МТУСИ

ФУМО ВО ИБ

ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник научных трудов
по материалам всероссийской
научно-теоретической конференции

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский технический университет связи и информатики»
(МТУСИ)

Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00
«Информационная безопасность»
(ФУМО ВО ИБ)

3 декабря 2021 г.

ВСЕРОССИЙСКАЯ НАУЧНО-ТЕОРЕТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СБОРНИК ТРУДОВ

Москва - 2021

УДК 004.056(082)
ББК 16.8я43
Т33

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Леохин Ю.Л., д.т.н., профессор, проректор по научной работе МТУСИ (председатель);
Белов Е.Б., заместитель председателя ФУМО ВО ИБ (заместитель председателя);
Шелухин О.И., д.т.н., профессор, заведующий кафедрой «Информационная безопасность» МТУСИ;
Кубанков А.Н., д.в.н., профессор, заведующий кафедрой «Безопасность телекоммуникаций» МТУСИ;
Лось В.П., д.в.н., профессор, президент МОО «Ассоциация защиты информации»;
Новиков С.Н., д.т.н., доцент, заведующий кафедрой «Безопасность и управление в телекоммуникациях» СибГУТИ;
Крылов Г.О., д.ф.-м.н., профессор кафедры «Безопасность телекоммуникаций» МТУСИ, профессор Финуниверситета, профессор НИЯУ МИФИ;
Панков К.Н., к.ф.-м.н., врио заведующего кафедрой «Теория вероятностей и прикладная математика» МТУСИ;
Киреева Н.В., к.т.н., доцент, декан факультета «Телекоммуникации и радиотехника» ПГУТИ;
Красов А.В., к.т.н., доцент, заведующий кафедрой «Защищенные системы связи» СПбГУТ;
Безумнов Д.Н., старший преподаватель кафедры «Интеллектуальные системы в управлении и автоматизации» МТУСИ (секретарь).

ISBN 978-5-905376-22-1
9 785905 376221

УДК 004.056(082)
ББК 16.8я43
Т33

ОГЛАВЛЕНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

ЛОГИЧЕСКИЕ УЯЗВИМОСТИ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ В ОС WINDOWS 6

НАУЧНАЯ СЕКЦИЯ
«КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И СЕТЕВАЯ БЕЗОПАСНОСТЬ»

ПОДХОД К УЛУЧШЕНИЮ СУЩЕСТВУЮЩЕЙ ИРАКСКОЙ СИСТЕМЫ ГОЛОСОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ДИСТАНЦИОННОГО ГОЛОСОВАНИЯ 11
НЕКОТОРЫЕ ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ 20
МОДЕЛЬ НУЛЕВОГО ДОВЕРИЯ: РЕКОМЕНДАЦИИ ПО ВНЕДРЕНИЮ И ВОЗМОЖНЫЕ ПРОБЛЕМЫ 24
ТЕЛЕМЕДИЦИНСКАЯ СИСТЕМА МОНИТОРИНГА ПОКАЗАТЕЛЕЙ ЖИЗНЕДЕЯТЕЛЬНОСТИ НА ОСНОВЕ ПРОТОКОЛОВ АТРИБУТИВНОГО КОНТРОЛЯ ДОСТУПА 28
ЗАЩИТА ОТ УТЕЧКИ ИНФОРМАЦИИ НА ОСНОВЕ РАЗДЕЛЕНИЯ ЗАШИФРОВАННЫХ И СЖАТЫХ ДАННЫХ 36
ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ, ИСПОЛЬЗУЮЩИХ МОДЕЛЬ «ИЗДАТЕЛЬ-ПОДПИСЧИК» 44
ПРИМЕНЕНИЕ НЕЙРОКРИПТОГРАФИИ В БРАУЗЕРАХ С ИСПОЛЬЗОВАНИЕМ WEBASSEMBLY 50
ОБ ОДНОМ ПОДХОДЕ К ГЕНЕРАЦИИ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНЫХ ВОЗМОЖНОСТЕЙ КВАНТОВОГО КОМПЬЮТЕРА 56
ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА BLE ДЛЯ ЗАЩИТЫ И УПРАВЛЕНИЯ ДОСТУПОМ 62
ОРГАНИЗАЦИЯ СТЕГАНОГРАФИЧЕСКОГО КАНАЛА С ПОМОЩЬЮ МЕТОДА LACK НА ПРИМЕРЕ ПРОТОКОЛА RTP 68
МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ РАЗЛИЧНЫХ СТРАТЕГИЙ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 74
ИССЛЕДОВАНИЕ АЛГЕБРАИЧЕСКИХ СВОЙСТВ АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ MV-3 80
ПРИБЛИЖЕНИЕ ОПЕРАЦИИ ДИЭДРАЛЬНОЙ ГРУППЫ ОПЕРАЦИЕЙ СЛОЖЕНИЯ 87
АДАТИВНЫЙ МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПКФС НА ОСНОВЕ СИСТЕМОЛОГИЧЕСКОГО ПОДХОДА 92
ОСОБЕННОСТИ ГОЛОСОВОЙ ИДЕНТИФИКАЦИИ В МНОГОФУНКЦИОНАЛЬНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ 98
ЗАДАЧАОРИЕНТИРОВАННОЕ СРАВНЕНИЕ СРЕДСТВ АНАЛИЗА СЕТЕВОГО ТРАФИКА 103
ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫЕ СЕТИ В ЗАДАЧЕ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ 108
ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ СЕРТИФИКАТОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ WEB – РЕСУРСОВ УЧЕБНЫХ УЧРЕЖДЕНИЙ.....117

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПРОТИВОДЕЙСТВИЯ DDOS-АТАКАМ НА ОБРАЗОВАТЕЛЬНЫЕ УЧРЕЖДЕНИЯ 122
СИСТЕМЫ ЗАЩИТЫ БАЗ ДАННЫХ 126

НАУЧНАЯ СЕКЦИЯ
«БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИЙ»

Подсекция
«Организационно-технические проблемы защиты телекоммуникаций»

ОСОБЕННОСТИ СОВРЕМЕННЫХ КОММУНИКАЦИЙ....130
ПРОБЛЕМА БЕЗОПАСНОСТИ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ....135
АНАЛИЗ МНОГОФУНКЦИОНАЛЬНЫХ ПОИСКОВЫХ ПРИБОРОВ 139
МОБИЛЬНЫЙ ПОДХОД В ЗАЩИТЕ ИНФОРМАЦИИ....144
ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТА ИНФОРМАТИЗАЦИИ....148
НАУЧНЫЕ РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ ПРОЕКТА «РАЗРАБОТКА МЕТОДОВ И АЛГОРИТМОВ МОДЕЛИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ» 152
АНАЛИЗ И ОЦЕНКА УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЛАСТИ ФИНАНСОВОЙ ДЕЯТЕЛЬНОСТИ....158
ИНСТРУКТАЖ, КАК МЕТОД ПОВЫШЕНИЯ ДОВЕРИЯ К ПЕРСОНАЛУ 164
МЕТОДЫ КАРТОГРАФИРОВАНИЯ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА....172
МОДЕЛИ И АЛГОРИТМЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В НАКАПЛИВАЕМЫХ ДАННЫХ МОНИТОРИНГА СОСТОЯНИЯ КИБЕРФИЗИЧЕСКОГО ОБЪЕКТА....179
ИСПОЛЬЗОВАНИЕ ФИДОВ ПРИ ВНЕДРЕНИИ ПРОЦЕССА КИБЕР-РАЗВЕДКИ....196
ФОРМИРОВАНИЕ СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ 200
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С РАЗВИТИЕМ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ 205
ПУТИ РЕШЕНИЯ ЗАДАЧ РАЗВЕРТЫВАНИЯ СИСТЕМ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ 210
ИДЕНТИФИКАЦИЯ ВИДОВ МОДУЛЯЦИИ СИГНАЛОВ В КАНАЛАХ СВЯЗИ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ С ИСПОЛЬЗОВАНИЕМ САМООРГАНИЗУЮЩИХСЯ ИССКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ....215
ПЛАТФОРМА ЗАЩИЩЕННОГО ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ 221
ГИБРИДНЫЕ МЕТОДЫ И АЛГОРИТМЫ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧАХ РАСПОЗНАВАНИЯ БИОМЕТРИЧЕСКИХ ОБРАЗОВ С ОБЕСПЕЧЕНИЕМ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ЭТАЛОНОВ ОТ КОМПРОМЕТАЦИИ....229

Подсекция
"Аппаратно-программные средства защиты телекоммуникаций"

ИСПОЛЬЗОВАНИЕ ТЕОРИИ ДУФФУЗИИ ИННОВАЦИЙ ДЛЯ МАТЕМАТИЧЕСКОГО ОПИСАНИЯ ДИНАМИКИ РЕАЛИЗАЦИИ КОМПЬЮТЕРНОЙ АТАКИ 241
МЕТОДЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОРПОРАТИВНУЮ СИСТЕМУ ПРЕДПРИЯТИЯ: СРАВНЕНИЕ И АНАЛИЗ....247

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ SSRF ПРИ ЭКСПЛУАТАЦИИ WEB-ПРИЛОЖЕНИЙ 253
РАЗРАБОТКА НАБОРА СИГНАТУР ДЛЯ ОБНАРУЖЕНИЯ АТАК ТИПА LLMNR POISONING 258
ИССЛЕДОВАНИЕ ВОЗДЕЙСТВИЯ DDoS-АТАКИ НА ВИРТУАЛЬНУЮ МАШИНУ ПРИ НАЛИЧИИ И ОТСУТСТВИИ ТЕХНОЛОГИИ FIREWALL 263
ФОРМИРОВАНИЕ КОДА АУТЕНТИФИКАЦИИ ИЗ БИОМЕТРИЧЕСКИХ ДАННЫХ НА ОСНОВЕ АВТОМАТИЧЕСКОГО ОБУЧЕНИЯ НОВОГО КЛАССА ИСКУССТВЕННЫХ НЕЙРОНОВ СРЕДНЕГО ГАРМОНИЧЕСКОГО 270
УСТРОЙСТВО КОММУТАЦИИ IMEI И SIM-КАРТ АБОНЕНТСКИХ ТЕРМИНАЛОВ ДЛЯ ИЗМЕРЕНИЯ ВРЕМЕНИ АУТЕНТИФИКАЦИИ В СЕТЯХ СОТОВОЙ СВЯЗИ 2G-4G 277
ПРИМЕНЕНИЕ СТАНДАРТА IEEE 802.1X ДЛЯ УПРАВЛЕНИЯ ДОСТУПОМ В КОРПОРАТИВНЫХ СЕТЯХ 286
АЛГОРИТМ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ЗЛОУМЫШЛЕННИКА С ПОМОЩЬЮ DAS В 3-D ПРОСТРАНСТВЕ 290
ИССЛЕДОВАНИЕ УГРОЗ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ КОГНИТИВНОГО РАДИО 298
МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ НА ОСНОВЕ ХАОТИЧЕСКОГО ПРИМЕНЕНИЯ ОРТОГОНАЛЬНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ 303
ОЦЕНКА ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ SDR-ПРИЕМНИКА ДЛЯ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ 311
ОГРАНИЧЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТЕВОГО СКРЫТОГО КАНАЛА ПО ВРЕМЕНИ С УЧЕТОМ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ СЛЕДОВАНИЯ ПАКЕТОВ В СЕТИ 318
МЕТОДИКИ ОБНАРУЖЕНИЯ ДАННЫХ СЕТИ TOR 328
ИССЛЕДОВАНИЕ МЕТОДОВ АНАЛИЗА СЕТЕВОГО ТРАФИКА И РАЗРАБОТКА СИСТЕМЫ ВЫЯВЛЕНИЯ АНОМАЛИЙ ТРАФИКА В КОМПЬЮТЕРНЫХ СЕТЯХ С ПРИМЕНЕНИЕМ ИСКУССТВЕННЫЙ НЕЙРОННЫХ СЕТЕЙ АДАПТИВНО-РЕЗОНАНСНОЙ ТЕОРИИ 334
МЕТОДИКА ИСПОЛЬЗОВАНИЯ ФИЗИЧЕСКИХ ЭФФЕКТОВ ПРИ ПРИМЕНЕНИИ СИСТЕМНОГО ПОДХОДА К ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЕ РЕЧЕВОЙ ИНФОРМАЦИИ 343
ПРИМЕНЕНИЕ ТЕХНОЛОГИИ BLOCKCHAIN ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДОКУМЕНТАЛЬНОМ СОПРОВОЖДЕНИИ ЛОГИСТИЧЕСКИХ ПРОЦЕССОВ МОРСКИХ ГРУЗОПЕРЕВОЗОК 356

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Кравец В.В.
АО «Перспективный мониторинг», начальник отдела,
Vasily.Kravets@amonitoring.ru
Иванов О.А.
АО «Перспективный мониторинг», руководитель направления
Oleg.Ivanov@amonitoring.ru
Шорин Р.В.
АО «Перспективный мониторинг», исследователь
Roman.Shorin@amonitoring.ru

ЛОГИЧЕСКИЕ УЯЗВИМОСТИ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ В ОС WINDOWS

Аннотация: В рассматриваемой теме вынесен довольно широкий класс существующих уязвимостей, которые широко распространены и часто встречаются в современном программном обеспечении. В качестве подтверждения можно привести в пример опыт, с которым за два года столкнулись и зарегистрировали более 10 таких уязвимостей в программах с огромным количеством установок и пользователей. Список зарегистрированных уязвимостей: CVE-2019-14743, CVE-2019-15316, CVE-2019-17180, CVE-2019-19247, CVE-2019-19248, CVE-2019-20383, CVE-2020-23967 и CVE-2021-25261. Среди уязвимого программного обеспечения встречаются и игровые лаунчеры (Steam, Origin, GOG Galaxy), программы распределенного хранения (Dropbox), антивирусы (Dr. Web) и программы общего назначения (ABBYY FineReader).

Признаки уязвимостей

Слово «логические» в контексте уязвимостей противостоит критерию «бинарные». Различие состоит в том, что бинарные уязвимости эксплуатируют особенности работы с памятью, вызовы опасных функций и другую работу, которая происходит на уровне бинарного кода, а логические уязвимости эксплуатируют логическое поведение программы, принуждая программное обеспечение выполнять не те действия, которые были задуманы разработчиками. Из-за такой разницы, сразу можно выделить некоторые преимущества логических уязвимостей: они более стабильны к внесению изменений в программное обеспечение (даже минимальное изменение программы может нарушить работу бинарной уязвимости, а логические уязвимости могут оставаться актуальными даже при глобальных обновлениях) и сложно детектируемы, поскольку нормальное функционирование программы не нарушается.

Отдельная часть рассматриваемой темы уже соответствует собственному классу уязвимостей – повышение привилегий в ОС Windows, поэтому кратко опишем предметную область. Рассмотрим классификацию пользователей ОС Windows по двум критериям – наличие у пользователя высоких прав доступа и наличие у пользователя ограничений функциональных возможностей. Примеры пользователей: Guest (нет высоких прав доступа, есть ограничения), стандартный пользователь (нет высоких прав доступа, нет ограничений), пользователь NT AUTHORITY\SERVICE (есть высокие права доступа, есть ограничения) и пользователь NT AUTHORITY\SYSTEM (есть высокие права доступа, нет ограничений). Фактически, любая уязвимость, которая позволяет из одного класса в данной классификации перейти в другой может рассматриваться как повышение привилегий. Но чаще всего понимается переход от пользователя без высоких прав к пользователю с высокими правами, без ограничения на получение ограничений в контексте высоких прав.

Реализация уязвимостей

Для реализации уязвимостей логического повышения привилегий обычно сначала находят некоторый примитив в операциях, который уже может быть использован непосредственно для выполнения кода с повышенными правами.

Основными примитивами являются:

1) Создание файла с «свободными» правами доступа (под свободными понимаются права, которые позволят далее данный файл поменять без дополнительных привилегий);
2) Перемещение файлов в подконтрольных пользователю директориях;
3) Изменение прав доступа на файлы, директории и ветки реестра;
4) Удаление файлов и папок в подконтрольных пользователю директориях;
5) Запуск внешних программ.

Все эти примитивы при определенных условиях могут использованы, чтобы получить повышенные права.

Кроме основных примитивов, также стоит рассмотреть и типовые техники, которые используются в работе с логическими уязвимостями.

1) Работа с динамическими библиотеками (dll);
2) Использование символических ссылок;
3) Работа с журналами;
4) Нарушение принципа Керкгоффса.

Рассмотрим каждую из ранее затронутых техник подробнее.

Использование загружаемых динамических библиотек часто открывает возможности по загрузке легитимным программным обеспечением сторонние библиотеки. В качестве типового примера можно привести классическую уязвимость dll hijack: при старте программа до выполнения основного кода, осуществляет поиск динамических библиотек, которые используются в работе, и может загрузить не ту библиотеку, которые предполагались программистами. Такие ситуации возникают из-за того, что поиск библиотек начинается рядом с программой, а только потом в системных директориях. При наличии прав на запись в директорию с программой, нарушитель может подложить специальную dll, которая будет загружена вместо системной, что приведет к выполнению кода из этой библиотеки. Данная техника уже редко используется, поскольку давно известна, но все равно иногда попадается программное обеспечение, которое от нее не защищено. Кроме того, сейчас существует и развитие этого метода в виде атаки DotLocal redirection (.local redirection) – эта техника позволяет при определенных обстоятельствах загружать динамическую библиотеку в программу, даже если нет возможности создать файлы рядом с исполняемым файлом.

Отдельно можно обратить технику dll hijack и вместо того, чтобы подкладывать dll к программе, сделать наоборот и взять легитимный исполняемый файл и подложить его к библиотеке с полезной нагрузкой. При запуске такого бинарного файла будет исполнен код из библиотеки, но в контексте скопированного исполняемого файла. Такие действия позволяют обходить проверки подписи, поскольку подпись будет проверяться только у основного бинарного файла, а именно его мы взяли как легитимную часть.

Другой распространенной техникой является использование символических ссылок. В ОС Windows существует большое количество симлинков: нативные симлинки в файловой системе, символические ссылки для реестра, точки повторной обработки NTFS (reparse point) и другие. Использование таких ссылок позволяет создать видимость для программы, что она работает с одним файлом, хотя на самом деле все действия будут происходить с другими.

Чтобы создать символическую ссылку с одного файла на другой необходимы высокие права (фактически, нужно быть администратором). Но есть способ сделать аналогичный симлинк, но без прав администратора. Для этого нужно использовать комбинацию методов. Предположим, что необходимо создать ссылку для файла

C:\1\file.txt с целью в виде файла C:\2\another.txt. Для достижения такой цели необходимо создать точку повторной обработки на месте директории C:\1, и указать целью объектную директорию \RPC Control. Директория \RPC Control не является папкой в файловой системе, это специальная директория, в которой хранятся объекты, используемые для синхронизации – события, семафоры и прочие. Несмотря на то, что это не полноценная папка, она может быть целью точки повторной обработки. Далее в этой объектной директории уже можно создать симлинк с \RPC Control\file.txt на C:\2\another.txt и создание такого симлинка не требует повышенных прав. В результате, при обращении к файлу C:\1\t.txt процесс будет перенаправлен сначала через точку повторной обработки на путь \RPC Control\1.txt, а затем по симлинку на файл C:\2\another.txt.

Очень часто многие программы ведут журналы своей работы и такие журналы могут быть очень полезны при поиске уязвимостей. Даже просто читая отладочные сообщения можно получить много информации о том, как работает программа, что она делает и какие реакции ожидает. Но помимо роли источника информации, журналы могут быть и непосредственно источником уязвимости. Нередко программисты обеспечивают ротацию логов, которая реализуется, например, через переименование файла журнала.

Например, пусть известно, что ротация журнала для некоторого ПО происходит через переименование файла C:\logs\data.txt в файл C:\logs\data.txt.old. В таком случае можно воспользоваться приемом, аналогичным тому, как создается символическая ссылка вида файл-файл.

Создается три символических ссылки:

1) C:\logs\ <-> \RPC Control\
2) \RPC Control\data.txt <-> C:\from\file
3) \RPC Control\data.txt.old <-> C:\to\file

В таком случае вместо изменения имени файла C:\logs\data.txt в файл C:\logs\data.txt.old произойдет перемещение файла C:\from\file по новому пути C:\to\file.

Однако стоит отметить, что одной из самых серьезных проблем для программистов можно считать нарушение принципа Керкгоффса. Сам по себе принцип Керкгоффса обычно применяется к разработке криптографических методов и в одной из формулировок звучит так: «Нужно, чтобы не требовалось сохранение системы в тайне; попадание системы в руки врага не должно причинять неудобств». Это правило указывает, что сами методы, например, шифрования, должны быть открыты, защищать нужно только ключ. При разработке программного обеспечения, программисты нередко придумывают способы как оставить себе возможность выполнить какой-то код с повышенными привилегиями, надеясь, что сохранение этого метода в тайне защитит пользователей. Но на практике такие ситуации легко находятся и эксплуатируются нарушителем. В качестве типового примера можно привести программы, которые выполняют команды пришедшие к ним по системам межпроцессного взаимодействия, например, через пайпы.

Рассмотрим пример уязвимости в лаунчере Origin. Если минимизировать, то можно описать программу работы так: привилегированный сервис получал зашифрованные алгоритмом AES команды от приложения, которое должно быть подписано цифровой подписью. С точки зрения атакующего, эти защиты ничтожны – проверку подписи можно было обычной методом обратного dll hijack, а шифрование не имело особо смысла, поскольку ключ легко вычитывался в открытом виде.

Заключение

Логические уязвимости повышения привилегий – это интересный способ проверить насколько хорошо программисты понимают, что они делают и с чем могут столкнуться. Для исследователя, который ищет такие уязвимости каждая программа — это своя головоломка, которую надо постараться решить. Защититься от таких уязвимостей можно только если самому встать на место исследователя и применить

типовые методы, понять, как они работают и проверить реакцию программы на такие внешние воздействия.

СПИСОК ЛИТЕРАТУРЫ

1. Полякова Т.А., Химченко А.И. Правовые проблемы информационной безопасности при использовании облачных технологий // Правовая информатика. 2013. №2.
2. Общие уязвимости и риски [Электронный ресурс]: - CVE 2018 г.
3. Широкова Е. А. Облачные технологии // Современные тенденции наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). - Уфа: Лето, 2011.
4. Крис Хинкли, PCI DSS 3.0: влияние на ваши операции по обеспечению безопасности.
5. Башлы П.Н., Баранова Е.К. Информационная безопасность: учебно-практическое пособие.
6. Барсуков В.В., Водолазкий В.В. Современные технологии безопасности. Интегральный подход. - М .: Нолидж, 2015.
7. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Колдуев Н.А. Обеспече-информационная безопасность бизнеса / 2-е издание перераб. и доп. - М .: Альпина Паблишерз, 2014.
8. Репин Д.С. Разработка алгоритмов и безопасности обнаружения и предотвращения угроз информации, повторного отказа в обслуживании с.48 2017г
9. 24. Мищенко В. И. Защита информации в государственных информационных системах / В. И. Мищенко, А. К. Шилов // Вестник компьютерных и информационных технологий. - 2015. - №3.
10. Амрит Т. Уильямс, Марк Николетт, Повысьте ИТ-безопасность с помощью управления уязвимостями.

НАУЧНАЯ СЕКЦИЯ
«КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И СЕТЕВАЯ БЕЗОПАСНОСТЬ»

Руководители: **Шелухин Олег Иванович**,
Московский технический университет связи и информатики,
заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор

Панков Константин Николаевич,
Московский технический университет связи и информатики,
врио заведующего кафедрой
«Теория вероятностей и прикладная математика»
кандидат физико-математических наук

Секретарь: **Симонян Айрапет Генрикович**,
Московский технический университет связи и информатики,
доцент кафедры «Информационная безопасность»,
кандидат технических наук, доцент

Салман В.Д
СПбГУТ, аспирант,
wasan.salman@mail.ru

ПОДХОД К УЛУЧШЕНИЮ СУЩЕСТВУЮЩЕЙ ИРАКСКОЙ СИСТЕМЫ ГОЛОСОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ДИСТАНЦИОННОГО ГОЛОСОВАНИЯ

Предложен подход к совершенствованию иракской системы голосования с использованием технологии блокчейн и алгоритмов криптографии. Сформулированы требования к функциям безопасности системы голосования в предлагаемом протоколе. Сделан вывод о том, что использование блокчейна и методов криптографии для дистанционного голосования может обеспечить решение многих проблем, возникающих в современных избирательных системах, таких как анонимность избирателей, тайна голосования и защита голосов от манипуляций.

Электронное голосование становятся популярной тенденцией наших дней. Внедрение безопасных систем электронного голосования очень важно в каждой стране. Основными преимуществами внедрения системы электронного голосования являются увеличение числа участников выборов, снижение затрат и улучшение подсчета результатов выборов [1].

Поскольку в каждой стране действуют разные законы и их реализация, предложить универсальную структуру практически невозможно. В данном исследовании рассматриваются решения актуальные для выборов в Ираке. Целью данной работы является исследование подходов по улучшению существующей иракской системы голосования. Предлагается совершенствование иракской системы голосования осуществлять с использованием технологии блокчейн и алгоритмов криптографии. Разработана модель протокола с подробным объяснением каждого шага его работы. Предлагаемая система отвечает следующим требованиям: уникальность, аутентификация избирателей, целостность, конфиденциальность, анонимность.

Рассмотрим подходы к построению системы голосования, которые были предложены в разных странах.

В [2] рассмотрена мировая практика использования технологии блокчейн при голосовании. Отдельно анализируются технические решения, используемые в наиболее активно развивающихся проектах, направленных на разработку собственного программного обеспечения для проведения электронного голосования с использованием технологии блокчейн. А также рассматриваются некоторые проблемы голосования с использованием технологии блокчейн, такие как идентификация и тайна голосования.

В [3] предложено решение с использованием блокчейна для устранения недостатков традиционных выборов в Турции. В этой работе, система голосования разделена на уровни: от самого низкого уровня до самого высокого уровня. На самом низком уровне (уровень 0) каждый блок будет состоять из одной транзакции, и в каждом блоке будет храниться вся связанная информация о транзакции. На верхних уровнях, голоса поступающие с одного нижнего уровня, хранятся в кластерах, которые передаются через разные временные сегменты, и все они хранятся как монолитная структура. Преимущества этой структуры: низкая задержка, быстрая и безопасная система. Эта

система подходит для использования в другой стране с большим трудом, потому что в каждой стране разные законы и разная избирательная система. В системе использовались блокчейн Ethereum и алгоритм консенсуса DPoS. В этой работе не обсуждается криптографические алгоритмы. Преимуществом системы является уровневая структура. В этой системе существует разное количество уровней в зависимости от потребностей страны. Недостаток этой системы, использующей блокчейн Ethereum, этот тип блокчейна требует высокой энергии.

В [4] реализован и протестирован пример приложения для электронного голосования в Индии, работающего в качестве смарт-контракта для сети Ethereum с использованием электронных кошельков. В этом исследовании проблема поддельных голосов была решена с использованием технологии блокчейн. Недостатком этой работы является то, что избирателям приходится платить небольшую сумму.

Исследование в [5] было сосредоточено на разработке системы электронного голосования на основе блокчейна для Индонезии, где каждый избиратель имеет право участвовать в выборах и обязан отдать свой голос, напрямую. В этой работе построена программа моделирования с использованием веб-фреймворка Django на основе Python. В работе приводятся следующие характеристики сисемы: в ходе голосования было собрано 10,000 голосов примерно за 2585 секунд (43 минуты 5 секунд). Каждый блок состоял из 20 голосов в качестве транзакций. Таким образом, максимальный размер каждого блока составлял 1000 байт. В данной работе этап регистрации и способ хранения ключей не обсуждаются.

В [6] предлагается структура мобильного голосования для Нигерии, которая использует технологию блокчейна для безопасного хранения поданных голосов и многофакторной аутентификации избирателей до того, как они отдадут свои голоса, а также обеспечивает легкодоступную, безопасную и прозрачную систему мобильного голосования. Недостаток этого подхода заключаются в том, что у мобильных устройств недостаточно ресурсов, чтобы быть майнером/узлом в блокчейн - сети и для мобильных устройств нужно другое средство, чтобы они могли отправлять свои транзакции или голоса в блокчейн – пул для хранения.

В [7] подробно описана схема электронного голосования для Пакистана, а также ее реализация с использованием многоцепочечной платформы (MultiChain). В системе используются отпечатки пальцев для защиты от двойного голосования. Криптографический хэш транзакции, отправленный избирателю по электронной почте, используется в качестве доказательства того, что его голос был зарегистрирован правильно. В работе не обсуждался этап регистрации, метод шифрования, расшифровки голосования и подсчета голосов.

В (Табл. 1) представлены результаты предыдущих исследований в соответствии с наиболее важными функциями безопасности в сравнении с предлагаемыми решениями.

Табл. 1. Сравнительный анализ предыдущих исследований и наших предложений

Исследования	Архитектура и дизайн	Безопасность голосования
[3]	- Блокчейн	- Целостность данных о голосах - Конфиденциальность избирателей

[4]	- Ethereum Блокчейн; Смарт-контракты; Электронный кошелёк; Solidity язык; Truffle; Metamask; Ganache.	- Конфиденциальность - Публичная проверка результатов
[5]	- Блокчейн; SHA3-256; Python; SQLLite3; Django web framework; Алгоритм цифровой подписи на эллиптической кривой	- Конфиденциальность - Честность - Справедливость
[6]	- Мобильная система голосования; Блокчейн; Многофакторная аутентификация.	- Защита поданных голосов
[7]	- Блокчейн -Multichain платформа.	- Анонимность избирателей - Конфиденциальность голосования
Наш протокол	- Мобильное приложение; Разрешенный Блокчейн (HF); Смарт-контракт; Двухфакторная аутентификация; Гомоморфное шифрование (Пэйе криптосистема); Схема разделения секрета	- Конфиденциальность - Анонимность - Уникальность - Аутентификация избирателей - Целостность

Система голосования в Республике Ирак

Главным органом избирательной системы Ирака является Независимая Высшая Избирательная Комиссия Ирака (IHEC). Избирательная система Ирака представляет собой пропорциональную систему представительства провинций и состоит из 329 мест. Голосование не является обязательным. Избиратели, имеющие право голоса, имеют иракское гражданство, возраст не менее 18 лет, зарегистрированы в списке избирателей, имеют электронную карту и удостоверение личности с фотографией или биометрическую карту избирателя. Иракская система голосования состоит из следующих этапов: *регистрация, голосование, подсчет голосов и объявление результатов голосования* [8].

Основные недостатки существующей иракской системы голосования:

- Запугивание или подкуп сотрудников IHEC или избирателей;
- Фальсификация;
- Подрыв тайны голосования;
- Кража или уничтожение ящиков для голосования;
- Изменение голосов;
- Замедление избирательного процесса.

Чтобы устранить недостатки и улучшить эту систему, необходимо перейти к электронному дистанционному голосованию.

Подход к улучшению системы голосования в Ираке

Предлагаемая схема голосования представлена на Рис. 2. В протоколе использует блокчейн Hyperledger fabric (HF), как среда выполнения смарт-контрактов. В системе голосования HF - это частный блокчейн, в котором частная организация может создать свою собственную блокчейн-сеть [11-12]. В HF смарт - контракт называется цепным кодом (chaincode). HF использует алгоритм консенсуса Practical Byzantine Fault Tolerance (PBFT) [9]. Термин “Смарт-контракт” был впервые введен в середине 1990-х годов ученым - специалистом по компьютерам и криптографии Сабо [14], который определил смарт-контракт как “набор обещаний, определенных в цифровой форме, включая протоколы, в рамках которых стороны выполняют эти обещания. Смарт-контракты представлены в виде компьютерных программ, работающих в сети блокчейн, и могут

выражать условия и бизнес-логику для обеспечения сложных программируемых транзакций [13]. HF разрабатывает смарт-контракты с использованием ПО Go, Java и т. д. Он использует контейнер Docker для выполнения кода. Жизненный цикл смарт-контракта состоит из четырех основных этапов: создание, публикация, выполнение и завершение [14-17].

a) Создание смарт-контракта. После нескольких раундов обсуждений между сторонами может быть достигнуто соглашение. Затем инженеры-программисты преобразуют это соглашение, написанное на естественных языках, в смарт-контракт, написанный на компьютерных языках.
b) Публикация смарт-контракта. Проверенные смарт-контракты могут быть развернуты на платформах поверх блокчейнов. Контракты, хранящиеся в блокчейнах, не могут быть изменены. После развертывания смарт-контрактов в блокчейнах все стороны могут получить доступ к контрактам через блокчейны.
c) Исполнения смарт-контрактов. При достижении условий процедуры (или функции) контракты будут выполняться автоматически.
d) Завершение смарт-контрактов. После выполнения смарт-контракта обновляются новые состояния всех сторон. Соответственно, транзакции во время выполнения смарт-контрактов, а также обновленные состояния хранятся в Блокчейнах.

Для пояснения принципа работы смарт-контракта рассмотрим пример договора о переводе денег между Алисой и Бобом (Рис. 1). После нескольких раундов обсуждения между Алисой и Бобом, они приходят к соглашению. Затем соглашение реализуется с помощью языка смарт-контрактов (например, Golang в fabric). Далее код смарт-контракта компилируется с помощью компилятора, который генерирует машинный код, выполняемый поверх контейнеров Docker на клиенте смарт-контракта. После публикации смарт - контракта в сети блокчейн клиенту возвращается уникальный адрес контракта для поддержки будущих взаимодействий. После этого пользователи могут взаимодействовать с блокчейн-сетью, выполняя транзакции в смарт-контракте (например, вычесть указанную сумму денег из цифрового кошелька Алисы и увеличить соответствующую сумму денег в кошельке Боба). Стоит отметить, что каждая транзакция должна быть проверена в сети блокчейн с помощью алгоритмов консенсуса. Проверенная транзакция затем добавляется в список транзакций [16].

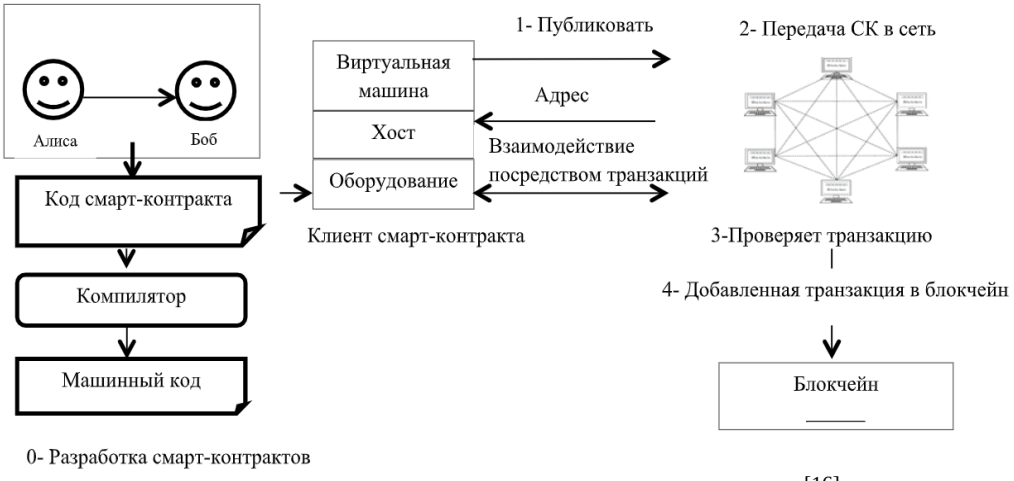


Рис. 1. Рабочий процесс смарт-контракта [16]

Алгоритм консенсуса - это процесс достижения соглашения между узлами сети о добавлении данных в распределенные системы. Алгоритм консенсуса играет важную роль в поддержании безопасности и эффективности блокчейна [10]. Существует два типа алгоритмов консенсуса: алгоритм консенсуса на основе доказательств и на основе голосования. Основная концепция алгоритма консенсуса, основанного на доказательствах, заключается в том, что среди многих узлов, присоединяющихся к сети, узел, выполнивший достаточное доказательство, получит право добавить новый блок в цепочку и получить вознаграждение. Алгоритмы консенсуса, основанные на доказательствах, это - POW, POS и др. В алгорита консенсуса на основе голосования (PBFT, Raft/paxos, POA,…и др.): все узлы в сети должны совместно проверять транзакции или блоки. Они будут общаться друг с другом, прежде чем решат добавлять предлагаемые ими блоки в свою цепочку или нет. Алгоритм консенсуса должен удовлетворять следующим свойствам: масштабируемость (scalability); низкая задержка (low latency); высокая производительность (high throughput); децентрализация [10][17-20]. В предлагаемом протоколе использует алгоритмы консенсуса подтверждения полномочий (Proof-of-Authority (PoA)) - это новое семейство византийских отказоустойчивых алгоритмов консенсуса. PoA - изначально был предложен как часть экосистемы Ethereum для частных сетей. Алгоритмы PoA полагаются на набор из N доверенных узлов, называемых авторитетами.Каждый участник идентифицируется уникальным идентификатором, ибольшинство из них считаются честными, и по крайней мере, честным должно быть (N/2 + 1) узлов [20].

