areas in the field of information technology is the development and implementation of software for the needs of various companies. In addition to the issues of development and implementation, there is also the issue of ensuring information security. Various attacks, e-fraud, and data breaches are a pressing issue today, so implementing and maintaining security-aware software becomes an important task. A well-defined concept for developing secure software reduces possible risks to the project. The article considers the popular practice of DevOps, which received its turn of development. DevSecOps is a development of the concept of DevOps, where in addition to the development processes and Operation, the aspects of information security are affected.
Key words: DevSecOps, software lifecycle, software development methodology.

Kozhanov J. Asymmetric Encryption for Commercial Use. – PP. 498–502.
A method of symmetric encryption with private keys for commercial use is considered. The storage of users' private keys is carried out in the key server. The Erlang formula is used to encrypt plaintext.
Key words: encryption, decryption, Erlang formula.

Kolmykov D., Lipatnikov V. Model of DDoS / DoS Attacks on Information and Computer Networks. – PP. 503–508.
The analysis of methods for protecting information networks from the most relevant types of attacks based on traffic reflection and amplification is presented. The advantages and disadvantages are revealed. A model for the protection of information networks against DDoS attacks with prediction is proposed.
Key words: DDoS attack, statistical analysis, traffic analysis, distributed networks.

Kolomeets M. Analysis of Statistical Features of Social Media Profiles for Bot Detection. – PP. 509–512.
The paper discusses statistical features collected from social network profiles, as well as their usefulness in the bot detection problem. To do this, we generate two groups of accounts based on the accounts of bots and users – groups that containing bots, and groups without bots. We propose statistical features and an analysis of their correlation with each other and with the bot tag.
Key words: bot detection, social media analysis, information security, machine learning.

Komarkov V., Okuneva D. Automated Testing of Information Bases 1C:Enterprise 8 Systems. – PP. 512–516.
At the moment, the 1C:Enterprise 8 system is one of the most popular and convenient tools for creating business applications. The 1C:Enterprise 8 platform allows you to create flexible and quickly customizable applications, is cross-platform, has the means to support large corporate systems, and runs on mobile devices. Development volumes are quite large, and you have to spend a lot of time to test the developed solutions. But there is a solution – this is automated testing. The article discusses the mechanism of automated testing of the 1C:Enterprise 8.3

platform, the goals of its creation, the ways of writing an automated test, and describes the possibility of writing complex testing within one or more information databases.
Key words: automated testing, 1C:Enterprise 8.

Korzhik V., Yakovlev V. Probabilities of Errors in the Distribution of Keys Over Noiseless Communication Channels Using the Addition of Artificial Noise. – PP. 516–522.
The protocol of key distribution over public noiseless channels (of the Internet type) is investigated. In the previously investigated protocols, legal users to obtain raw key bits exchanged noisy matrices consisting of Gaussian random numbers and, based on modeling, estimates of the probabilities of coincidence of the raw key bits between users and the eavesdropper were obtained. In the proposed simple protocol, correspondents exchange random Gaussian numbers. Analytical relations are obtained for calculating the probability of key bit mismatch for legal users and the probability of key bit mismatch between a legal user and an eavesdropper, which are confirmed by experimental studies.
Key words: cryptography, key distribution

Kosov N., Pavlotsky I. Analysis of Password Storage Systems Vulnerability in Web Browsers. – PP. 522–526.
In the modern world, in which the Internet has become inseparable from human life, it is impossible to imagine an ordinary user who doesn't use a web browser to access the World Wide Web. Browsers have undergone massive changes in recent years, and now they are not just tools to access websites. Today, the browser offers the user many additional functions, including a built-in password manager that allows you to save passwords and other credentials for various services in a database. This database is synchronized between different devices, such as a PC and smartphone. At the same time, this solution poses a security risk as it creates the possibility of stealing user credentials. This article discusses what vulnerabilities may contain password storage systems in the most popular browsers, how attackers can exploit them, and possible solutions to the identified problem.
Key words: information security, web browser, password manager, DPAPI, vulnerability.

Kosov N., Timofeev R. Comparison of Conventional Neural Network Training Methods. – PP. 526–530.
This article describes the differences in training methods for a convolutional neural network that allows you to classify images. As a development tool, the Python programming language and the Keras library, which is the API of the TensorFlow framework, were used. In order to show the result closest to reality, the supervised learning method and the unsupervised learning method were chosen.
Key words: neural network, convolutional neural network, neuron, convolutional layer.

Kotenko I., Puchkov V. Analysis of Methods for Assessing the Security of Cyber-Physical Systems. – PP. 531–536.
The paper analyzes the currently used methods for assessing the security of cyber-physical systems. The advantages and disadvantages of existing methods are considered. The main attention is paid to the methods of assessing the security of cyber-physical systems based on the analysis of attack graphs.
Key words: cyberphysical systems, security analysis techniques, attack graphs.

Kotenko I., Khmyrov S. Analysis of Current Methods of Attributing Cyber Security Offensers in the Implementation of Targeted Attacks on Objects of Critical Infrastructure. – PP. 536–541.
Targeted attacks on critical infrastructure not only cause serious damage to the economic and national security of the country, but in most cases do not allow the identification of a cybersecurity intruder. A variety of high-tech tools and anti-forensic techniques allows you to go unpunished and takes cyber terrorism and cyber-attacks to a new level, which are often supported by external government organizations. Attribution of cybersecurity violators is one of the urgent tasks in the field of ensuring the protection of critical infrastructure facilities. This study examines the methods of attribution of cybersecurity violators, highlighting their disadvantages and advantages.
Key words: targeted attacks, critical infrastructure, cyber intruder attribution, cyber security.

Krasov A., Krylov A. Analysis of Vulnerabilities in IoT Protocols of Smart Cities. – PP. 541–545.
The Internet of Things (IoT) is an emerging technology focused on connecting devices with each other, with the Internet and users. IoT technology is expected to become a necessary requirement in the development of smart cities, as it offers convenience and efficiency to city dwellers so that they can achieve a better quality of life. The application of the IoT model in smart cities poses many new security challenges in terms of confidentiality, authenticity and data integrity. These challenges make smart cities extremely vulnerable to various types of online threats. Therefore, it is necessary to identify possible security risks in order to obtain a complete assessment of the security status. This article applies the Critical Threat, Asset and Vulnerability Assessment (OCTAVE Allegro) methodology to assess the security risks of smart cities. The OCTAVE Allegro method focuses on information assets and looks at various information containers such as databases, physical documents, and people. The key objectives of this study are to highlight various IoT-based vulnerabilities in order to identify risks and propose approaches to mitigate them.
Key words: smart cities, Internet of Things (IoT), OCTAVE Allegro, security risk assessment.

Kuznetsov V. Verification of Optical Time-Domain Reflectometers. – PP. 545–550.
Reflectometry measurements are the most important part of the work, which is carried out during erecting and operating of the fibre-optical communication lines. Optical time-domain reflectometers have a number of metrological performances, and failure to meet them may significantly impact these lines' quality. This article describes such performance as error of the optical reflectometer when measuring the loss and proposes alternative method of its determination.
Key words: fibre-optical communication line, optical time-domain reflectometer, verification, loss, error.