Для республики Ирак предлагается схема дистанционного электронного голосования (ДЭГ), представленная на (Рис.2). Она включает в себя (комиссию ДЭГ, избирателя, блокчейн и наблюдателя). Взаимодействия между ними, отмеченные стрелками на схеме, осуществляются согласно разработанному протоколу.

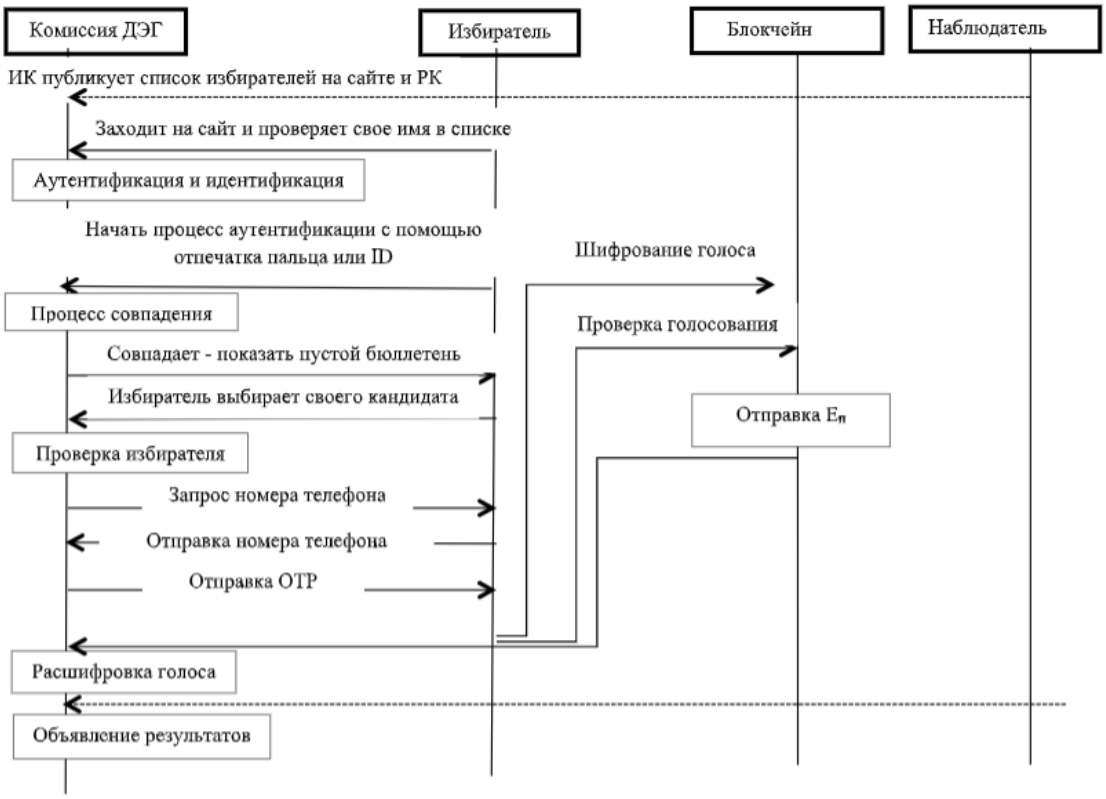


Рис.2 Предлагаемый протокол голосования

Первый этап - регистрация. Этот этап выполняется перед выборами в автономном (off-line) режиме. Избирательная комиссия регистрирует персональные и биометрические данные избирателей и обновляет списки избирателей до начала выборов, а также регистрирует кандидатов, которые хотят участвовать в выборах. Избирательная комиссия (ИК) публикует список избирателей на сайте регистрации избирателей. В день выборов избиратель проверяет свое имя в списке избирателей. На данном этапе, протокол TLS используется для обеспечения безопасных соединений между избирателем и регистрационным сервером. Роль наблюдателей на этапе регистрации заключается в наблюдении и контроле за тем, сколько избирателей участвуют в голосовании, а также в сравнении количества избирателей с количеством голосов на этапе регистрации. Это позволит избежать фальсификации процесса голосования.

Второй этап - аутентификация. На этом этапе начинается процесс аутентификации личности избирателя. Когда начинается процесс голосования, избиратель нажимает на ссылку и подключается к серверу аутентификации, чтобы сервер проверил избирателя, используя его отпечатки пальцев - для избирателей, у которых есть смартфон. Избиратели, у которых нет смартфона, для аутентификации должны будут использовать номер национальной карты (ID). Серверы регистрации и аутентификации разделены. Совпадение с данными, хранящимися на сервере, позволит ему получить доступ к серверу голосования, а не совпадение - будет считать его нелегитимным избирателем.

Третий этап - голосование. Избиратель ставит галочку перед своим кандидатом. После того, как избиратель выберет своего кандидата, начнется процесс аутентификации для верификации избирателя. Избиратель обязан ввести свой номер телефона, после чего сервер аутентификации отправит ему секретный код, избиратель повторно отправляет секретный код на сервер аутентификации по SMS. То есть используется алгоритм SMS OTP (алгоритм одноразового пароля). Основным средством обеспечения секретности голосования в электронной системе является асимметричная криптография. Избирательная комиссия генерирует ключевую пару криптосистемы Пэйе (*pk, sk*) и публикует открытый ключ (*pk*) на веб-сайте. Избиратель отдает свой голос следующим образом: (1) Избиратель выбирает одного из кандидатов. (2) Избиратель вызывает функцию шифрования Пэйе, нажав на кнопку "голосовать". (3) Избиратель отправляет в блокчейн транзакцию зашифрованное голосование. (4) Смарт - контракт проверяет правильность зашифрованного голосования. (5) Если голосование является действительным, смарт-контракт отправляется избирателю сообщения, что его голос принят. (6) Смарт - контракт хранит голос в блокчейне. Для защиты секретного ключа (*sk*), он разделяется на части (доли), используя схему разделения секрета. Данный протокол использует блокчейн в качестве базы данных для хранения и подсчета зашифрованных голосов. Как только избиратель зашифрует свой голос и отправит его в смарт-контракт в сети блокчейн. В блокчейн начнется проверка голосов. Узел проверки проверяет данные СК. Когда все участвующие узлы проверят СК, будет создан новый блок и добавлен в блокчейн. На (Рис.3) показаны сохраненные зашифрованные голоса в блокчейне.

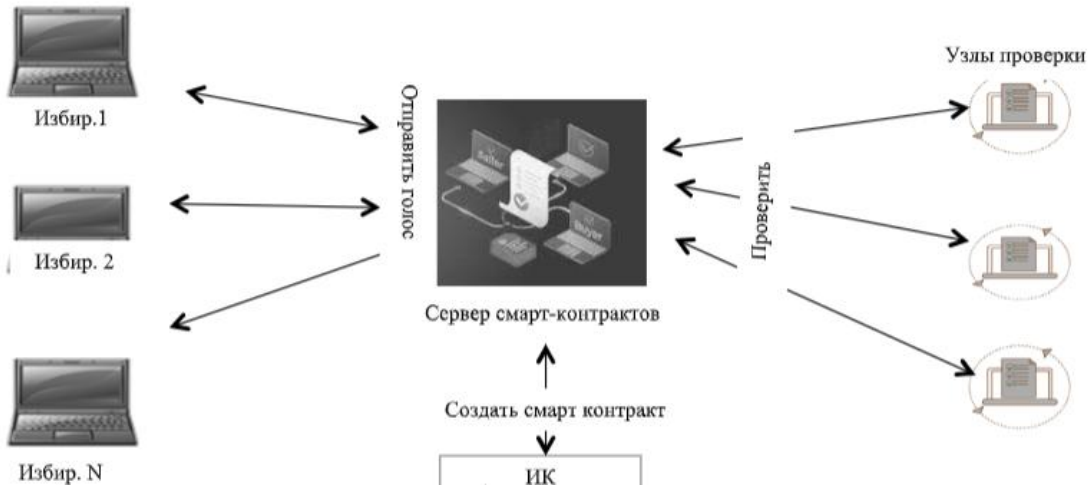


Рис. 3. Сохранение зашифрованных голосов на Блокчейне

Четвертый этап - процесс подсчета голосов. Здесь используется свойство аддитивного гомоморфизма криптосистемы Пэйе. Пусть $E_П$ – произведение всех зашифрованных голосов. Смарт - контракт отправляет $E_П$ в избирательную комиссию. Избирательная комиссия собирает секретный ключ из долей и расшифровывает $E_П$ с его помощью как сумму голосов всех избирателей. ИК публикует на сайте результаты голосования V (совместно с ID избирателей, принявших участие в голосовании). По ID каждый избиратель может проверить, что его голос был учтен и при этом он знает, что сохранена тайна голосования.

Последний этап – объявление результатов. Здесь избирательная комиссия публикует результаты выборов на своем веб-сайте.

Таким образом, предложенная схема и протокол голосования обеспечивают выполнение требований, приведенных в Табл.2

Табл. 2. Выполнения требований по безопасности в предлагаемой системе

№	Требования к безопасности системы голосования	Используемые методы защиты
1.	Аутентификация избирателей	Использование биометрических технологий и удостоверений личности (ID) позволяет системе защитить от нелегитимных избирателей, а также использовать алгоритм OTP для аутентификации избирателей.
2.	Уникальность	Использование биометрических технологий позволяет системе защитить от многократного голосования.
3.	Целостность	Использование блокчейна позволяет системе защитить от изменения или удаления голосов.
4.	Конфиденциальность	Использование криптосистемы Пэйе позволяет обеспечивать конфиденциальность содержимого бюллетеней.
5.	Анонимность	Использование криптосистемы Пэйе позволяет обеспечить тайну поданного голоса при подсчете голосов

Заключение

В работе предложен подход к построению протокола голосования для улучшения нынешней иракской системы голосования и решающий основные проблемы в ней.

Предлагаемое дистанционное электронное голосование для Ирака основано на использовании следующих преобразований: блокчейн, одноразовый пароль и биометрические технологии аутентификации избирателей, криптосистема Пэйе шифрования голосов и алгоритм (разделение секрета) для защиты закрытого ключа. Эта система отвечает следующим требованиям безопасности: уникальность, аутентификация избирателей, целостность, конфиденциальность, анонимность. Реализация этой предлагаемой структуры может принести много преимуществ в избирательном секторе, и некоторые из этих преимуществ заключаются в том, что: в день выборов избиратель, имеющий право голоса, может голосовать в любом месте и в любое время, что означает, что правительству не нужно считать день выборов государственным праздником; несколько средств аутентификации, предотвращает голосование нелегитимных избирателей; поданные голоса, благодаря технологии блокчейн, нельзя удалить или изменить; использование свойство гомоморфизма криптосистемы Пэйе позволяет сохранить в секрете результаты выборов до завершения избирательного процесса и обеспечить анонимность избирателей.

Дальнейшие исследования следует провести в направлении оценки производительности этой системы и сравнения ее с другими системами онлайн-голосования.

СПИСОК ЛИТЕРАТУРЫ

1. Mesbahuddin S. The Roadmap to the Electronic Voting System Development: A Literature Review. *Int. J. Adv. Eng. Manag. Sci. // IJAEMS*. vol. 2. No. 5. p. 6. 2016.
2. Кутейников Д. Л. Особенности применения технологий распределенных реестров и цепочек блоков (блокчейн) в народных голосованиях // *Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)*. 2019. p. 12. DOI: 10.17803/1994-1471.2019.106.9.041-052.
3. Rumeysa B., Alperen K. and Safa K. Blockchain-Based Electronic Voting System for Elections in Turkey // Rumeysa. p. 7. 2019.
4. Canessane R. A., Srinivasan N., Beuria A., Singh A. and Kumar B. M. Decentralised Applications Using Ethereum Blockchain // *Fifth Int. Conf. Sci. Technol. Eng. Math.* p. 5. 2019.
5. Prasetyadi G. C. , Mutiara A. B. and Refianti R. Blockchain-based electronic voting system with special ballot and block structures that complies with indonesian principle of voting // *International Journal of Advanced Computer Science and Applications*. vol. 11.No. 1. pp. 164–170. 2020. doi: 10.14569.
6. Abayomi-Zannu . A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication // *J. Phys. Conf. Ser.* vol. 1378. p. 9. 2019. doi: 10.1088/1742-6596/1378/3/032104.
7. Khan K. M., Arshad J., and Khan M. M.. Secure digital voting system based on blockchain technology // *International Journal of Electronic Government Research*. vol. 14. no. 1. pp. 53–62. 2018. doi: 10.4018/IJEGR.2018010103.
8. Салман В. Д. Анализ системы голосования в республике ирак и пути перехода к системе электронного голосования // *10TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2021*. С. 400-403. [Online]. Available: https://www.sut.ru/doci/nauka/1AEA/APINO/10-APINO-2021.T.2.pdf.

9. Yu B. *et al.* Platform-Independent Secure Blockchain-Based Voting System // *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. vol. 11060 LNCS. pp. 369–386. 2018. doi: 10.1007/978-3-319-99136-8_20.
10. Sankar L. S. , S. M, and Sethumadhavan M. Survey of Consensus Protocols on Blockchain Applications // *A Global Road Map for Ceramic Materials and Technologies: Forecasting the Future of Ceramics, International Ceramic Federation - 2nd International Congress on Ceramics, ICC 2008, Final Programme*. 2008. p. 5.
11. Foschini L., Gavagna A., Martuscelli G., and Montanari R. . Hyperledger Fabric Blockchain: Chaincode Performance Analysis. 2020. p. 6.
12. Sukhwani H., Wang N.,Trivedi K.S, and Rindos A. Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network). p. 10.
13. Shuai W. , Liwei O., Yong Y. , Xiaochun N., and Xuan H. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends // *2266 IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS*. 2019. p. 12.
14. Szabo N. Smart Contracts : Building Blocks for Digital Markets. No. c. 1–11.2015.
15. Mourouzis T. and Tandon J. Introduction to Decentralization and Smart Contracts. 2019. [Online]. Available: http://arxiv.org/abs/1903.04806.
16. Zheng Z. *et al.* An overview on smart contracts: Challenges, advances and platforms // *Future Generation Computer Systems*. vol. 105. pp. 475–491. 2020. doi: 10.1016/j.future.2019.12.019.
17. Pajooh H.H, Rashid M, Alam F, and Demidenko S. Hyperledger fabric blockchain for securing the edge internet of things // *Sensors (Switzerland)*. vol. 21. No. 2. pp. 1–29. 2021. doi: 10.3390/s21020359.
18. Kaur S., Chaturvedi S., Sharma A., and Kar J. A Research Survey on Applications of Consensus Protocols in Blockchain // *Secur. Commun. Networks*. vol. 2021. doi: 10.1155/2021/6693731.
19. Du M., Ma X., Zhang Z., Wang X., and Chen Q. A review on consensus algorithm of blockchain // *IEEE International Conference on Systems, Man, and Cybernetics, SMC*. vol. 2017. pp. 2567–2572. doi: 10.1109/SMC.2017.8123011.
20. Rasid H. Blockchain Technology in e-Voting : Comparative Study. p. 1–8. 2020.

Гимазетдинова А.И.
БашГУ, студент,
alsu.gimazetdinova@list.ru
Миронова Н.Г.
БашГУ, доцент, к.филос.н.
om_aks@mail.ru

НЕКОТОРЫЕ ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Цифровая индустрия развивается, технологичные средства безопасности становятся доступнее. Частные компании используют новые технологии обеспечения безопасности информационной среды для общего технологического совершенствования рабочих и технологических процессов (безопасность стала частью бизнес-процессов), для усиления своих конкурентных позиций среди конкурентов. Менеджмент должен анализировать тенденции в сфере технологий безопасности, чтобы понимать, в какие инновационные решения стоит вкладывать время и деньги и как они могут помочь общему развитию компании.

Для обеспечения конфиденциальности, целостности и доступности информации компании, организации в настоящее время могут выбирать свое из множества методов и технологий. По мере того как вычислительные и сетевые ресурсы становятся все более неотъемлемой частью бизнеса, необходима бдительность в отношении того, как используются, защищаются информационные частные и корпоративные ресурсы. Мобильные устройства, некоторые виды периферии и smart-техники устройства могут быть перепрофилированы для доступа к корпоративным службам, создавая канал для кибер-атаки на последние.

В современных условиях организациям необходимо передавать свою информацию через Интернет или через внешние носители. Даже при надлежащим образом выстроенных процедурах контроля доступа и средствах аутентификации, несанкционированное лицо может получить доступ к данным. Чтобы снизить риски несанкционированного доступа и утечек информации для каждого информационного ресурса, которым организация управляет, целесообразно иметь списки пользователей, которые могут выполнять определенные действия в корпоративной информационной среде и продуманную систему описания полномочий и доступных им ресурсов (для пользователя, которого нет в списке, затруднено несанкционированное проникновение в информационный ресурс, поскольку он не знает, что ресурс существует). Доступ в защищаемым ресурсам должен ограничиваться надежными методами аутентификации. Пока наиболее распространенной формой аутентификации является двухфакторная (через идентификатор пользователя и пароль), но для злоумышленника ее становится легко обмануть, если пользователи не соблюдают требований безопасности (например, используют для обоих способов аутентификации одно и то же устройство, используют слабые пароли и т.п.; целесообразны более сильные формы аутентификации (например, биометрическая по факторам внешности). Идентификация человека только по тому, что у него есть, какой-либо ключ и т.д., тоже может быть проблематичной. Использование более простых технологий идентификации пользователя уязвимо. В целом, для

обеспечения того, чтобы пароли не могли быть взломаны, необходимо внедрить продуманную «политику паролей».

Снизить риски неавторизованного доступа в компьютерную систему или сеть корпоративной среды помогает система обнаружения вторжений. Повысить эффективность защиты ресурсов позволяет использование идентификаторов безопасности, которые приписываются учетным записям и т.д.; идентификаторы можно настроить для отслеживания определенных действий пользователей и процессов, чтобы предупреждать сотрудников службы безопасности о нарушении политики защиты; идентификаторы также позволяют отслеживать различные типы трафика в сети для последующего анализа.

Организация может создать самую лучшую схему аутентификации, создать контроль доступа и средства предотвращения вторжений, но ее безопасность не может быть достаточно хорошей без создания физической безопасности оборудования и сетевых компонентов, которые хранят и передают информационные ресурсы. Для обеспечения физической безопасности организация должна идентифицировать все уязвимые ресурсы и принять меры для обеспечения того, чтобы эти ресурсы нельзя было физически подделать или украсть. Еще одним методом, который организация должна использовать для повышения безопасности в своей сети, является брандмауэр, аппаратный или программный, который защищает серверы и компьютеры компании при работе в сети, фильтруя пакеты из-за пределов сети организации, которые не соответствуют строгому набору критериев. Брандмауэр также может быть настроен для ограничения потока пакетов, покидающих организацию. Если сотруднику, работающему на дому, требуется доступ к некоторым из этих ресурсов во внутренней корпоративной сети из удаленной точки, безопасным способом доступа может служить виртуальная частная сеть (VPN), которая позволяет пользователю за пределами корпоративной сети получить доступ к внутренней сети извне. Благодаря сочетанию программного обеспечения и мер безопасности это позволяет организации предоставлять ограниченный доступ к своим сетям и в то же время обеспечивать общую безопасность. Еще одним эшелоном защиты данных должны быть средства шифрования там, где это уместно.

Существуют решения обнаружения и реагирования «расширенного» функционала, которые автоматически собирают и сопоставляют данные, полученные из нескольких систем безопасности, позволяя своевременно обнаруживать угрозы и реагировать на инциденты безопасности. Например, попытки внедрения вредоносного ПО, осуществляющиеся через электронную почту, конечную точку и через сеть — это, на самом деле, одна комплексная атака.

Компании должны реализовывать своевременно обновляемые политики безопасности, отвечающие уровню и специфике информационных угроз. Политика безопасности не только содержит руководящие принципы использования сотрудниками информационных ресурсов компании, но предоставляет компании юридические основания для действий в отношении внутренних нарушителей.

Глубокое машинное обучение стало одной из технологий обеспечения информационной безопасности, включаясь в инфраструктуру безопасности компаний и предприятий. Нейросети применяются при создании автоматизированных систем безопасности, которые, дополняя возможности ИБ-специалиста, позволяют оперативно обрабатывать значительные массивы данных о событиях безопасности быстрее, чем это

способен делать человек или группа людей. ИИ-технологии перспективна не только для крупных компаний со значительными объемами данных, но и для малых или средних компаний, чьи службы безопасности могут быть недостаточно обеспечены ресурсами. Инструменты на базе искусственного интеллекта отвечают различным потребностям в кибербезопасности, в т.ч. обеспечивают оперативное обнаружение или прогнозирование кибератак, отслеживание подозрительных событий и процессов, аутентификацию; среди систем безопасности с интеллектуальными функциями можно назвать такие:

- SIEM-системы (агрегация, категорирование, обнаружение связей событий безопасности, уведомление о выявленных подозрительных событиях службы ИБ) (например, Kaspersky Unified Monitoring & Analysis Platform (KUMA) от российской компании «Лаборатория Касперского», зарубежные FortiSIEM от Fotrinet, NetWitness Platform от RSA, Rapid7 insightIDR и т.д.)
- DLP-системы (например, Traffic Monitor, «Гарда Предприятие» – интеллектуальная системы защиты от утечек информации),
- системы обнаружения и предотвращения вторжений (пассивные IDS-системы (Intrusion Detection System - обнаружение вторжений) и активные IPS-системы (Intrusion Prevention System, отвечающие на вторжение разрывом соединения или блокировков трафика злоумышленника и т.д.) (например, Snort, Tripwire, IBM ISS, McAfee, нейросетевая система обнаружения атак AUBAD (Automated User Behavior Anomaly Detection system (разработчик - университет Мельбурна) и др.). В основе подобных систем могут быть заложены те или иные интеллектуальные технологии (нейросетевые модели, модели знаний, искусственные иммунные системы и генетические алгоритмы и т.д.)
- DPI-системы (например, Kaspersky Industrial Cybersecurity) с технологиями глубокого анализа трафика и т.п. ИИ может идентифицировать, определять приоритеты рисков, оперативно обнаруживать «вредоносные» события до наступления их негативных последствий.

Кроме того, автоматическая идентификация граждан с помощью нейросетей является популярным средством автоматизации правоприменительной практики, используются для распознания правонарушений, поиска преступников, распознания действий злоумышленников, пытающихся получить доступ к защищаемым сетевым ресурсам и сервисам. [5]

Современные SOC позволяют обеспечивать высокий уровень автоматизации и оркестровки процессов информационной безопасности именно благодаря увеличению присутствия в их составе интеллектуальных технологий и функций.

СПИСОК ЛИТЕРАТУРЫ

1. Сидоров, В.Д. Аппаратное обеспечение ЭВМ /В.Д. Сидоров, Н.В. Струмпэ, 2014. – 314 с.

2. Аппаратное обеспечение вычислительных систем. - М.: Маркет ДС, 2016. - 184 с.

3. Вендров, А. М. Практикум по проектированию программного обеспечения экономических информационных систем / А.М. Вендров. - М.: Финансы и статистика, 2011. - 192 с.

4. Гроувер, Д. Защита программного обеспечения / Д. Гроувер, Р. Сатер, и др.. - М.: Мир, 2011. - 283 с.

5. Миронова, Н.Г. Глава 5. Безопасность использования когнитивных информационных технологий принятия решений // Экономика и право: монография / В.В. Арбекова, Ю.А. Быченок, М.Л. Вартанова, А.В. Григорищин, Е.Н. Иванова, Л.А. Костыгова, В. Н. Круглов, Н.Г. Миронова, Т.С. Орлова, А.П. Пичугин, Т.А. Рягузова, Д.А. Савченко, Л.С. Силуанова, А.Т. Стадник, Д.В. Тютин, Е.А. Чуйко, Д. Б. Яхяев / гл. ред. Э.В. Фомин. – Чебоксары: ИД «Среда», 2021. – 184 с. – URL: https://www.elibrary.ru/download/elibrary_46291292_50473306.pdf (DOI: 10.31483/r-98432) – С. 126.

Малинский С.В.
РУТ (МИИТ), доцент, к.т.н., доцент,
Malinskiy_Stas@mail.ru

МОДЕЛЬ НУЛЕВОГО ДОВЕРИЯ: РЕКОМЕНДАЦИИ ПО ВНЕДРЕНИЮ И ВОЗМОЖНЫЕ ПРОБЛЕМЫ

В последние годы при реализации политики информационной безопасности (ИБ) во многих организациях набирает популярность концепция «нулевого доверия» (Zero Trust). Так, по оценкам ряда исследовательских агентств за 2019 год, 78% отделов и управлений ИБ уже использовали ее в своих организациях или планировали на нее перейти [1].

Долгое время при решении задач ИБ компании реализовывали политику «защиты периметра». Эта политика была очень популярной и эффективной, пока доверенная зона ограничивалась локальной сетью и подключенными к ней стационарными устройствами. Однако, пандемия COVID-19 и вынужденные изменения в организации работы большинства предприятий (организация работы сотрудников с удаленных "офисных" рабочих мест, в непрерывном перемещении, активное использование огромного количества мобильных гаджетов и облачных сервисов и пр.) фактически уничтожили понятие периметра, который следовало защищать. При этом проникнуть внутрь доверенной зоны и беспрепятственно перемещаться по ней стало значительно проще, чем и стали пользоваться злоумышленники. Статистика киберпреступлений 2019-2020 годов убедительно подтверждает эту тенденцию [2].

Проблема защиты «размытого» периметра не нова, она возникла более 10 лет назад. Первый официальный документ с описанием основных компонент архитектуры нулевого доверия опубликован Национальным институтом стандартов и технологий США (NIST) [3]. В этом документе также сформулированы семь принципов нулевого доверия:

1. Все источники данных и услуг считаются ресурсами. При этом в корпоративной сети предприятия могут работать устройства разного класса. Компания сами вправе классифицировать любые, включая персональные, устройства в качестве ресурсов, если эти устройства могут получить доступ к данным и услугам, принадлежащим предприятию.

2. Все коммуникации в корпоративной сети должны быть защищены вне зависимости от их местоположения. Доверие и безопасность не должны оценивать местоположение устройств или пользователей.

3. Доступ к отдельным корпоративным ресурсам предоставляется индивидуально для каждой сессии. Аутентификация и авторизация при доступе к одному ресурсу не дают доступа к другому ресурсу.

4. Доступ к ресурсам определяется реализуемой политикой информационной безопасности, при которой необходимо непрерывно контролировать наблюдаемое состояние идентификации клиента, приложений и других атрибутов.

5. Предприятие гарантирует максимальную безопасность всех принадлежащих ему устройств, непрерывно мониторит и контролирует свои активы, чтобы гарантировать их максимальную безопасность.

6. Все решения, обеспечивающие аутентификацию и авторизацию, являются динамическими, регулярно обновляемыми и строго контролируются. Решения реализуют полный цикл получения доступа, мониторинга и оценки угроз, адаптации, оценки и переоценки доверия к текущей связи. Предприятие должно иметь все необходимые системы управления учетными данными, активами и доступом, включая многофакторную аутентификацию.

7. Предприятие непрерывно собирает максимум информации о текущем состоянии корпоративной инфраструктуры и коммуникаций, которую в дальнейшем использует для повышения собственной информационной безопасности. Данные о сетевом трафике в корпоративной сети и запросах доступа также непрерывно собираются и анализируются с целью последующего совершенствования применяемой политики информационной безопасности.

Ведущие организации и специалисты в области обеспечения ИБ принимают эти принципы в рамках различных проектов [4,5]. На практике, однако, необходимо учитывать, что каждая организация должна проектировать и внедрять свою уникальную систему и принципы нулевого доверия в культуру своего предприятия [6].

Хотя потребности каждой организации уникальны, вполне возможно предложить следующие рекомендации по развитию и внедрению модели нулевого доверия:

1. Произведите аудит безопасности всей организации. Определите поверхность атаки и выявите, какие данные, активы, приложения и сервисы (DAAS, Device as a Service, рабочий стол как услуга) являются наиболее важными в её рамках. Определите и проверьте любую пользовательскую информацию, действующую в вашей организации, и удалите неработающие аккаунты, которые не использовались, например, более 30 дней, а также пересмотрите все привилегии в плане риска и последствий. Оцените имеющийся инструментарий по обеспечению информационной безопасности организации и выявите все "пробелы" и "зазоры" в инфраструктуре. Сделайте так, чтобы наиболее важным активам был дан самый высокий уровень защиты в рамках архитектуры безопасности.

2. Создайте каталог для всех активов и добавьте к нему схему потоков транзакций. Определите, где находится важная информация, и каким пользователям требуется доступ к ней. Рассмотрите, как различные компоненты DAAS взаимодействуют друг с другом и обеспечьте совместимость инструментов безопасного доступа между этими ресурсами. Знайте, сколько сервисных аккаунтов у вас имеется, где и когда им нужно подсоединяться. Пересмотрите все протоколы аутентификации и либо удалите, либо повысьте сложность подсоединения любой устаревшей или слабой системы (LDAP, NTLM). Получите список всех санкционированных облачных сервисов и допускайте доступ только к сервисам с низкой степенью риска. Рассмотрите возможность удаления неиспользуемых аккаунтов и внедрите обязательную ротацию паролей.

3. Установите самые разнообразные превентивные меры защиты, как минимум:

- многофакторную аутентификацию;

- принципы наименьших привилегий (каждый пользователь корпоративной сети должен иметь доступ только к тем данным, которые необходимы ему для выполнения своих служебных задач);

- микросегментацию (микроперимetры выполняют функции пограничного контроля в рамках системы, персональных данных или прав доступа, они предотвращают любое неавторизованное продвижение по корпоративной системе).

4. Непрерывно производите мониторинг сети, выявляйте, где происходит необычная активность, и отслеживайте динамику активностей вокруг. Непрерывно проверяйте, анализируйте и фиксируйте все траффики и все данные без какого-либо перерыва. Собирайте и храните аутентификационные логи по аномальному или подозрительному трафику и деятельности. Имейте чёткий план действия на случай обнаружения аномалий поведения сервисных аккаунтов и других важных ресурсов. Перед тем, как начать разработку и внедрение политики нулевого доверия в организации, необходимо изучить и оценить возможные трудности, с которыми уже сталкивались другие организации при внедрении нулевого доверия.

1. Старые приложения, старые сетевые ресурсы, старые аутентификационные протоколы, административные инструменты – всё это является частью корпоративной сети и операций действующей организации. Мейнфреймы (mainframe), системы подбора и управления персоналом, средства конфигурирования операционных систем, утилиты для удаленного выполнения команд часто стараются исключить из архитектуры нулевого доверия при ее внедрении в организации. В последние годы сотрудники, работающие из дома, стали значительно чаще использовать протокол удалённого рабочего стола (RDP), а набор практик DevOps (DEVelopment OPeration) требует дистанционного вызова процедур (RPC) от виртуальных машин и облачных инстанций во многих локациях. Все эти элементы являются важными инструментами для многих операций в обновляемой корпоративной сети (например, в аутентификационных протоколах типа LDAP и NTLM), но они требуются и для существующих (сохраняемых) устаревших систем.

Как правило, из-за высокой цены обновления устаревших систем упомянутые выше элементы остаются незащищенными верификацией. Часто устаревшие системы исключаются из нового проекта, основанного на принципах нулевого доверия, что делает их самым слабым звеном. В других случаях, команды, обеспечивающие ИБ, создают неудобства для пользователей, и, когда это возможно, запрещают использовать устаревшие или необновленные инструменты, что снижает производительность сотрудников организации. Инструменты адаптивного доступа (Adaptive Access Tools) или доступа при определенных условиях (Conditional Access Tools) могут расширить реализацию поэтапной аутентификации для старых систем через многофакторную аутентификацию или технологию единого входа (Single Sign-On, SSO), предлагая удобную работу, которая не будет мешать сотрудникам в их каждодневной деятельности.

2. Законодательство и стандарты до сих пор не включили в себя модель нулевого доверия, а это означает, что организация, которой требуется соответствовать определённым правилам, может испытывать трудности с прохождением аудита. Так, например, если стандарт безопасности данных индустрии платёжных карт (PCI-DSS) требует использование брандмауэров и сегментацию важных данных, то, как пройти аудит, если брандмауэры отсутствуют? Попадает ли вся новая архитектура информационной безопасности организации под действующее законодательство? Что подразумевает под сегментацией действующее законодательство, и насколько это соответствует определениям при реализации новой архитектуры нулевого доверия? Вполне возможно, что для успешного внедрения нулевого доверия придётся менять или редактировать действующие законы, стандарты и пр.

3. Аудит и тестирование на проникновение являются весьма значимой процедурой каждого директора по ИБ. Для оценки реальной эффективности новой системы нужны

также и проверки при активных действиях со стороны «условного противника», которые имитировали бы актуальные проблемы и инциденты в рамках реальной среды. Оперативные данные из популярных баз знаний по вирусам и вирусным атакам (например, из АСОИ ФинЦЕРТ Банка России) могут помочь организациям понять, что за крупные группировки нападают на них и их интересы, и какие шаги можно предпринять, чтобы минимизировать вред от потенциальных нападающих.

4. Видимость и контроль в сети – это часто один из основных факторов, бросающий вызов внедрению сетей нулевого доверия. У большинства организаций не имеется достаточных компетенций или реальной возможности на установку протоколов для всех сервисных аккаунтов, отдельных пользователей и привилегий для каждого в их сети. Поэтому они уязвимы перед угрозами, которые содержат устройства без регулярных обновлений (патчей), старые системы или пользователи с избыточными привилегиями и пользователи, чьи аккаунты не используются.

Все эти трудности лишь подчёркивают тот факт, что нам ещё предстоит долгий путь, прежде чем организации ИБ станут на 100% соответствовать концепции нулевого доверия. В ближайшее время, по-видимому, следует ожидать переход к гибридному подходу, который будет реализовывать в части инфраструктуры политику нулевого доверия, предоставляя другой части инфраструктуры возможность работать по старинке.

СПИСОК ЛИТЕРАТУРЫ

1. Zero Trust Adoption Report [Электронный ресурс]. URL: https://www.cybersecurity-insiders.com/portfolio/2019-zero-trust-adoption-report/ (дата обращения: 05.11.2021).
2. Малинский С.В. Пандемия COVID-19 повышает требования к информационной безопасности // Цифровые технологии и решения в сфере транспорта и образования: нац. науч. - практич. конф. (Москва, 19 ноября 2020 г.). Москва: Изд-во Белый ветер, 2020. С.95-111.
3. NIST Special Publication 800-207. Zero Trust Architecture [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата обращения: 05.11.2021).
4. Implementing a Zero Trust Architecture [Электронный ресурс]. URL: https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf (дата обращения: 17.11.2021).
5. Zero Trust Project - Use Cases [Электронный ресурс]. URL: https://www.actiac.org/zero-trust-project-use-cases (дата обращения: 17.11.2021).
6. NIST Announces Tech Collaborators on NCCoE Zero Trust Project [Электронный ресурс]. URL: https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/ (дата обращения: 17.11.2021).

Пономарёв К.Ю.
ТюмГУ, старший преподаватель
Захаров А. А.
ТюмГУ, заведующий кафедрой, д.т.н., профессор

ТЕЛЕМЕДИЦИНСКАЯ СИСТЕМА МОНИТОРИНГА ПОКАЗАТЕЛЕЙ ЖИЗНЕДЕЯТЕЛЬНОСТИ НА ОСНОВЕ ПРОТОКОЛОВ АТРИБУТИВНОГО КОНТРОЛЯ ДОСТУПА

Аннотация: Технологии Интернета вещей имеют широкое применение в сфере медицины и здравоохранения. Одной из основных проблем таких систем является безопасность данных пациентов, а именно: конфиденциальность пользовательских сведений при передаче по открытой сети и хранении в облачном хранилище. В статье рассматривается оригинальная методика защита на основании алгоритмов атрибутивных криптосистем. Предлагается модель платформы Интернета вещей и прикладные протоколы взаимодействия. Рассматривается прототип предлагаемого решения.

Ключевые слова: Интернет вещей, телемедицина, методы контроля доступа.

Введение. Технологии Интернета вещей (*Internet of Things, IoT*), как экосистемы автономных устройств, постепенно проникают во многие области человеческой деятельности. Например, в телемедицине они позволяют в автоматическом режиме проводить анализ показаний пациентов с различных диагностических устройств и информировать лечащих врачей при обнаружении отклонений показателей жизнедеятельности от установленной нормы [1].

При разработке и эксплуатации систем IoT пристальное внимание уделяется обеспечению информационной безопасности. Использование традиционных методов и алгоритмов, разработанных для построения современных Интернет-сервисов, ориентированных на взаимодействие с человеком, осложнено по многим причинам: децентрализованные архитектуры, гетерогенность элементов ИВ, слабые вычислительные мощности конечных устройств, масштабирование, большие объёмы информации, автономное поведение [2-4]. В связи с чем вектор атак гораздо более многообразен. К тому же возникают дополнительные проблемы защиты данных при взаимодействии «один-ко-многим»; зачастую в современных динамических системах круг субъектов доступа заранее неизвестен, его лишь можно описать неким набором правил. Более того актуальными являются вопросы конфиденциальности данных при их хранении в облачных системах и промежуточных узлах. Поэтому разработка новых средств обеспечения информационной безопасности для систем IoT, в том числе механизмов контроля доступа, является актуальной задачей [5-7].

Перспективным методом защиты данных для сетей Интернета вещей считаются модели атрибутивного контроля доступа и атрибутивные криптосистемы (*Attribute based encryption, ABE*). Они позволяют решить проблему защиты данных от облачного провайдера, детального контроля доступа [8]. В этих схемах структура доступа включена в шифртекст, а пользовательские ключи ассоциированы с неким набором атрибутов. Соответственно, пользователь может расшифровать сообщение тогда и только тогда, когда его ключевой набор атрибутов соответствует структуре доступа из сообщения.

Главный элемент таких схем - атрибутивный центр, ответственный за формирование криптографических ключей – как приватных пользовательских, так и открытых, необходимых для шифрования сообщений.

В научных публикациях было представлено большое количество криптографических схем ABE, обладающих самыми различными свойствами [9-12]. Большое количество работ посвящено применению ABE в телемедицинских системах [13-14]. Однако вопросы практического использования и интеграции разработанных моделей с существующими механизмами безопасности остаются слабо изученными. В связи с чем разработка прикладных протоколов и аппаратно-программных средств, использующих алгоритмы атрибутивного шифрования, является актуальной задачей.

В данной работе будет представлена модель платформы Интернета вещей для сбора и хранения показаний с устройств IoT. Будут представлены прикладные протоколы взаимодействия внутри платформы, которые обеспечивают защиту от угроз несанкционированного доступа.

Предлагаемая модель будет рассматриваться на примере системы сбора показаний ЭКГ с жителей юга Тюменской области. На данный момент по жителям Тюменской области отсутствует датасет электрокардиограмм с подробными численными показателями. Предлагаемая в работе платформы может использоваться как прототип, позволяющий удалённо собирать данные ЭКГ с пациентов в домашних стационарах, с целью их дальнейшей обработки в едином хранилище и определения риска сердечно-сосудистых заболеваний по представленными предикторам.

Теоретическая и практическая значимость. Разработанные методы и модели могут быть использовании при создании прикладных протоколов и архитектур систем Интернета вещей. Так как предложенные методы и алгоритмы могут использовать любую ABE схему атрибутивного шифрования, то с их применением увеличивается гибкость и вариативность в выборе схем для механизмов контроля доступа.

Программная архитектура платформы Интернета вещей. Далее будут представлены модель, протоколы и прототип для распределённой системы сбора данных с устройств Интернета вещей. Например, для системы мониторинга и сбора медицинских показателей с пациентов. Назначение системы заключается в автоматической обработке медицинских данных (ЭКГ), снятых с пациентов в медицинских учреждениях или домашнем стационаре. Данные будут поступать в облачные приложения, занимающиеся обработкой и хранением медицинских сведений. Специализированное программное обеспечение, использующее алгоритмы анализа данных и методы машинного обучения, будет искать отклонения в собранных медицинских показателях и, при необходимости, уведомлять об этом врачебный персонал и самого пациента.

Ключевая особенность протоколов заключается в том, что в рассматриваемой модели устройства сбора медицинских данных не обладают достаточными характеристиками для выполнения вычислительно сложных криптографических операций. Поэтому предлагается вынести операции шифрования в соответствующие облачные сервисы. Однако возникает проблема доступа шифровальных сервисов к данным пациентов: выполняя за устройства пациентов операции шифрования и имея соответствующий ключ атрибутивной криптосистемы, облачные сервисы могут скомпрометированы, и тогда злоумышленник от имени пациента сможет записать ложные данные или получить доступ к имеющимся. Для решения такой проблемы в системах, где

устройства Интернета вещей не могут выполнять тяжёлые криптографические операции, в научной литературе были предложены схемы атрибутивного шифрования на основе туманных вычислений. Однако их практическое применение весьма ограничено, так как каждая такая схема предлагает свой набор математических операций, из-за чего они не является взаимозаменяемыми, следовательно, практические реализации средств защиты будут сильно завязаны на конкретные схемы. Предлагаемые в этой главе протоколы не привязаны к конкретным схемам атрибутивного шифрования, могут оперировать практически с любыми из них.

Основными элементами модели являются:

- портативные диагностические устройства: считывают медицинские показатели пациентов, в их роли могут выступать, например, недорогие кардиомониторы;
- сервисы IoT: служат взаимодействия с конечными портативными устройствами, таких сервисов может быть несколько видов, т.к. диагностические устройства могут работать по разным протоколам;
- облачное хранилище и облачные сервисы: предоставляет интерфейс доступа к медицинским показателям пациентов, в рамках разрабатываемого прототипа предполагается хранение данных в облаке в зашифрованном виде;
- провайдер аутентификации: обеспечивает механизмы авторизации и аутентификации, имеет общий секретный ключ с каждым из пациентов, хранит сведения по пациентам и их портативным устройствам, а также политики доступа к записям пациентов;
- сервисы автоматизированной обработки: обращаются к облачным сервисам за сведениями по пациентам, предварительно пройдя процедуру проверки прав доступа, при необходимости и наличии доступа могут получать предыдущие записи из медицинской карты.

Представим процесс обработки медицинских показателей внутри предлагаемого прототипа.

1. Кардиомонитор или другие портативное устройство инициирует отправка данных в облаке через сервис IoT. Для этого они выполняют специализированный протокол записи вместе с провайдером аутентификации, на первом этапе этого протокола происходит аутентификация пользовательского устройства.

2. На втором этапе протокола записи происходит запись сведений в облачное хранилище. Сервис IoT предварительно выполняет процедуру шифрования, чтобы обеспечить конфиденциальность электронных медицинских карт при их хранении.

3. Сервисы IoT также отправляют уведомления для обработчиков, чтобы они могли в реальном времени начать обработку новых данных.

4. Получив сведения о новых медицинских записях, сервисы обработки инициируют запрос к облачным сервисам. Вместе с провайдером аутентификации они выполняют специализированный протокол чтения, целью которого является проверка прав доступа обработчиков к медицинским записям пациента.

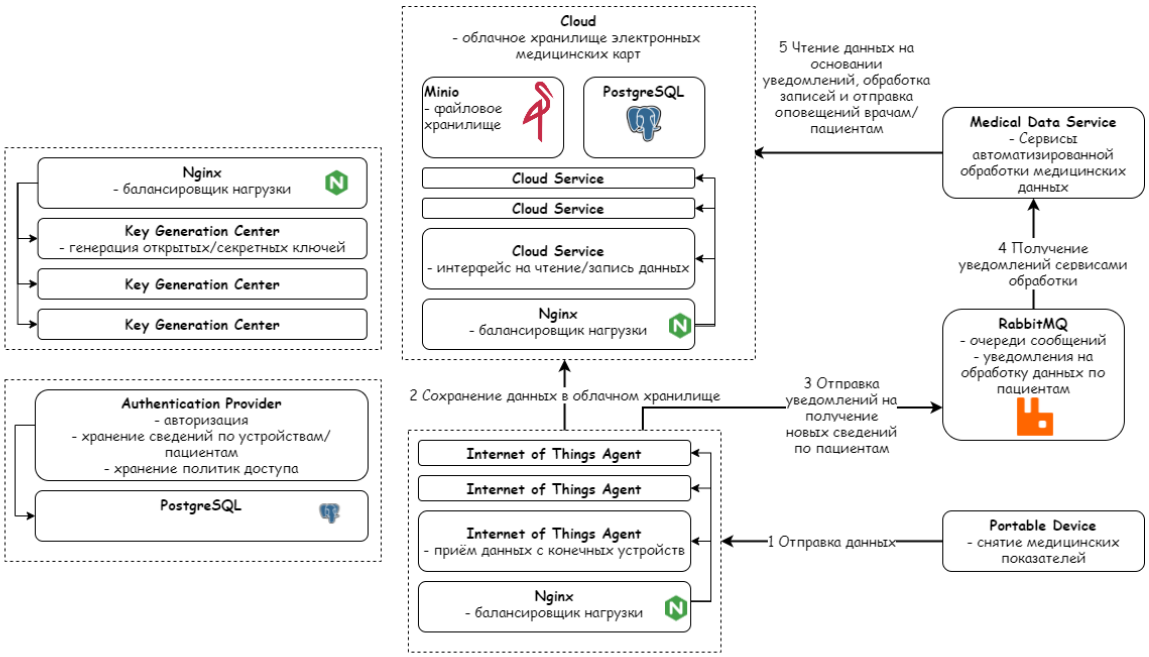


Рис. 1. Архитектура телемедицинской системы

5. Обработчики анализируют показатели с использованием методов анализа данных и машинного обучения, при наличии отклонений отправляют оповещения пациентам и их лечащим врачам.

Протоколы взаимодействия. Перечислим основные сущности предлагаемой модели защиты данных в телемедицинских системах. *Authentication Provider* (*AP*) - провайдер аутентификации, хранит список всех устройств пациентов, верифицирует запросы от устройств и генерирует токены на запись данных для других сервисов. Все основные данные по каждому медицинскому устройству, необходимые для функционировать провайдера, хранятся в следующей таблице:

- ID_P - идентификатор пациента;
- *K* - общий секретный ключ провайдера и пациента;
- *AS* (*Access Structure*) - структура доступа на запись сведений по пациенту;
- *DataList* - список метаданных по всем событиям записи данных пациента;
- Атрибутивный центр (*Attribute Authority*) - выполняет функции формирования общего открытого ключа и секретных ключей атрибутивной криптосистемы.
- Брокер или агент (*IoT Agent*) - непосредственно взаимодействует с медицинскими устройствами, принимает данные, выполняет процедуру шифрования и сохраняет данные в облачное хранилище.

Опишем протокол записи показателей в облачное хранилище.

$$D \rightarrow IoTA: ID_P \quad (1)$$

На первом шаге устройство инициирует протокол с брокером, отправляя ему идентификатор пациента.

$$IoTA \rightarrow D: R_D \quad (2)$$

В ответ брокер отдаёт случайный сессионный идентификатор.

$$D \rightarrow IoTA: T_D = H(H(data) \,||\, K \,||\, R_D \,||\, ID_P), data \quad (3)$$

Далее *D* формирует запрос, содержащий сами данные от пациента (*data*, его медицинские показатели, например, ЭКГ) и код аутентификации сообщения (*HMAC*), полученный с помощью общего секретного ключа с провайдером аутентификации.

$$IoTA \rightarrow AP: T_D, ID_P, R_D, H(data) \quad (4)$$

Брокер пересылает полученный токен к провайдеру аутентификации, добавив сведения о пациенте и сессионный идентификатор. *AP* проверяет токен (хэш-код аутентификации сообщения), если проверка не прошла - выполнение протокола прерывается. Если токен корректен: провайдер формирует собственный токен - подпись под хэшем данных от устройства и сессионным идентификатором. Также провайдер сохраняет сессионный идентификатор в соответствующем списке *DataList*.

$$AP \rightarrow IoTA: T_{AP} = S_{AP}(ID_P, R_D, H(data)), AS \quad (5)$$

Провайдер в ответ пересылает токен и структуру доступа к данным.

$$IoTA: CT = E_{ABE}(data, AS \cup R_D) \quad (6)$$

Агент устройств ИВ формирует шифртекст через выполнение операции шифрования схемы атрибутивного шифрования, используя для этого открытый мастер-ключ от атрибутивного центра и добавляя к структуре доступе случайный сессионный идентификатор. Добавление идентификатора к структуре доступа позволит отследить действия брокера. Если *IoTA* будет скомпрометирован злоумышленником, тогда он не сможет подделывать медицинские данные, так как наличие одинаковых сессионных идентификаторов вызовет подозрения. К тому же использование идентификаторов R_D и подписей к ним позволяет выполнять аутентификацию источника - злоумышленник не сможет подделать данные в облачном хранилище или создать новые.

$$IoTA \rightarrow Cloud: CT, ID_P, R_D \quad (7)$$

На финальном этапе брокер сохраняет данные в облачном хранилище и сигнализирует *D* об успешном окончании процедуры записи.

Далее опишем протокол чтения медицинских данных из облачного хранилища с целью дальнейшего их анализа. Пусть сервис автоматизированной обработки медицинских показателей *S* хочет прочитать данные по пациенту ID_P, представленные следующими переменными:

$$CT, R_D, AS, ID_P \quad (8)$$

Вначале сервис инициирует к атрибутивному центру запрос на секретный ключ схемы атрибутивного шифрования. В ответ он получает случайный идентификатор (R_{AA}),

который должен быть подписан провайдером аутентификации — это означает, что сервису может быть выдан ключ на запрашиваемую структуру доступа.

$$S -> AA: AS \cup R_D \quad (9)$$

$$AA -> R_{AA} \quad (10)$$

Сервис выполняет процедуру атрибутивного рукопожатия с провайдером аутентификации, для выполнения процедуры авторизации на доступ к данным пациента.

$$S -> AP: ID_P, R_D, R_{AA} \quad (11)$$

$$AP -> S: E_{ABE}(R_{AP}, AS) \quad (12)$$

Где R_{AP} - случайное число, зашифрованное под структурой доступа к данным пациента.

$$S -> AP: H(R_{AP} \,||\, R_D \,||\, ID_P \,||\, R_{AA}) \quad (13)$$

Сервис расшифровывает сообщение и отправляет значение R_{AP} обратно.

$$AP -> S: T_{AA} = S_{AP}(ID_P, R_D, R_{AA}) \quad (14)$$

Провайдер аутентификации проверяет хэш-код, только тот, кто владеет секретным ключом на структуру доступа AS может получить доступ к данным. Далее он формирует подпись под случайным числом от атрибутивного центра.

$$S -> AA: T_{AA} \quad (15)$$

$$AA -> S: K_{ABR} \quad (16)$$

Сервис пересылает токен в атрибутивный центр. В ответ он получает приватный ключ схемы атрибутивного шифрования, позволяющий ему расшифровать сообщение со структурой доступа $AS \cup R_D$.

Прототип. В рамках исследования был описан прототип системы сбора медицинских показаний и хранилища информации для анализа рисков ишемических болезней сердца по пациентам Тюменской области. В проекте будут использоваться персональные электрокардиографы CardioQVARK (https://cardioqvark.ru/). Они позволяют отслеживать динамику состояния сердца и собирать такие сведения, как расчёт RR, P, PR, QRS, QT, параметры ВСР, разметка аритмии, артериальное давление. Разработчики предоставляют программный интерфейс (*API*) для медицинских организаций, позволяющий загрузить данные по конкретными кардиомониторам и пациентам для дальнейшего анализа на собственных вычислительных мощностях. Пример работы с кардиомониторами приведён в репозитории - https://github.com/drmckay-kirill/EHealth.

В качестве источника данных будут выступать не диагностические устройства напрямую, а программные средства, забирающие ЭКГ через API системы CardioQVARK. Они будут хранить список идентификаторов пациентов и электрокардиографов, в фоновом режиме запрашивать сведения из API внешней системы и далее по описанному ранее алгоритму производить процедуры записи данных в облачное хранилище.

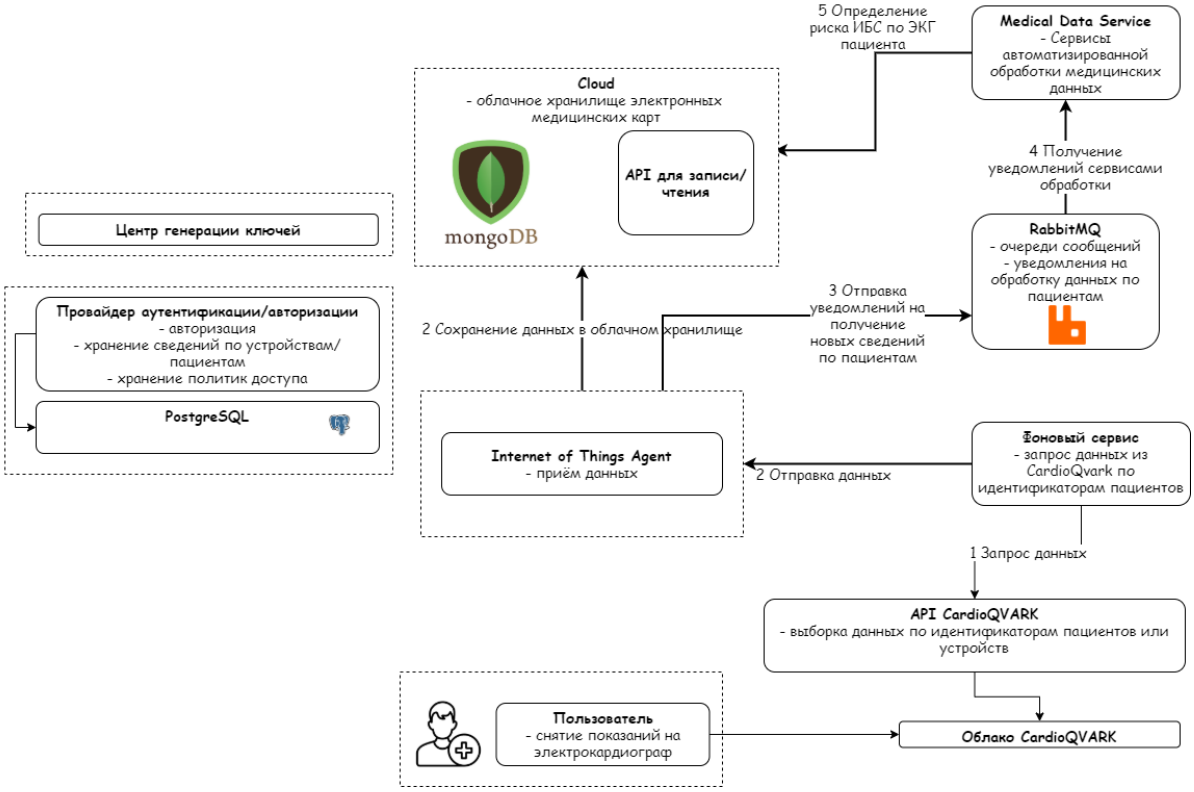


Рис. 2. Прототип телемедицинской системы

Заключение. Были предложены модель платформы Интернета вещей и прикладные протоколы взаимодействия для элементов платформы. Для обеспечения безопасности при хранении и обработке данных были использованы алгоритмы атрибутивного шифрования. Для работы с устройствами Интернета вещей, обладающими слабыми вычислительными мощностями, криптографические процедуры были вынесены в облачные сервисы. Данная модель может быть использована при работе телемедицинских систем. Был представлен прототип хранилища информации для анализа рисков и выявления предикторов болезней сердца по пациентам Тюменской области.

СПИСОК ЛИТЕРАТУРЫ

1. Guizani K., Guizani S. IoT Healthcare Monitoring Systems Overview for Elderly Population //2020 International Wireless Communications and Mobile Computing (IWCMC). – IEEE, 2020. – С. 2005-2009.
2. La Manna M. et al. Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update //Sensors. – 2021. – Т. 21. – №. 2. – С. 515.
3. Yang Y. et al. A Novel Attribute-Based Encryption Approach with Integrity Verification for CAD Assembly Models //Engineering. – 2021.

4. Meng F., Cheng L., Wang M. Ciphertext-policy attribute-based encryption with hidden sensitive policy from keyword search techniques in smart city //EURASIP Journal on Wireless Communications and Networking. – 2021. – Т. 2021. – №. 1. – С. 1-22.
5. Li H. et al. An efficient ciphertext-policy weighted attribute-based encryption for the Internet of health things //IEEE Journal of Biomedical and Health Informatics. – 2021.
6. Шабрина С. А., Аминова А. Информационная безопасность облачных вычислений в здравоохранении //Высокие технологии, наука и образование: актуальные вопросы, достижения и инновации. – 2021. – С. 52-54.
7. Zhang Y. et al. Attribute-based encryption for cloud computing access control: A survey //ACM Computing Surveys (CSUR). – 2020. – Т. 53. – №. 4. – С. 1-41.
8. Козлов А. С., Дудник С. В., Култазин Н. М. Система поиска по образцам кодовых последовательностей для «Интернета вещей» и «Интернета всего» //Наука, техника и образование. – 2020. – №. 10 (74).
9. Meng F. et al. ABDKS: attribute-based encryption with dynamic keyword search in fog computing //Frontiers Comput. Sci. – 2021. – Т. 15. – №. 5. – С. 155810.
10. El Gafif H., Toumanari A. Efficient Ciphertext-Policy Attribute-Based Encryption Constructions with Outsourced Encryption and Decryption //Security and Communication Networks. – 2021. – Т. 2021.
11. Han D., Pan N., Li K. C. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection //IEEE Transactions on Dependable and Secure Computing. – 2020.
12. Cui H. et al. Key regeneration-free ciphertext-policy attribute-based encryption and its application //Information Sciences. – 2020. – Т. 517. – С. 217-229.
13. Zeng P. et al. Efficient Policy-Hiding and Large Universe Attribute-Based Encryption with Public Traceability for Internet of Medical Things //IEEE Internet of Things Journal. – 2021.
14. Lin H. Y., Jiang Y. R. A Multi-User Ciphertext Policy Attribute-Based Encryption Scheme with Keyword Search for Medical Cloud System //Applied Sciences. – 2021. – Т. 11. – №. 1. – С. 63.

Спирин А.А.
Академия ФСО России, сотрудник
spirin_aa@bk.ru

ЗАЩИТА ОТ УТЕЧКИ ИНФОРМАЦИИ НА ОСНОВЕ РАЗДЕЛЕНИЯ ЗАШИФРОВАННЫХ И СЖАТЫХ ДАННЫХ

Информационно-аналитические агентства выявляют устойчивый рост количества утечек конфиденциальных данных. Согласно отчету экспертно-аналитического центра ГК Infowatch в 2020 году в России около 79% зафиксированных утечек произошли по вине внутреннего нарушителя, 77% из них являлись умышленными. Одной из наиболее частых причин возрастающего количества утечек защищаемых данных является наличие внутреннего нарушителя, способного осуществлять передачу чувствительной информации за периметр организации, обходя существующие механизмы защиты.

Для защиты информации от внутренних нарушителей применяют средства обнаружения и предотвращения утечек информации, использующие поиск цифровых сигнатур и слепков, регулярных выражений, алгоритмы машинного обучения и поведенческие подходы. Однако существующие средства не способны с высокой точностью обнаружить передачу зашифрованных или сжатых данных в виду их статистической схожести и высокой энтропии, кроме того существующие механизмы классификации используют заголовки контейнеров файлов, содержащих в себе цифровые сигнатуры [1-3]. Данный факт позволяет нарушителю обходить существующие механизмы анализа файлов в DLP-системах, например, посредством замены сигнатур на неизвестные значения с дальнейшим их восстановлением.

Таким образом, была обнаружена практическая проблема – низкая точность классификации зашифрованных и сжатых данных без учета цифровых сигнатур и заголовочных частей файлов [4-5].

Модель угроз и модель внутреннего нарушителя в корпоративной сети представлены ниже (Рис. 1).

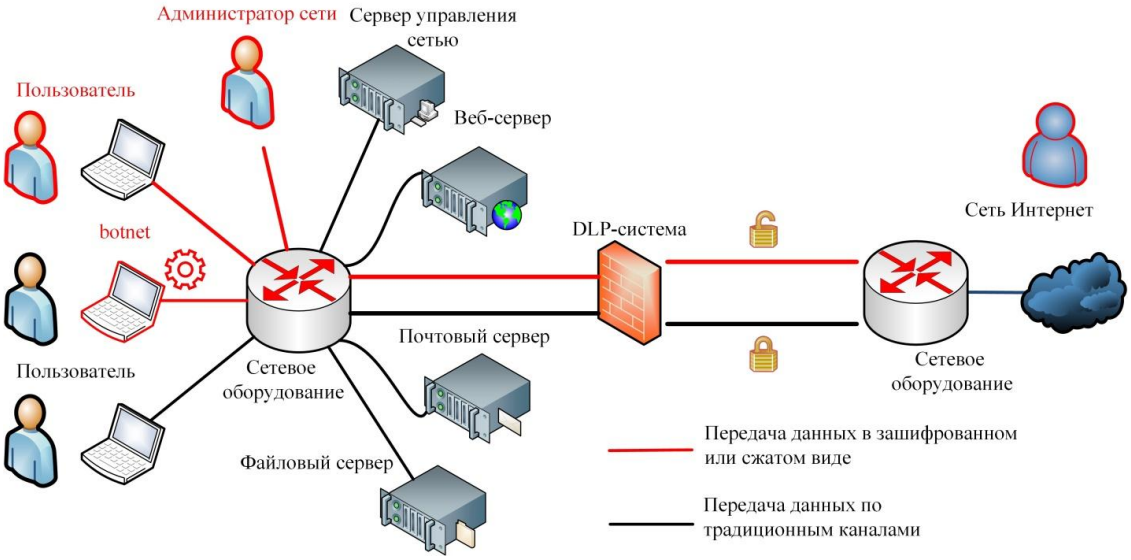


Рис. 1. Модель угроз и модель внутреннего нарушителя

Внутренним нарушителем может являться персонал: привилегированный или обладающий стандартными правами; технические устройства, зараженные внутренним пользователем умышленно или внешним злоумышленником. Угроза информации может быть реализована посредством зашифрования защищаемой информации и её передачей за контролируемый периметр организации. Учитывая обнаруженный недостаток существующих методов классификации зашифрованных и сжатых необходимо разработать механизмы повышения точности классификации зашифрованных и сжатых данных.

Для решения обнаруженной проблемы было принято решение сформировать модель псевдослучайных последовательностей (ПСП), т.е. последовательностей обладающих высокой энтропией и проходящих статистические тесты NIST на случайность. Разработка модели позволит учесть характеристические свойства указанных последовательностей и на основании них разработать алгоритм классификации зашифрованных и сжатых данных.

Для проведения исследований была сформирована выборка, состоящая из 2000 файлов, содержащих осмысленный текст. Далее было сформировано две группы файлов: зашифрованные (OpenSSL: AES, 3DES, Camellia, RC4 и ГОСТ 34.12 «Кузнечик» в режиме простой замены) и сжатые (WinRAR: RAR, ZIP и 7Zip: 7Z, XZ, GZ, BZ2). Размер файлов в полученной выборке составил 600 кбайт, а общее количество элементов возросло до 22000.

В работе [6] авторы сделали вывод о необходимости удаления заголовков файлов, так как они содержат цифровые сигнатуры, позволяющие классифицировать тип данных с высокой точностью. При проведении экспериментов по построению модели ПСП с целью исключить влияние заголовков файлов и цифровых сигнатур на процедуру классификации были отброшены первые 10 кбайт файлов из сформированной выборки.

На первом этапе построения модели ПСП сформировано распределение байт в последовательностях двух классов, нормированных по среднему значению частоты встречаемости байт в выборке файлов (Рис. 2).

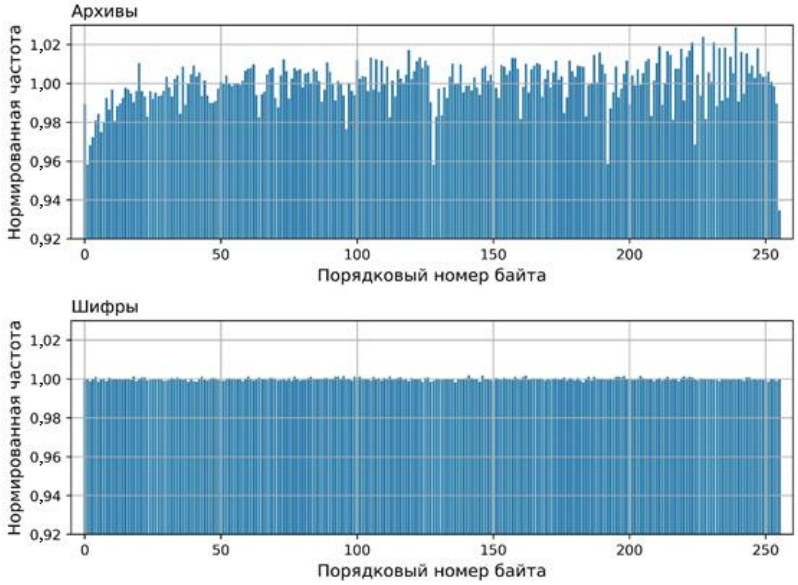


Рис. 2. Распределение байт для зашифрованных и сжатых последовательностей

Признаковое пространство на основе распределения байт может быть представлено выражением (1):

$$V_{Bytes} = F\left(b_i\right), i \in 0,\ldots,255, \tag{1}$$

где $F\left(b_i\right)$ – значение частоты появления байта i анализируемой ПСП.

Результаты экспериментов по определению точности классификации зашифрованных и сжатых последовательностей различными алгоритмами машинного обучения при использовании признаков на основе значений частот распределения байт были получены в программной среде Python (2).

$$\begin{cases} Acc_{RF}\left(V_{Bytes}\right) = F\left(V_{Bytes}\right) = 0,9 \\ Acc_{DT}\left(V_{Bytes}\right) = F\left(V_{Bytes}\right) = 0,88 \\ Acc_{kNN}\left(V_{Bytes}\right) = F\left(V_{Bytes}\right) = 0,89 \end{cases}, \tag{2}$$

где V_{Bytes} – признаковое пространство (1), $Acc_{RF,DT,kNN}$ – метрики «точность классификации» ПСП соответствующим алгоритмом машинного обучения.

Полученные результаты позволяют построить классификатор зашифрованных и сжатых последовательностей, однако точность классификации недостаточно высока. Распределение байт для данных, обладающих высокой энтропией, например для зашифрованных и сжатых данных, подчиняется равномерному закону распределения. В литературе встречаются исследования, приводящие к выводу о невозможности классификации зашифрованных и сжатых данных с высокой точностью при использовании распределения байт [7], что объясняется другой предметной областью исследования, связанной с обнаружением вредоносного ПО, где размеры анализируемых данных недостаточно велики.

В некоторых работах [8] применяются статистические тесты NIST для извлечения признаков из анализируемых данных.

Далее для построения модели ПСП были использованы статистические тесты NIST. Элементами модели являлись значения p-value, полученные в результате прохождения статистических тестов, диаграмма размаха полученных средних значений p-value (Рис. 3).

В результате было установлено, при уровне значимости α=0,05 100% зашифрованных последовательностей прошли все тесты на случайность, а сжатые последовательности – 98%. На основании выявленных закономерностей (схожие значения энтропии, прохождение тестов NIST на случайность) было принято решение обозначить зашифрованные и сжатые последовательности как псевдослучайные.

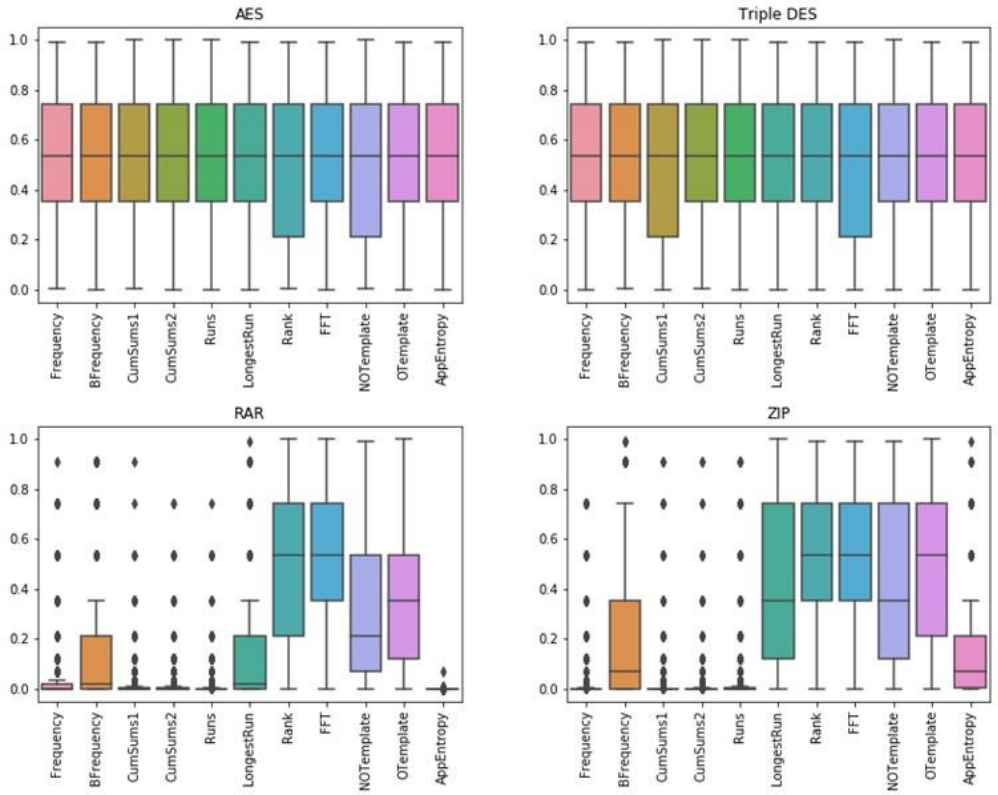


Рис. 3. Диаграммы размаха значений p-value тестов NIST для различных типов ПСП

Таким образом, модель ПСП на основе распределений значений p-value тестов NIST представляет собой усредненные значения p-value, полученные в результате выполнения 11 статистических тестов: частотный побитовый p_{freq}, блочный частотный p_{Bfreq}, тесты кумулятивных сумм p_{CS1}, p_{CS2}, тест на последовательность одинаковых бит p_{Runs}, тест на самую длинную последовательность единиц в блоке p_{LRuns}, тест рангов бинарных матриц p_{Rank}, спектральный тест p_{FFT}, тест на обнаружение неперекрывающихся шаблонов p_{NOT}, тест на обнаружение перекрывающихся шаблонов p_{OT}, тест приблизительной энтропии шаблонов p_{AEnt}. Таким образом, признаковое пространство на основе тестов NIST является вектором, определяемым выражением 6:

$$V_{NIST} = \left\langle \begin{matrix} p_{freq}, p_{Bfreq}, p_{CS1}, p_{CS2}, p_{Runs}, \\ p_{LRuns}, p_{Rank}, p_{FFT}, p_{NOT}, p_{OT}, p_{AEnt} \end{matrix} \right\rangle, \quad (3)$$

где: p_i – средние значения p-value по выборке данных для соответствующих тестов NIST.

Для оценки применимости признакового пространства на основе выполнения тестов NIST были проведены эксперименты (Табл. 1).

Табл. 1. Оценка точности классификации алгоритмами машинного обучения при использовании модели ПСП на основе тестов NIST

Алгоритм	**Accuracy**
Random Forest	0,643
Decision Tree	0,575
kNN	0,684

При использовании модели на основе тестов NIST точность классификации ПСП по сравнению с моделью на основе распределения байт значительно ухудшилась. Данный факт объясняется тем, что тесты NIST направлены на обнаружение закономерностей в анализируемых последовательностях, проверку их на случайность возникновения символов.

Кроме того, процедура тестирования предполагает получение результатов в 10 возможных интервалах и вычислении p-value на основе табличных значений (критерий Хи-квадрат и равномерное распределение), что стирает статистические различия между рассматриваемыми ПСП, но позволяет оценить гипотезу о случайности анализируемых данных.

В статистических тестах NIST присутствует тест на проверку непересекающихся шаблонов. Методика тестирования предполагает разбиение анализируемой последовательности на N блоков данных длиной M бит и поиска в них бинарных шаблонов длиной m бит (подпоследовательностей). В случае обнаружения подпоследовательности его частота увеличивается на 1, и окно поиска сдвигается на следующий бит после последнего бита найденного шаблона. Для подтверждения гипотезы о случайности последовательности вычисляются математическое ожидание и дисперсия (7) частоты встречаемости шаблонов в теоретически случайном распределении.

$$\mu = \frac{M-m+1}{2^m}, \sigma^2 = M * \left(\frac{1}{2^m} - \frac{2m-1}{2^{2m}} \right) * \frac{M-m+1}{2^m}, \tag{7}$$

где μ – математическое ожидание частоты встречаемости шаблона длиной m бит в теоретически случайной последовательности, разделенной на M блоков данных.

Итоговое решение о прохождении теста принимается на основе вычисленного значения $p-value$ согласно неполной гамме-функции (8).

$$p-value = igamc\left(\frac{N}{2}, \frac{\chi^2_{obs}}{2} \right), \tag{8}$$

где $igamc$ – неполная гамма-функция.

Неполная гамма-функция в общем виде определяется выражением (9):

$$Q(\alpha, x) = 1 - P(\alpha, x) = \frac{\Gamma(\alpha, x)}{\Gamma(\alpha)} = \frac{1}{\Gamma(\alpha)} \int_x^{\infty} e^{-t} t^{\alpha-1} dt, \tag{9}$$

где $Q(\alpha, 0) = 1$ и $Q(\alpha, \infty) = 0$.