Kushnir D., Nesterov I., Sukhanov D. Analysis of Remote Code Usage Vulnerabilities in Application Software. – PP. 550–554.
The article analyzes the interrelated vulnerabilities of remote code use. The problems of information security are presented. The results of experiments aimed at identifying the same type of vulnerabilities under different configurations and characteristics of the same installed application software are presented.
Key words: computer vulnerabilities, software, unauthorized access, remote code use, security

Kushnir D., Churikov A. Methods for Organizing Secure Communication Channels and Possible Functions of Intermediate Nodes in Quantum Networks. – PP. 555–560.
The article discusses possible approaches to the organization of secure communication channels between subscribers of quantum networks. Significant advances in the field of quantum information allow you to come close to the issue of building fully or partially quantum networks. The paper analyzes possible methods for constructing quantum networks and the problem of their scaling.
Key words: quantum cryptography, quantum repeaters, quantum key distribution protocols, quantum networks, trusted nodes.

Kushnir D., Shemyakin S. Features of the Formation of Key Data in a Quantum Cryptographic Network. – PP. 560–564.
The article discusses a number of aspects influencing the formation of key data in the formation of a quantum cryptographic network. The authors analyze the methods of generating keys between the end nodes, the technical difficulties of the direct formation of key data and approaches to solving the indicated problems.
Key words: quantum cryptography, quantum repeaters, quantum key distribution protocols, quantum networks.

Lebedyantsev V., Pavlov I. Nonlinear Invariant Echo Canceller for Duplex Data Transmission System. – PP. 565–570.
The article discusses the use of a new mathematical apparatus for the communication theory for the synthesis of duplex data transmission systems - the theory of transformation groups, which opens up the possibility of developing echo cancellers with properties invariant with respect to the characteristics of echo paths. A block diagram of a nonlinear invariant echo canceller for a duplex data transmission system is presented.
Key words: invariant echo canceller, echo signal, echo path, projective transformation, vector lengths, noise immunity, relative error.

Levshun D. Architecture of the Youth Survey System in VKontakte Social Network for Identifying Negative Personal Trends. – PP. 570–572.
The youth survey system in VKontakte social network is an application developed using the VK mini app technology. The process of user interaction with the application can be divided into three stages: (1) passing the questionnaire (name, surname, gender, age, university, faculty and group); (2) passing psychological tests (Ego-structure Ammon's Test, State-Trait Anxiety Inventory, Ways of Coping Questionnaire, Rotter's Subjective Control Questionnaire and Well-Being Activity Mood Questionnaire); (3) collection of data about the user's page through the API of the social network. The task of the questionnaire is to connect personalities of users with information from their pages in the social network, since the latter are characterized by filling in with fictitious data. The task of psychological tests is to form an idea of the psycho-emotional state of users, to identify negative personal tendencies. The task of the data collection process is to form an idea of the content of pages of the users for further analysis of their correlation with the results of psychological tests.
Key words: social networks, analysis of psycho-emotional state, identification of negative personality tendencies, questionnaires, collection and analysis of data.

Lepekhin N., Manichev S. Heterochronicity of Agile Team Development in the Process of Project Tasks Implementation. – PP. 573–577.
The organization of the work of agile project teams should take into account not only the formal frameworks of agile methodologies, but also the stages of development of teams, the heterochronicity of the development of areas of team activity, the development of a team mental model and leadership style. A study of the project work of 20 agile IT teams - specialists confirmed that the formal frameworks (ways of working) set by the organization should be filled with qualitatively different psychological interventions depending on the stage of the team's development, the level of development of the general mental model, leadership style and proactivity of team members..
Key words: agile teams, stages of development, heterochronicity, leadership style, proactivity.

Lepeshkin O., Permyakov A., Shuravin A. User Information Profile. – PP. 578–582.
The article hypothesizes that all electronic devices surrounding the user, as well as their totality and nature of use, create a unique information portrait (digital fingerprint). For companies, it is more valuable than a person's personal data, because it allows you to get information about many aspects of their life and use it to promote products and services. At the same time, the use of this information is not regulated in any way. The article considers the process of forming an information portrait of a user, its composition, as well as a formalized representation.
Key words: personal data, identification, digital fingerprint.

Lobastova M., Lytkina E., Ponamarenko K., Sharipova I. The Main Aspects of the Network Reliability Evaluation for Synchronization Clock Network. – PP. 582–587.
Currently, there is a rapid development of communication networks. This leads not only to the emergence of new communication services, but also to stricter requirements for the construction of communication networks, as well as their reliability. Not a single, even the most modern communication service can be provided if it is not supported by the transport infrastructure, one of the components of which is the synchronization network. That is why the issue of reliability of the clock synchronization network should be given great attention.
Key words: network clock synchronization, network reliability, network element reliability, generator equipment, synchronization network operation modes, matrix theory, graph theory, Markov circuits.

Matveeva E., Somov K. Infocommunication System for the Functioning of a Warehouse Loading Point. – PP. 587–592.
Currently, practically all organizations use modern achievements of infocommunications. With regard to the digitalization of business processes, it does not mean the creation of automated systems, but the creation of infocommunication systems that use all means of communication available in the organization. The construction of such systems is difficult, expensive work, during which the specialist needs to take into account a large number of nuances and factors.
Key words: infocommunication system, hardware-program complex, business process, loading point, automation.

Melnikov V., Okuneva D. Modern Technologies to Improve Customer Service of Hosting Providers. – PP. 593–596.
In terms of client service, response time is one of the most important metrics. Hence, implementation of modern artificial intelligence technologies has been proposed in order to improve the quality of service and significantly reduce the response time. A number of typical issues that are advisable to automate have been outlined in this article.
Key words: hosting, support, customer service, artificial intelligence.

Minyaev A. Information Security System Development of Geographically Distributed Information Systems. – PP. 597–600.
Creation of an integrated system for protecting information of complex, difficult to formalize and poorly structured processing. This is due to the fact that to solve this kind of problem, it is necessary to use a systematic approach, which allows initiating many processes in the information security system. This article proposes a method for developing a protection system for geographically distributed information based on cognitive modeling. The method also allows us to study the problem of developing an information security system, distributed information systems, information systems security systems (its IT infrastructure).
Key words: development of information security systems, geographically distributed ISs, cognitive modeling.

Muthanna A., Tagandurdyyev N. Analysis of Methods and Problems of Using UAVs in a Smart City. – PP. 601–605.
Before the development of 5G technologies, it was almost impossible to create a network that would support the idea of mass machine-to-machine communication with low latency at ultra-high speeds. The implementation of these services with 5G technologies has opened an opportunity for the development of smart city ideas. A smart city, thanks to 5G technology and the use of drones as telecommunication nodes, can help solve the problems of monitoring the city's environment, traffic, etc. This will make the city as safe and convenient as possible in the management and control of the urban environment.
This article analyzes the organization of unmanned aerial vehicles together with MEC and SDN technologies to implement the concept of a smart city. This article illustrates the functional features of the architecture of the urban network of the future. The features of the interaction of urban communication centers with the network infrastructure are also shown.
Key words: 5G, IoT, Smart City, UAV.