Если значение $p-value$ больше, чем выбранный порог α, то принимается решение о подтверждении нулевой гипотезы и анализируемая последовательность считается случайной с уровнем доверия, определяемым выбранным пороговым значением α. В противном случае нулевая гипотеза отвергается и последовательность считается неслучайной. Тест предназначен для тестирования последовательностей длиной не менее 10^6 бит, что составляет примерно 122 кбайт. В описании теста указано, что длина шаблонов должна быть 9 или 10 бит, количество блоков длины M бит $N \le 100$. Длина каждого блока задана в процедуре тестирования и равняется значению 131072. При использовании другого значения должны соблюдаться условия $M \ge 0,01 * n$ и $N = \left\lfloor \frac{n}{M} \right\rfloor$. Данные условия необходимы для обеспечения статистической значимости получаемых значений $p-value$.

В описании теста не указана причина использования подпоследовательностей длины 9 и 10 бит, кроме того, на их использование наложены достаточно жесткие ограничения в виде разделения подпоследовательности на определенное количество блоков определенной длины.

На основании данного теста была выдвинута гипотеза о возможности построения модели ПСП с использованием частот встречаемости подпоследовательностей ограниченной длины N бит.

Для проверки гипотезы и выявления статистических особенностей в анализируемых ПСП были проведены эксперименты по подсчету частот встречаемости подпоследовательностей различной длины $N = [4, \text{K}, 11]$ бит без перекрытия. При их обнаружении дальнейший подсчёт начинается со следующего бита после последнего бита подпоследовательности, если же совпадение не обнаружено, то происходит смещение на 1 бит. Подсчет частот встречаемости подпоследовательностей был выполнен согласно выражению (10):

$$f_j = F(j) = \frac{n(j)}{(M - N(j) + 1)}, j \in \{0, \ldots, 2^N\}, \quad (10)$$

где f_j – частота встречаемости подпоследовательности j в анализируемой ПСП; $n(j)$ – количество вхождений подпоследовательности j в анализируемую ПСП; M – длина анализируемой ПСП в битах; $N(j)$ – длина подпоследовательности j в битах.

Данный подход, в отличие от статистических тестов NIST, где используются только непериодические шаблоны определенной длины, позволит проверить все возможные подпоследовательности и определить их дискриминирующую способность [9]. Внедрение в разрабатываемую модель периодических последовательностей не достаточно обосновано с точки зрения статистических критериев на проверку случайности, однако имеет рациональное объяснение с точки зрения получения признаков, характеризующих конкретный класс ПСП.

Таким образом, модель ПСП представляет собой вектор статистических характеристик, определяемый выражением (11):

$$V = \left(f_j, \ldots, f_{2^N}, b_0, \ldots, b_{255}, B_{mean}, B_{sko}, b_{min}, b_{max} \right), \quad (11)$$

где B_{mean} – среднее значение, B_{sko} – среднеквадратическое отклонение, b_{min} – минимальное, b_{max} – максимальные значения количества байт в ПСП.

Оценка точности классификации зашифрованных и сжатых данных на основе разработанной модели ПСП (Табл. 2) позволяет сделать вывод о повышении точности классификации [10].

Табл. 2. Оценка точности классификации алгоритмами машинного обучения при использовании модели ПСП на основе тестов NIST

Алгоритм	**Accuracy**
Random Forest+Decision Tree	0,97
Decision Tree	0,92
kNN	0,91

Для оценки влияния количества признаков, используемых в модели ПСП, на точность классификации были проведены эксперименты (Рис. 6).

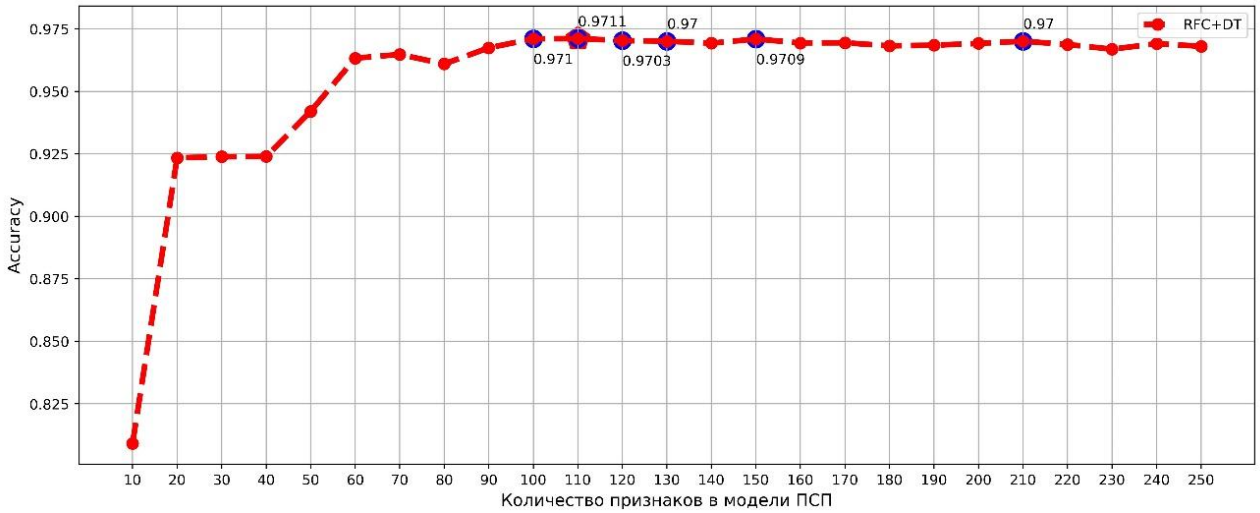


Рис. 6. Оценка влияния количества признаков в модели ПСП на точность классификации

Наибольшая точность классификации была достигнута при использовании 110 признаков, однако точность классификации при 100 признаках меньше на 0,0001 пункт, а с ростом их количества в модели линейно увеличивается время выполнения процедуры извлечения признаков и классификации. Таким образом, на основе применения разработанного алгоритма классификации ПСП, учитывающего веса признаков и редуцирующего наименее значимые, был получен классификатор ПСП, достигающий точности классификации ПСП в 0,97.

СПИСОК ЛИТЕРАТУРЫ

1. Srinivas, M. Forged File Detection and Steganographic content Identification (FFDASCI) using Deep Learning Techniques / M. Srinivas, A. Nayak, A. Bhatt // In CLEF (Working Notes). – 2019. http://ceur-ws.org/Vol-2380/paper_142.pdf
2. Konaray, S. K. Detecting File Types Using Machine Learning Algorithms / S.K. Konaray, A. Toprak, G.M. Pek, H. Akçekoce, D. Kılınç // Innovations in Intelligent Systems and Applications Conference (ASYU). – 2019. – pp. 1–4. DOI: 10.1109/ASYU48272.2019.8946393.
3. Karampidis, K. File type identification-computational intelligence for digital forensics / K. Karampidis, G. Papadourakis, // Journal of Digital Forensics, Security and Law. – 2017. – vol. 12, no. 2. – p. 6. DOI: https://doi.org/10.15394/jdfsl.2017.1472.
4. De Gaspari F., Hitaj D., Pagnotta G., De Carli L., Mancini L. V. EnCoD: Distinguishing Compressed and Encrypted File Fragments // International Conference on Network and System Security, Springer, Cham, 2020, pp. 42-62. DOI: https://doi.org/10.1007/978-3-030-65745-1_3.
5. Mousavi S. S. Detecting Disk Sectors Data Types Using Hidden Markov Model // 17th International ISC Conference on Information Security and Cryptology (ISCISC), 2020, pp. 60-64. DOI: 10.1109/ISCISC51277.2020.9261906.
6. Scaife, N. Cryptolock (and drop it): stopping ransomware attacks on user data / N. Scaife, H. Carter, P. Traynor, K.R. Butler // 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), – 2016. – pp. 303–312. DOI: 10.1109/ICDCS.2016.46.
7. Raff, E. An investigation of byte n-gram features for malware classification. / E. Raff, R. Zak, R. Cox, J. Sylvester, P. Yacci, R. Ward, C. Nicholas // Journal of Computer Virology and Hacking Techniques. – 2018. – vol. 14, no. 1. –pp. 1–20. DOI: https://doi.org/10.1007/s11416-016-0283-1.
8. Casino, F. Hedge: Efficient traffic classification of encrypted and compressed packets / F. Casino, K.K.R. Choo, C. Patsakis // IEEE Transactions on Information Forensics and Security. – 2019. – vol. 14, no.11. – pp. 2916-2926. DOI: 10.1109/TIFS.2019.2911156.
9. Козачок, А.В. Алгоритм классификации псевдослучайных последовательностей / А.В. Козачок, А.А. Спирин // Вестник ВГУ. Серия: Системный анализ и информационные технологии. – 2020. – № 1. – С. 87–98. DOI: https://doi.org/10.17308/sait.2020.1/2595.
10. Козачок, А.В. Алгоритм классификации псевдослучайных последовательностей на основе построения случайного леса / А.В. Козачок, А.А. Спирин, О.М Голембиовская // Доклады Томского государственного университета систем управления и электроники. – 2020. – Т. 23. – № 3. – С. 55–60. DOI**:** 10.21293/1818-0442-2020-23-3-55-60.

Дикий Д.И.
ИТМО, инженер, к.т.н.,
dimandikiy@mai.ru

ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ, ИСПОЛЬЗУЮЩИХ МОДЕЛЬ «ИЗДАТЕЛЬ-ПОДПИСЧИК»

Введение. Развитие современных технологий привело к появлению полностью и частично автоматизированных систем. Одной из ветвей их развития является концепция Интернет вещей [1]. Она состоит в использовании множества небольших устройств, которые считывают информацию об окружающей среде, обрабатывают ее, передают, хранят либо выполняют какие-либо атомарные функции и операции. Наряду с этим популярной становится идея использования микросервисной архитектуры [2], где нагрузка выполнения трудоемких задач распределена между множеством серверов. Чтобы нагрузка равномерно распределялась, используются балансировщики, а взаимодействие между серверами происходит по модели издатель-подписчик. Однако, несмотря на все преимущества ранее описанного подхода, стоит обратить внимание на аспекты информационной безопасности. Ведь наряду с задачей передачи информации к системе передачи также предъявляются требования по экономичности.

Анализ аспектов безопасности.

Общедоступный специализированный узел сети, который отвечает за логистику сообщений называется шлюзом или брокером (рис. 1.). Как правило, это сервер на одной из широко распространенных операционных систем с открытыми соответствующими портами для приема и передачи сообщений.

Рис. 1. Основные этапы модели «издатель-подписчик»: А) установление соединения между устройством и шлюзом, Б) подписка устройства на тему, В) публикация сообщения.

При анализе модели издатель-подписчик была выявлена угроза DoS атаки сообщениями для установления соединения со шлюзом прикладного уровня. [3]. Вторым направлением исследования является разработка модели оценки рисков для сетей издатель-подписчик, в которых реализовано управление доступом, как, например, представлено в работе [4].

Аутентификация.

Согласно результатам, полученным в ходе анализа модели «издатель-подписчик», важной уязвимостью этой модели является аутентификация устройств. Как представлено в работах [5-9], для защищенной аутентификации предлагается использовать протокол TLS между устройствами и шлюзом, использующий алгоритмы Диффи-Хеллмана (DH [10] или ECDH [11]) и симметричного или асимметричного алгоритма шифрования, например, AES, RSA, ChaCha20 и хэш-функции, например, SHA256 [12].

В качестве альтернативного подхода к уже рассмотренным алгоритмам аутентификации было предложено использовать подход «Zero knowledge» - алгоритмы без разглашения (англ.).

Одним из направлений применения не интерактивных алгоритмов «Zero knowledge» является вектор, разработанный Шнорром для организации подписи [13] и аутентификации. В работе [14] представлена модификация протокола Шнорра и Окамото с применением криптографии на эллиптических кривых, а также дана сводная таблица развития протоколов аутентификации, основанных на тех же принципах.

Разработанный в рамках данного исследования алгоритм аутентификации рассмотрен в [15]. Для сравнения предлагаемого алгоритма с протоколом TLS была собрана экспериментальная установка (рис. 2).

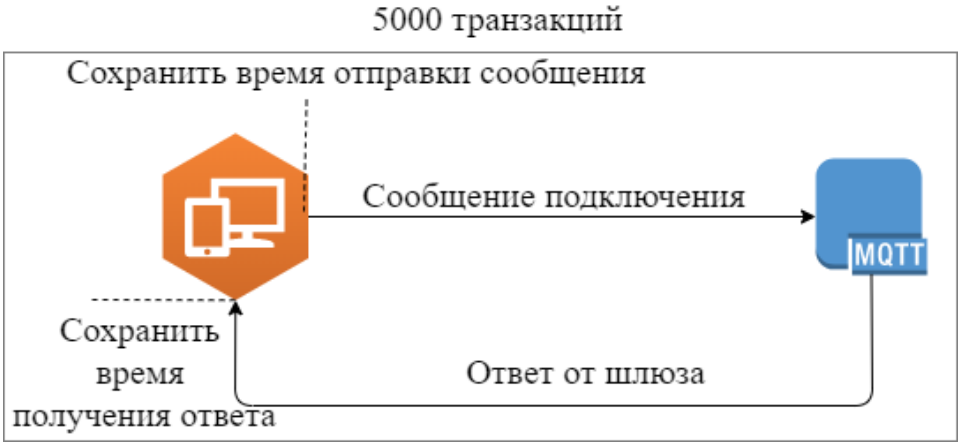


Рис. 2. Схема экспериментальной установки для проведения сравнения

В ходе эксперимента были получены статистические параметры времени подключения конечного устройства к шлюзу в зависимости от используемого алгоритма аутентификации. Данные представлены в таблице 1 и рисунке 3.

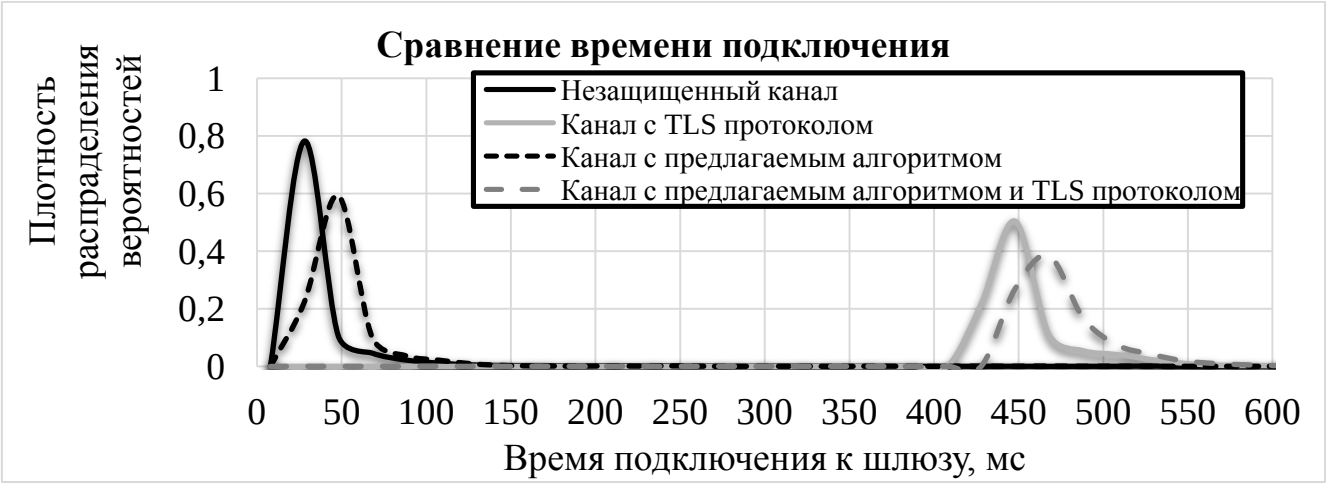


Рис. 3. Сравнение времени, потраченного на подключение по открытым и защищенным каналам.

Табл. 1. Сравнение статистических данных о времени аутентификации по открытым и защищенным каналам.

Параметр	Тип алгоритма			
	Открытый канал	TLS протокол	Предлагаемый алгоритм	Предлагаемый алгоритм и TLS протокол
Минимальное время подключения, мс	8	415	19	421
Максимальное время подключения, мс	3015	3438	1978	4659
Среднее время подключения, мс	36.2	460.0	45.7	480.7
Среднеквадратичное отклонение времени подключения	104.1	121.8	71.1	156.4

Согласно результатам эксперимента, аутентификация по небезопасному каналу является самой быстрой, но в то же время имеет не наименьшее среднеквадратичное отклонение. При использовании протокола TLS процесс аутентификации значительно замедляется. Таким образом, среднее время подключения устройства к шлюзу примерно в 12 раз медленнее, чем по открытому каналу и занимает около полсекунды. Предложенный алгоритм имеет более высокую скорость выполнения, чем протокол TLS. Например, среднее время соединения относительно аутентификации по открытому каналу, примерно в полтора раза медленнее (60% соединений заняло менее 50 мс) и примерно в десять раз быстрее, чем через протокол TLS. Однако предлагаемый алгоритм имеет меньшие значения дисперсии и среднеквадратичного отклонения. Использование обоих механизмов безопасности одновременно во время аутентификации дало худшие результаты.

Модель расчета рисков.

Использование модели «издатель-подписчик» позволяет перейти к новой методике оценки рисков. Ключевым элементом является ценность информации, помеченной темой. Таким образом, можно более детально оценить риски при реализации той или иной угрозы в отношении устройств и инфраструктуры сети Интернет вещей.

Производится группировка имеющихся объектов сети Интернет вещей на четыре класса: оконечные устройства (*M*), шлюзы (*N*), коммуникационное оборудование (*C*), облачные приложения и центры обработки данных и администрирования (*E*).

Для оценки рисков на первом этапе определяется ценность информации, которая передается под той или иной темой. Обозначим S_i, как ценность информации *i*-ой темы из всего множества тем *I*. Для каждой *j*-ой угрозы *y* определяется вероятность ее реализации $P(y_j)$ в отношении каждого оконечного устройства из класса *M*. Таким образом, каждому устройству m_k будет сопоставлена вероятность реализации y_j-ой угрозы, как $P(y_{jm_k})$. Данные шаги можно наглядно представить в табличной форме (таблица 2).

Табл. 2. Табличное представление вероятностей реализаций угроз для оконечных устройств Интернет вещей.

Угрозы	Устройства			
	m_1	m_2	$m_{...}$	m_K
y_1	$P(y_{1m_1})$	$P(y_{1m_2})$	$P(y_{1m_{...}})$	$P(y_{1m_K})$
y_2	$P(y_{2m_1})$	$P(y_{2m_2})$	$P(y_{2m_{...}})$	$P(y_{2m_K})$
$y_{...}$	$P(y_{...m_1})$	$P(y_{...m_2})$	$P(y_{...m_{...}})$	$P(y_{...m_K})$
y_J	$P(y_{Jm_1})$	$P(y_{Jm_2})$	$P(y_{Jm_{...}})$	$P(y_{Jm_K})$

Для каждой *i*-ой темы определяется перечень устройств $G_i \in M$, на которых обрабатываются, передаются или генерируются сообщения этой темы. Среди всех устройств множества G_i, определяется максимальная вероятность реализации y_j-ой угрозы в отношении *i*-ой темы:

$$P(y_{ji}) = \max\left(P(y_{jm_k})\right), \textit{если } m_k \in G_i \quad (1)$$

Значение риска информационной безопасности от реализации y_j-ой угрозы в отношении *i*-ой темы будет вычисляться следующим образом:

$$R_{ji} = P(y_{ji}) \times S_i \quad (2)$$

А итоговое значение риска от реализации y_j-ой угрозы на слое оконечных устройств можно представить, как сумму R_{ji}:

$$R_j = \sum_{i=1}^{I} R_{ji} \quad (3)$$

На сетевом уровне предлагаемой модели рисков для шлюзов (устройств из множества *N*) расчет рисков производится аналогично. Присутствует лишь одно большое отличие. Если шлюз единственный в сети «издатель-подписчик», то вычисления значения рисков значительно упрощаются, исходя из того предположения, что шлюз обрабатывает все существующие темы. Тогда расчет рисков можно представить в следующем виде:

$$R_j = P(y_{jn_1}) \times \sum_{i=1}^{I} S_i \quad (4)$$

Так как современные сети Интернет вещей построены на проводных и беспроводных технологиях, то для устройств класса *C*, могут отличаться актуальные угрозы. Беспроводные средства связи реализованы на иных физических принципах по сравнению с проводными, что, несомненно, влияет на перечень рассматриваемых угроз.

Предполагается, что устройства из этого класса используются для передачи информации всех тем. В противном случае методика расчетов рисков аналогична устройствам класса *M*. Тогда расчет рисков можно выполнить по формуле:

$$R_j = \max\left(P\left(y_{jc_k}\right)\right) \times \sum_{i=1}^{I} S_i, \;\; c_k \in C \qquad (5)$$

Для устройств класса *E* расчет рисков можно произвести, исходя из того, какая информация на каком устройстве обрабатывается. Если разграничения доступа нет, что небезопасно, то можно воспользоваться формулой (5). Если есть четкое разграничение прав доступа, то для более объективной оценки рисков следует воспользоваться формулами 1-3.

Заключение. Согласно анализу модели издатель-подписчик для среды Интернет вещей была выявлена уязвимость, при которой частая отправка сообщений подключений по протоколу TLS может блокировать шлюз. Чтобы защититься от этой угрозы, был предложен алгоритм на базе принципа нулевого знания, который позволяет установить защищенное соединение в разы быстрее. Также предлагаемый алгоритм позволяет сгенерировать общий сессионный ключ и способен противостоять современным атакам. Использование модели издатель-подписчик позволяет формализовать и четко определить информационные потоки в замкнутой информационной системе. На основе этого была предложена модель оценки рисков, которая позволяет более точно оценить риски за счет того, что направления передачи и получения информации заранее известны.

СПИСОК ЛИТЕРАТУРЫ

1. Gubbi, J. Internet of Things (IoT): A vision, architectural elements, and future directions / J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami// Future Generation Computer Systems – 2013. -Vol. 29(7)- Pp. 1645-1660 doi: 10.1016/j.future.2013.01.010.
2. Dragoni, N. Microservices: Yesterday, today, and tomorrow/ N. Dragoni, S. Giallorenzo, A.L. Lafuente, M. Mazzara, F. Montesi, R. Mustafin, L. Safina// Present and Ulterior Software Engineering.-2017.-Pp. 195-216. doi: 10.1007/978-3-319-67425-4_12
3. Dikii, D.I. Denial-of-service attack analysis by MQTT protocol/D. I. Dikii// Scientific and Technical Journal of Information Technologies, Mechanics and Optics.-2020.- Vol. 20(2)-Pp. 223-232. doi: 10.17586/2226-1494-2020-20-2-223-232
4. Dikii, D.I. Remote Access Control Model for MQTT Protocol/D. I. Dikii// 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2020. – 2020.- Pp. 288 – 291 doi: 10.1109/EIConRus49466.2020.9039122
5. Al-Fuqaha, A. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash // IEEE Communications Surveys & Tutorials. — 2015.—Vol. 17(4)—Pp. 2347–2376.doi:10.1109/comst.2015.2444095.
6. Pticek, M. Architecture and functionality in M2M standards / M. Pticek, V. Cackovic, M. Pavelic, M. Kusek, G. Jezic // 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). — 2015. doi:10.1109/mipro.2015.7160306.

7. Fremantle, P. Federated Identity and Access Management for the Internet of Things / P. Fremantle, B. Aziz, J. Kopecky, P. Scott // International Workshop on Secure Internet of Things. — 2014.—Pp. 10-17.doi:10.1109/siot.2014.8.
8. Nastase, L. Security in the Internet of Things: A Survey on Application Layer Protocols / L. Nastase // 21st International Conference on Control Systems and Computer Science (CSCS). — 2017. doi: 10.1109/cscs.2017.101.
9. Yassein, M. B. Internet of Things: Survey and open issues of MQTT protocol / M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, R. Al-Hatmi // International Conference on Engineering & MIS (ICEMIS). — 2017.doi:10.1109/icemis.2017.8273112.
10. Diffie, W. New directions in cryptography / W. Diffie, M. Hellman // IEEE Transactions on Information Theory. — 1976.—Vol. 22(6)—Pp. 644–654.doi:10.1109/tit.1976.1055638.
11. Standards for Efficient Cryptography Group (SECG). SEC 1: Elliptic Curve Cryptography [Электронный ресурс]. — 2009. — URL: https://www.secg.org/sec1-v2.pdf (дата обращения: 44020).
12. Keys, ciphers, messages: how TLS works [Электронный ресурс]. — 2019.— URL: https://tls.dxdt.ru/tls.html#ecdsa (дата обращения: 44020).
13. Martín-Fernández, F. Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Things / F. Martín-Fernández, P. Caballero-Gil, C. Caballero-Gil // Sensors. — 2016. —Vol. 16(1)—Pp. 1-20.doi:10.3390/s16010075.
14. Онацкий, А.В. Модификация протоколов Шнорра и Окамото на эллиптических кривы / А.В. Онацкий // Восточно-Европейский журнал передовых технологий. — 2013.—Vol. 9(66)—Pp. 14-18.
15. Dikii, D. Authentication Algorithm for Internet of Things Networks Based on MQTT Protocol/ D. Dikii// Serbian Journal of Electrical Engineering. – 2020.- Vol.17(3)- Pp. 389-403 doi: 10.2298/SJEE2003389D

Карабутов М.В.
СГТУ, аспирант,
max.karabutoff2010@yandex.ru
Байбурин В.Б.
СГТУ, профессор, д.ф-м.н.
Baiburinvb@rambler.ru
Розов А.С.
Senior Software Developer, к.ф-м.н
General Arcade Pte. Ltd.
fog545@mail.ru

ПРИМЕНЕНИЕ НЕЙРОКРИПТОГРАФИИ В БРАУЗЕРАХ С ИСПОЛЬЗОВАНИЕМ WEBASSEMBLY

Введение

Одной из проблем, с которыми сталкиваются разработчики при разработке средств криптографии в браузере – поиск быстрого и безопасного способа шифрования и дешифрования.

В этой статье показано, почему криптография на стороне браузера является сложной в реализации проблемой, и какие последние технологические достижения могут обеспечить решение данной проблемы.

На текущий момент можно с уверенностью сказать, что наиболее универсальным языком с поддержкой браузера является язык JavaScript, Учитывая всё выше сказанное, желательно чтобы криптографические функции были доступны непосредственно из JavaScript.

Здесь и далее в качестве примера рассмотрены браузеры с использованием технологий WebKit, Gecko [1]. На сегодняшний день можно выделить 3 основных способа по использованию криптографии в браузере.

1. Выполнение криптографии в плагине.

Плагины – это скомпилированный код, который запускается в браузере и может вызываться с помощью JavaScript.

Существуют библиотеки криптографии, реализованные на других языках, как правило, эти реализации очень быстры, но, к сожалению, они требуют от пользователей установки плагинов для браузера, что может быть не доступным, если выполнение программ и просмотр сайтов идёт на общедоступном или корпоративном компьютере, где установка сторонних плагинов запрещена.

Также возможен другой вариант – использовать собственный клиент на базе Chromium, который позволяет браузерам запускать машинный код, скомпилированный из C/C++. Опять же, такие реализации могут быть очень быстрыми,

Таким образом, хотя плагины и собственный клиент имеют свои преимущества в скорости, им не хватает переносимости и масштабируемости, поскольку они требуют от пользователей установки определенных сторонних компонентов.

2. Web Crypto API.

Web Crypto API предоставит собственные криптографические примитивы в языке JavaScript, что позволяет веб-приложениям использовать относительно быстрые процедуры шифрования и дешифрования. Однако этот API все еще находится на стадии разработки и тестирования, в частности известны его уязвимости [2], как правило в современных браузерах используется только метод crypto.getRandomValues().

До тех пор, пока веб-криптографический API не станет широко внедренным, он не является жизнеспособным вариантом для криптографии на стороне браузера.

3. Выполнение криптографии непосредственно в JavaScript.

Преимущество этого подхода состоит в том, что он отлично подходит как для стационарных так портативных систем. Все браузеры могут запускать JavaScript, поэтому все браузеры смогут запускать библиотеку криптографии, написанную JavaScript.

Идея состоит в использовании Emscripten.

Emscripten – набор средств и инструментов компилятора с открытым исходным кодом для технологии WebAssembly [3]. Используя Emscripten, разработчик способен скомпилировать код C/C++, или любой другой язык, использующий LLVM [2], в WebAssembly(WASM) и запустите его в браузере, сервере Node.js, или любой другой средой выполнения WASM.

Практически любая кодовая база C/C++ может быть скомпилирована в WebAssembly с использованием Emscripten, начиная от высокопроизводительных игр, которые должны отображать графику, воспроизводить звуки, загружать и обрабатывать файлы, системами потокового видео, обработки больших массивов данных заканчивая такими известными реализациями многих коммерческих проектов включая, такие как Unreal Engine 4 и Unity Engine [3], при этом криптография должна выполняться на клиентской стороне.

Основным преимуществом описанного подхода является то, что *встраивание сторонних плагинов не требуется* возможно использовать библиотеки шифрования, написанные на C/C++, в том числе и сертифицированные ФСТЭК [4, 5].

Общая схема использования C/C++ кода показана на рис.1

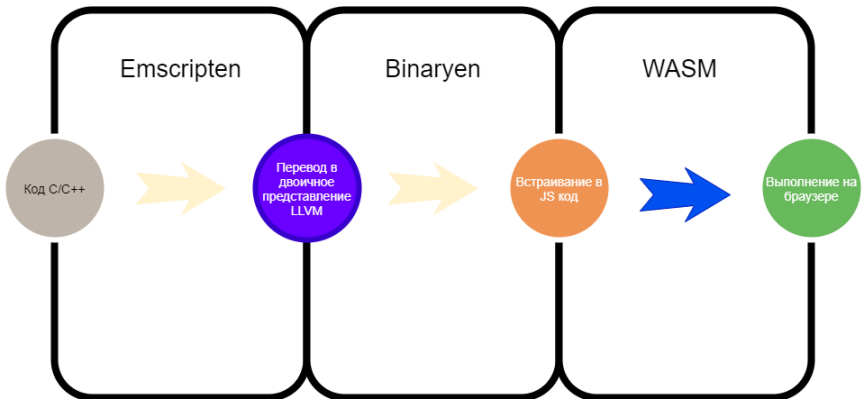


Рис. 1. Пробразоавание C/C++ кода в код JS для барузера

2. Реализация нейрокриптографической системы

В работе [6] авторы, показали создание нейрокриптографической системы для шифрования сообщений в мессенджере, система показала свою применимость. Коротко опишем суть алгоритма.

Суть идеи, состоит в синхронизации двух нейронных сетей типа древовидной машины чётности(ДМЧ). Древовидная машина чётности – это особый тип нейронной сети прямого распространения, она состоит из трех слоев: выходного слоя, содержащего один нейрон, скрытого слоя, содержащего K нейронов, и входного слоя, содержащего $K * N$ нейронов. Каждый из N входных нейронов связан только со скрытым нейроном. Пример нейронной сети такого типа с параметрами при K = 2, N = 3 показан на рис. 2.

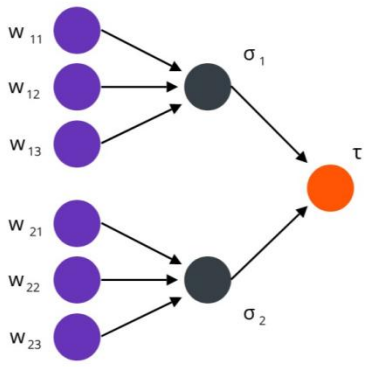


Рис. 2. ДМЧ при K = 2 и N = 3.

Входные нейроны могут принимать следующие значения:

$$x_{i,j} \in \{-1,+1\}, \tag{1.1}$$

Веса между входными и скрытыми нейронами сети ограничены числом L следующим образом:

$$w_{i,j} \in \{-L...,0,...,+1\}, \tag{1.2}$$

Значения скрытых нейронов вычисляются путем применения функции активации к сумме входного значения нейрона и его веса [1,3] в соответствии с формулами:

$$\sigma_i = \mathrm{sgn}(\sum_{j=1}^{N} w_{ij} x_{ij}), \tag{1.3}$$

$$\mathrm{sgn}(x) = \begin{cases} -1, x \le 0 \\ 1, x > 0 \end{cases}, \tag{1.4}$$

Таким образом, скрытые нейроны могут принимать только значения (-1 и 1).

Значение выходного нейрона вычисляется путем умножения значений всех скрытых нейронов, и, следовательно, оно также является двоичным:

$$\tau = \prod_{i=1}^{k} \sigma_i, \tag{1.5}$$

Каждый подписчик инициализирует сеть доверенного платформенного модуля в своём браузере, заполняя значения весов случайными значениями.

Для шифрования мы используем стандартный алгоритм Диффи-Хеллмана, где веса нейронной сети являются начальными векторами для системы шифрования.

Чтобы добиться равенства весов, мы выполняем следующие действия:

1. Инициализация нейронной сети. В начале процесса синхронизации значения весовых коэффициентов задаются случайным образом.
2. Создание случайного входного вектора, который подается на сетевой вход.
3. Вычисление значения скрытых и выходных нейронов.
4. Проверка того, равны ли выходные значения обеих сетей.
5. Если выходные значения не совпадают, вернитесь ко второму шагу. Если выходные значения равны, то для каждой сети мы используем одно из трех правил обучения, представленных выше.
6. После достижения полной сетевой синхронизации ключ шифрования генерируется на основе полученных весовых коэффициентов.

Затем абоненты начинают синхронизацию сетей в соответствии со следующими правилами:

Правило Хебба:

$$w_i^{`} = g(w_i + \sigma_i x_i \theta(\sigma_i \tau)\theta(\tau^A \tau^B), \tag{1.6}$$

анти-правило Хебба

$$w_i^{`} = g(w_i - \sigma_i x_i \theta(\sigma_i \tau)\theta(\tau^A \tau^B), \tag{1.7}$$

Случайное блуждание

$$w_i^{`} = g(w_i +_i x_i \theta(\sigma_i \tau)\theta(\tau^A \tau^B), \tag{1.8}$$

Где $g(x)$ и $\theta(a,b)$ можно определить по формуле:

$$g(x) = \begin{cases} x = -L, x < -L \\ x, -L \le x \le L \\ x = L, x > L \end{cases}$$
$$\theta(a,b) = \begin{cases} 1, a = b \\ 0, a \ne b \end{cases}, \tag{1.9}$$

Эти правила обучения изменяют только веса, связанные со скрытыми весами $\sigma_i = \tau$. Таким образом, невозможно определить, какие веса обновляются, не зная внутреннего представления (σ_1, σ_2,..., $\sigma_K \sigma_k$). Это свойство является основополагающим для криптографического применения явления нейронной синхронизации. Правила обучения должны обеспечивать, чтобы веса оставались в допустимом диапазоне от $-L$ до $+L$. Если какой-либо вес находится за пределами этой области, он сбрасывается до ближайшего предельного значения $\pm L$, что достигается функцией $g(x)$ в каждом правиле обучения. Более детальное описание системы показано в работе [6].

Однако в работе [6], остался нерешенным ряд вопросов: насколько криптография JavaScript может быть безопасной так как в алгоритме использовался метод Math.random(), который обладает рядом минусов. Хотя следует отметить, что Math.random() не является

хорошим источником случайности, в современных браузерах есть метод crypto.getRandomValues(), который обеспечивает достаточную случайность, однако он не подходит для алгоритмов написанных с использованием C/C++ и он в свою очередь сертифицирован. Также для обеспечения для обеспечения синхронизации и безопасности использовалось большое число нейронов в сети (500), что обеспечивало приемлемый результат в плане безопасности, однако, скорость работы алгоритма была низкой. Для решения этой проблемы была создана реализация описанного выше алгоритма м использованием языка Emcsripten и языка C/C++.

Ниже, показано сравнение работы описанного выше алгоритма шифрования выполнено на чистом JavaScript (Табл. 1), и с использованием Emscripten (Табл. 2). При этом в качестве генератора случайных числе использовалась сертифицированная ФСТЭК функция [4, 7].

Табл. 1. Реализация алгоритма на чистом JavaScript

Правило обучения и размерность	**Среднее время сходимости**	**Число обновлений сети**
$K = 10, N = 5, L = 10$		
Правило Хебба	0,0357	364
Анти-правило Хебба	0,0323	267
Свободное блуждание	0,0262	175
$K = 10, N = 25, L = 10$		
Правило Хебба	0,1680	652
Анти-правило Хебба	0,1599	422
Свободное блуждание	0,1625	625
$K = 100, N = 25, L = 10$		
Правило Хебба	3,6788	945
Анти-правило Хебба	4,5163	1305
Свободное блуждание	6,2228	1536

Как видно, из данных таблиц 1 и 2, предложенный способ реализации обладает большей скоростью работы. При этом подобная реализация может быть применена и другим способом шифрования, в частности OpenSSL и ГОСТ.