Ovchinnikov M. Analysis of Supply Problems Information Security in High-Frequency Communication in Power Supply Networks. – PP. 605–612.
Features of power supply networks allow using high-frequency communications to transmit information over long distances directly to recipients. However, the physical insecurity of communication channels and the obsolescence of high-frequency communication technology reduce the security of the transmitted security of the transmitted information.
Key words: information security, high-frequency communications, power supply networks.

Okuneva D., Polyanskaya A. Error Handling Mechanisms on the 1C:Enterprise 8 Platform. – PP. 613–616.

The article describes the features of the 1C:Enterprise 8 platform for the search, processing and analysis of errors.

While working with the 1C:Enterprise 8 system users often encounter errors, do not understand the reasons for their occurrence and how to solve them, contact technical support specialists and wait for the error to be resolved. This process takes a lot of time for both technical support specialists and users themselves.

Analysis of existing error handling mechanisms will increase the speed and quality of the process of troubleshooting, significantly reducing the user's waiting time, and will reduce the downtime in the company's work schedule.

Key words: 1C:Enterprises, error search, error handling, error analysis, target group, error categories, error handler, error report.

Parashchuk I., Fedorchenko E. Analysis of Effectiveness of the Information Security Management System of the Industrial Internet of Things Using Methods of Fuzzy Sets Theory. – PP. 617–621.

The article presents a generalized review of methods of fuzzy sets theory considering their possible application for solving particular problems of analyzing the effectiveness of the information security management system of the industrial Internet of things. The application of fuzzy methods that reduce the level of uncertainty in the formulation of target integral metrics that should answer the questions of security assessment and in the selection of protective measures to counter threats is considered. Recommendations for the practical application of the considered methods are given.

Key words: industrial Internet of things, fuzzy sets, security, model, efficiency, information security, management system, metric.

Petriv R., Starodubova D., Starodubov R. Attacks on Wireless Networks and Their Detection. – PP. 621–624.

Today, the security issues of wireless networks are relevant due to their ubiquity. The security of wireless systems is to prevent unauthorized access or damage to computers by intruders. The risks associated with the use of WLAN networks range from listening to targeted internal attacks, as well as attacks aimed at external sites.

Key words: information security, wireless networks, Wi-Fi networks.

Pomogalova A. Development of a Distributed System for the Storage, Indexing and Issuance of Digital Documents. – PP. 624–628.

The work is devoted to the creation of a distributed system for the storage, recording and issuance of digital documents, which include the whole range of documents, including higher education documents, certificates, professional re-qualification documents and similar. This topic is extremely important, as it allows to digitize the large segment of document circulation. The work discusses the architectural features of the solution, the problem of the chosen domain, as well as the stack of technologies used for its successful implementation. The system being developed makes it possible to store documents, confirm their relevance and record any changes, as well as to reissue the document in case of loss in the shortest possible time. It is also necessary to mention the possibility of forming the necessary design of the document, which makes the system universal.

Key words: blockchain, Ethereum, smart contract, decentralized app, DApp, distributed system, distributed storage, digital documents.

Pomogalova A., Tarabanov I., Tirbach L., Fedoseev I. Copyright Protection System Based on Ethereum Platform Using IPFS Technology. – PP. 629–633.
The work is devoted to the creation of a copyright protection system based on Ethereum platform using IPFS technology. The system allows uploading and download works stored in the system, as well as to authenticate. The system also allows to check the authenticity of the work based on the hash function check of the source document.
Key words: cloud technology, Ethereum, IPFS, Metamask, Ropsten, blockchain, smart contract, hash function, framework, react.js, web3.js, Ganache CLI, Infura.

Reznikov B., Sivukhin A. Application of MIMO Technologies in Optical Communication. – PP. 633–637.
This article presents a novel beam-domain multiple-input multiple-output (MIMO) communication system for optical wireless communications. An optical base station equipped with massive optical transmitters communicates with a number of user terminals through a transmitting lens. Focusing on LED transmitters, we analyze the refraction of light by lenses and establish a channel model for optical massive MIMO transmissions.
Key words: MIMO, optical communications, BDMA.

Rogov S., Saltykov A. Quantum Technologies in Infocommunications. – PP. 638–642.
In recent years, considerable attention has been paid to the research and implementation of quantum technologies in the field of information processing and transmission. The huge computational potential of quantum computers makes it possible in the future to solve quite quickly problems that were considered difficult to solve with the help of conventional computing tools. This applies, in particular, to the task of deciphering reliable secret codes used in the transmission of classified information. On the other hand, on the basis of quantum methods, a new method of transmitting secret codes was developed, which is fundamentally protected from hacking by the laws of quantum mechanics.
Key words: quantum computer, quantum computing, quantum cryptography.

Saenko I., Khinenzon A. Analysis of Social Media Metadata to Detect Abnormal Behavior. – PP. 642–647.
Social networks can be represented as an information model, with some attributes and relationships. Such models allow us to identify a number of features that are applicable for detecting abnormal user behavior in a social network. In the article, abnormal user behavior is understood as a deviation from the statistical norm.
Key words: social networks, abnormal user behavior in a social network, information security, detection of anomalies.

Seryozhin E., Yakovlev V. Development of a Modified Protocol for Secure Determination of Users Points of Interest for Highly-Loaded Networks. – PP. 647–652.
Modifications of the protocol for the secure determination of the location of points of interest (POI) of users, based on the homomorphic cryptosystems of Paillier and Rabin, adapted to

work in highly loaded networks, have been developed. The proposed modifications reduce the load on the server and reduce the response time to the user. The modifications are based on three options for segmenting the terrain map and applying a two-step request, which allows the server to process dozens of times more requests. In connection with the development and active use of unmanned aerial vehicles, a modification of the protocol using a three-dimensional map is considered. The quantitative characteristics of the effectiveness of the protocol with these modifications are given
Key words: anonymous calculation, points of interest, geomaps, homomorphic encryption.

Sinelshchikov S., Tsvetkov A. Personal Data Protection in the Enterprise. – PP. 653–657.
Confidentiality is the main problem in the modern information society. To protect the privacy of individuals, businesses must follow certain privacy rules when collecting and processing personal data. In this paper, we consider the two most common approaches to personal data within the enterprise – E-P3P and audit.
Key words: personal data protection, E-P3P, personal data audit, information security.

Skorykh M. Using of the Zeek Framework and ELK-Stack for Malware Distribution Analysis. – PP. 658–661.
There are many types of computer attacks today. One of the types of computer attacks is the distribution of malicious software via e-mail. Comprehensive analysis of such mailings is not a trivial task for information security specialists. This article discusses an approach to analyzing malicious software mailings using the Zeek network traffic analysis framework and ELK-stack.
Key words: computer attack detection, malware, Zeek, ELK-stack.