Табл. 2. Реализация алгоритма на C/C++

Правило обучения и размерность	**Среднее время сходимости**	**Число обновлений сети**
$K = 10, N = 5, L = 10$		
Правило Хебба	0,0321	364
Анти-правило Хебба	0,0320	267
Свободное блуждание	0,0262	175
$K = 10, N = 25, L = 10$		

Правило Хебба	0,0504	652
Анти-правило Хебба	0,04797	422
Свободное блуждание	0,04875	625
$K = 100$, $N = 25$, $L = 10$		
Правило Хебба	0,91071	945
Анти-правило Хебба	1,21071	1305
Свободное блуждание	1,51071	1536

СПИСОК ЛИТЕРАТУРЫ

1. Лоусон, Б. Изучаем HTML 5. Библиотека специалиста [Текст] / Б. Лоусон, Р. Шарп. – Спб.: Питер, 2011. – 253 с.
2. MDN Web Docs. Math.random() Электронный ресурс]. — Режим доступа https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Math/random
3. Сайт Emscripten [Электронный ресурс]. — Режим доступа : https://emscripten.org.
4. ГОСТ Р ИСО 28640-2012. [Электронный ресурс]. – Режим доступа: http://files.stroyinf.ru/cgi-bin/ecat/ecat.fcgi?b=0&i=53898&pr=1.
5. ГОСТ 34.11-2018. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200161707.
6. Karabutov M.V. N Development neurocryptographic system for messengers / Karabutov M.V., A.S.Rozov, P.D. Cherepanov // 2021 5th Scientific School Dynamics of Complex Networks and their Applications (DCNA 2011). — 2021 Страницы 92 – 94.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 373-377.

Крючков А. А.
РТУ МИРЭА, ассистент, аспирант
andrai12@mail.ru

ОБ ОДНОМ ПОДХОДЕ К ГЕНЕРАЦИИ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНЫХ ВОЗМОЖНОСТЕЙ КВАНТОВОГО КОМПЬЮТЕРА

Введение. В современной классической криптографии при симметричном шифровании для выработки случайной последовательности применяются генераторы случайных чисел (ГСЧ). В настоящее время выделяют три типа ГСЧ по способу генерации последовательностей:

– ГСП. Источником случайности является физический процесс;

– ГПСП. Источником случайности является детерминированный алгоритм;

– КГПСП. Комбинированный метод генерации чисел. Начальное состояние берется из ГСП, после чего при помощи КГПСП формируется случайная последовательность.

Надежность выдаваемых ГСЧ данных до сих пор остается объектом исследований среди криптоаналитиков, целью которых является подтверждение безопасности получаемых результатов. В большинстве случаев при раскрытии начальных параметров ГСЧ, злоумышленнику предоставляется возможность по восстановлению всего значения сгенерированной последовательности.

Одним из последних технических решений создания непредсказуемых последовательностей является квантовый генератор случайных чисел (КГСЧ). Его механизмы базируются на фундаментальных законах квантовой физики, которые исключают наличие корреляции среди получаемых результатов.

На тему генераторов случайных последовательностей, использующих квантовые эффекты, написано несколько научных работ, среди которых стоит выделить диссертацию И. В. Радченко [1], где исследователь предложил компактный квантовый генератор случайных чисел в авторском исполнении со скоростью выходного бинарного потока в 1.0 Мбит/с и показал успешное прохождение генерируемой последовательности статистических тестов NIST, а также статью российских ученых, предложивших КГСЧ, основанный на Пуассоновской статистике фотоотсчетов [2].

Из коммерческих производителей в области по технической реализации и распространению аналогичных продуктов можно назвать швейцарскую компанию «IDQuantique» [3].

Так как данное решение – это исключительно платный продукт, являющийся недоступным массовому потребителю, а для настройки и тестирования КГСЧ по предложенным методикам в работах [1-2] у автора отсутствовало необходимое лабораторное оборудование, было решено проверить возможности не так давно появившегося квантового компьютера компании IBM, предоставляющего свой вычислительный потенциал всему научному сообществу в свободное использование.

Кубит. Суперпозиция. Вентиль Адамара.

Рассмотрим способ генерации случайной последовательности классических бит на примере цикличного использования одного кубита.

Двухуровневая квантово-механическая система задается линейной суперпозицией ее собственных состояний, каждое из которых является носителем одного бита классической информации (1):

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

где α и β – комплексные коэффициенты, характеризующие вероятность перехода кубита в одно из двух возможных состояний и удовлетворяющие равенству (2):

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2)$$

Для того чтобы кубит перешел в состояние суперпозиции используется вентиль Адамара (H-gate), задающийся следующей матрицей (3):

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (3)$$

Применив данный вентиль к (1) получим следующее математическое описание состояния кубита (4):

$$|\Psi\rangle = \frac{\alpha}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) + \frac{\beta}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \quad (4)$$

или (5):

$$|\Psi\rangle = \alpha|+\rangle + \beta|-\rangle \quad (5)$$

Схема применения вентиля Адамара к кубиту с его дальнейшим измерением для получения из квантового состояния классического бита представлена на Рис. 1:

Рис. 1. Схема применения вентиля Адамара к кубиту с его дальнейшим измерением

Для получения таким способом последовательности необходимой длины достаточно запустить данную схему в цикл с требуемым количеством повторений. Особенности квантового компьютера гарантируют, что каждое отдельное измерение будет независимо от всех остальных. Таким образом, в теории корреляция между получаемыми данными должна полностью отсутствовать.

Генерация случайных последовательностей в квантовой лаборатории IBM.

Компания IBM одной из первых в мире заявила о создании квантового компьютера. Преследуя цель дальнейшего развития нового направления информационных технологий, она предоставила всему научному сообществу доступ к своим вычислительным устройствам в облачном режиме.

Каждый желающий имеет возможность пройти процедуру регистрации на официальном сайте квантовых разработок IT-компании [4], после чего у него появляется доступ к квантовым компьютерам фирмы. Каждое имеющееся квантовое устройство имеет свои ограничения, среди которых разрядность системы, количество повторений программного кода и др.

Существует две платформы по запуску и отладке программного кода – “Quantum Composer” [5], куда направляется программа на языке OpenQASM, и “Quantum Lab” [6], использующая средства квантового языка программирования Qiskit. В связи с накладываемыми ограничениями на режим работы в “Quantum Composer”, а также учитывая особенности форматирования результатов выполнения программы, был сделан выбор в пользу использования квантовой лаборатории IBM.

Для генерации случайной последовательности бит с использованием одного кубита был написан программный код [7], циклично инициализирующий кубит, с дальнейшим применением к нему вентиля Адамара и проведением измерения. Для удобочитаемости выдаваемых результатов последовательность в формате ASCII разбивалась на 64 бита в строку. Всего было сгенерировано две последовательности длиной 640.000 и 1.280.000 бит.

Далее полученные данные отправлялись на виртуальную машину Kali Linux, где подвергались исследованию на случайность тестами NIST STS [8].

Проверка полученных результатов средствами тестов NIST.

Для проверки полученных данных на наличие зависимостей в сгенерированных последовательностях были использованы тесты NIST (The National Institute of Standards and Technology).

Успешное прохождение сгенерированного битового потока статистических тестов NIST является необходимым условием для того, чтобы считать последовательность случайной. Представим результаты проведенных серий тестов в Табл. 1.

Табл. 1. Результат проверки полученных последовательностей тестами NIST

Длина п-ти, бит	P-value			Proportion (test’s count pass)			Test
	1 bitstream	10 bitstream	20 bitstream	1 bitstream	10 bitstream	20 bitstream	
640000	-	0.534	0.213	1/1	10/10	20/20	Frequency
1280000	-	0.122	0.213	1/1	10/10	20/20	
640000	-	0.534	0.122	1/1	10/10	19/20	Block Frequency
1280000	-	0.122	0.534	1/1	10/10	20/20	
640000	-	0.534; 0.911	0.066; 0.637	1/1 (2)	10/10 (2)	20/20 (2)	Cumulative Sums
1280000	-	0.739; 0.739	0.275; 0.637	1/1 (2)	10/10 (2)	20/20 (2)	

640000	-	0.213	0.35	1/1	10/10	20/20	Runs
1280000	-	0.035	0.437	1/1	10/10	20/20	
640000	-	0.066	0.739	1/1	10/10	20/20	Longest run
1280000	-	0.035	0.213	1/1	9/10	20/20	
640000	-	0.534	0.09	1/1	10/10	20/20	Rank
1280000	-	0.739	0.739	1/1	9/10	20/20	
640000	-	0.008	0.637	1/1	10/10	20/20	FFT
1280000	-	0.534	0.911	1/1	9/10	19/20	
640000	-	0.739; 0.911	0.534; 0.911	1/1 (2)	10/10 (2)	20/20 (2)	Serial
1280000	-	0.213; 0.534	0.35; 0.534	1/1 (2)	10/10 (2)	20/20 (2)	
640000	-	0.534	0.350	1/1	9/10	20/20	Linear Complexity
1280000	-	0.534	0.35	1/1	10/10	20/20	
640000	-	0.000	0.000	1/1	0/10	0/20	Universal
1280000	-	0.000	0.000	1/1	0/10	0/20	
640000	-	0.350	0.834	1/1	9/10	19/20	Approximate Entropy
1280000	-	0.911	0.534	1/1	10/10	20/20	
640000	-	0.004÷ 0.911	0.008÷ 0.911	1/1 (149)	9÷10/10 (149)	18÷20/20 (149)	N.O.T. (149 тестов)
1280000	-	0.035÷ 0.911	0.09÷ 0.991	1/1 (149)	9÷10/10 (149)	18÷20/20 (149)	

Для уменьшения объема полученных сведений результаты тестов приведены в сокращенном виде. С полной версией результатов тестов можно ознакомиться в [7]. В скобках указывается количество серий тестов с разными входными параметрами. Для получения полных сведений по применяемым методам тестирования следует обратиться к документации [8].

Обращаясь к результатам универсального статистического теста Маурера, стоит сказать, что в случае, когда проверке подвергалась последовательность целиком (‘*bitstreams’* равняется единице), результат выполнения тестирования подтверждает предположение о том, что исследуемый битовый поток представляет собой случайную последовательность с равномерным законом распределения. Однако при изменении параметра ‘*bitstreams’* на 10 и 20 – тест выдает нулевой результат.

Исходя из описания данного теста [8] можно сделать вывод, что при заданной длине битового потока и параметре ‘*bitstreams’* 10/20 тест на сжатие не срабатывает из-за невозможности соблюдения предъявляемых требований по количеству входных данных. В случае, когда последовательность рассматривается целиком, результат универсального статистического теста Маурера подтверждает невозможность сжатия входной строки без потери информации, что говорит о случайном распределении исходной последовательности.

Для выявления зависимости между последовательностями, генерируемыми в квантовой лаборатории IBM, были получены десять строк длиной в 100.000 бит. Далее они были объединены в один файл и подвергнуты испытаниям с использованием теста расчета рангов непересекающихся подматриц (из набора тестов NIST), построенных из

исходной последовательности. Результаты данного теста подтвердили отсутствие зависимости между генерируемыми последовательностями.

Необходимо отметить, что в силу отсутствия универсального набора критериев, оценивающих, насколько исследуемая последовательность случайна, прохождение NIST Statistical Test Suite является необходимым, но не достаточным условием для выдвижения предположения о случайности последовательности. В качестве дополнительного независимого исследования полученных последовательностей целесообразно провести их проверку на случайность набором статистических тестов DieHard [9] или другими аналогичными программными решениями.

В то же время всегда стоит учитывать утверждение Дональда Кнута [10], указывающего, что в рамках математической статистики следует осторожно использовать критерии равномерности распределения, так как положительный результат конкретного испытания последовательности еще не говорит о ее истинной непредсказуемости. Однако каждая успешно проведенная последующая проверка последовательности на наличие зависимостей дает право с большей вероятностью делать вывод о ее случайности.

Выводы.

Были сгенерированы последовательности средствами квантовой лаборатории IBM, которые в дальнейшем были проверены статистическими средствами NIST STS. Анализ полученных результатов подтверждает, что с точки зрения вопросов обеспечения безопасности данные последовательности можно считать случайными, а квантовые компьютеры способны выступать в качестве генераторов случайных чисел. Для подтверждения данного тезиса стоит провести серию дальнейших испытаний по генерации и проверке последовательностей много большей длины.

СПИСОК ЛИТЕРАТУРЫ

1. Радченко И. В. Приготовление и измерение состояний в протоколах квантовой коммуникации : дисс. канд. физ.-мат. наук: 01.04.21 / Радченко Игорь Васильевич. – М., 2016.
2. Балыгин К. А., Зайцев В. И., Климов А. Н., Кулик С. П., Молотков С. Н. Квантовый генератор случайных чисел, основанный на Пуассоновской статистике фотоотсчетов, со скоростью около 100 Мбит/с / К. А. Балыгин, В. И. Зайцев, А. Н. Климов, С. П. Кулик, С. Н. Молотков. – М., Журнал экспериментальной и теоретической физики, том 153, вып. №6, 2018. – 879 с.
3. Официальный сайт производителя квантовых криптографических решений “ID Quantique” [Электронный ресурс]. – 2021. – Режим доступа: https://www.idquantique.com.
4. Облачный квантовый компьютер компании IBM [Электронный ресурс]. – 2021. – Режим доступа: https://quantum-computing.ibm.com.
5. Квантовый компоновщик “IBM Quantum Composer” [Электронный ресурс]. – 2021. – Режим доступа: https://quantum-computing.ibm.com/composer.
6. Квантовая лаборатория “IBM Quantum Lab“ [Электронный ресурс]. – 2021. – Режим доступа: https://quantum-computing.ibm.com.

7. Программный код генерации случайной последовательности на квантовом компьютере, Qiskit [Электронный ресурс]. – 2021. – Режим доступа: https://github.com/Che-Guevara22/QuantumData.
8. Набор статистических тестов NIST [Электронный ресурс]. – 2021. – Режим доступа: https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software.
9. Набор статистических тестов DieHard [Электронный ресурс]. – 2021 – Режим доступа: https://github.com/emeryberger/DieHard.
10. Кнут Д. Искусство программирования для ЭВМ. Т.2. М.: Мир, 1977. – 727 с.

Дунюшкина Ксения Сергеевна
БашГУ, студент
ksdynushkina@gmail.com

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА BLE ДЛЯ ЗАЩИТЫ И УПРАВЛЕНИЯ ДОСТУПОМ

Bluetooth LE (Low Energy) — это сравнительно новая технология беспроводной связи, которая позволяет осуществлять передачу данных с низким энергопотреблением, то есть расход заряда аккумулятора при использовании данной технологии значительно снижается. Стандарт BLE имеет скорость передачи данных – 1Мбит в секунду, что позволяет получать и передавать необходимые данные в нужном нам объеме, достаточно быстро, при чем, мы можем быть уверены в их безопасности благодаря, двухуровневой защите протокола.

В данной статье мы рассмотрим, как устроен данный протокол и его применение в СКУД, а также в умных домах.

Технология Bluetooth Low Energy создавалась для того, некоторые устройства могли держать непрерывную связь между собой, такие устройства как смартфон и наушники, а так же множество других различных устройств. Протокол энергосбережения работает по следующим принципам:

— Данные передаются короткими пакетами;

— Если передача данных прекращается, то передатчик возвращается в спящий режим.

Технологии BLE затрачивает гораздо меньше энергии и именно поэтому ее применяют, когда устройствам необходимо держать непрерывную связь длительное время.

Технологии BLE и обычный Bluetooth функционируют в одном и том же диапазоне, но принцип их работы различается. Стек протоколов **Bluetooth Low Energy (BLE) имеет две основные части это – контроллер** (Controller) и узел сети (Host), как и обычный, всем известный **Bluetooth. Контроллер данного стека протоколов состоит из физического и канального уровня. Чаще всего он имеет вид системы-на-кристалле (СнК) и так же интегрированный беспроводной трансивер. Вторая часть данного стека – узел сети реализовывается программно на микроконтроллере приложений и содержит в себе опции верхних уровней, таких как:**

— уровень логической связи (Logical Link Control — LLC);

— протокол адаптации (Adaptation Protocol — L2CAP);

— протокол атрибутов (Attribute Protocol — ATT);

— протокол атрибутов профилей устройств (Generic Attribute Profile — GATT); протокол обеспечения безопасности (Security Manager Protocol — SMP);

— протокол обеспечения доступа к функциям профиля устройств (Generic Access Profile (GAP).

Нижняя и верхняя части стека взаимодействуют между собой при помощи интерфейса Host Controller Interface (HCI), а поверх уровня узла сети могут реализовываться дополнительные функции прикладного уровня.

На рисунке 1 рассмотрим структуру стека протоколов BLE.

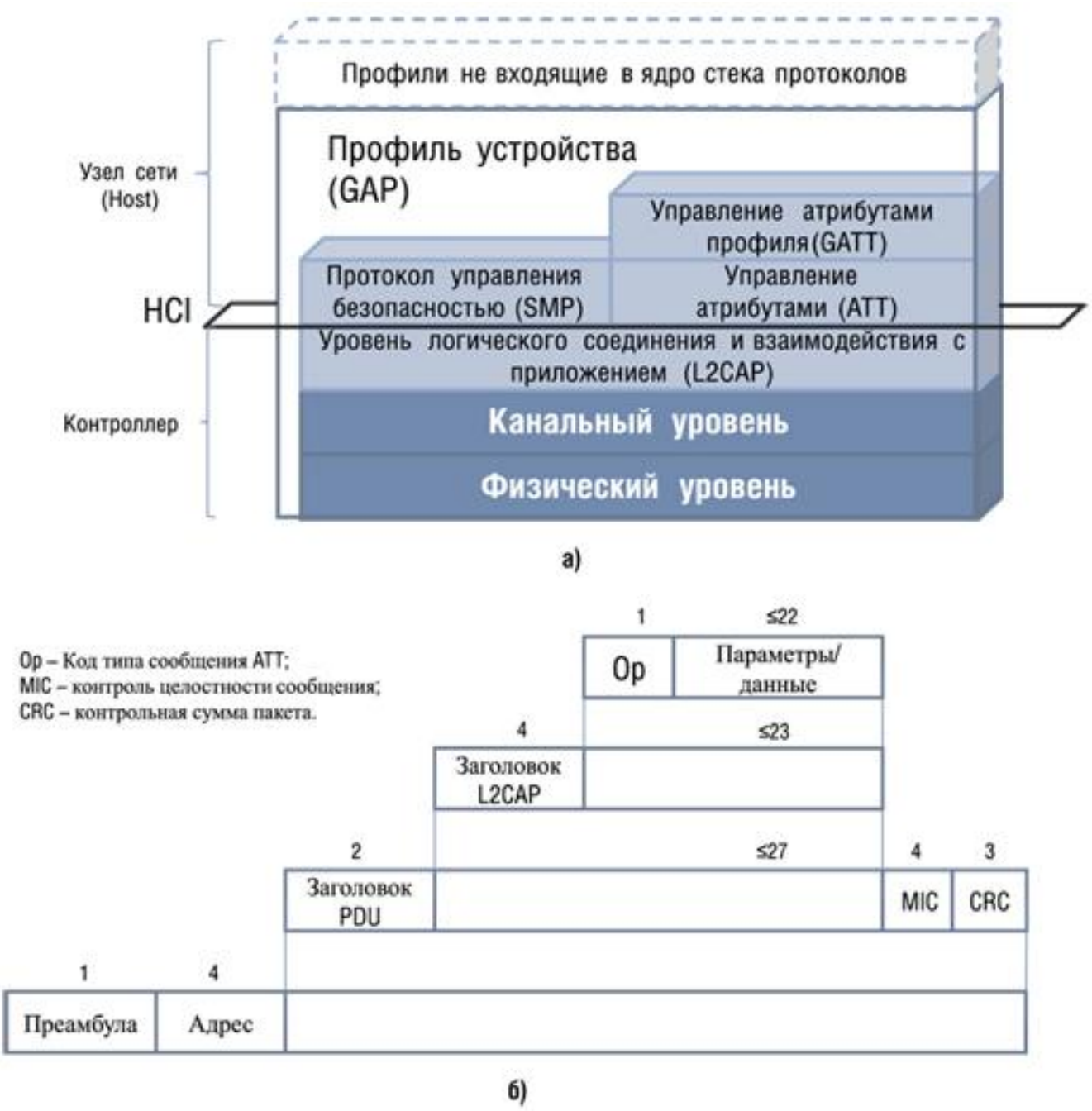


Рис. 1. а) - структура стека протоколов Bluetooth Low Energy (BLE);
б) - пакета данных BLE

Протокол использует так называемый режим Advertising. Его суть заключается в том, что большее количество времени (около 99%) необходимые нам устройства находятся в спящем режиме, тем самым экономят энергию. В нужный момент они просыпаются на небольшой период времени, чтобы обменяться данными, после чего снова переходят в спящий режим. При этом, чтобы устройства могли пребывать в режиме Advertising, в первую очередь гаджетам необходимо синхронизироваться между собой.

Впервые технология BLE нашла свое применение в так называемых мобильных ключах. Она очень быстро распространилась среди гостиничных СКУД. Создавалась специальная сеть (приложение), которая объединяла весь отель, гостю достаточно было всего лишь скачать такое приложение либо подключиться к сети, чтобы его ключ от

номера находился всегда под рукой и он имел возможность в любое время получать интересующие его услуги. Технология BLE позволяет передать некоторый набор данных в устройство пользователя «по воздуху», прежде чем ему отправляется мобильный ключ, все его данные защищаются, а так же происходит верификация гостя (его устройства).

По тому же принципу многие предприятия и организации уже переходят на данную технологию. Некоторые разработки позволяют легко включить в уже имеющиеся СКУД такие мобильные ключи, причем с минимальными затратами, ведь внедрение и реализация такой технологии стоит дешево. Достаточно добавить поддержку BLE протокола и обновить интерфейс устройства. Такая технология позволяет сотрудникам быстрее и легче проходить идентификацию на предприятии и авторизоваться на своем рабочем месте, при этом нет необходимости контактировать с другими сотрудниками, что очень актуально в последнее время. Протокол BLE имеет достаточно широкий радиус действия, благодаря этому прохождение верификации можно начать заблаговременно, к примеру: если работнику предприятия необходимо проехать на автомобиле через шлагбаум, технология позволит сделать это без каких-либо задержек. Но так же технология предусматривает уменьшение радиуса действия, если, допустим, вам необходима авторизация на вашем рабочем месте для доступа к компьютеру, достаточно поднести мобильный телефон к считывающему устройству на расстоянии нескольких сантиметров.

Новый протокол BLE работает по принципу – периодическая передача данных и их длительная обработка. Чаще всего здесь используются двухрежимные устройства BLE в ноутбуках, смартфонах, планшетах. Однорежимные уже получил достаточно большое распространение и нашел свое применение во многих сферах деятельности, например, это такие сферы как красота и здоровье, автоматизация устройств, управление, анализ, и многие другие.

Если в радиусе двухуровневого модуля находятся другие одноуровневые BLE устройства, то это позволяет решать множество различных задач. В список таких проборов будут входить так называемые приборы – сигнализаторы. Они имеют возможность уведомлять своего владельца об отдалении от него кошелька, сумки, пакета и любых других личных вещей, которые оснащены BLE модулем. Очень хорошим решением для родителей станут различные брелоки и устройства, оснащенные BLE технологией, которые могут использоваться в качестве маячков для их ребенка, чтобы в местах большого скопления людей, они могли исключить потерю малыша.

Благодаря своей устойчивой работе и минимальному энергопотреблению, а так же дешевизне производства и установки протокола BLE, его можно рассматривать в качестве замены технологии NFC, а именно RFID меток. Так как технология BLE может обеспечивать нас довольно большим радиусом и достаточно устойчивой работой, а NFC технология отвечает за логическое сопряжение пары, а так же может гарантировать очень надежную защиту, из-за малого радиуса действия, мы можем использовать протокол как полную замену технологии NFC, так и их функции совместно.

Сейчас большое распространение имеют различные так называемые технологии умных домов. Технология Bluetooth Low Energy позволит нам легко открывать удаленно ворота, при въезде вашего автомобиля в гараж, открывать двери при входе, если ваши руки будут чем-то заняты, и обеспечивать работу множества других механизмов с достаточно большого расстояния. А так как эта технология затрачивает минимальное

количество энергии это позволит сократить расходы, долго не меняя аккумулятор в вашем компактном устройстве управления. Помимо всего этого, если на вашем смартфоне, который у большинства людей всегда с собой, будет иметься BLE модуль, вы с легкостью сможете управлять с большого расстояния – находясь не далеко от дома или в другой комнате, различными приборами и устройствами умного дома, такими как, оборудование для приготовления пищи или уборки дома, через сопряженные каналы устройств**.**

К BLE устройствам относятся:

— Устройства удаленного вызова, примером может послужить радио-няня;

— Так называемые умные ключи, используемые в СКУД;

— Различные приборы, используемые для занятий спортом, такие как шагомеры, устройства измеряющие пульс и так далее;

— Сенсоры, измеряющие температуру, влажность;

— Медицинская техника, служащая для измерения глюкозы в крови, температуры в теле человека, а так же тонометры;

— Беспроводная бытовая электроника (клавиатуры и мыши), различные панели и пульты управления;

— Устройства, помогающие обеспечить безопасность, такие как – тревожные кнопки, бесконтактные ключи и многое другое.

Технология Bluetooth Low Energy находится в модулях со встроенным ПО. Такими модулями оборудуются конечные устройства. В роли таких модулей можно выделить такие как:

1. BT111 – используется для приложений, работающих со стандартными протоколами Bluetooth и BLE. Рассмотрим на рисунке 2.

Рис. 2. Модуль BT111.

2. BLE112 – является однорежимным BLE модулем, используется для различных приборов с батарейным питанием. Рассмотрим на рисунке 3.

Рис. 3. Модуль BLE112.

3. USB BLED112 – модуль, подобный модулю BLE112, с такими же свойствами, но имеющий другой форм фактор (USB флешки). Рассмотрим на рисунке 3.

Рис. 4. Модуль BLE112 (USB флешка).

Защита канала передачи данных устройств в протоколе BLE имеет 2 режима безопасности LE Security Mode 1, который работает на Data Link Layer (DLL) и LE Security Mode 2, работающий на AT&T, а так же состоит из нескольких уровней, которые используются в зависимости от типа соединения. На Data Link Layer (DLL) имеется аутентификация и шифрование, при помощи построения аутентификационного кода сообщения из блочного алгоритма шифрования (CCM) и шифра AES – 128.

Рассмотрим на рисунке 5.

Режим	Уровень безопасности	Тип соединения (Pairing)	Шифрование	Проверка целостности	Уровень стека
LE Security Mode 1	Уровень 1	Нет	Нет	Нет	Канальный уровень (Link Layer)
	Уровень 2	Без аутентификации	Есть	Есть	
	Уровень 3	Аутентификация	Есть	Есть	
LE Security Mode 2	Уровень 1	Без аутентификации	Нет	Есть	Уровень ATT (ATT Layer)
	Уровень 2	Аутентификация	Есть	Есть	

Рис. 5. Уровни безопасности протокола BLE.

Соединение будет проходить в три этапа:

1. Оба модуля на канальном уровне обмениваются нужной информацией, в которой содержатся данные о возможностях ввода – вывода, которые сейчас доступны. После этого выбирают по какому из них будет происходить дальнейшее взаимодействие.
2. Далее начинается создание некоего ключа под названием «временный ключ краткосрочного значения». Его передача может осуществляться тремя способами:
   - Шестизначный код, который создается пользователем;
   - Использование канала NFC;
   - Либо без аутентификации, при невозможности проведения первых двух способов.
3. Происходит обмен тремя 128 битными ключами всех конечных точек.

После этого, если не было выявлено никаких нарушений, происходит синхронизация пары.

Таким образом, можно сделать некоторые выводы. Данная BLE технология является новой и только набирает свои обороты, но она уже нашла применение во многих сферах жизни человека и сделала их гораздо удобнее. Протокол имеет достаточно хорошую защиту и стабильную работу, что позволяет ему устойчиво чувствовать себя на рынках СКУД. В дальнейшем возможна разработка некоторого приложения, либо интерфейса, который будет позволять вам использовать свой смартфон в качестве ключа, при входе в университет, на работу. Будет возможна авторизация пользователей на объектах и зданиях, с помощью нескольких кнопок на одном экране, с помощью вашего мобильного устройства, которое находится всегда под рукой, что гораздо упростит и обезопасит жизнь людей.

СПИСОК ЛИТЕРАТУРЫ

1. Стрельцов, А. А. Обеспечение информационной безопасности России: учеб. пособие/ под ред. В. А. Садовничего и В. П. Шерстюка. – Москва: МЦНМО, 2014. – 296с. - ISBN 5-94057-061-5.
2. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 592 с. – ISBN 690-5-7695-5435-7.
3. Гришина, Н.В. Организация комплексной системы защиты информации: учебное пособие - М.: МГУЛ, 2015 – ISBN 965-3-7695-6664-6.
4. Байер, Доминик Microsoft ASP .NET. Обеспечение безопасности: учебное пособие/ Доминик Байер. - М.: Питер, Русская Редакция, 2013. - 430 с. – ISBN 975-3-97544-754-5.
5. Bluetooth [Электронный ресурс] // Bluetooth : официальный сайт Bluetooth / Режим доступа : / URL : www.biuetooth.com (дата обращения 21.12.2020 г.).
6. Bluetooth: технология и ее применение [Электронный ресурс] // IXBT.com : образовательный портал / Режим доступа : / URL : Bluetooth: технология и ее применение (ixbt.com) / (дата обращения 21.12.2020 г.).
7. Версии Bluetooth и их отличия [Электронный ресурс] // Highscreen : онлайн магазин / Режим доступа : / URL : Версии Bluetooth и их отличия (hs-store.ru) (дата обращения 21.12.2020 г.).
8. ВСЕ О BLUETOOTH [Электронный ресурс] // Radio Secure : портал о технологии Bluetooth / Режим доступа : / URL : Bluetooth (radio-secure.ru) / (дата обращения 21.12.2020 г.).
9. Лекция 7: Обзор технологии Bluetooth [Электронный ресурс] // НОУ Интуит : образовательный портал / Режим доступа : / URL : НОУ ИНТУИТ | Лекция | Обзор технологии Bluetooth (intuit.ru) / (дата обращения 21.12.2020 г.).
10. Описание стандарта беспроводных сетей Bluetooth [Электронный ресурс] // КроссАвтоматика : образовательный портал / Режим доступа : / URL: Технология Bluetooth (crossgroup.su) / (дата обращения 21.12.2020 г.).

Салита А.С.
СПбГУТ, студент,
salita@internet.ru
Красов А.В.
СПбГУТ, заведующий кафедрой, к.т.н., доцент,
krasov@inbox.ru

ОРГАНИЗАЦИЯ СТЕГАНОГРАФИЧЕСКОГО КАНАЛА С ПОМОЩЬЮ МЕТОДА LACK НА ПРИМЕРЕ ПРОТОКОЛА RTP

Сегодня в IP-телефонии для трансляции двустороннего голосового общения используется стек протоколов IPv4/UDP/RTP с помощью технологии VoIP. RTP - (англ. Real-time Transport Protocol) протокол, использующийся для передачи трафика в реальном 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 (Табл. 1). Эти параметры позволяют при минимальных задержках определить порядок и момент декодирования каждого пакета, а также интерполировать потерянные пакеты.

Из перечисленного выше следует, что без потери передаваемых данных для организации стеганографического канала пригодно поле Заполнение. Изменение полей SSRC, Метка времени и Порядковый номер ведет к потере передаваемых данных у получателя. Частое изменение полей SSRC и Метка времени может вести к обнаружению стегаконтейнеров, так как данные поля не меняются на протяжении одной сессии. Систематическое изменение поля Метка времени также может вести к обнаружению системами защиты стеганографического канала. Также некоторая последовательность RTP-пакетов может иметь идентичные значения полей Метка времени, если логически они создаются одновременно (например, при передаче видеокадра), искажение одного из данных полей приведет к неправильной сборке и передачи данных пользователю.

Табл. 1 Структура заголовка RTP пакета

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						
96+(CC×32)+X*(32+32×EHL)	Данные						
если P=1	Заполнение (Padding data)						Счетчик заполнения (Padding count)

Исходя из этого на основе данного протокола возможна реализация метода Lost Audio Packets Steganography (LACK). LACK – метод, предполагающий намеренную задержку пакетов IP-телефонии. Отправитель генерирует пакет, несущий в себе скрытую информацию, и затем намеренно задерживает его. Пакеты, пришедшие с чрезмерной задержкой, отбрасываются приложением и не используются получателем, но, если получатель знает о существовании стеганографического канала, то данные RTP-пакеты могут быть считаны с помощью сторонней программы, и скрытая в них информация будет доставлена адресату. Подробнее о вложениях в пакеты голосового трафика и о сетевой стеганографии можно прочесть в [1-6].

Стегоанализ LACK трудно выполнить, в виду того, что данный метод строится на задержке пакетов. В современных IP сетях задержка пакетов достаточно распространена, поэтому, используя данный метод в разумных пределах можно осуществить стеганографическую передачу данных.

Основная цель текущего исследования – практическая реализация метода LACK сетевой стеганографии, для этого необходимо выбрать подходящий инструмент для передачи и манипуляции сетевым пакетом. Из-за простоты устройства данного стека протокола, повсеместного его использования и избыточности его поля заголовка возможно создание скрытого канала передачи данных с помощью языка программирования Python и библиотеки Scapy.

Scapy — это мощная интерактивная библиотека языка программирования Python для обработки пакетов. Она может подделывать или декодировать пакеты широкого ряда протоколов, отправлять их по сети, захватывать их, выполнять большинство классических задач, таких как сканирование, трассировка, зондирование, модульные тесты, атаки или обнаружение сети, внедрять недопустимые кадры, изменять значения поля заголовка пакета. Scapy изначально работает в Linux, Windows, OSX и в большинстве Unix с libpcap. Одна и та же кодовая база изначально работает как на Python 2, так и на Python 3. Всё это позволяет развернуть написанную с помощью данной библиотеки программное обеспечение на большинстве современных устройств.

С помощью Scapy существует возможность организовать стеганографический канал по описанному выше методу LACK для стека протоколов IPv4/UDP/RTP в рамках одной сессии разговора. На базе языка программирования Python был создан манипулятор полей заголовков RTP-пакетов. Благодаря нему может быть осуществлено вложение в поле Заполнение 254 байта информации с сохранением всей остальной части данных пакета. На рис. 1 представлен класс RTP пакета в библиотеке Scapy. При осуществлении вызова с помощью функций данной библиотеки можно менять любое из полей значений отправленного пакета или добавлять дополнительные поля с вложением в пакет, который находится в потоке. На рис. 2 показан дополнительный класс стеганографического вложения в RTP-пакет. В дальнейшем было осуществлено вложение в один пакет случайно сгенерированной информации размером 254 байта. Естественно то, что при осуществлении манипуляции над полями пакета проходит некоторое количество времени, которое можно дополнительно намеренно увеличить, тем самым создается задержка в отправки пакета. Тем не менее он всё равно будет доставлен адресату и если адресат его ожидает, то с помощью функций Scapy он сможет отследить пакеты стеганографического канала.

```
class RTP(Packet):
    name = "RTP"
    fields_desc = [BitField('version', 2, 2),
                   BitField('padding', 0, 1),
                   BitField('extension', 0, 1),
                   BitFieldLenField('CSRC count', None, 4, count_of='CSRC'),
                   BitField('marker', 0, 1),
                   BitEnumField('payload_type', 0, 7, _rtp_payload_types),
                   ShortField('sequence', 0),
                   IntField('timestamp', 0),
                   IntField('SSRC', 0),
                   FieldListField('CSRC', [], IntField("id", 0), count_from=lambda pkt:pkt.numsync)]
```

Рис. 1 класс полей заголовка RTP-пакета в программе.

```
class RTPSteganography(Packet):
    name = "RTP steganography"
    fields_desc = [BitField("padding data", 0, 2032),
                   BitField("padding count", 0, 8)]
```

Рис. 2 класс стеганографического вложения в поля заголовка RTP-пакета в программе.

Вложение может быть осуществлено разными способами, основных: перехват пакет и внедрение в него вложения или генерация нового пакета и осуществление вложения во время создания пакета. При использовании в разумных пределах это не повлияет на качество связи за счет возможности интерполяции протокола RTP [7].

Для осуществления связи допустимо использовать любой программный клиент IP-телефонии, осуществляющий связь по стеку протокола IPv4/UDP/RTP. В тестировании технологии использовался программный клиент linphone, связь осуществлялась по локальной сети между двумя компьютерами с установленными клиентами linphone, в один пакет было вложено 254 байта в поле Заполнение (Padding data), и он был успешно передан без потери качества разговора. Задержка пакета составила приблизительно 2 секунды. На рис. 3 и рис. 4 показаны дампы пакетов адресанта и адресата. Следует сделать вывод о том, что так как качество разговора не было потеряно, пакет, отправленный с задержкой, не был воспроизведен, из этого имеет смысл вкладывать дополнительный стеганографический контейнер вместо полезной нагрузки пакета, тем самым можно сохранить размер пакета, что поможет дополнительно защитить пакет от стеганографического анализа, либо использовать максимум возможности передачи пакета будучи неограниченным в размерах полей заголовка.