Starodubova D., Starodubov R., Ushakov I. Network Traffic Anomaly Detection Model. – PP. 661–665.
Network anomaly detection is an important and rapidly developing area of research. Currently, despite the intensive development in the field of network technologies, attackers are constantly increasing the number of attacks on the network infrastructure. Network anomaly detection systems play an important role in ensuring network security. Due to the dynamic changes of malicious software in network traffic data, traditional tools and methods are unable to protect networks from penetration attacks. The paper proposes a model for detecting anomalies. The structure and algorithms of the functioning of the anomaly detection system are described.
Key words: network anomalies, network traffic, anomaly detection, network traffic analysis, neural networks.

Suyundukova A., Fitsov V. Corporate Network Control System. – PP. 665–670.
By virtue, a connection control system is described that makes decisions based on data from OSS / BSS systems. It is assumed that network connections are made by objects that are the source of the flow of information. The device is an IoT device or user. In addition to other tasks, the OSS / BSS system determines the list of allowed and forbidden object interactions. More efficient operation of the connection control system is achieved using OSS / BSS, SDN and DPI technologies. The SDN network controller is used to manage network connections, after making decisions about their admissibility by the control system. DPI traffic inspection is used to convey content used for application use. The connection control system determines the admissibility of network interactions of objects with each other. To simplify the work on the

implementation of the control system, an algorithm for the operation of the connection control system using the above technologies has been developed and presented.
Key words: connection control system, OSS / BSS technology, DPI technology, software-defined network, business processes, information security, work algorithm.

Tarabanov I., Shvidkiy A. Evaluating Approaches to Analyzing Diagnostic Information of Hyperconverged Infrastructure Nodes. – PP. 670–674.
The article presents the main ways of collecting and analyzing diagnostic information and compares several implementations for solving such problems. Based on the results of the analysis, the most appropriate solutions for this type of tasks, in a hyperconverged infrastructure was selected.
Key words: cloud technology, hyperconverged infrastructure, diagnostic information.

Fedorova O., Tsvetkov A. Linux Kernel Modules. – PP. 675–679.
All (or almost all) processors that Unix-like OS manufacturers have ever been interested in have hardware support for privilege separation. We are talking about "kernel mode" (kernel land) and "user mode" (user land). Different OS kernel architectures differ primarily in the approach to which parts of the OS code should be executed in kernel land, and which parts should be executed in user land? This question is important because the vast majority of processors switch between the two modes takes a significant amount of time. Kernel modules have direct access to memory and kernel functions. For user-space programs, this access is limited to the compiler's library interfaces. A module is essentially the same as a regular program. The module also has an entry and exit point and is located in its binary file. Let's look at the features of using a particular type of kernel and describe the vulnerabilities associated with the modular kernel.
Key words: modular kernel, monolithic kernel, Linux operating system, vulnerability, RootKit.

Fitsov V. Modification of the Hooke-Jeeves Method for Searching by Decreasing Function Under Prescribed Constraints. – PP. 679–684.
This article describes the finding algorithm of function values that meet the specified criteria using the modified Hooke-Jeeves method. When calculating deep packet inspection systems, there is a decreasing function of the processing time of traffic flows from the number of hardware resources of the system. At the same time, there are certain limitations associated with the maximum allowable analysis time and the cost of equipment. For such a function, the classical Hooke-Jeeves method requires a large number of search steps. Therefore, its modification was required to work with a decreasing function. An attempt is made in the work to reduce the number of search steps to find the desired value, and to increase the accuracy of the obtained values. As a result, the conditions were determined under which it is advisable to use the modified Hooke-Jeeves method.
Key words: programmatic search, maximum element method, Hooke-Jeeves method, deep packet inspection (DPI).

Tsvetkov A., Ellaui I. Finding Security Vulnerabilities in Software. – PP. 684–688.
This paper describes methods for detecting software vulnerabilities and consider modern approaches to software analysis. The purpose of this article is improving the security of applications by searching for vulnerabilities in them.

Key words: vulnerabilities, static analysis, dynamic analysis.

Shypota N. Analysis of Features of Holographic Network Applications. – PP. 688–692.
The relevance of the research topic is due to the need for a theoretical study of holographic communications. At present, projects are being actively implemented that use holographic bell technologies, visualization of holograms, the observed trend towards an increase in holographic content actualizes the problem under study. The article discusses the prospects for the development of holographic communication. The main problem points in the development of network applications are outlined. The features of holographic network applications are analyzed. A plan for researching the traffic of holographic copies is presented. Approaches to the development of a traffic model for holographic applications are outlined.
Key words: network applications, network traffic models, holographic communication, holographic call, holographic network applications.

Yakovlev V. Authentication Method Diffie-Hellman Values Based on Pre-Distributed Binary Sequences and Strictly Universal Hash Functions. – PP. 693–698.
A method is proposed for authenticating Diffie-Hellman values between two correspondents using pre-distributed random authentication sequences and the Wegman-Carter authentication algorithm. Relationships are obtained for estimating the probability of a false alarm (due to a mismatch between pre-distributed chains) and the probability of undetected deception a DH-value.
Key words: authentication, distribution of keys, Diffie-Hellman method, man-in-the-middle attack, universal hash functions.

Yakovlev V. Optimization of the Parameters of the Authentication Method Diffie-Hellman Values Based on Preliminary Distributed Binary Sequences and Strictly Universal Hash Functions. – PP. 698–703.
A technique for optimizing the parameters of the authentication method for Diffie-Hellman values based on binary sequences (authentication sequences) pre-distributed between users is proposed. Authentication is performed by dividing the Diffie-Hellman value into N blocks and generating an authenticator of length v bits for each block using strictly universal hash functions, the keys for which are blocks of authentication sequences. The technique includes the following stages: estimating the probability of a false key rejection and determining the acceptable decision thresholds for different lengths of authenticated blocks; calculating the the probability of undetected deception a DH-value for the selected block lengths and selecting only those block lengths that meet the requirements for the probability of undetected deception and the probability of a false rejection of the DH-value and minimize the total length of authenticators. An example of application of the technique for authentication of a 256-bit Diffie-Hellman value is given.
Key words: authentication, distribution of keys, Diffie-Hellman method, universal hash functions.