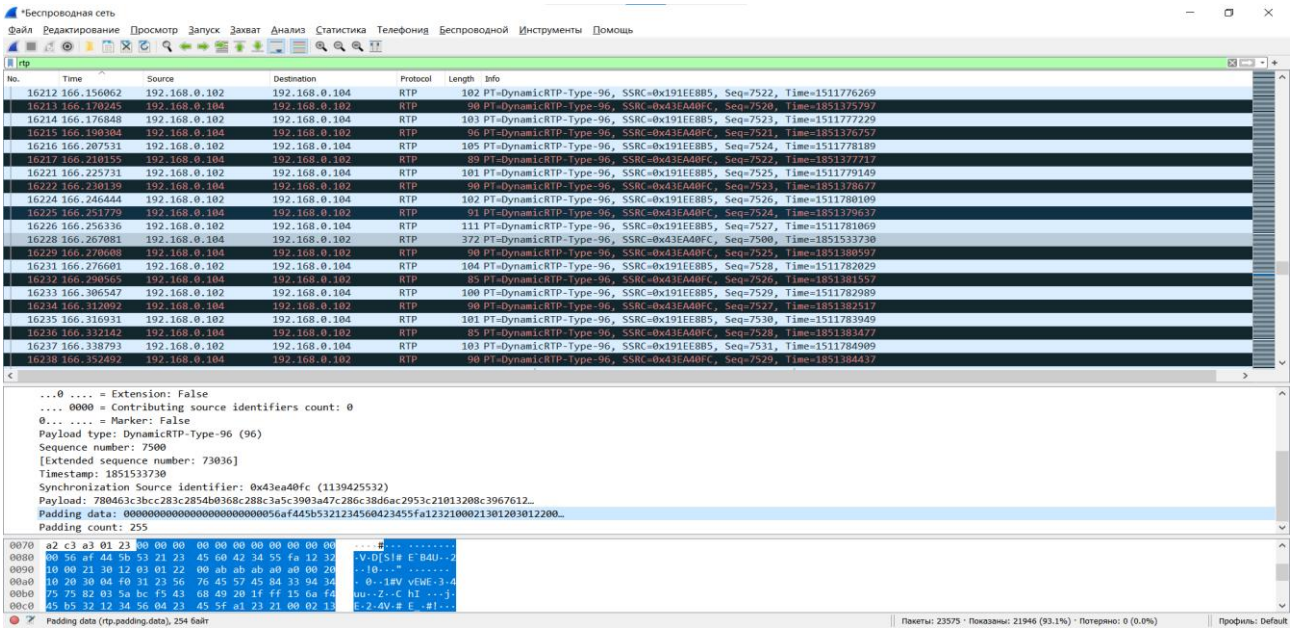


Рис. 3 вложенный пакет со стороны адресанта.

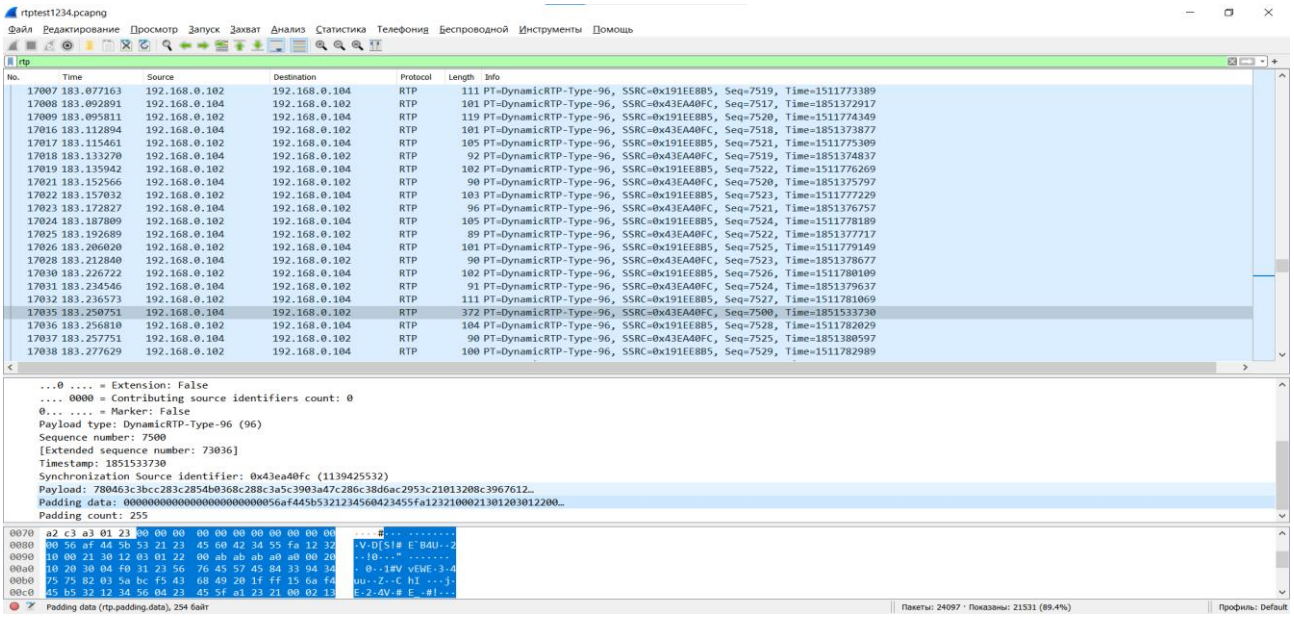


Рис. 4 вложенный пакет со стороны адресата.

В течение трехминутного разговора было передано свыше десяти тысяч пакетов от каждой стороны, заменяя каждый пятисотый пакет можно добиться передачи показанным методом примерно 4500 байт информации теряя 0,2% или 0,36 секунды разговора в течение трёх минут, что несильно повлияет на его качество. Пределом передачи данных следует считать использование не только полей заголовка RTP-пакета, но в дополнении к этому возможность вкладывать в информацию в поля заголовка протокола IPv4 и изменяя полезную нагрузку самого пакета, с учетом потери безопасности данных можно добиться повышения пропускной способности в количестве примерно 1400 байт за один пакет. Если же делать пакет максимально защищенным используя данный метод передачи, то разумнее всего вкладывать информацию в данные пакета и поля его заголовка в том объеме, в котором он был изначально, что составляет замену примерно 60 байт из в среднем 100 байт информации пакета.

Заключение. Из полученного результата следует, что возможность передачи без потери качества соединения через RTP протокол существует. Так как пакет отправляется с задержкой и не будет проигрываться программой со стороны адресата, то имеет смысл формировать стегоконтейнер и из полезной нагрузки самого пакета. Также существует возможность вкладывать дополнительную информацию в некоторые поля заголовков протокола IPv4, тем самым повышая пропускную способность стеганографического канала. Отслеживание данных туннелей затруднено ввиду большого количества передаваемых пакетов потоком без дополнительного анализа, а также в виду того, что пакеты могут задерживаться достаточно часто и невозможно однозначно определить причину задержки.

СПИСОК ЛИТЕРАТУРЫ

1. P. I. Sharikov. Research of the Possibility of Hidden Embedding of a Digital Watermark Using Practical Methods of Channel Steganography / P. I. Sharikov, A. V. Krasov, A. M. Gelfand, N. A. Kosov // Intelligent Distributed Computing XIII, St.-Petersburg, 07–09 октября 2019 года. – St.-Petersburg: Springer Verlag, 2019. – P. 203-209. – DOI 10.1007/978-3-030-32258-8_24.
2. Шелухин О.И. Стеганография. Алгоритмы и программная реализация / Шелухин О.И., Канаев С.Д. // Горячая линия – Телеком 2017. 592 с.
3. Красов, А. В. Практическое применение сетевой стеганографии на примере протокола ICMP / А. В. Красов, Е. И. Степанов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2018 года / Под редакцией С.В. Бачевского. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 510-513.
4. Салита, А. С. Стеганографические вложения в протоколах VOIP / А. С. Салита, Е. М. Гетьман, А. В. Красов // Технологии информационного общества : Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», Москва, 03–04 марта 2021 года. – Москва: ООО "Издательский дом Медиа паблишер", 2021. – С. 52-54.
5. Диордица, В. Н. Исследование современных методов сетевой стеганографии / В. Н. Диордица, А. В. Красов, А. И. Таргонская // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020) : IX Международная научно-техническая и научно-методическая конференция : сборник научных статей, Санкт-Петербург, 26–27 февраля 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020. – С. 404-409.
6. Костырин, А. С. Реализация метода канальной стеганографии с использованием протокола ICMP / А. С. Костырин, А. В. Красов // Региональная информатика и информационная безопасность : сборник научных трудов, Санкт-Петербург, 01–03 ноября 2017 года / Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. – Санкт-Петербург: Санкт-Петербургское

общество информатики, вычислительной техники, систем связи и управления , 2017. – С. 313-316.
7. Волкогонов В.Н. СОКРЫТИЕ ИНФОРМАЦИИ В ПРОТОКОЛАХ RTP, RTCP / Волкогонов В.Н., Гетьман Е.М., Салита А.С. //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). сборник научных статей: в 4 т.. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. С. 183-188.

Окулесский В.А.
МГТУ ГА, к.т.н, доцент
ova175305@mail.ru
Ганичев А.А.
МГТУ ГА, аспирант
sandrooss@rambler.ru

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ РАЗЛИЧНЫХ СТРАТЕГИЙ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение

Трудно найти универсальную меру эффективности созданных или спроектированных систем защиты информации. Если принять основную предпосылку, что главной целью защиты информации является снижение риска для организации в результате несоответствия или нарушения требований информационной безопасности, то основной мерой эффективности должно быть изменение уровня угрозы информационной безопасности и риска нанесения ущерба организации.

Оценка стратегий взаимодействия различных программных мер и оценка их эффективности — это, на первый взгляд, сложная алгоритмическая задача. Очевидно, что единственным подходящим математическим инструментом является теория игр, с помощью которой можно попытаться количественно оценить уровень инвестиций в различные меры системы безопасности организации для снижения риска, который может возникнуть в результате действий злоумышленника.

В принципе, проблема может быть решена, если начальная информация о противнике совершенно не определена. Модель поведения противника может быть недоступна или модель может быть слишком общей для оценки ущерба, вызванного действиями противника.

Рассмотрим более распространенный сценарий модели безопасности 3 [4], в котором серия защитных мер может эффективно снизить риск, связанный с серией угроз, устраняющих слабые места объекта. В этом случае многочисленные защитные меры могут быть использованы для снижения совокупного риска нескольких угроз до приемлемого уровня и достижения приемлемого уровня остаточного риска для модели информационной безопасности.

Основная идея "игрового" подхода заключается в следующем.

Предположим, что планируется комплексная система защиты от вредоносного ПО. Предположим, что существует несколько наборов мер по предотвращению угроз - например, набор, использующий антивирусное ПО, набор, защищающий от направленных атак, набор, управляющий устройствами, и т.д.; назовем их M1, M2..... Mn. Каждый набор требует затрат в размере m1, m2.. mn. Более того, мы предполагаем, что воздействие вредоносных программ также может быть различным; назовем их Z1, Z2…. .Zk. .Zk. Мы предполагаем, что эти действия выполняются спонтанно и независимо, т.е. не следуют какой-либо заранее продуманной стратегии. В зависимости от набора применяемых мер безопасности, эти действия могут привести к различным потерям zij (i = 1...n, j = 1...k). Таким образом, если применяется набор мер Mi и выполняется действие Zj, то общий

ущерб организации равен сумме sij = mi + zij. Эти данные образуют матрицу, представленную ниже:

	Z_1	Z_2	.....	Z_k
M_1	m_1+z_{11}	m_1+z_{12}	.....	m_1+z_{1k}
M_2	m_2+z_{21}	m_2+z_{22}	.....	m_2+z_{2k}
....	.....	.....	.....	.....
M_n	m_n+z_{n1}	m_n+z_{n2}	.....	m_n+z_{nk}

Используя эту матрицу, известную в теории игр как матрица альтернативных потерь, можно сравнить различные стратегии минимизации возможных потерь.

Подготовка данных

Пусть, для определенности, количество видов воздействий, которым может подвергаться защищаемая система, равно пяти, а число вариантов мер безопасности равно трем. Данные, характеризующие деструктивные намерения, приведены в табл. 1. Допустим, что ущерб описывается в условных единицах.

Табл.1

Исходные данные	**Всего**	***Z1***	***Z2***	***Z3***	***Z4***	***Z5***
Кол. инцидентов в год	**12**	**5**	**2**	**1**	**3**	**1**
Вероятность инцидента	**0,20**	**0,4167**	**0,167**	**0,083**	**0,25**	**0,0833**
Средний ущерб от одного инцидента	**23,92**	**17**	**25**	**29**	**34**	**21**
Суммарный ущерб за год	**287**	**85**	**50**	**29**	**102**	**21**

Ущерб определяется при отсутствии каких-либо мер безопасности или при уже существующей системе.

Эффективность проектируемых мер безопасности и затраты на их осуществление приведены в табл. 2

Табл.2

Затраты на комплекс мер	**У.Е.**	**Ущерб от одного инцидента после затрат на безопасность**				
		Z1	***Z2***	***Z3***	***Z4***	***Z5***
M1	**10**	**8**	**15**	**18**	**22**	**13**
M2	**15**	**6**	**7**	**11**	**13**	**9**
M3	**20**	**0**	**5**	**9**	**8**	**7**

Располагая данными табл.1 и 2, можно построить матрицу альтернативных потерь или убытков по схеме, указанной во Введении. Такая матрица представлена в табл.3.

Табл.3

Матрица убытков	**Суммарный убыток**						
	Z1	***Z2***	***Z3***	***Z4***	***Z5***	**Min**	**Max**
M1	**50**	**40**	**28**	**49**	**23**	**23**	**50**
M2	**45**	**29**	**26**	**54**	**24**	**24**	**54**
M3	**20**	**30**	**29**	**44**	**27**	**20**	**44**

Исходя из данных таблицы 3, возможно сделать оценку предполагаемых решений. Для того чтобы использовать методы оценки и терминологию, заимствованную из теории "игры с природой" [1, 2], преобразуем матрицу потерь в [условную] матрицу выигрышей. Мы выполняем это преобразование следующим образом:

$$V_{ij} = C - U_{ij} \qquad (1)$$

где C - константа, удовлетворяющая условию $C > U_{ij}, \forall i, j$.

Выберем значение ***C = 100.***

Введем еще одно понятие, называемое в [1] риском, а в [2] - последствием неправильного решения. Для удобства и краткости будет использован первый подход. Его суть заключается в следующем: предполагая, что мы заранее знаем, что нас атакует только тип Zj, мы применяем набор действий Mi таким образом, чтобы наш выигрыш был максимальным. Значение этого выигрыша - максимальное значение столбца bj, помещенного в строку с меткой b.

Теперь мы имеем матрицу условного выигрыша, показанную в таблице 4.

Табл.4

	Условный выигрыш: C - U (Убыток)						
	Z1	**Z2**	**Z3**	**Z4**	**Z5**	**Min**	**Max**
M1	**50**	**60**	**72**	**51**	**77**	**50**	**77**
M2	**55**	**71**	**74**	**46**	**76**	**46**	**76**
M3	**80**	**70**	**71**	**56**	**73**	**56**	**80**
b	**80**	**71**	**74**	**56**	**77**		

Последние два столбца в таблицах 3 и 4 содержат максимальные и минимальные значения соответствующих строк, а последняя строка в таблице 4 содержит максимальные значения соответствующих столбцов.

Риск r_{ij} применения набора действий Mi при условии наступления события Zj обозначается как разница между выигрышем, который мы получили бы, если бы знали условия Zj, и выигрышем, который мы получили бы, если бы выбрали решение Mi, не зная этих условий. В этом случае риск определяется по следующей формуле:

$$r_{ij} = b_j - v_{ij} \qquad (2)$$

Матрица рисков, соответствующая табл. 4, приведена в табл.5.

Табл.5

Матрица рисков						
	Z1	**Z2**	**Z3**	**Z4**	**Z5**	**Max**
M1	**30**	**11**	**2**	**5**	**0**	**30**
M2	**25**	**0**	**0**	**10**	**1**	**25**
M3	**0**	**1**	**3**	**0**	**4**	**4**

В теории «игры с природой» используются различные критерии оценки качества решений. Некоторые из них рассмотрены ниже.

Оценка качества решений.

1. Максиминный критерий Вальда. Согласно этому критерию, игра с природой подобна игре с умным и агрессивным противником, причем оба они призваны помешать нам добиться успеха. В этом случае оптимальным считается решение, при котором достигается максимальный из минимальных выигрышей, то есть гарантированный выигрыш, который не меньше, чем "малая стоимость игры с природой" [1]:

$$W = \max_i \min_j v_{ij} \qquad (3)$$

Этот критерий отражает "крайне пессимистическое" отношение и требует сосредоточиться на наихудшем сценарии, т.е. подкрепляет предположение, что "хуже быть не может".

2. Критерий минимаксного риска Сэвиджа.

Опять же, этот критерий крайне пессимистичен, но предполагает, что риск (в описанном выше смысле), а не вознаграждение, должен быть ориентиром при принятии решений о выборе, и что решения должны приниматься таким образом, чтобы минимизировать риск:

$$S = \min_i \max_j r_{ij} \qquad (4)$$

Основой этого подхода является то, что при принятии решений избегается любой значительный риск.

3. Критерий Гурвица. Суть этого критерия в том, что при выборе и принятии решений не следует впадать в крайности - ни в крайний пессимизм ("всегда предполагать худшее"), ни в необоснованный оптимизм ("удача обязательно придет"). Решения принимаются условно на основе этого критерия:

$$H = \max_i \left[x \min_j v_{ij} + (1 - x) \max_j v_{ij} \right] \qquad (5)$$

где ***x*** - «коэффициент пессимизма», выбираемый между нулем и единицей.

Критерий Гурвица становится критерием Вальда, когда x=1, и критерием "крайнего оптимизма", когда x=0, отражая надежду на максимальный доход. Некоторое среднее значение получается, когда 0 < x < 1, но выбор коэффициента x всегда произволен.

О выборе критериев. Как только что было подчеркнуто, в оценке приведенных критериев всегда присутствует элемент произвольности, поэтому для получения "пищи для размышлений" и выводов в конкретной ситуации следует использовать несколько критериев с их помощью, учитывая (по большей части) совпадение в оценке различных критериев.

Пример выбора решения.

Чтобы проиллюстрировать это, предлагается рассмотреть несколько примеров рисованных таблиц.

Критерий Вальда. Согласно табл. 4, в предпоследнем столбце находим, что ***W*** = 56, что соответствует решению ***M3***. Заметим, что решению ***M3*** отвечает ***минимальное значение максимального убытка*** (см. табл. 3), т.е. относительно убытков **максиминный** критерий превращается в **минимаксный**:

$$W = \min_i \max_j v_{ij} \qquad (6)$$

и $\overline{W} = 44$

Критерий Сэвиджа. Из матрицы рисков находим, что минимум максимального риска ***S*** = 4 также соответствует решению ***M3***.

Критерий Гурвица. Значения критерия при разных коэффициентах пессимизма приведены в табл. 6, из которой видно, что при всех значения ***x*** в пределах от нуля до единицы предпочтение отдается решению ***M3***.

Табл.6

	Оценки Гурвица				
	Оптимистические		**Средняя**	**Пессимистические**	
x =	**0**	**0,3**	**0,5**	**0,7**	**1**
M1	**77**	**68,9**	**63,5**	**58,1**	**50**
M2	**76**	**51,8**	**61**	**55**	**46**
M3	**80**	**72,8**	**68**	**63,2**	**56**

Это означает, что случайно выбранные для примера числа дают стабильный результат: все критерии в пользу решения ***M3***. Это можно объяснить удачным сочетанием снижения затрат и случайного ущерба в данной альтернативе. Чтобы проиллюстрировать работу этих критериев, мы проанализируем случаи, в которых один и тот же результат получен при разных затратах. Результаты этого анализа представлены в таблице 7.

Табл. 7.

	Q3 =	20	25	26	30
Вальд		**M3**	**M3**	**M1, M3**	**M1**
Сэвидж		**M3**	**M3**	**M3**	**M3**
Гурвиц	**Оптим.**	**M3**	**M1**	**M1**	**M1**
	Пессим.	**M3**	**M3**	**M1 (x<1)**	**M1**

Из этой таблицы хорошо видно, что при увеличении стоимости варианта ***M3*** (при одинаковых результатах) предпочтение постепенно смещается к варианту ***M1,*** при этом к варианту ***M3*** применяется только критерий Сэвиджа, но при Q3 > 30 он отказывается от варианта ***M3*** в пользу ***M2***.

Заключение

Предлагаемая методика может быть легко алгоритмизирована и может служить основой для разработки приложений для предварительной оценки эффективности различных стратегий построения/совершенствования системы обеспечения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Вентцель Е.С. Исследование операций. Задачи, принципы, методология. - М.: Наука, 1988.
2. Ланге О. Оптимальные решения. Основы программирования. - М.: Прогресс, 1967.
3. Гермейер Ю.Б. Введение в теорию исследования операций. - М.: Наука, 1971.
4. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 13335-1-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2006 г. N 317-ст)
5. ГОСТ Р ИСО/МЭК 27005 – 2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
6. ГОСТ Р ИСО/МЭК 27000 – 2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.
7. ГОСТ Р ИСО/МЭК 27001 – 2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
8. Конституция Российской Федерации (действ.ред. 01.07.2020).
9. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 № 646).
10. Федеральный закон от 27.07.2006 №149-ФЗ (ред.от 25.11.2017) «Об информации, информационных технологиях и о защите информации».

Ермаков К.Д.
Филиал МГУ имени М.В. Ломоносова в г. Сарове, магистр
ermakov-kir@mail.ru
Милешин И.Г.
Филиал МГУ имени М.В. Ломоносова в г. Сарове
komrad.mileshin@yandex.ru
Николаев Д.Б.
СарФТИ НИЯУ МИФИ, заведующий кафедрой, д.т.н., доцент
dim010307@yandex.ru

ИССЛЕДОВАНИЕ АЛГЕБРАИЧЕСКИХ СВОЙСТВ АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ MV-3

Введение

В информационном обществе одной из основных задач является сохранение информационных ресурсов, а также их защита от несанкционированного доступа [1-4]. Одним из эффективных способов создания защиты в электронных системах является применение криптографических методов защиты. Большую часть таких методов составляют симметричные алгоритмы шифрования, которые разделяются на блочные и поточные.

Алгоритмы поточного шифрования играют важную роль в практической криптографии, в частности, для шифрования длинных потоков данных [5-7]. В криптосистемах поточного шифрования один и тот же ключевой поток (гамма) не должен использоваться для шифрования двух разных сообщений. Для решения этой проблемы такие криптосистемы были оснащены алгоритмом инициализации ключа, который принимает начальный вектор (IV) и относительно короткую строку ключа в качестве входных данных [8-10]. После этого генерируется произвольно длинный ключевой поток.

В 2007 г. Keller [1] представил поточный шифр на основе слов (32-разрядные целые числа без знака), называемый MV-3. MV-3 разрабатывался посредством модификации RC4- подобных алгоритмов поточного шифрования для достижения большей скорости шифрования данных. MV3 поддерживает ключи различных размеров, вплоть до 8192 бит, также было заявлено, что для ключей длиной до 256 бит, не может быть проведена атака быстрее, чем полный перебор ключа.

Целью данной работы является исследование алгебраических свойств алгоритма поточного шифрования MV-3, в том числе восстановление исходного внутреннего состояния автомата, моделирующего модифицированный алгоритм, по состоянию на фиксированном такте и выработанной гамме.

Алгоритм поточного шифрования MV-3

MV3 – система поточного шифрования на основе слов (32-разрядные целые числа без знака), которая была представлена на конференциях CT-RSA 2007 и SASC 2007. Несмотря на то, что она поддерживает ключи различных размеров до 8192 бит, заявка на безопасность MV3 состоит в том, что никакая атака быстрее, чем полный перебор ключа, не может быть произведена для ключей длиной до 256 бит. Целью разработчиков данного шифра было создание аналога RC4- подобных алгоритмов поточного шифрования, использующего большие размеры символов (слова размером 32 бита).

Основными компонентами внутреннего состояния mv-3 являются три смещающихся массива A, B и C длиной 32 двойных слова (32-разрядные целые числа без знака) каждое и таблица T, состоящая из 256 двойных слов.

Кроме того, существуют известные значения i и u (где $i \in \{0 \dots 31\}$, $u \in \{ 0 \dots 255\}$) и секретные значения $j, c,$ и x (c, x - двойные слова, j - беззнаковый байт).

Инициализация ключа проходит в 2 этапа. На первом этапе три вектора A, B, C и таблица T инициализируются целым числом без знака 0xEF. Алгоритм принимает длинную строку ключа длины K, которая может быть кратна 32, а также меньше или равна 8192 (рекомендуемый размер, по крайней мере, 96). Эта фаза, используя строку ключа K, обновляет записи таблицы T. На втором этапе алгоритма начальный вектор (IV) используется для обновления записей таблицы T. Поскольку долгосрочный ключ K фиксирован, для каждого шифрования выбирается новый IV, и, таким образом, выполняется только вторая фаза алгоритма.

В виде псевдокода, алгоритм инициализация ключа выглядит, как представлено ниже:

Input: ключ *k* и начальный вектор *IV*, оба длины *kl* двойных слов
Output: внутреннее состояния зависящее от the *k* и *IV*
j, x, u ≔ 0
c := 1
заполнение A, B, C, T числами 0xEF
for i = 0 to 3
for l = 0 to 255
    T_{i+1} := T_{i+1} + (*k*[l mod *kl*] >>> 8i) + l.
конец for
выработать 1024 байта гаммы mv-3
зашифровать T полученной гаммой
конец for
for i = 4 to 7
for l = 0 to 255
    T_{i+1} ≔ T_{i+1} + (IV[l mod *kl*] >>> 8i) + l.
конец for
выработать 1024 байта гаммы mv-3
зашифровать T полученной гаммой
конец for
конец

Алгоритм выработки гаммы шифра MV-3. Каждые 32 шага массивы сдвигаются влево: $A \coloneqq B, B \coloneqq C$ и C очищается. В Таблице T каждые 32 шага обновляется одна запись, применяя следующие две операции ($x >>> a$ означает циклический сдвиг двойного слова x на a битов вправо):

$$u \coloneqq u + 1, (1)$$

$$T_u \coloneqq T_u + (T_j >>> 13). (2)$$

Другими словами, u-ый элемент таблицы, обновляется с помощью j-ого элемента. В свою очередь, значение j меняется, как описано ниже:

$$j \coloneqq j + (B_i \ (mod\ 256), (4)$$

где i значение номера цикла. Значение j используется для обновления x:

$$x \coloneqq x + T_{\mathrm{j}}, \text{ (4)}$$

которое используется для заполнения буфера C как

$$(C_{\mathrm{i}} \coloneqq (x >>> 8)). \text{ (5)}$$

Кроме того, каждые 32 шага множитель c аддитивно и мультипликативно обновляется следующим образом:

$$c \coloneqq c + (A_0 >>> 16) . \text{ (7)}$$

$$c \coloneqq c \vee 1 . \text{ (8)}$$

$$c \coloneqq c^2 . \text{ (9)}$$

Последним компонентом основного цикла шифра является алгоритм по выработке гаммы. Он принимает следующий вид:

$$\text{output: } (x \cdot c) \oplus A_{9\mathrm{i}+5} \oplus (B_{7\mathrm{i}+18} >>> 16) \text{ (10)}$$

В результате, алгоритм выработки гаммы выглядит, как показано ниже (алгоритм представлен в виде псевдокода):

Начальное заполнение: $A, B, C, T, j, x, c; i = u = 0;$

Ввод: длина l

Вывод: поток длины l

повторить l/32 раз

for i = 0 to 31

$j \coloneqq j + (B_{\mathrm{i}} \ (mod\ 256)$

$x \coloneqq x + T_{\mathrm{j}}$

$C_{\mathrm{i}} \coloneqq (x >>> 8)$

вывод $(x \cdot c) \oplus A_{9\mathrm{i}+5} \oplus (B_{7\mathrm{i}+18} >>> 16)$

конец for

$u \coloneqq u + 1$

$T_{\mathrm{u}} \coloneqq T_{\mathrm{u}} + (T_{\mathrm{j}} >>> 13)$

$c \coloneqq c + (A_0 >>> 16)$

$c \coloneqq c \vee 1$

$c \coloneqq c^2$

$A \coloneqq B, B \coloneqq C$

конец.

Стоит отметить, что для вычисления верных результатов все операции сложения и умножения должны проводиться по модулю 2^{32} .

Исследование свойств алгоритма MV-3

Для определения начального состояния автомата, моделирующего алгоритм, алгоритм был модифицирован. Массивы A, B и C были уменьшены до длин по 8 двойных слов (8-разрядные целые числа без знака) каждое. Размеры таблицы T были уменьшены до размера в 16 двойных слов. Также были изменены значения сдвига слов и выработки гаммы.

Алгоритм получения возможного внутреннего состояния автомата на предыдущем такте, моделирующего модифицированный алгоритм mv-3, выглядит следующим образом:

Начальное данные: A, B, C, T, j, x, c, u на t такте ; $Z = 0, x_1 = 0$.

Вывод: A, B, C, T, j, x, c, u на $(t-1)$ такте

$B \coloneqq A$

$c \coloneqq \sqrt{c} \pmod{256}$

Для каждого полученного c

$c \in Z$

$(c-1) \in Z$

$(T_u) \coloneqq T_u - (T_j >>> 3)$

$u \coloneqq u - 1$

For i = 0 to 7

$j \coloneqq j$ - (B_i mod 16)

$x \coloneqq x$ - T_j

Для каждого c ∈ Z

Перебор возможных корней уравнения (неизвестное - x_1):

$$c = x_1 + ((\Gamma_0 \oplus x_1 \cdot x \oplus (B_1 >>> 6)) >>> 5)$$

Для каждого полученного x_1

for i = 7 to 0

$A_i \coloneqq \Gamma_i \oplus (x \cdot c) \oplus A_i \oplus (B_{4i+1} >>> 6)$

j ≔ j - (B_i mod 16)

x ≔ x – T_j

конец for

Проверим его работу экспериментально. Заполним массивы A, B, таблицу T, а также x, c, u, j псевдослучайными значениями, для определения их в дальнейшем. Начальные данные (представлены в десятичной системе счисления для удобства):

$$A = (41,35,190,132,225,108,214,174),$$
$$B = (82,144,73,241,241,187,233,235),$$
$$T = (36,94,13,28,6,183,71,222,179,18,77,200,67,187,139,166),$$
$$x = 96, c = 122, u = 6, j = 5.$$

Запустив цикл на выработку гаммы длины 8, получаются следующие значения:

$$A = (82,144,73,241,241,187,233,235),$$
$$B = C = (143,7,16,167,234,153,107,194),$$
$$T = (36,94,13,28,6,183,71,169,179,18,77,200,67,187,139,166),$$
$$x = 11, c = 137, u = 7, j = 1,$$
$$\Gamma = (231,149,124,38,221,30,230,126).$$

При l=8 основной цикл отработал только 1 раз.

Следовательно, начиная с конца, первой обратно считается операция смещения

$$A \coloneqq B, B \coloneqq C. \quad (11)$$

Тогда

$$B = A = \{82,144,73,241,241,187,233,235\},$$
$$C = \{143,7,16,167,234,153,107,194\}.$$

Массив A неизвестен. Его необходимо вычислить.

Следующей операцией является

$$c \coloneqq c^2, \quad (12)$$

что значит необходимо найти решение уравнения:

$$X^2 = 137 \bmod 2^8. \quad (13)$$

У данного уравнения есть 4 корня, ими являются

$$c \in \{61,67,189,195\}.$$

Операция $c = c \vee 1$ увеличивает количество возможных c,что значит,

$$c \in \{60,61,67,66,189,188,194,195\}.$$

Касательно операции $c = c + (A_0 >>> 5)$, имеются 2 неизвестных c и A_0.

Также имеется гамма, фрагменты которой вычисляются как

$$(x \cdot c) \oplus A_0 \oplus (B_0 >>> 6)\ . (14)$$

Значит, можно определить, в участии создания какого фрагмента гаммы также использовалось A_0. Такой является $\Gamma_i=\Gamma_0=231$.Т.е.

$$231 = (x \cdot c) \oplus A_0 \oplus (B_1 >>> 6) = (x \cdot c) \oplus A_0 \oplus 66. (15)$$

Отсюда неизвестны переменные x, c, A_0. Переменную x можно найти, для этого сначала необходимо обратить операцию

$$T_u := T_u + (T_j >>> 3)\ . (16)$$

Отсюда, подставляя известные значения:

$$169 = T_u + (94 >>> 3) \bmod 256, (17)$$

$$169 = T_u + (203) \bmod 256, (18)$$

$$T_u = 222. (19)$$

Начальная таблица T найдена. Далее, x определяется из операций:

$$j := j + (B_i \bmod 16), (20)$$

$$x = x + T_j\ . (21)$$

Т.е. для получения x при i=0,необходимо 7 раз вычислить j и отнять T_j. Отсюда x=62.

Обозначив $c=x_1, A_0=x_2$, получаются системы уравнений, где операции сложения и умножения происходят по модулю 256.

Перебирая все возможные значения секретного слова c (2^8 переборов), получаются возможные значения $c \in \{24,54,84,122,152,182,212,250\}$

Отсюда, A_0 может быть следующим:

$$A_0 \in \{117,177,253,41,117,177,253,41\}.$$

Далее, по фрагментам гаммы можно восстановить оставшиеся элементы массивов (цикл представлен в виде псевдокода):

```
for i = 7 to 0
    A_i := Γ_i ⊕ (x · c) ⊕ A_i ⊕ (B_{4i+1} >>> 6)
    j := j - (B_i mod 16)
    x := x – T_j
конец for.
```

В итоге получаются следующие массивы A:

A=(117,219,62,24,151,96,156,152) при c=24;

A=(177,147,190,156,141,116,218,194) при c =54;

A=(253,75,62,16,131,136,96,12) при c =84;

A=(41,35,190,132,225,108,214,174) при c =122;

A=(117,219,62,24,23,96,28,24) при c =152;

A=(177,147,190,156,13,116,90,66) при c =182;

A=(253,75,62,16,3,136,224,140) при c =212;

A=(41,35,190,132,97,108,86,46) при c =150.

При проверке все эти массивы дают корректную гамму Г:

Г =(231,149,124,38,221,30,230,126).

Т.е. было найдено 8 таких исходных состояний, при которых вырабатывается одинаковая гамма. Трудоёмкость нахождения внутреннего состояния автомата на предыдущем такте равна трудоемкости перебора 2^8 значений переменной c. Количество возможных исходных состояний равно количеству корней полученных уравнений. Применяя выработанный метод нахождения исходного состояния к алгоритму шифрования MV-3, получается, что необходимо перебрать 2^{32} значений, что значительно меньше $2^{32}*2^{1024}=2^{1056}$ (количество переборов возможных значений переменной c и массива A).

Однако при длине выработанной гаммы шифра l=64 , количество переборов увеличивается до $2^{32}+2^{32}=2^{33}$, так как будет необходимо восстановить внутреннее состояние автомата на двух предыдущих тактах работы. В то же время, перебор двух массивов (A, B) и секретного значения c займет $2^{32}*2^{1024}*2^{1024}=2^{2080}$ переборов.

Заключение

В результате работы было проведено исследование алгебраических свойств алгоритма поточного шифрования MV-3. Было успешно получено исходное состояние автомата моделирующего алгоритм, по его конечному состоянию и выходной гамме. Также были найдены аналогичные значения массива A и секретного слова c, при котором вырабатывается корректное значение гаммы. Из этого следует, что у графа состояний автомата, моделирующего алгоритм поточного шифрования, существуют подходы.

СПИСОК ЛИТЕРАТУРЫ

1. Грибунин В.Г., Костюков В.Е., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Современные методы обеспечения безопасности информации в атомной энергетике: Монография / Под ред. А.И. Астайкина. – Саров: ФГУП «РЯФЦ-ВНИИЭФ», 2014. – 636 с. – ил.

2. Шишкин, Г. Селекторы цифровых команд. Часть 2 / Г. Шишкин, Д. Николаев // Компоненты и технологии. – 2009. – № 8(97). – С. 112-116.

3. Шишкин, Г. Селекторы цифровых команд. Часть 3 / Г. Шишкин, Д. Николаев // Компоненты и технологии. – 2009. – № 9(98). – С. 116-120.

4. Патент № 2402810 C2 Российская Федерация, МПК G06F 21/22, G06F 12/14. Устройство защиты от несанкционированного доступа к информации : № 2009102674/08 : заявл. 27.01.2009 : опубл. 27.10.2010 / А. А. Курочкин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко

5. Мартынов А.П., Мартынова И.А., Фомченко В.Н. Аксиоматические основы функций подстановки в системе счисления ряда факториальных множеств и их характеристики: Монография. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2019. – 210 с.: ил.