АВТОРЫ СТАТЕЙ

АББАСОВ Эльсевер Азер оглы — диссертант кафедры телекоммуникации и информационные безопасности Азербайджанского технического университета, elsever.abbasov95@gmail.com

АБДЕЛЛАХ Али Рефаии — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alirefaee@azhar.edu.eg

АБРАМЕНКО Георгий Тимофеевич — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, georgabramenko2010@mail.com

АБРАМОВ Сергей Степанович — доктор технических наук, доцент, заведующий кафедрой радиотехнических устройств Сибирского государственного университета телекоммуникации и информатики, академик МАС, abramov@sibsutis.ru

АБРАМОВА Евгения Сергеевна — кандидат технических наук, доцент, доцент кафедры радиотехнических устройств Сибирского государственного университета телекоммуникации и информатики, evgenka_252@mail.ru

АЛЕННИКОВ Евгений Михайлович — студент группы ИКТм-91 Поволжского государственного университета телекоммуникаций и информатики, ealennikov@yandex.ru

АЛИЕВА Алмаз Али кызы — кандидат технических наук, доцент кафедры информационных технологии Мингечаурского государственного университета, almaz40@gmail.com

АНДРЕЕВА Елена Ивановна — кандидат физико-математических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreeva.elena@sut.ru

АНТОНЕНКО Анастасия Дмитриевна — студентка группы ИКТИ-05м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glutton02@gmail.com

АХМЕТШИНА Милена Энверовна — студентка группы ИКТБ-07М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ahmet-mil@yandex.ru

АХРАМЕЕВА Ксения Андреевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cbor.mail@gmail.com

БАБКОВ Иван Николаевич — кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ib9809@mail.ru

БАКАТОВ Виталий Николаевич — студент группы ИСТ-851 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bakatovvitalij@gmail.com

БАЛИНА Анастасия Вадимовна — студентка группы ИКТО-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasiyabalina0660@gmail.com

БАТЕНКОВ Кирилл Александрович — доктор технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

БЕЛОВ Александр Владимирович — кандидат технических наук, старший преподаватель кафедры общепрофессиональных дисциплин Военной академии связи им. Маршала Советского Союза С. М. Буденного, belov-a.v@mail.ru

БЕРЕЗИНА Елизавета Олеговна — студентка группы ИКТБ-97М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, berezinaelizaveta@icloud.com

БОГДАНОВА Любовь Николаевна — студентка группы ИКТБ-97М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, lyubogdanova1996@yandex.ru

БОРИСЕНКО Николай Павлович — кандидат технических наук, доцент, начальник Центра системного анализа АО «РЦЗИ «ФОРТ», npbor@yandex.ru

БОРОДИН Алексей Сергеевич — кандидат технических наук, кандидат политических наук, представитель РФ в Международном союзе электросвязи, ПАО «Ростелеком», alexey.borodin@rt.ru

БРАНИЦКИЙ Александр Александрович — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук; доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, branitskiy@comsec.spb.ru

БУЗЮКОВ Лев Борисович — кандидат технических наук, заместитель заведующего базовой кафедрой конфигурируемых бизнес приложений, профессор кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникация им. проф. М. А. Бонч-Бруевича, levbuz@mail.ru

БУКШИН Иван Дмитриевич — магистрант группы ИКТЗ-91м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, trace.bn@yandex.ru

БУРДИН Антон Владимирович — доктор технических наук, профессор кафедры линии связи и измерения в технике связи Поволжского государственного университета телекоммуникаций и информатики, заместитель генерального директора по научной работе и развитию АО "Научно-производственное объединение Государственный оптический институт им. С. И. Вавилова", bourdine@yandex.ru

БУРДИН Владимир Александрович — доктор технических наук, профессор, заведующий кафедрой линии связи и измерения в технике связи Поволжского государственного университета телекоммуникаций и информатики, burdin@psati.ru

БУРМИСТРОВ Максим Дмитриевич — студент кафедры защищенных систем связи Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, burmistrovm@live.ru

БУСАРОВ Юрий Олегович — студент группы ИСТ-813 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, busarov.yo@spbgut.ru

БУХАРИН Владимир Владимирович — доктор технических наук, доцент, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bobah_buch@mail.ru

БЫЛИНА Мария Сергеевна — кандидат технических наук, доцент, заведующая кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, BylinaMaria@mail.ru

БЫСТРОВ Илья Сергеевич — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, ilya.bystrov@outlook.com

ВАСИН Николай Николаевич — доктор технических наук, профессор, заведующий кафедрой сетей связи Поволжского государственного университета телекоммуникаций и информатики, академик АТИ, vasin-nn@psuti.ru

ВЕРШЕННИК Елена Валерьевна — кандидат технических наук, старший преподаватель кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, Yelena.Vershennik@mail.ru

ВЕРШИНИНА Ксения Витальевна — студентка группы ИКТФ-06м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, xenia.vershinina@mail.ru

ВИКУЛОВА Александра Юрьевна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bp@sut.ru

ВИТКОВА Лидия Андреевна — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, vitkova@comsec.spb.ru

ВЛАДИМИРОВ Сергей Сергеевич — кандидат технических наук, доцент, доцент кафедры сетей связи и передача данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВОЛКОВ Артем Николаевич — аспирант кафедры сетей связи и передача данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artemanv.work@gmail.com

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

ВОЛОСТНЫХ Виктор Анатольевич — кандидат военных наук, доцент, научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, ra1alo@mail.ru

ВОРОНИНА Кристина Сергеевна — студентка (магистрант) группы ИКМ-03з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kristina2897@gmail.com

ВОРОНОВ Андрей Олегович — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andre.voronov2011@yandex.ru

ВОРОШНИН Григорий Евгеньевич — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, voroshnin.g@yandex.ru

ГАВРИЛЕНКО Егор Владимирович — студент группы ПБ-81з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k1llo2810@gmail.com

ГАЙФУЛИНА Диана Альбертовна — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, gaifulina@comsec.sbp.ru

ГАПОНЕНКО Владислав Александрович — студент группы ИБС-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gapon70@gmail.com

ГЕЛЬФАНД Артем Максимович — старший преподаватель кафедры защищенные системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, amgelfand@mail.ru

ГЕРАСЬКИН Валерий Кириллович — студент группы ИКВТ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, geraskin.valery@gmail.com

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

ГЕТЬМАН Евгения Михайловна — студентка группы ИКБ-73, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, janget@ya.ru

ГЛАГОЛЕВ Сергей Федорович — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glagolevsf@yandex.ru

ГОГОЛЬ Александр Александрович — доктор технических наук, профессор, заведующий кафедрой телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Al.Gogol@mail.ru

ГОЛОВАНОВ Эрик Сергеевич — студент группы ИКТК-76 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, golovanoveric@hotmail.com

ГОЛОВКОВА Елизавета Евгеньевна — студентка группы ИКТС-72 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lizaveta.golovkova0113@gmail.com

ГОЛОЛОБОВ Никита Вячеславович — студент группы ИКБ-72 Санкт-Петербургского государственного университета телекоммуникаций им. проф. Бонч-Бруевича, neptu133@gmail.com

ГОЛУБОВ Никита Александрович — студент группы ИКБ-74-1 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, amittone@mail.ru

ГОЛУЗИНА Дарья Романовна — студентка группы ИКТБ-08м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, goluzinadasha@gmail.com

ГОРЛИНА Анастасия Витальевна — студентка группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Gorlina.a.v@mail.ru

ГОРСКОВ Вячеслав Сергеевич — магистрант группы ИКМ-92з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gorskov.miroslav@yandex.ru

ГОФМАН Максим Викторович — кандидат технических наук, доцент, доцент кафедры «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения Императора Александра I, maxgof@gmail.com

ГРЕБЕНЩИКОВА Александра Андреевна — аспирант и ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sgreben1@mail.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 Артем Андреевич — студент группы ИКТЗ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gromartem2000@gmail.com

ГУЛЕВИЧ Владислав Денисович — бакалавр кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sterbent.fox@gmail.com

ГУРБАТОВ Глеб Олегович — студент группы ИКТБ-07м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, 12345678987654321geb@mail.com

ГУСЕЙНОВ Наил Шаигович — студент группы ИКПИ-73 Санкт-Петербургского государственного университета телекоммуникация им. проф. М. А. Бонч-Бруевича, doom2.hulk2@mail.ru

ДАВЫДОВ Вадим Владимирович — доктор физико-математических наук, профессор кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, davydov_vadim66@mail.ru

ДАШКОВ Михаил Викторович — кандидат технических наук, доцент кафедры линии связи и измерения в технике связи Поволжского государственного университета телекоммуникаций и информатики, mvd.srttc@gmail.com

ДЕДУХОВА Анастасия Андреевна — студентка группы ИКТВ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anabad@list.ru

ДЕСНИЦКИЙ Василий Алексеевич — кандидат технический наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, vasily.desnitsky@mail.ru

ДЖАФАРОВА Эльнаре Миртаги кызы — диссертант кафедры телекоммуникации и информационные безопасности Азербайджанского технического университета, elnara.axadova@mail.ru

ДМИТРИЕВА Диана Сергеевна — студентка группы ИКФ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitrievadiana1405@gmail.com

ДМИТРИЕВА Юлия Сергеевна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitrieva.julia.serg@yandex.ru

ДМИТРИЕВА Виктория Викторовна — ассистент кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitrieva.vv0@gmail.com

ДОКШИН Александр Денисович — студент группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.dokshin007@gmail.com

ДОМБРОВСКИЙ Ярослав Аркадьевич — начальник факультета автоматизированных систем управления Военной академии связи им. Маршала Советского Союза С. М. Буденного, shchuk@rambler.ru

ДОНСКОВ Евгений Андреевич — аспирант Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, radion2002@gmail.com

ДОЦЕНКО Сергей Эдуардович — инженер кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 0472895@gmail.com

ДУНАЙЦЕВ Роман Альбертович — кандидат технических наук, доцент, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.dunaytsev@spbgut.ru

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, доцент кафедры инфокоммуникационных систем, начальник управления организации научной работы и подготовки научных кадров Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v.elagin@spbgut.ru

ЕРЁМЕНКО Владимир Александрович — студент группы ИКФ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, veremenko148@gmail.com

ЕРМОЛАЕВ Егор Евгеньевич — студент группы ИКВТ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egoulya@mail.ru

ЕСАЛОВ Кирилл Эдуардович — ассистент кафедры инфокоммуникационных систем, начальник научно-образовательного центра «Инфокоммуникационных технологий и нейрокогнитивных архитектор» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kesalov@spbgut.ru

ЖЕРНОВА Ксения Николаевна — аспирант, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, zhernova@comsec.spb.ru

ЗАДОРОЖНЯЯ Алина Александровна — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alina27812@mail.ru

ЗАРУБИН Антон Александрович — кандидат технических наук, доцент, заведующий кафедрой инфокоммуникационных систем, проректор по цифровой трансформации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, azarubin@sut.ru

ЗЕЛИЧЕНОК Игорь Юрьевич — студент (магистрант) группы ИКТБ-98м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zelichenok.igor@gmail.com

ИБРАГИМОВ Байрам Ганимат оглы — доктор технических наук, профессор кафедры телекоммуникации и информационных безопасности Азербайджанского технического университета, i.bayram@mail.ru

ИВАНОВ Владимир Степанович — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vsivanovspb@yandex.ru

ИВАНОВ Константин Эдуардович — студент группы ИКТВ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kosta_98@list.ru

ИГНАТОВА Ирина Олеговна — студентка группы ИКТУ-77 Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, ira-ignatova98@mail.ru

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, konstantin.izrailov@mail.ru

ИСМАЙЛОВА Севиндж Рамиз кызы — кандидат технических наук, старший преподаватель кафедры информационных технологии и программирование Азербайджанского технического университета, sevinc_ism@hotmail.com

КАЗАНЦЕВ Алексей Анатольевич — аспирант кафедры защищенные системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, farvest.ax@yandex.ru

КАЗАЧКИН Антон Владимирович — преподаватель кафедры «Защиты информации» Академии Федеральной службы охраны Российской Федерации, zilog.82@ya.ru

КАЛАШНИКОВ Александр Сергеевич — студент группы ИКМ-02з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreeva.elena@sut.ru

КАРЕЛЬСКИЙ Павел Владимирович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pasha.karelscky@yandex.ru

КАТАСОНОВ Александр Игоревич — студент группы ИКТБ-07м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksasha716@yandex.ru

КАТУНИН Роман Эдуардович — студент группы ИКТВ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, romakatunin@rambler.ru

КИЛИЧЕВА Клавдия Хайруллоевна — студентка кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bambosik@yandex.ru

КИРИЛЛОВ Даниил Игоревич — старший преподаватель кафедры защищенные системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, daniil.kirillov@gmail.com

КИРИЛОВА Ксения Сергеевна — студентка группы ИКТЗ-54 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksen_98@mail.ru

КИРИЧЕК Руслан Валентинович — доктор технических наук, доцент, заведующий кафедрой программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirichek@sut.ru

КИСЛЯКОВ Сергей Викторович — кандидат технических наук, доцент кафедры инфокоммуникационных систем, преподаватель базовой кафедры инновационных технологий телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s.v.kislyakov@gmail.com

КИСТРУГА Антон Юрьевич — специалист по проектированию и построению систем обеспечения информационной безопасности в сетях передачи данных, ООО «Фаст Лейн», anton.kistruga@gmail.com

КЛОЧКОВ Марк Леонидович — студент группы ИКПИ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, m.l.klochkov@yandex.ru

КОВАЛЕВ Илья Алексеевич — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cov.cov.cov70@gmail.com

КОВЦУР Максим Михайлович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@mail.ru

КОЖАНОВ Юрий Федорович — кандидат технических наук, доцент кафедры «Инфокоммуникационных систем» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, juriy.kozhanov@mail.ru

КОЛМЫКОВ Дмитрий Витальевич — ефрейтор, старший оператор роты (научной) Военной академии связи им. Маршала Советского Союза С. М. Буденного, dima370656@gmail.com

КОЛОМЕЕЦ Максим Вадимович — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, kolomeec@comsec.spb.ru

КОМАРЬКОВ Владислав Юрьевич — студент группы ИКПИ-72 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, komarkov1111@mail.ru

КОНОНОВ Павел Александрович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kononov.pa@spbgut.ru

КОПТЕЛОВА Валентина Александровна — студентка (магистрант) группы ИКТБ-07м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, koptelova.va@spbgut.ru

КОРЖИК Валерий Иванович — доктор технических наук, профессор, почётный профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, val-korzhik@yandex.ru

КОРНИЕНКО Анатолий Адамович — доктор технических наук, профессор, заведующий кафедрой «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения Императора Александра I, kaa.pgups@yandex.ru

КОСОВ Никита Алексеевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kosov.n.a@mail.ru

КОТЕНКО Игорь Витальевич — доктор технических наук, профессор, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук; профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivkote@comsec.spb.ru