6. Мартынова, И.А., Машин, И.Г., Фомченко, В.Н. Теория поля и защита информации: Монография. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2017. – 209 с. : ил.

7. Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и электроника / Под ред. А.И. Астайкина. 2-е издание, переработанное и дополненное. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2020. – 552 с.

8. Методы и средства комплексной защиты информации в технических системах. Учебное пособие / Э.В. Запонов и др. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2019. – 224 с.

9. Криптография и безопасность цифровых систем / В. Г. Грибунин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко ; ФГУП «РФЯЦ-ВНИИЭФ». – Саров : ФГУП «РФЯЦ-ВНИИЭФ», 2011. – 411 с.

10. Мартынов, А. П. Обеспечение безопасного взаимодействия компонентов интегрированной системы / А. П. Мартынов, К. О. Волков, Д. Б. Николаев // Инновации в условиях развития информационно-коммуникационных технологий. – 2008. – № 1. – С. 136-138.

Ермаков К.Д.
Филиал МГУ имени М.В. Ломоносова в г. Сарове, магистр
ermakov-kir@mail.ru
Милешин И.Г.
Филиал МГУ имени М.В. Ломоносова в г. Сарове
komrad.mileshin@yandex.ru
Николаев Д.Б.
СарФТИ НИЯУ МИФИ, заведующий кафедрой, д.т.н., доцент
dim010307@yandex.ru

ПРИБЛИЖЕНИЕ ОПЕРАЦИИ ДИЭДРАЛЬНОЙ ГРУППЫ ОПЕРАЦИЕЙ СЛОЖЕНИЯ

Введение

Для криптоаналитика, при анализе алгоритмов шифрования, как блочных, так и поточных, важно найти эффективный метод уменьшения их стойкости линейному криптоанализу. Как известно, большое количество алгоритмов шифрования обычно состоит из нескольких действий или операций.

Операция сложения по модулю 2^n, особенно при n равном длине цифрового слова (таком как 8,16 или 32), является одной из распространённых операций, повсеместно используемой в алгоритмах шифрования [1-3]. Большой объем полученных результатов исследований по операции сложения можно найти в [4-16].

В работах [5,6] аналитиками рассматривается аппроксимация данной операции до операции сложения по модулю 2. В данных исследованиях криптоаналитики объясняют различия между данными операциями, а также зависимость вероятности появления бита переноса при сложении чисел от порядка данного бита в двоичном представлении числа результата.

Значимой алгебраической системой, изучаемой криптоаналитиками, является группа симметрий многоугольника, называемой группой диэдра. Данная группа обладает рядом свойств, позволяющих использовать ее в алгоритмах шифрования.

Группа диэдра является неабелевой (некоммутативной) и наиболее похожей на нее абелевой группой является аддитивная группа кольца вычетов. Операция сложения в кольце встречается в большом количестве алгоритмов шифрования, в криптоанализе аналитики стараются аппроксимировать ее до максимально похожих операций, обычно до побитового сложения по модулю 2. В данной работе, аппроксимация проводится до операции в группе диэдра для выявления различных свойств, способных помочь в линейном криптоанализе различных алгоритмов шифрования, в которых применяется данная операция.

На данный момент, в открытых источниках, работ, связанных с аппроксимированием операций сложения в кольце и операцией в группе диэдра, найдено не было. Учитывая тот факт, что операция в группе диэдра является некоммутативной, логично исследовать данную область.

Аппроксимация операции Диэдральной группы

Симметрии правильного многоугольника с $n \geq 3$ сторонами составляют неабелеву группу порядка $2n$. Вершины нумеруются числами $1,2,\dots,n$ по часовой стрелке. Все симметрии порождаются вращением a и отражением b.

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$$

В данной группе $a^n = 1, b^2 = 1, ba = a^{-1}b$.Более того, эти отношения полностью определяют группу, так как любой элемент, порожденный a и b, имеет вид $a_1^i b_1^i \dots a_r^i b_r^i$, и благодаря равенству $ba = a^{-1}b$ каждый элемент может быть приведен к виду a^i или $a^i b$ при $i = 0,1,\dots,n-1$.

Для определения свойств аппроксимации было принято решение провести эксперимент для группы диэдра D_4. При количестве вершин равном 4 в группе диэдра существует 8 элементов. Они представлены на рисунке 1 ниже.

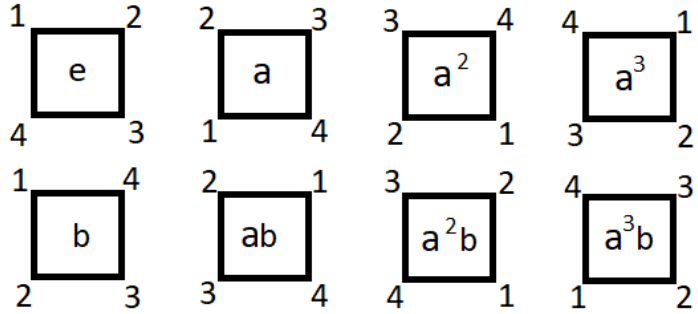


Рис. 1. Элементы группы D_4

Элементы данной группы можно также представить в виде подстановок. В таблице 1 приведена таблица Кэли группы D_4, где операцией является композиция подстановок. Необходимо отметить, что операция не является коммутативной.

Табл. 1 Таблица Кэли для группы D_4

	e	b	a	ab	a^2	a^2b	a^3	a^3b
e	e	b	a	ab	a^2	a^2b	a^3	a^3b
b	b	e	ab	a	a^2b	a^2	a^3b	a^3
a	a	a^3b	a^2	b	a^3	ab	e	a^2b
ab	ab	a^3	a^2b	e	a^3b	a	b	a^2
a^2	a^2	a^2b	a^3	a^3b	e	b	a	ab
a^2b	a^2b	a^2	a^3b	a^3	b	e	ab	a
a^3	a^3	ab	e	a^2b	a	a^3b	a^2	b

Для аппроксимации данной операции на операцию сложения в аддитивной группе кольца Z_8 необходимо биективно отобразить группу D_4 в аддитивную группу кольца Z_8 так, чтобы таблицы Кэли обеих операций максимально совпадали. Для этого, после каждого возможного отображения подсчитаем максимальный коэффициент c совпадения бит соответствующих элементов таблицы, $0 \leq c \leq 1$. Допустим $i-$ номер элемента таблицы Кэли, $x_i -$ расстояние Хэмминга между векторами $i-$ых элементов таблицы,

$y-$ число бит, необходимое для двоичного представления числа $2^n - 1$. Коэффициент для кольца Z_{2^n} равен:

$$c = \frac{\sum_{i=0}^{2^{2n}-1} \frac{x_i}{y}}{2^{2n}} \quad (1)$$

Опытным путем, перебирая все возможные отображения, наилучшей кодировкой является следующая:

$$e \to 0; b \to 1; a \to 2; ab \to 3; a^2 \to 4; a^2b \to 5; a^3 \to 6; a^3b \to 7; \quad (2)$$

Коэффициент совпадения при данной кодировке составляет 0,8(3). Таблица 2 отображает некоторые возможные кодировки множества $\{e, b, a, ab, a^2, a^2b, a^3, a^3b\}$, при которых коэффициент c является наибольшим.

Табл. 2 Возможные кодировки группы D_4

Кодировка элементов D_4	**Коэффициент**
0 1 2 3 4 5 6 7	0,8(3)
0 1 2 7 4 5 6 3	0,791667
0 1 2 7 4 5 3 6	0,708(3)
0 1 2 3 6 4 5 7	0,75

Полученные свойства аппроксимации

Из результатов эксперимента была выдвинута гипотеза о такой кодировке группы $D_{2^{n-1}}$, при которой коэффициент совпадения максимален:

$$a^i \to 2i, (2)$$
$$a^ib \to 2i + 1, \text{ где } i \in \{0,1, \dots, 2^{n-1} - 1\} \quad (3)$$

Данная гипотеза подтверждается экспериментально. При увеличении числа n значение коэффициента совпадения c уменьшается. Также было определено количество полностью совпадающих элементов таблиц Кэли. При оптимальной кодировке и операции вида $x * y$, где x и y закодированные элементы группы диэдра, (*) – операция композиции подстановок, полностью совпадают элементы соответственно при:

$$x = e \text{ или } x = a^{2^{n-2}} \text{ и } y \in D_{2^{n-1}}, \quad (4)$$
$$x \in D_{2^{n-1}} \text{ и } y \text{ вида } 2k, k \in \{0,1, \dots, 2^{n-1} - 1\} \quad (5)$$

Всего количество полностью совпадающих элементов таблицы Кэли при аппроксимации операций групп $D_{2^{n-1}}$ и Z_{2^n} равно:

$$2^n\left(\frac{2^n}{2} + 1\right) = 2^n(2^{n-1} + 1) = 2^{2n-1} + 2^n \quad (6)$$

Также в ходе проведения экспериментов с различными значениями n было замечено, что даже если элементы таблиц не совпадают полностью, то всегда как минимум 1 бит в их двоичном представлении будет совпадать. Количество чисел с совпадением ровно в 1 бит равно 2^n, все они имеют вид a^i , $i \in \{0,1, \dots, 2^{n-1}-1\}$ в группе диэдра.

Объединив полученные данные и считая, что у оставшихся элементов совпадает минимум 2 бита в их двоичном представлении можно привести оценку нижней границы коэффициента совпадения таблиц Кэли данных операций:

$$\frac{2^{2n-1}(n+2)+2^n(n+1)-2^{n+2}}{2^{2n}n^2} \quad (7)$$

Помимо полученных свойств был разработан и запрограммирован алгоритм получения точного коэффициента таблиц Кэли групп заданного порядка. Алгоритм для определения коэффициента состоит из двух этапов. На первом (подготовительном) этапе определяется и кодируется группа диэдра порядка 2^{n-1}, после чего составляются таблицы Кэли для $D_{2^{n-1}}$ и Z_{2^n}. На втором (заключительном) этапе вычисляется коэффициент совпадения таблиц. На рисунке 2 представлены результаты работы алгоритма.

n	коэффициент совпадения	количество полностью совпадающих элементов таблиц Кэли	количество элементов в таблице Кэли
3	0,8(3)	40	64
4	0,8125	144	256
5	0,8	544	1024
6	0,791667	2112	4096
7	0,785714	8320	16384
8	0,78125	33024	65536
9	0,77778	131584	262144
10	0,775	525312	1048576
11	0,7772727	2099200	4194304

Рис. 2. Результаты работы алгоритма

Заключение

В результате работы было проведено исследование свойств аппроксимации операций на группе диэдра и аддитивной группе кольца вычетов. Успешно была определена успешная кодировка для наибольшего совпадения, а также оценена нижняя граница коэффициента совпадения бит в двоичном представлении элементов групп. В работе был представлен алгоритм по нахождению точного коэффициента совпадения при заданном числе элементов. Алгоритм был реализован на языке C++ в среде Visual Studio.

СПИСОК ЛИТЕРАТУРЫ

1. M. Matsui, Linear cryptanalysis method for DES cipher, In Advance in Cryptology-Eurocrypt 1993, LNCS 950, pp.366-275, Springer-Verlag, 1995.
2. K. Nyberg, Linear approximations of block ciphers, In Advances in CryptologyEurocrypt 1994, LNCS 950, pp.439-444, Springer-Verlag, 1995.

3. D. Coppersmith, S. Halevi and C. Jutla, Cryptanalysis of stream ciphers with linear masking, In Advances in Crypto 2002, LNCS 2442, Springer-Verlag, pp.515532, 2002.

4. K. Nyberg and J. Wall´ en, Improved Linear Distinguishers for SNOW 2.0, In:M.J.B.Robshaw.(ed.) FSE 2006. LNCS 4047, pp.144-162, 2006.

5. J. Wall´ en, Linear Approximations of Addition Modulo 2n, FSE 2003, LNCS 2887, Spring-Verlag, pp.261–273, 2003.

6. T.A. Berson, Diff erential Cryptanalysis Mod 232 with Applications to MD5, EUROCRYPT92, LNCS658, pp.71-80, 1993.

7. H. Lipmaa and S. Moriai, Efficient algorithms for computing diff erential properties of addition. In Fast Software Encryption 2001, LNCS 2355, pp.336C350, Springer-Verlag, 2002.

8. N.T. Courtois and B. Debraize, Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0, ICICS2008, LNCS5308, pp.328-344, 2008.

9. A. Maximov and T. Johansson, Fast Computation of Large Distributions and Its Cryptographic Applications, ASIACRYPT2005, LNCS 3788, pp.313-332, 2005.

10. K. Nyberg, Correlation theorems in cryptanalysis, Discrete Applied Mathemaics, pp.177-188, 2001.

11. Шишкин, Г. Селекторы цифровых команд. Часть 1 / Г. Шишкин, Д. Николаев // Компоненты и технологии. – 2009. – № 6(95). – С. 96-101.

12. Шишкин, Г. Селекторы цифровых команд. Часть 2 / Г. Шишкин, Д. Николаев // Компоненты и технологии. – 2009. – № 8(97). – С. 112-116.

13. Шишкин, Г. Селекторы цифровых команд. Часть 3 / Г. Шишкин, Д. Николаев // Компоненты и технологии. – 2009. – № 9(98). – С. 116-120.

14. Шишкин, Г. Селекторы цифровых команд. Часть 4 / Г. Шишкин, Д. Николаев // Компоненты и технологии. – 2009. – № 11(100). – С. 102-106.

15. Схемотехническая реализация автомата / С. Гончаров, Д. Николаев, В. Никитин, В. Писецкий // Компоненты и технологии. – 2013. – № 2(139). – С. 126-128.

16. Патент № 2256053 C2 Российская Федерация, МПК E05B 49/00. Устройство управления электронными замками : № 2003101484/12 : заявл. 20.01.2003 : опубл. 10.07.2005 / С. Н. Гончаров, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко.

Полтавцева М.А.
СПбПУ, доцент, к.т.н., доцент
poltavtseva@ibks.spbstu.ru

АДАТИВНЫЙ МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПКФС НА ОСНОВЕ СИСТЕМОЛОГИЧЕСКОГО ПОДХОДА

Сегодня большое число индустриальных систем с цифровым управлением доступны для злоумышленника [1,2]. Происходит расширение функций мониторинга безопасности в сторону интеграции с системами SOAR (Security Orchestration, Automation and Response), анализа рисков, прогноза [3,4]. Введение SOC требует представления объекта защиты в различных ракурсах [5].

Система мониторинга становится сложным интеллектуальным комплексом, поставляющим готовые данные для принятия решений в систему управления безопасностью. Она должна гибко реагировать на изменения задач безопасности и характеристик объекта защиты. Сегодня системы мониторинга информационной безопасности прошли большой путь начиная от локальных решений и анализа сигнатур до распределенных центов безопасности, интегрированных с другими системами, собирающих разнородные потоки данных и подготавливающих их для принятия решений [3-8].

Решение задачи оперативной обработки данных для разнородных методов решения задач безопасности в современных условиях невозможно без интеграции мониторинга с самими методами, так как именно они выступают в роли «потребителей» данных и определяют какая информация, в каком объеме и в какой срок должна быть подготовлена [9]. В этих условиях происходит интеграция систем мониторинга, методов анализа данных и решения задач безопасности.

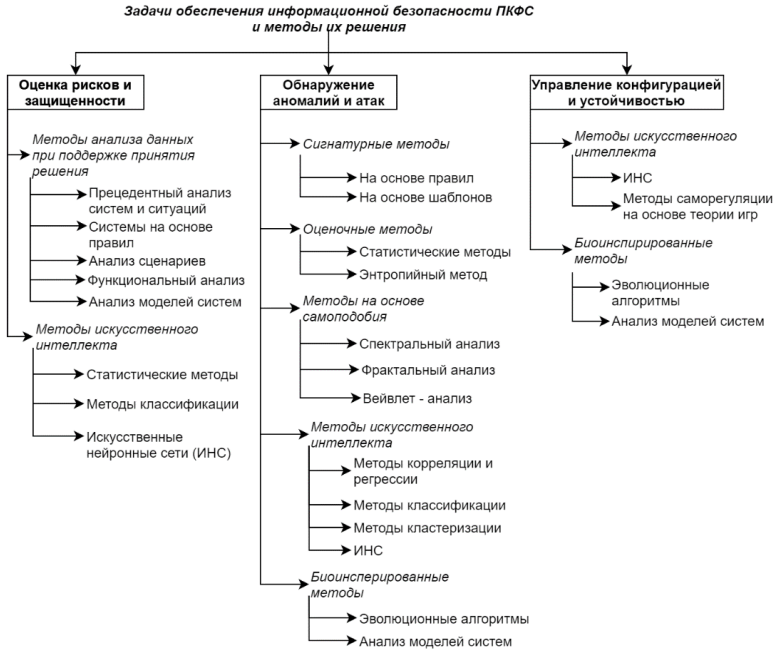


Рис. 1. Методы решения задач безопасности при МИБ ПКФС

Промышленные киберфизические системы, как объект мониторинга информационной безопасности, являются объектом применения широкого спектра

методов решения задач безопасности (рисунок 1). Возникает противоречие между разнородными требованиями методов к данным и самой системе мониторинга и ростом вычислительной нагрузки, обусловленной размером, гетерогенностью и скоростью поступления данных в промышленных киберфизических системах [10-12]. Решение этого противоречия заключается в адаптации системы мониторинга к ключевым процессам объекта защиты. При этом важным фактором является сохранение таких характеристик как оперативность, полнота и достоверность данных для принятия решения.

Для решения этой проблемы предлагается системологический подход к адаптивному мониторингу ИБ ПКФС, включающий принципы целостности, конвергенции и иерархической связности.

Принцип целостности, согласно общей теории систем и методологии системного анализа, обуславливает рассмотрение промышленной киберфизической системы с учетом взаимосвязи и взаимодействия различных компонентов, включая данные, методы их обработки и решаемые таким образом задачи.

Принцип иерархической связности обуславливает возможность декомпозиции или агрегации компонентов ПКФС в зависимости от задачи безопасности и метода ее решения, включая возможности построения структурных иерархий, иерархий процессов, и других представлений, необходимых центрам безопасности.

Принцип конвергенции подчеркивает взаимосвязь внешней среды, включая пул решаемых задач, с характеристиками объекта защиты, применяемыми методами мониторинга и управления безопасностью.

Для реализации подхода предлагается методология управления адаптивным мониторингом информационной безопасности ПКФС, основанная на согласовании собираемых наборов данных объекта защиты и методов решения задач безопасности с текущим перечнем этих задач. Существование тройственного отображения между задачами безопасности, методами решения и данными показывает возможность решения заданного набора задач безопасности при имеющихся данных и методах.

При интеллектуальном управлении адаптивным мониторингом информационной безопасности ПКФС на основе взаимных отображений водится понятие схемы мониторинга [12]. Схема мониторинга - набор и порядок методов, применяемых для обработки и анализа данных объекта защиты при решении текущих задач безопасности, то есть $S = \langle (I^{Cur},\ M^{Cur},\ D^{Cur}), F_{IM}, F_{MD} \rangle$ где F_{IM}, F_{MD} функции взаимного отображения методов, данных и задач; $U = (I^{Cur},\ M^{Cur},\ D^{Cur})$, тройка, где I^{Cur} – множество зафиксированных задач, M^{Cur} – множество применяемых в данной схеме методов решения этих задач, D^{Cur} - множество данных объекта защиты, нужных для решения задач. Метод управления направлен на достижение максимальной эффективности мониторинга с соблюдением требуемых ограничений на основе решения задачи оптимального выбора над множеством возможных схем.

На основании наборов данных, методов и задач безопасности, и отображений между ними, формируется множество всех возможных схем мониторинга, которое затем сокращается. Целевая функция схемы для в целом определяется на основе совокупности целевых функций отдельных параметров. Определяется набор граничных условий для всех параметров, в отношении которых они должны быть заданы. Над схемами мониторинга вводятся отношения эквивалентности и доминирования. После редукции исходного набора полученное множество схем мониторинга в общем случае является

оптимальным по Парето и нуждается в дальнейшем сокращении. В данной задаче предлагается использовать метод сужения Парето-множества до единственного решения на основе приоритетов, позволяющий получить единственное оптимальное решение - схему мониторинга для текущих наборов данных, методов и задач.

Для того, чтобы обеспечить полноту мониторинга, модель объекта защиты должна обладать универсальностью и адаптивностью к изменяющимся потребностям задач безопасности [12]. Это достигается за счет разработанной метамодели на основе концепции универсального решателя системных задач (УРСЗ) и системы моделей, приведенной на рисунке 2.

Рис. 2. Система моделей объекта защиты на основе УРСЗ

Промышленная киберфизическая система как сложный объект представляется в виде иерархии определенного рода систем – начиная от исходной до нужного уровня абстрагирования. Выделяется базовая модель объекта защиты, или система данных, и на ее основе по требованию задаются частные модели, или в терминологии решателя - порождающие подсистемы, основанные на некоторых гипотезах об объекте. Частные модели могут быть объединены в метасистему для проведения общей оценки.

Для практического моделирования был выбран подход на основе данных, позволяющий создавать имитационные модели сложных цифровых систем обеспечивая их адекватность через сбор и оценку данных объекта моделирования. [13-15]. Для представления базовой и частных моделей выбран аппарат связанных графов, как позволяющий формировать любые иерархические представления промышленной киберфизической системы, востребованные методами защиты или представлениями объекта в Центре управления безопасностью.

Базовая модель объекта защиты представляется как орграф $G_0(V_0, E_0)$. Вершины орграфа - $v_{0,i} \in V_0$ ассоциированы с компонентами ПКФС $v_{0,i} \rightarrow \langle ID,\ D,\ Params \rangle$, ребра $e_{0,k} \in E_0$ формируются на основе коммуникационной информации ПКФС $e_{0,k} \rightarrow \langle ID, v_{0,i}, v_{0,j}, Dt,\ Params \rangle$, где ID – идентификатор вершины/ребра графа, D – множество структур данных, $Params$ – множество параметров, Dt – временные характеристики

суммарного потока данных по ребру. Тогда любой процесс $p_k \in P$ объекта защиты – маршрут на орграфе $G_0(V_0, E_0)$.

Частные модели объекта защиты задаются как T_I - дерево, представляющее I-ю структурную, функциональную или иную иерархию, описывающую объект защиты. Узлы дерева - агрегации подграфов нижележащего уровня модели. Ребра – отношения наследования (PCr – связи) между узлами. Каждый уровень такого дерева – граф вида $\mathrm{G_l(V_l, E_l)}$ $\mathrm{l} \in (0, \mathrm{L})$ – уровень дерева, вершины и ребра: $\mathrm{v_{l,i}} \rightarrow \langle \mathrm{ID},\ \mathrm{F^V_{l-1,l}(G_{l-1})},\ \mathrm{Params} \rangle$, $\mathrm{e_{l,k}} \rightarrow \langle \mathrm{ID}, \mathrm{v_{l,i}}, \mathrm{v_{l,j}}, \mathrm{Dt}, \mathrm{F^E_{l-1,l}(G_{l-1})} \rangle$, где $\mathrm{F^V_{l-1,l}}$, $\mathrm{F^E_{l-1,l}}$ - функции формирования параметров вершин и ребер ассоциированного графа. В качестве примера рассматривается построение такой иерархии для решения задачи оценки запаса устойчивости промышленной системы с учетом функциональных характеристик компонентов.

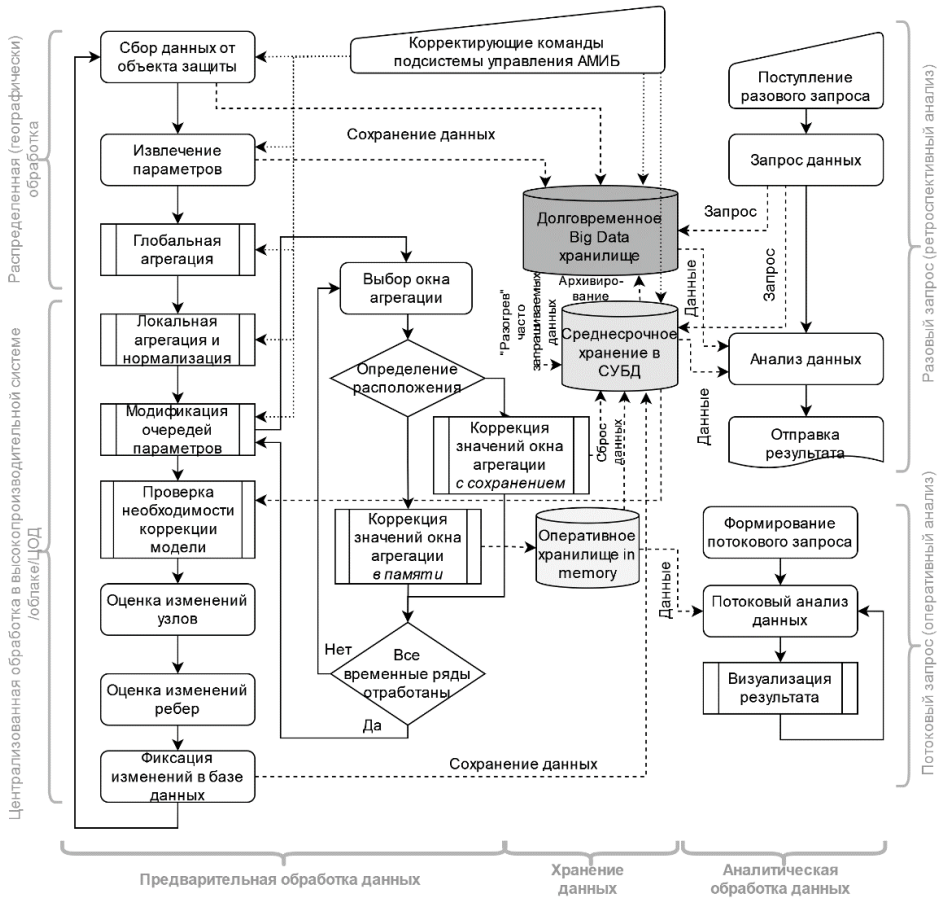


Рис. 3. Схема управления Большими данными при АМИБ ПКФС

Был сформирован метод управления Большими данными в системе адаптивного мониторинга информационной безопасности ПКФС, обеспечивающий оперативность и достоверность мониторинга вместе с остальными решениями, и включающий этап общей предварительной обработки данных и этап анализа, поддержку трех типов хранилищ данных с миграцией между ними и поддержку двух моделей запроса (рисунок 3).

В результате исследования предложен системологический подход и методология адаптивного управления МИБ ПКФС, позволяющие обеспечить полноту, достоверность и оперативность информирования об инцидентах безопасности ПКФС в условиях эволюционных изменений объекта защиты и среды его функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ «громких» инцидентов в сфере информационной безопасности в 2019 году [Электронный ресурс] – 2020. – Режим доступа: https://www.tadviser.ru/a/498885
2. Кибератаки на системы АСУ ТП в энергетике в Европе. Первый квартал 2020 года [Электронный ресурс] – 2020. – Режим доступа: https://ics-cert.kaspersky.ru/reports/2020/09/03/cyberthreats-for-ics-in-energy-in-europe-q1-2020/
3. Stevens M. Security Information and Event Management (SIEM). Presentation // TheNEbraska CERT Conference, August 9–11, 2005. - Электронный ресурс]. – 2005. – Режим доступа: http://www.certconf.org/presentations/2005/files/WC4.pdf
4. Клянчин А.И. Марков А.С., Фадин А.А., Илюхин М.В. SIEM – технология как основа построения защищенных систем // Информатизация и информационная безопасность правоохранительных органов. XXII всероссийская научная конференция. Москва – 2013. – С.270-273.
5. Лукацкий А. Измерение эффективности SOC. Часть 2 // Информационная безопасность. - №3. - 2020. [электронный ресурс] https://www.itsec.ru/articles/izmerenie-effectivnosti-soc-part-2
6. Нашивочников Н.В., Лукашин А.А., Большаков А.А. Применение аналитических средств в системе операционного мониторинга и анализа безопасности киберфизических систем для предприятий топливно-энергетического комплекса // Математические методы в технике и технологиях–ММТТ-32. – 2019. – Т. 2. – С.1-5
7. Siddiqui S., Khan M. S., Ferens K., Kinsner W Fractal based cognitive neural network to detect obfuscated and indistinguishable internet threats // 2017 IEEE 16th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC). 2017. – P. 297-308. doi: 10.1109/ICCI-CC.2017.8109765.
8. Knapp, E. D., Langill J.T. Chapter 12 - Security Monitoring of Industrial Control Systems // Editor(s): Eric D. Knapp, Joel Thomas Langill, Industrial Network Security (Second Edition). Syngress. 2015, - P. 351-386 DOI:0.1016/B978-0-12-420114-9.00012-5
9. Pavlenko E., Poltavtseva M. (2021) Mathematical Methods for Implementing Homeostatic Control in Digital Production Systems. In: Schaumburg H., Korablev V., Ungvari L. (eds) Technological Transformation: A New Role For Human, Machines And Management. TT 2020. Lecture Notes in Networks and Systems, vol 157. Springer, Cham. https://doi.org/10.1007/978-3-030-64430-7_1
10. Полтавцева, М.А. Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем // Вопросы кибербезопасности. - 2021. - № 2. - С. 51-60.
11. Klir G. J. Architecture of Systems Problem Solving. / N.Y.: Plenum Publishing Corporation. 1985. - 354 p.
12. Полтавцева, М.А. Управление адаптивным мониторингом информационной безопасности КФС // Защита информации. Инсайд. - 2021. - № 3. - С. 2-8.
13. Полтавцева М.А. Моделирование промышленных киберфизических систем на основе данных при мониторинге информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. - №4. - 2020. - С. 95-106
14. Кондратьева, Н.В., Валеев С.С. Моделирование жизненного цикла сложного технического объекта на основе концепции больших данных // G.A. Timofeeva, A.V. Martynenko (eds.): Proceedings of 3rd Russian Conference "Mathematical Modeling and

Information Technologies" (MMIT 2016). - Yekaterinburg, Russia: 2016. - С. 216-223.

15. Ge Z. Review on data-driven modeling and monitoring for plant-wide industrial processes // Chemometrics and Intelligent Laboratory Systems. Vol. 171. 017. - P. 16-25, doi: 10.1016/j.chemolab.2017.09.021

Лушников Н.Д.
БашГУ, аспирант
luschnikovnikita@yandex.ru
Исмагилова А.С.
БашГУ, заведующий кафедрой, д.ф.-м.н., доцент
ismagilovaas@yandex.ru

ОСОБЕННОСТИ ГОЛОСОВОЙ ИДЕНТИФИКАЦИИ В МНОГОФУНКЦИОНАЛЬНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Информация является неотъемлемой частью каждого из нас. Данные могут быть представлены в разном виде. В особенности, информация зачастую хранится на устройствах, которыми пользуются физические и юридические лица, начиная от обычного пользователя и заканчивая крупными организациями.

Защита информации пользователей является актуальной проблемой в наше время. Каждый из нас повседневно использует девайсы и хранит в них свои персональные данные. Физические и юридические лица затрачивают немалые ресурсы для того, чтобы оставить свои персональные данные, доступные им или ограниченному кругу лиц, в неприкосновенности. Для того, чтобы информация не стала частью плана злоумышленников, следует предоставить требуемый уровень защищенности пользователям. К инструментам защиты информации можно отнести биометрические элементы, включая акустические средства. Данный инструмент является дополнительным фактором для подтверждения личности устройства [1]. Помимо этого, рассматриваемое средство защиты информации является одной из основных частей реализуемого многофакторного биометрического программного комплекса по защите учетных записей пользователей любых устройств на основе тренировочных моделей и нейронных сетей [2].

Акустический элемент защиты информации реализован с помощью языка программирования Python 3.8. Выбор представленного языка программирования основывался на возможностях библиотек, сверточной нейронной сети и функции многопоточности, которая реализуется с помощью команды «ffmpeg» [3].

На начальном этапе включены все необходимые для реализации импортируемые элементы [4].

```
'exec(%matplotlib inline)'
import librosa
import librosa.display
import IPython
import numpy as np
import pandas as pd
import scipy
import matplotlib.pyplot as plt
import seaborn as sns
import dlib
import platform
```

```
import wx
import sys
import pyaudio
import wave
import threading
import time
import subprocess
import os
from tqdm import tqdm
from collections import defaultdict
from scipy.spatial import distance
```

После представленных библиотек, программа готова реализовывать представленный алгоритм. Затем производится запись считываемого аудиофайла в соответствии с указанными параметрами микрофона:

```
  def __init__(self):

    self.open = True
    self.rate = 28800
    self.frames_per_buffer = 1024
    self.channels = 1
    self.format = pyaudio.paInt16
    self.audio_filename = "temp_audio2.wav"
    self.audio = pyaudio.PyAudio()
```

После записи аудиофрагмента происходит сохранение аудиофайла:

```
def file_manager(filename):

    local_path = os.getcwd()

    if os.path.exists(str(local_path) + "/temp_audio2.wav"):
        os.remove(str(local_path) + "/temp_audio2.wav")
```

Сохранив аудиофайл в базе данных, производится вычисление мощности звука и октав голоса первого образца с выводом подробного графика в формате изображения:

```
y,sr=librosa.load(r'temp_audio.wav')

y_harmonic, y_percussive = librosa.effects.hpss(y)

chroma=librosa.feature.chroma_cens(y=y_harmonic, sr=sr)
plt.figure(figsize=(15, 5))
librosa.display.specshow(chroma,y_axis='chroma', x_axis='time')
```

```
plt.colorbar()

chroma_mean=np.mean(chroma,axis=1)
chroma_std=np.std(chroma,axis=1)
#plot the summary
octave=['C','C#','D','D#','E','F','F#','G','G#','A','A#','B']
plt.figure(figsize=(15,5))
plt.title('Mean CENS')
sns.barplot(x=octave,y=chroma_mean)

plt.figure(figsize=(15,5))
plt.title('SD CENS 1')
sns.barplot(x=octave,y=chroma_std)
#Generate the chroma Dataframe
chroma_df=pd.DataFrame()
for i in range(0,12):
   chroma_df['chroma_mean_'+str(i)]=chroma_mean[i]
for i in range(0,12):
   chroma_df['chroma_std_'+str(i)]=chroma_mean[i]
chroma_df.loc[0]=np.concatenate((chroma_mean,chroma_std),axis=0)
chroma_df
plt.savefig('График1.png')
shape1=np.concatenate((chroma_mean,chroma_std),axis=0)
print(shape1)
```

Обработав первый аудиофайл, производится вычисление мощности звука и октав голоса второго образца с выводом подробного графика в формате изображения:

```
y,sr=librosa.load(r'temp_audio2.wav')

y_harmonic, y_percussive = librosa.effects.hpss(y)

chroma=librosa.feature.chroma_cens(y=y_harmonic, sr=sr)
plt.figure(figsize=(15, 5))
librosa.display.specshow(chroma,y_axis='chroma', x_axis='time')
plt.colorbar()

chroma_mean=np.mean(chroma,axis=1)
chroma_std=np.std(chroma,axis=1)
#plot the summary
octave=['C','C#','D','D#','E','F','F#','G','G#','A','A#','B']
plt.figure(figsize=(15,5))
plt.title('Mean CENS')
sns.barplot(x=octave,y=chroma_mean)
```

```
plt.figure(figsize=(15,5))
plt.title('SD CENS 2')
sns.barplot(x=octave,y=chroma_std)
#Generate the chroma Dataframe
chroma_df=pd.DataFrame()
for i in range(0,12):
   chroma_df['chroma_mean_'+str(i)]=chroma_mean[i]
for i in range(0,12):
   chroma_df['chroma_std_'+str(i)]=chroma_mean[i]
chroma_df.loc[0]=np.concatenate((chroma_mean,chroma_std),axis=0)
chroma_df
plt.savefig('График2.png')
shape2=np.concatenate((chroma_mean,chroma_std),axis=0)
print(shape2)
```

В основе сравнения и обработки дух файлов с голосовыми образцами находится формула Евклидова расстояния (1.1):

$$p(x,y) = \| x - y \| = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + ... + (x_n - y_n)^2} = \sqrt{\sum_{k=1}^{n} (x_k - y_k)^2} \quad (1)$$

Данный метод защиты информации в области информационной безопасности реализуется впервые. Уровень точности обработки голосовых образцов составляет 99.4. Погрешность составляет 0.6. Данный уровень погрешности охарактеризован допустимым уровнем отклонения при идентификации пользователя (простуда, хрипота) [5]. Для корректной идентификации голоса пользователя аудиофрагмент обрабатывается по двенадцати характеристикам (октавам). Были взяты все параметры голоса. Голосовой образец, который хранится в базе данных, рекомендуется обновлять один раз в течение трех месяцев, т.к. голос пользователя может незначительно меняться в определенные промежутки времени [6].