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КРУГЛОВА Александра Евгеньевна — студентка группы ИКТУ-77 Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, alexandra535@yandex.ru

КРЫЛОВ Алексей Вадимович — студент группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Krylov180497@yandex.ru

КУЗНЕЦОВ Вячеслав Сергеевич — аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, slava_kuznetsov@inbox.ru

КУЗНЕЦОВА Екатерина Александровна — студентка группы ИКТИ-95м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cotti31@gmail.com

КУЛИКОВ Илья Александрович — студент группы ИКТЗ-01м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wyzzus@gmail.com

КУЛИКОВ Дмитрий Александрович — студент группы ИКТК-76 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivamspasibo@gmail.com

КУЛИКОВ Евгений Юрьевич — студент группы ИКВТ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; сотрудник ООО «Естественный интеллект», ekulikov@naint.ru

КУЧЕРЯВЫЙ Андрей Евгеньевич — доктор технических наук, профессор, заведующий кафедрой сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akouch@mail.ru

КУШНИР Дмитрий Викторович — кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitry.kushnir@gmail.com

ЛЕБЕДЕВА Надежда Александровна — студентка группы ИКТИ-95м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lebedeva.na.97@bk.ru

ЛЕБЕДЯНЦЕВ Валерий Васильевич — доктор технических наук, профессор, заведующий кафедрой автоматической электросвязи Сибирского государственного университета телекоммуникации и информатики, lebvv1951@mail.ru

ЛЕВШУН Дмитрий Сергеевич — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, levshun@comsec.spb.ru

ЛЕПЕХИН Николай Николаевич — кандидат психологических наук, доцент кафедры эргономики и инженерной психологии Санкт-Петербургского государственного университета, n.lepehin@spbu.ru

ЛЕПЕШКИН Олег Михайлович — доктор технических наук, доцент, доцент кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, lepechkin1@ya.ru

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛОБАСТОВА Мария Викторовна — старший преподаватель кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mlobastovabk1@rambler.ru

ЛОБАЧ Денис Антонович — студент группы ИКТУ-78 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lo-de@mail.ru

ЛОШАКОВА Анна Вадимовна — бакалавр кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ann.losh99@mail.ru

ЛЫТКИНА Екатерина Александровна — студентка группы ИКТУ-78 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kartoguru1998@mail.ru

МАЛОФЕЕВ Валерий Александрович — курсант факультета автоматизированных систем управления Военной академии связи им. Маршала Советского Союза С. М. Буденного, valeron12.1366@gmail.com

МАМЕДОВА Фахранда Вагиф кызы — диссертант кафедры телекоммуникации и информационные безопасности Азербайджанского технического университета, faxranda.mammadova@mail.ru

МАНИЧЕВ Сергей Алексеевич — кандидат психологических наук, доцент, заведующий кафедрой эргономики и инженерной психологии Санкт-Петербургского государственного университета, s.manichev@spbu.ru

МАРОЧКИНА Анастасия Вячеславовна — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, amarochkina@naint.ru

МАТВЕЕВА Елена Александровна — кандидат технических наук, доцент кафедры «Прикладная информатика» Поволжского государственного университета телекоммуникаций и информатики, elenaa_matveeva@mail.ru

МЕЛЬНИКОВ Владимир Николаевич — студент группы ИКВТ-82 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, thev0v4n@gmail.com

МИНЯЕВ Андрей Анатольевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minyaev.a@gmail.com

МИСЛИВСКИЙ Борис Сергеевич — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mislivskyboris@yandex.ru

МИХАЙЛОВА Анастасия Валерьевна — студентка группы ИКТЗ-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ova.007@yandex.ru

МИХЕЕВА Светлана Николаевна — студентка (магистрант) группы ИКТИ-95М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ms.mixeewa@mail.ru

МОРДВИНОВ Егор Юрьевич — студент группы ИКТС-93м Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, ey.mordvinov@gmail.com

МУРАШКИН Никита Анатольевич — студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, niwhalea23@gmail.com

МУТХАННА Аммар Салех Али — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, muthanna.asa@spbgut.ru

НАМАЗОВ Манафедин Бешир оглы — кандидат технических наук, доцент кафедры автоматика и электроэнергетике Бакинского инженерного университета, manaf1963@mail.ru

НЕСТЕРОВ Иван Максимович — студент группы РК-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vano.nestor@yandex.ru

НИЖГОРОДОВ Антон Олегович — аспирант кафедры линии связи и измерения в технике связи Поволжского государственного университета телекоммуникаций и информатики, anton.socol2017@yandex.ru

НИКИТИН Борис Константинович — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nbk117@mail.ru

ОВЧИННИКОВ Максим Алексеевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, testov73@ya.ru

ОГАНЕСЯН Арарат Гагикович — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ararat1999@yandex.ru

ОГОРЕЛЬЦЕВ Павел Анатольевич — студент группы ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, paul.ogorelcev@gmail.com

ОКУНЕВА Дарина Владимировна — кандидат технических наук, декан факультета инфокоммуникационных сетей и систем, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, darina_okuneva@mail.ru

ОНИЩУК Антон Денисович — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; сотрудник ООО «Естественный интеллект», aonishchuk@naint.ru

ОСИЧЕВ Илья Юрьевич — заместитель генерального директора по техническим вопросам и новым технологиям АО “ГАТР” (Телеканал «Санкт-Петербург»)

ПАВЛОВ Иван Иванович — кандидат технических наук, доцент, и.о. заведующего кафедрой систем автоматизированного проектирования, доцент кафедры техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, академик МАС, iipavlov02@mail.ru

ПАВЛОВА Мария Сергеевна — ассистент кафедры радиотехнических устройств Сибирского государственного университета телекоммуникации и информатики, mspavlova@ngs.ru

ПАВЛОЦКИЙ Иван Павлович — студент группы ИКТЗ-74 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavlotskiy.iv@gmail.com

ПАНИЧЕВ Артём Дмитриевич — студент группы ИКТБ-07м Санкт-Петербургского государственного университет, robogiar2@inbox.ru

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук; профессор кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С.М. Буденного, shchuk@rambler.ru

ПАРФЕНОВА Анна Андреевна — студентка группы ИКТИ-95М Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, parfenovaa@yandex.ru

ПАРФИРОВ Виталий Александрович — кандидат технических наук, начальник лаборатории научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, vitaly.parfirov@yandex.ru

ПЕРМЯКОВ Александр Сергеевич — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, permyak.as@ya.ru

ПЕТРИВ Роман Богданович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.petriv@mail.ru

ПЕТРОВ Владислав Андреевич — студент группы ИКТЗ-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевич, vladpetrovvv@gmail.com

ПЕТРОВ Борис Михайлович — АО “ГАТР” (Телеканал «Санкт-Петербург»),

ПИЛИПОВА Валерия Михайловна — студентка группы ИКФ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lera_pilipova@mail.ru

ПОДГОРНАЯ Ксения Александровна — студентка группы ИКТГ-94М Санкт-Петербургского государственного университета, ksenia.podgornaya@mail.ru

ПОЛЯНСКАЯ Анастасия Владимировна — студентка группы ИКПИ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasiap244@gmail.com

ПОМОГАЛОВА Альбина Владимировна — ассистент, заместитель заведующего кафедрой по научной работе кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.l.b.i.n.a@bk.ru

ПОНОМАРЕНКО Кирилл Максимович — студент группы ИКТУ-77 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirill.ponomarenko@mail.ru

ПОПОНИН Антон Сергеевич — студент группы ИКВТ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, apoponin@naint.ru

ПОТЕМКИН Павел Андреевич — студент группы ИКТЗ-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, potiomkinpa98@gmail.com

ПУЧКОВ Владимир Викторович — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, puchkov-81@bk.ru

РЕДРУГИНА Наталия Михайловна — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, redrugina.nm@spbgut.ru

РЕЗНИКОВ Богдан Константинович — преподаватель кафедры фотоники и линий связи, преподаватель кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rznkff@gmail.com

РОГОВ Сергей Александрович — доктор физико-математических наук, профессор, профессор кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sarogov@mail.ru

РОЖКОВ Максим Александрович — аспирант кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, monolittiran@gmail.com

САВЕЛЬЕВА Анастасия Андреевна — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saa@spbgut.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, ibsaen@mail.ru

САЛИТА Андрей Сергеевич — студент группы ИКБ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, salita.a.s9@gmail.com

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

САМОЙЛОВ Георгий Юрьевич — студент группы ИКФ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rez1jkeee@gmail.com

СЕРГЕЕВ Алексей Николаевич — старший преподаватель кафедры фотоники и линии связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a32@bk.ru

СЕРЁЖИН Евгений Антонович — студент группы ИКТБ-98М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, se271196@yandex.ru

СИВУХИН Андрей Алексеевич — инженер группы поддержки пользователей рабочих станций, прикладного программного обеспечения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, androidsiv5@gmail.com

СИНЕЛЬЩИКОВ Владимир Сергеевич — студент группы ИКБ-73 Санкт-Петербургского государственного университета телекоммуникаций имени проф. М. А. Бонч-Бруевича, vov4kman@gmail.com

СКОРЫХ Марк Андреевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mark.skorykh@bk.ru

СОМОВ Кирилл Алексеевич — студент группы ПИм-91 Поволжского государственного университета телекоммуникаций и информатики, kirillsmv@mail.ru

СПИРКИНА Анастасия Валентиновна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasia.4991@mail.ru

СТАРОДУБОВ Роман Дмитриевич — студент группы ИКТБ-97 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, niochem@list.ru

СТАРОДУБОВА Дарья Дмитриевна — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, starodubova.95@mail.ru

СУББОТСКАЯ Анна Юрьевна — студентка группы ИКТм-91 Поволжского государственного университета телекоммуникаций и информатики, subotann@mail.ru

СУДАРЕВ Андрей Владимирович — студент группы ИКПИ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, AndrewSudarev@yandex.ru

СУХАНОВ Данил Сергеевич — студент группы РК-01М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, suhanov.s.d@yandex.ru

СУЮНДУКОВА Алина Аликовна — студентка группы ИКТВ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s_alina_a98@mail.ru

ТАГАНДУРДЫЕВ Нурмурад — студент группы ИКТМ-02м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nuriktagan@gmail.com

ТАРАБАНОВ Илья Федорович — студент группы ИКТК-76 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, tarabanov.ilya@yandex.ru

ТАРГОНСКАЯ Алина Игоревна — студентка группы ИКТБ-98М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевич, targonskaya.ai@gmail.com

ТАХИРОВА Конул Мобил кызы — адъюнкт Военной Академии Вооруженных Сил Азербайджанской Республики, konul_tahirova@yahoo.com

ТЕРЕБЕНИНА Юлия Дмитриевна — студент группы ИКТС-72 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, terebeninayuliya@gmail.com

ТЕСЛЯ Сергей Петрович — старший преподаватель кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, Yelena.Vershennik@mail.ru

ТИМОФЕЕВ Родион Сергеевич — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rodyamilk@gmail.com

ТИРБАХ Лада Алексеевна — студентка группы ИБ-61В Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tirbakh1988@gmail.com

ТЯН Ангелина Алексеевна — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, angeline.tyan612@gmail.com

УЛЯШЕВА Виктория Романовна — студентка группы ИКБ-82 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ulyasheva1838@gmail.com

УШАКОВ Игорь Александрович — кандидат технических наук, старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФЕДОРОВ
Илья Викторович
оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного
ilyafed1996@mail.ru

ФЁДОРОВА
Анастасия Эдуардовна
студентка группы ИКТЗ-74 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
fyodorova.aaee@gmail.com

ФЁДОРОВА
Ольга Вячеславовна
студентка группы ИКТЗ-74 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
olgafedorova666@gmail.com

ФЕДОРЧЕНКО
Елена Владимировна
кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук; доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
doynikova@comsec.spb.ru

ФЕДОРЧЕНКО
Андрей Владимирович
младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук,
fedorchenko@comsec.spb.ru

ФЕДОСЕЕВ
Илья Александрович
студент группы ИКТВ-83 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
641027B@gmail.com

ФЕДОТОВ
Илья Олегович
студент группы ИКВТ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
fedotow.ilja@gmail.com

ФИЛИН
Егор Дмитриевич
аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
filin.ed@mail.ru

ФИЦОВ Вадим Владленович — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, noldi@iks.sut.ru

ФОМИН Артем Игоревич — студент группы ИКТГ-04м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artem.fomin633@gmail.com

ХИНЕНЗОН Александра Витальевна — студентка группы ИКТБ-98М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевич, Khinenzon.av@gmail.com

ХМЫРОВ Семен Сергеевич — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, khmyrov.s.s@gmail.com

ХРАМЦОВ Дмитрий Олегович — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khramtsov2010@mail.com

ХРИЧКОВ Валентин Александрович — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hrichkovv@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

ЧУРИКОВ Антон Андреевич — магистр группы ИКТЗ-91м. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. antonch421@gmail.com

ШАЛЯПИН Сергей Олегович — генеральный директор ООО "Естественный Интеллект", shalyapin@naint.ru

ШАРИПОВА Ирина Дмитриевна — студентка группы ИКТУ-77 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sharipova.irine@yandex.ru

ШВИДКИЙ Артем Александрович — ассистент кафедры инфокоммуникационных систем, начальник научно-образовательного центра «Программно-определяемых систем» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича shvidkiy@sut.ru

ШЕМЯКИН Сергей Николаевич — кандидат технических наук, доцент кафедры защищенных систем связи. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. s4421764@yandex.ru

ШУРАВИН Андрей Сергеевич — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, and.shuravin@ya.ru

ШУТОВА Любовь Сергеевна — студентка группы ИКФ-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, libre.jester00@mail.ru

ШЫПОТА Николай Александрович — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksarn.kelben@gmail.com

ЭЛЛАУИ Юнес Брахимович — студент группы ИКТЗ-73 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ellaui.iunes@gmail.com

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, viyak@bk.ru

АВТОРСКИЙ УКАЗАТЕЛЬ

СПбГУТ)))