Далее производится сравнение двух голосовых образцов с помощью формулы Евклидова расстояния и вывод соответствующей информации в окне реализуемого программного комплекса:

```
a = distance.euclidean(shape1, shape2)
print(a)

if a >= 0.6:
   print("Пользователь не идентифицирован, повторите попытку")
else:
   print("Вы являетесь пользователем системы")
```

Следует учитывать вывод окна аутентификации «логин-пароль» при неудачной идентификации голоса. Дается две попытки ввода полей. При первых двух успешных попытках программа попросит пользователя вновь пройти голосовую идентификацию. При неудачной второй аудиоидентификации программа автоматически выключит устройство. При неудачной первой попытке – ввести логин и пароль пользователю

представится еще одна попытка. Если же пользователь неудачно пройдет аутентификацию во второй раз, то программа также автоматически выключит устройство. Данный процесс цикличен и войти в систему сможет только искомый пользователь.

Программный комплекс представлен в виде приложения в формате *.exe вместо запуска на консоли CMD. Каждый программный модуль выполняет свою функцию и взаимосвязан друг с другом.

Таким образом, представленное решение является эффективным и оптимальным средством защиты информации. Дополнительный фактор при идентификации пользователя служит барьером для злоумышленников. Для того, чтобы нивелировать компрометацию данных пользователя, файл с данным программным кодом зашифрован ассиметрично. Представляемый софт подходит для реализации на любом устройстве (ПК, смартфон). При реализации представленного программного продукта пользователю предоставляется требуемый уровень защиты [7].

СПИСОК ЛИТЕРАТУРЫ

1. Ван Лянпэн, Петросян О.Г. Распознавание лиц на основе классификации вейвлет признаков путем вейвлет нейронных сетей // Информатизация образования и науки. 2018. № 4 (40). С.129-139.
2. Исмагилова А.С., Лушников Н.Д. Многофункциональное ПО для защиты учетных записей пользователей с использованием биометрических технологий // Защита информации. Инсайд. 2021. №2. С. 28-31.
3. Кручинина Е.В. Видеоидентификация – ключ в мире адресных услуг // Системы безопасности. – 2016 – №6. – С.110-111.
4. Мамаев В. Многофакторная биометрическая идентификация // Системы безопасности. 2017, №5. С. 78-79.
5. Немков Р.М. Исследование сверточной нейронной сети, обученной с помощью метода применения нестандартных рецептивных полей при распознавании изображений // Известия Южного федерального университета. 2015, № 7 (168). С. 79-90.
6. Осовский, С. Нейронные сети для обработки информации: учебное пособие / С. Осовский - М.: Телеком, 2017. – 448 с.
7. Пчеловодова Н. Российский биометрический рынок в 2019-2022 годах. Результаты масштабного исследования J’son & Partners Consulting // Системы безопасности. 2019, №2. С. 88-91.
8. Смит, Ричард Э. Аутентификация: от паролей до закрытых ключей: учебное пособие / Ричард Э. Смит – М.: Вильямс, 2015. – С. 425-432.
9. Суомалайнен, А. Биометрическая защита: обзор технологии: учебное пособие / А. Суомалайнен – М.: ДМК, 2016. – С. 99-104.
10. Тропченко А.А., Тропченко А.Ю. Нейросетевые методы идентификации человека по изображению лица // Известия высших учебных заведений. Приборостроение. 2012. Т.55, №10. С.31-36.

Скорых М.А.
СПбГУТ, ассистент
mark.skorykh@bk.ru
Израилов К.Е.
СПбГУТ, доцент, к.т.н.
СПб ФИЦ РАН, старший научный сотрудник,
konstantin.izrailov@mail.ru
Башмаков А.В.
ГУМРФ им.адм. С. О. Макарова, доцент, к.т.н., доцент
abashm@mail.ru

ЗАДАЧАОРИЕНТИРОВАННОЕ СРАВНЕНИЕ СРЕДСТВ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Введение

Информационные технологии являются неотъемлемой частью любого современного общества, что имеет, в том числе, ряд негативных сторон. Так, ежедневно происходит большое количество компьютерных атак (далее — КА), ведущих к различным угрозам информационной безопасности [1]. Б*о*льшая часть таких атак выявляется во время анализа сетевого трафика с использованием сигнатурного и/или поведенческого метода обнаружения. Однако, после детектирования специализированными средствами факта вредоносной активности верификация их результатов ложится на плечи аналитиков информационной безопасности (далее — АИБ). Для выполнения вышеупомянутой задачи АИБ исследует содержимое сетевого трафика при помощи различных средств анализа. При этом, АИБ может решать целый набор частных задач, что так или иначе должно повлиять и на выбор используемых средств. В ином случае, эффективность анализа окажется значительно меньше возможной, поскольку средства будут использоваться необоснованно. Поэтому, требуется понимание того, как какое из средств может быть применено для одной из задач АИБ. Такое критериальное сравнение будет произведено в данной статье.

Средства анализа

Дадим краткое описание Топ-7 средств анализа сетевого трафика исходя из существующих практик противодействия сетевым атакам.

Tcpdump

Утилита Tcpdump работает из командной строки и предназначена для записи и анализа сетевого трафика. Данное средство часто используется для захвата трафика на сетевых сенсорах. Для обеспечения функций фильтрации поддерживается технология Berkeley Packet Filters, которая, как правило, используется на операционных системах семейства Linux и способна обрабатывать большое количество трафика.

Tshark

Утилита Tshark представляет собой консольный анализатор сетевых протоколов. Принцип функционирования очень похож на утилиту Tcpdump, а главное отличие заключается в разных механизмах фильтрации трафика. Аналогично, средство способно обрабатывать большое количество сетевого трафика.

Wireshark

Утилита Wireshark является графическим анализатором сетевых пакетов и относится к наиболее часто используемым инструментам для решения задач подобного рода. Данное средство представляет в удобном формате всю информацию, содержащуюся в сетевых пакетах, позволяя даже производить распаковку зашифрованных данных (при наличии соответствующего ключа).

NetworkMiner

Утилита NetworkMiner является открытой и предназначена для сетевой форензики; она также, как и Wireshark, обладает удобным графическим интерфейсом. Данное средство может использоваться как пассивный сниффер сетевого трафика для определения IP-адресов узлов сетевого взаимодействия, открытых портов, переданных файлов и т.д. Также, данное средство можно использовать для анализа уже записанного в файл трафика.

Arkime

Утилита Arkime, ранее называемая Moloch, представляет собой целую открытую масштабируемую систему захвата и поиска индексированных сетевых пакетов. Средство состоит из 3 основных модулей: захвата сетевого трафика — предназначенного для сниффинга пакетов и их записи в PCAP-формате; отображения — представляющего собой Web-приложение, созданное на базе node.js; хранения и индексирования сетевых пакетов — имеющего вид системы полнотекстового поиска Elasticsearch [2].

Brim

Утилита Brim имеет вид десктопного приложения и состоит из комплекса следующих подсистем: фреймворк Zeek, система обнаружения атак Suricata, поисковый движок Zed и графический пользовательский интерфейс на базе Electron и React. Совмещая сильные стороны вышеуказанный подсистем, средство позволяет проводить быстрый анализ сетевого трафика в интересах аналитики его безопасности.

Zeek

Утилита Zeek [3] является пассивным фреймворков для анализа сетевого трафика с открытым исходным кодом. Средство представляет собой монитор безопасности, проверяющий сетевой трафик на предмет наличия признаков подозрительной активности, генерируя множество журнальных файлов, описывающих зафиксированные данные. Средство является серверным продуктом, в состав возможностей которого входит построение кластера для обработки трафика большого объема.

Задачи

Как было сказано ранее, у АИБ могут возникать различные частные задачи при анализе сетевого трафика. Опишем далее Топ-5 наиболее востребованных из них.

Задача 1. Анализ общеизвестных атак

Под общеизвестными КА понимаются уже известны способы обнаружения (например, заданы с помощью сигнатур) [4]. Главной задачей АИБ в этом случае будет быстрое определение успешности и технических особенностей КА. Для выполнения задачи хорошо подойдут средства анализа трафика с графическим интерфейсом [5] и функциями сбора артефактов из сетевого трафика.

Задача 2. Анализ уязвимостей нулевого дня

Особенностью атак нулевого дня является отсутствие существующих механизмов их обнаружения [6]. Следовательно, средства анализа, собирающие артефакты из сетевого трафика, будут неспособны определить новые индикаторы компрометации. Для изучения сетевого трафика, содержащего КА нулевого дня, подойдут инструменты, способные предоставить подробную информацию о сетевых пакетах. Также, графический интерфейс позволит решать задачу анализа подобных КА более эффективно.

Задача 3. Поиск эксфильтруемых данных

АИБ сталкиваются с задачами поиска и восстановления эксфильтрованной из защищаемой системы информации [7] (например, в процессе отправка данных на нестандартный порт, утечка информации по служебным протоколом и др.). Для решения задачи удобны средства, включающие в себя возможности извлечения файлов и сбора статистической информации из трафика.

Задача 4. Анализ активности ПО

При анализе сетевой активности вредоносного программного обеспечения (далее — ВПО) [8] АИБ приходится сталкиваться с задачей нахождения нелегитимных сетевых взаимодействий среди большого массива трафика. А зачастую, при анализе сетевой активности ВПО, АИБ необходимо “раскручивать” цепочку индикаторов компрометации. Для решения задачи хорошо подойдут средства анализа с графическим интерфейсом, возможностями сбора статистической информации из трафика и поисковым движком.

Задача 5. Анализ DDoS

Особенностью анализа DDoS-атак является большой объем анализируемого сетевого трафика [9]. В качестве примера можно привести DDoS-атаки типа amplification, для которой АИБ должен определить ее мощность по нескольким метрикам. Для решения задачи подойдут серверные средства анализа, способные создавать кластеры из нескольких узлов, позволяющие определить необходимые метрики.

Сравнение средств

Оценим возможность применения каждого из описанных средств в интересах решения каждой из озвученных задач, используя их, как критерии сравнения (Табл. 1).

Исходя из критериального сравнения, можно сделать вывод о том, что наиболее пригодными средствами для анализа общеизвестных КА являются Arkime и Brim, т.к. они содержат в своем составе удобный графический интерфейс, поисковую систему, могут предоставлять статистическую информацию о сетевом трафике.

Табл. 1. Возможности применения средств анализа сетевого трафика при частных задач по противодействию угрозам информационной безопасности

	Задача 1	**Задача 2**	**Задача 3**	**Задача 4**	**Задача 5**
Tcpdump	low	medium	low	low	medium
Tshark	low	medium	low	low	medium
Wireshark	medium	high	medium	medium	low
NetworkMiner	medium	low	low	high	low

Arkime	high	low	medium	high	high
Brim	high	low	medium	high	low
Zeek	medium	low	medium	medium	high

Для анализа уязвимостей нулевого дня, наиболее подходящим средством является Wireshark, т.к. он предоставляет возможность просматривать любую информацию о сетевом пакете в удобном для АИБ виде.

Для поиска эксфильтруемых данных нет наиболее подходящей утилиты, т.к. не существует общих подходов к решению данной задачи. Для ее решения можно совместно использовать Wireshark, Arkime, Brim, Zeek.

Наиболее удобными утилитами для анализа функционирования ВПО являются средства NetworkMiner, Arkime, Brim, т.к. позволяют осуществлять быстрый поиск необходимой информации, анализировать артефакты, собранные из сетевого трафика.

Для анализа DDoS-атак наиболее подходящими средствами являются Arkime и Zeek, т.к. они способны обрабатывать большое количество сетевого трафика.

Выводы

В данной статье представлен обзор Топ-7 средств для анализа сетевого трафика с позиции решения АИБ Топ-5 задач в ходе мониторинга КА. Результаты сравнения средств с позиции решаемых ими задач позволяют сделать вывод о том, что нет единой утилиты для решения всех поставленных задач. АИБ должен использовать в своей деятельности набор средств анализа трафика.

Продолжение научного исследования может пойти по следующим путям. Во-первых, необходимо создание отдельного метода для комплексирования различных средств анализа сетевого трафика, имея при этом высокую эффективности их совместного применения. Во-вторых, возможно потребуется создание собственного средства, объединяющего достоинства каждого из перечисленных, а также нивелируя их недостатки [10]. И, в-третьих, для общей оценки и сравнения эффективности как отдельных средств, так и их комплексов необходим соответствующий комплекс научно-методических средств, что на данный момент является нерешенной задачей.

СПИСОК ЛИТЕРАТУРЫ

1. Израилов, К.Е. Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети / К.Е. Израилов // Вестник ИНЖЭКОНа. Серия: Технические науки. – 2012. – № 8 (59). – С. 150-153.
2. Федорова, В.А. Поиск и индексирование данных с использованием Elasticsearch / В.А. Федорова, Е.А. Ефремов, И.А. Колягина // Вопросы радиоэлектроники. – 2019. – № 3. – С. 74-77.
3. Скорых, М.А. Применение фреймворка Zeek И ELK-СТЕКА для анализа рассылок вредоносного программного обеспечения / М.А. Скорых // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021): сборник научных статей X международной научно-технической и научно-методической

конференции "Актуальные Проблемы Инфотелекоммуникаций в Науке и Образовании". – 2021. – С. 658-661.
4. Штеренберг, С.И., Разработка комплекса мер для защиты предприятия от фишинговых атак / Штеренберг С.И., Стародубцев И.В., Шашкин В.С. // Защита информации. Инсайд. – 2020. – № 2 (92). – С. 24-31.
5. Израилов, К.Е. Подход к выявлению последовательности одноцелевых сетевых атак с визуализацией их прогресса эксперту / К.Е. Израилов, А.И. Обрезков, П.А. Курта // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 68-69.
6. Рябышев, Д.И. Проблематика уязвимости нулевого дня и методы защиты / Д.И. Рябышев, А.Р. Газизов // Студенческий вестник. – 2019. – № 48-6(98). – С. 50-51.
7. Бубнов, Я.В. Текстовый анализ DNS запросов для защиты компьютерных сетей от эксфильтрации данных / Я.В. Бубнов, Н.Н. Иванов // Информатика. – 2020. – Т. 17. – № 3. – С. 78-86.
8. Buinevich M. Testing of Utilities for Finding Vulnerabilities in the Machine Code of Telecommunication Devices / M. Buinevich, K. Izrailov, A. Vladyko // The proceedings of 19th International Conference on Advanced Communication Technology. – 2017. – PP. – 408-414.
9. Яковлев, В.А., Моделирование комбинированного метода отслеживания источников DDOS-атак / В.А. Яковлев, И.И. Левин // Проблемы информационной безопасности. Компьютерные системы. – 2011. – № 2. – С. 47-61.
10. Ныркov, А.П. Методика проектирования безопасных информационных систем на транспорте / А.П. Ныркov, С.С. Соколов, А.В. Башмаков // Проблемы информационной безопасности. Компьютерные системы. – 2010. – № 3. – С. 58-61.

Боршевников А.Е.
ДВФУ, и.о. директора департамента,
borshevnikov.ae@dvfu.ru

ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫЕ СЕТИ В ЗАДАЧЕ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Современное развитие информационных технологий непрерывно ведет к увеличению роли систем информационной безопасности. Одним из механизмов, реализуемых современными системами информационной безопасности является система аутентификации. Системы аутентификации различаются по и по методам классификации, которые положены в основу их функционирования, так и по биометрическим характеристикам, по которым производится классификация пользователей. Особый интерес представляют биометрические характеристики, которые обладают высоким уровнем конфиденциальности данных и методы классификации, позволяющие сохранить конфиденциальность данных. Биометрической характеристикой, удовлетворяющей указанным требованиям, может выступить электроэнцефалограммы (ЭЭГ). Биометрические системы, соответствующие требованию сохранению конфиденциальности биометрических данных, принято называть системами высоконадежной биометрической аутентификации. Обычно это биокриптографические системы аутентификации, т.е. системы, которые на основе биометрических данных восстанавливают криптографический ключ.

Биокриптографические системы аутентификации основываются на использовании следующих двух архитектур: «нечетких» экстракторах [1] и больших/сверхбольших нейронных сетях (нейросетевых преобразователях «Биометрия – код доступа» [2,3].

Применение систем биометрической аутентификации требует большого количества примеров обучения. Одним из решений указанной проблемы может послужить генерация синтетических примеров биометрических данных на основе естественных примеров с использованием генеративно-состязательных сетей [7,8,9,10].

Возможность применения генеративно-состязательных сетей для атак на систему биометрической аутентификации уже было исследовано [11]. В результате подобных атак производится модификация произвольных биометрических данных ЭЭГ с помощью генеративно-состязательной сети. Было получено, что злоумышленник успешно может проходить процедуру идентификации с помощью модифицированных генеративно-состязательной сетью. Однако в рамках того же исследования было получено, что можно уменьшить ошибку второго рода для рассматриваемой системы биометрической аутентификации, сохранив значение ошибки первого рода, при переобучении системы идентификации на модифицированных генеративно-состязательной сетью данных. Это показывает, что данные сети возможно применять для генерации синтетических примеров ЭЭГ.

Рассмотрим принцип работы генеративно-состязательных сетей.

Из архитектуры генеративо-состязательных сетей (Рис. 1) следует, что основными компонентами являются генератор, цель которого создать с помощью входного многомерного случайного вектора ложное изображение, и дискриминатора, задача

которого сводится к тому, чтобы распознать и классифицировать изображение, то есть определить, является ли предлагаемый материал истинным или ложным.

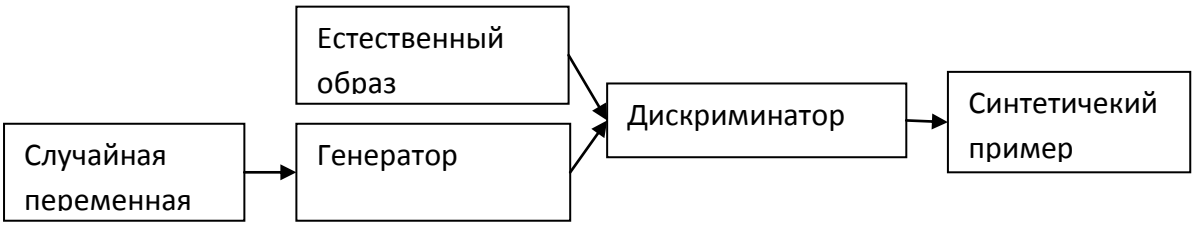


Рис. 1. Схема генеративно-состязательной сети

Формализуем алгоритм работы генеративно-состязательной сети.

Пусть $E(a)$ – функция ошибки алгоритма a; p_x – вероятностное распределение обрабатываемых данных; p_z – вероятностное распределение шума обрабатываемых данных; $G(z, \gamma_g)$ – функция генерации, представляемая многослойным персептроном; $D(z, \gamma_d)$ – функция дискриминации, представляемая многослойным персептроном. Тогда работу генеративно-состязательной сети можно описать формулой (1):

$$\min_G \max_D V(D, G) = E_{x \sim p_x}[lgD(x)] + E_{z \sim p_z}[\lg(1 - D(G(z)))] \quad (1)$$

Описанный алгоритм работы генеративно-состязательной сети для генерации синтетических примеров ЭЭГ было предложено применять следующим образом:

1. подать на вход генератора случайный естественный биометрический образ ЭЭГ случайного пользователя, подать на вход дискриминатора естественный биометрический пример ЭЭГ другого пользователя;
2. каждые n итераций работы генеративно-состязательной сети выбирать пример ЭЭГ в качестве синтетического примера ЭЭГ. Данная операция выполняется пока дискриминатор не классифицирует генерируемый образ как образ пользователя.

Проверка возможности использования генеративно-состязательных сетей для задачи высоконадежной биометрической аутентификации была произведена на нейросетевом преобразователе «Биометрия – код доступа» [4, 6]. В качестве теста проводился опыт по восстановлению злоумышленником секретного ключа при условии знания весовых коэффициентов нейросетевого преобразователя, обученного легитимным пользователем. Результаты данного исследования будут рассмотрены ниже.

Рассмотрим структуру нейросетевого преобразователя «Биометрия – код доступа». Нейросетевые преобразователи «Биометрия - код доступа» представляют собой однослойные и двухслойные нейронные сети прямого распространения с большим количеством выходов. В работе Маршалко [12] была показана возможность сведения задачи восстановления биометрических данных по значениям весовых коэффициентов и знанию выходной последовательности к задаче решения системы линейных неравенств. Данная атака получила название атаки Маршалко. Одним из условий, которые будут наложены на модель преобразователя, является условие того, что рассматриваемая нейронная сеть будет двухслойной. Это дает возможность сочетать при построении нейронной сети различных видов нейросетевых структур, а также незначительно увеличивает устойчивость модели перед атакой Маршалко [12].

В общем случае нейросетевой преобразователь можно описать следующим образом [13]:

$$NET(\bar{a}_i, \overline{w}_i, \overline{W}_r, \overline{net}_l, \Delta_r) = \overline{K}_{rest},\ 1 \le i \le I,\ 1 \le l \le L,\ 1 \le r \le R \quad (2)$$

$$\overline{K}_{rest} = \{k_r\}, \quad (3)$$

где $\overline{net}_l$ – вектор связей нейрона l; $\overline{w}_i$ – вектор весовых коэффициентов первого слоя нейронной сети; $\overline{W}_r$ – вектор весовых коэффициентов второго слоя нейронной сети; Δ_r – коэффициент использования нейрона первого слоя нейронной сети; $\overline{K}_{rest}$ – восстанавливаемый криптографический ключ.

Рассмотрим послойно описание нейронной сети преобразователя.

Для описания первого слоя введем следующее значение:

$$v_i = \bar{a}_i \cdot \overline{w}_i,\ 1 \le i \le I \quad (4)$$

Это нормированная величина вектора биометрических данных, полученных с канала электроэнцефалографа i, подающаяся затем на нейроны первого слоя нейронной сети. Было решено брать в качестве входных данных указанную величину для уменьшения количества входных параметров. Составим вектор входных нормированных значений:

$$\bar{v} = \{v_i\},\ 1 \le i \le I \quad (5)$$

Работу каждого нейрона первого слоя можно описать следующим образом:

$$x_{1,l} = \bar{v} \cdot \overline{net}_l,\ 1 \le l \le L, \quad (6)$$

$$\overline{net}_l = \{\Delta_i\}, 1 \le l \le L,\ 1 \le i \le I, \quad (7)$$

$$\Delta_i = PRNG(IV) = \begin{cases} \Delta_i = 1, v_i \in IN1 \\ \Delta_i = 0\ v_i \notin IN1 \end{cases}, 1 \le i \le I, \quad (8)$$

$$t_l = f_1(y_{1,l}) = \begin{cases} 1, y_{1,l} \ge 0 \\ -1, y_{1,l} < 0 \end{cases}, 1 \le l \le L, \quad (9)$$

где $x_{1,l}$ – это результат работы сумматора нейрона l первого слоя; Δ_i – коэффициент использования данных электрода i в нейроне; $y_{1,l}$ – передаточная функция первого слоя нейронной сети; $f_1(y_{1,l})$ – решающее правило для нейрона первого слоя; $PRNG(seed)$ – псевдослучайный генератор; IV – инициализирующий вектор.

Работу каждого нейрона второго слоя можно описать следующим образом:

$$x_{2,r} = \sum_{l=1}^{L} W_r \cdot t_l \cdot \Delta_r,\ 1 \le r \le R, \quad (10)$$

$$\Delta_r = PRNG(IV) = \begin{cases} \Delta_r = 1, t_l \in IN2 \\ \Delta_r = 0, t_l \notin IN2 \end{cases}, 1 \le r \le R,\ 1 \le l \le L, \quad (11)$$

$$k_r = f_2(y_{2,r}) = \begin{cases} 1, y_{2,r} \ge 0 \\ 0, y_{2,r} < 0 \end{cases}, 1 \le r \le R, \quad (12)$$

где $x_{2,r}$ – это результат работы сумматора нейрона r второго слоя; Δ_r – коэффициент использования компонента t_l в нейроне; $y_{2,r}$ – передаточная функция второго слоя нейронной сети; $f_2(y_{2,r})$ – решающее правило для нейрона второго слоя.

После восстановления ключа производится его хеширование:

$$Secret = h(\bar{K}_{rest}). \quad (13)$$

Полученное хешированное значение сравнивается с сохраненным в базе данных значением хешированного пароля. Так как значение секретного ключа появляется исключительно при его восстановлении, а при процедуре аутентификации производится сравнение значения хешированных данных, то можно утверждать, что при обеспечении невозможности доступа злоумышленника к этапу, описываемому формулой (13), данная модель обеспечивает безопасность парольной информации, так как парольная информация не используется нигде в открытом виде.

Также стоит привести процедуру выбора количества входов на нейрон преобразователя. Для введения данной величины необходимо задать величину выходного качества обученного нейрона (величины соответственно задаются для нейронов первого и второго слоев):

$$\bar{Q}(t_l) = \frac{|E_{\text{Чужой}}(t_l) - E_{\text{Свой}}(t_l)|}{\sigma_{\text{Свой}}(t_l)},\ 1 \le l \le L. \quad (14)$$

$$\bar{Q}(k_r) = \frac{|E_{\text{Чужой}}(k_r) - E_{\text{Свой}}(k_r)|}{\sigma_{\text{Свой}}(k_r)},\ 1 \le r \le R. \quad (15)$$

Число входов на нейроны первого и второго слоя вычисляются соответственно по формулам:

$$INP_1 = b_{01}\left\{\frac{Q(t_l)}{E(Q(t_l))}\right\}^2,\ 1 \le l \le L. \quad (16)$$

$$INP_2 = b_{02}\left\{\frac{Q(k_r)}{E(Q(k_r))}\right\}^2,\ 1 \le r \le R, \quad (17)$$

где b_{01}, b_{02} – экспериментально подбираемы нормирующие коэффициенты.

При построении модели нейросетевого преобразователя выбор вида передаточных функций и решающих правил имеет большую важность. Именно использование различных видов этих структур нейронной сети позволяет противодействовать атаке Маршалко. Одним из способов обеспечения безопасности против атаки Маршалко является выбор нелинейной передаточной функции. Использование -мерных решающих правил, ведет к усложнению обучения нейросетевого преобразователя, поэтому в качестве противодействия атаке Маршалко было решено взять для нейронов первого и второго слоев сигмоидальную передаточную функцию:

$$y_{1,l} = \frac{2}{1+e^{x_{1,l}}} - 1,\ 1 \le l \le L, \quad (18)$$

$$y_{2,r} = \frac{2}{1+e^{x_{2,r}}} - 1,\ 1 \le r \le R. \quad (19)$$

В результате использования указанного вида передаточной функции, в случае применения атаки Маршалко приводит ее неэффективности за счет увеличения сложности задачи, лежащей в основе данной атаки (вместо системы линейных неравенств злоумышленнику необходимо разрешить систему нелинейных неравенств). Выбор двухслойной нейронной сети также позволяет использовать различные виды передаточных функций (в частности, использование линейных передаточных функций) при условии обязательного использования в одном из слоев нейронной сети нелинейной передаточной функции.

Классификация пользователей на основе нейронной сети требует задания алгоритма для ее обучения. Для построения моделей систем высоконадежной биометрической аутентификации важно, чтобы алгоритм обучения не заходил в тупик экспоненциальной вычислительной сложности. Одним из выходов из данной ситуации является использование детерминированного алгоритма, описанного в стандарте ГОСТ Р 52633.5 [3].

Для обучения первого слоя нейронной сети принять рассчитывать величину входного качества -ого биометрического параметра:

$$Q(a_{ij}) = \frac{|E_{\text{Чужой}}(a_{ij}) - E_{\text{Свой}}(a_{ij})|}{\sigma_{\text{Свой}}(a_{ij})},\ 1 \le i \le I,\ 1 \le j \le J. \quad (20)$$

Весовые коэффициенты для первого слоя нейронной сети рассчитываются следующим образом:

$$w_{ij} = \frac{Q(a_{ij})}{\sigma_{\text{Чужой}}(a_{ij})},\ 1 \le i \le I,\ 1 \le j \le J. \quad (21)$$

Знак весового коэффициента получаем на основе расчета разностей математического ожидания данных образов «Свой» и «Чужой»:

$$sign(w_{ij}) = \begin{cases} sign\left(E_{\text{Свой}}(a_{ij}) - E_{\text{Чужой}}(a_{ij})\right), y_{1,l} = 1 \\ -sign\left(E_{\text{Свой}}(a_{ij}) - E_{\text{Чужой}}(a_{ij})\right), y_{1,l} = -1 \\ 1 \le i \le I, 1 \le j \le J. \end{cases} \quad (22)$$

Весовые коэффициенты рассчитываются для второго слоя нейронной сети по следующей формуле:

$$W_r = \frac{b\omega_r}{E(\omega_r)}, 1 \le r \le R, \quad (23)$$

где b – коэффициент стабилизации, экспериментально выбираемый для машинного обучения при разработке процедуры биометрической аутентификации, ω_r – индикатор стабильности -го разряда выходов нейронов первого слоя:

$$\omega_r = 2 \cdot \left|0{,}5 - P_{0,r}\right| = 2 \cdot \left|0{,}5 - P_{1,r}\right|, 1 \le r \le R, \quad (24)$$

где $P_{0,r}$ – вероятность появления состояния «0» в -м контролируемом выходе нейрона; $P_{1,r}$– вероятность появления состояния «1» в r-м контролируемом выходе нейрона.

Идентифицируем показатели эффективности системы.

Точность аутентификации определяется по следующей формуле [14]:

$$Acc = \frac{Tr}{All} \cdot 100\%, \tag{25}$$

где Tr – количество правильно аутентифицированных пользователей; All – общее количество попыток аутентификации.

В общем случае вероятность ошибки первого рода для нейросетевых преобразователей задается в зависимости от желаемого качества выходных значений нейронов [3]:

$$P_1 \approx \left|\frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{a_1 \bar{Q}(k_r)} e^{-\frac{t^2}{2}} dt\right|, \tag{26}$$

Исследования показали, что вероятность ошибки первого рода для нейросетевых преобразователей «Биометрия - код доступа» при корреляции выходных значений для образа «Свой», стремящейся к 1, соответствует следующему закону [5]:

$$P_1 \approx \int_1^{\infty} \frac{1}{2^{\frac{\Omega}{2}} \cdot \Gamma(\frac{\Omega}{2})} \cdot x^{\frac{\Omega}{2}-1} \cdot e^{-\frac{x^2}{2}} dx, \tag{27}$$

где Ω – количество степеней свободы в распределении X^2; X^2 – распределение хи-квадрат; $\Gamma(\frac{\Omega}{2})$ – гамма-распределение.

В случае, когда в проведенной серии испытаний по предъявлению биометрической характеристики образа «Свой», состоящей из n опытов, не обнаружен факт отказа в доступе, число степеней свободы в распределении X^2 вычисляется по формуле:

$$\Omega = \frac{1}{m+1}. \tag{28}$$

В остальных случаях Ω вычисляется как среднее расстояние Хемминга (количество разрядов, в которых криптографический ключ, полученный в рамках процедуры восстановления, отличается от криптографического ключа, хранимого в системе аутентификации) взятое по m проведенным опытам:

$$\Omega = \overline{H}(\overline{K}_{rest}). \tag{29}$$

Здесь под средним расстоянием Хемминга понимается отношение суммы расстояний Хемминга, полученных в рамках m опытов к количеству этих опытов.

Вероятность ошибки второго рода P_2 можно вычислить приближенно, исходя из гипотезы нормального закона распределения значений вероятности ошибок, по формуле (30) [5]:

$$P_2 \approx \frac{1}{\sqrt{2\pi}} \int_{\sqrt{n}E(q(a_{ij}))}^{\infty} e^{-\frac{x^2}{2}} dx, \quad (30)$$

где n – число учитываемых средством аутентификации биометрических параметров; $E(a_{ij})$ – среднее качество всех учитываемых средством биометрической аутентификации биометрических параметров.

Предложенным алгоритмом генерации синтетических примеров было сгенерировано 1000000000 примеров для разного количества итерационных шагов алгоритма работы генеративно-состязательной сети (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 20, 30, 40, 50 шагов соответственно).

В рамках исследования были получены следующие показатели точности аутентификации, вероятности ошибки первого и второго рода в зависимости от количества итерационных шагов в работе генеративно-состязательной сети для генерации синтетических примеров (Табл.1).

Эксперимент показал, что оптимальное количество шагов работы генеративно-состязательной сети для увеличения качества системы высоконадежной биометрической аутентификации составляет 10.

Полученные результаты в рамках экспериментов показывают эффективность применения генеративно-состязательных сетей для задачи высоконадежной биометрической аутентификации.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) №9/2020.

Табл. 1. Показатели эффективности аутентификации пользователей при обучении на синтетических примерах, сгенерированных на заданном количестве шагов работы генеративно-состязательной сети

Количество итеративных шагов работы генеративно-состязательной сети до выборки синтетического примера	**Точность, %**	**Вероятность ошибки первого рода**	**Вероятность ошибки второго рода**
Алгоритм не использовался	100	$7 \cdot 10^{-4}$	10^{-9}
1	99.5	$3 \cdot 10^{-2}$	$2 \cdot 10^{-2}$
2	99.8	$8 \cdot 10^{-2}$	$3 \cdot 10^{-5}$
3	99.8	$8 \cdot 10^{-2}$	
4	99.9	$5 \cdot 10^{-3}$	$4 \cdot 10^{-5}$
5	99.9	$5 \cdot 10^{-3}$	$2 \cdot 10^{-6}$
6	99.9	$5 \cdot 10^{-3}$	$2 \cdot 10^{-6}$
7	99.9	$5 \cdot 10^{-3}$	$2 \cdot 10^{-6}$
8	99.9	$5 \cdot 10^{-3}$	$5 \cdot 10^{-6}$

9	99.9	$5 \cdot 10^{-3}$	$7 \cdot 10^{-6}$
10	100	$7 \cdot 10^{-4}$	$<10^{-9}$
20	100	$7 \cdot 10^{-4}$	$<10^{-9}$
30	100	$7 \cdot 10^{-4}$	$<10^{-9}$
40	100	$7 \cdot 10^{-4}$	$<10^{-9}$
50	100	$7 \cdot 10^{-4}$	$<10^{-9}$

СПИСОК ЛИТЕРАТУРЫ

1. Dodis Y. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data / Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith // SIAM Journal on Computing. – 2008. – Vol. 38, №1. – P. 97-139.
2. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации: ГОСТ Р 52633.2-2010.- Введен впервые; Введ. 30.09.2010. – М.: Стандартинформ, 2011. – 17 с.
3. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия - код доступа: ГОСТ Р 52633.5-2011. – Введен впервые; Введ. 01.12.2011. – М.: Стандартинформ, 2012. – 20 с.
4. Гончаров С.М. Использование вейвлет-преобразования для выделения биометрических характеристик потенциала Р300 в задачах высоконадежной биометрической аутентификации / Гончаров С.М., Боршевников А.Е. // Журнал «Информация и безопасность». Том. 19, часть 4. Воронеж: ВГТУ, 2016. - С. 527-530.
5. Ахметов, Б.С. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: Монография / Б.С. Ахметов, А.И. Иванов, В.А. Фунтиков, А.В. Безяев, Е.А. Малыгина. – Алматы: ТОО «Издательство LEM», 2014. – 144 с.
6. Гончаров С. М., Боршевников А. Е. Нейросетевой преобразователь «Биометрия – код доступа» на основе электроэнцефалограммы в современных криптографических приложениях. // Вестник СИБГУТИ: – Новосибирск: Изд-во СИБГУТИ, 2016. – № 1. – С. 17–22.
7. T. Piplani, N. Merill and J. Chuang, "Faking it, Making it: Fooling and Improving Brain-Based Authentication with Generative Adversarial Networks," 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2018, pp. 1-7.
8. Aayush Bansal, Shugao Ma, Deva Ramanan, and Yaser Sheikh. Recycle-gan: Unsupervised video retargeting. In ECCV, 2018.
9. Jun-Yan Zhu, Philipp Krähenbühl, Eli Shechtman, and Alexei A Efros. Generative visual manipulation on the natural image manifold. In European Conference on Computer Vision, pages 597–613. Springer, 2016.
10. Raymond A Yeh, Chen Chen, Teck Yian Lim, Alexander G Schwing, Mark Hasegawa-Johnson, and Minh N Do. Semantic image inpainting with deep generative models. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 5485–5493, 2017.

11. Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. In Advances in neural information processing systems, pages 2672–2680, 2014.
12. Marshalko G. B. On the security of a neural network-based biometric authentication scheme //Математические вопросы криптографии. – 2014. – Т. 5. – №. 2. – С. 87-98.
13. Гончаров С. М., Боршевников А. Е. Расширенная модель нейросетевого преобразователя "Биометрия-код доступа" на основе ЭЭГ // Вестник Морского государственного университета. – 2017. – №. 78. – С. 11-15.
14. Palaniappan R. Electroencephalogram-based brain–computer interface: An introduction //Guide to Brain-Computer Music Interfacing. – Springer, London, 2014. – С. 29-41.

Байбурин В.Б.
СГТУ, заведующий кафедрой, д.ф.-м.н., профессор
baiburinvb@rambler.ru
Корчагин С.А.
СГТУ, доцент,
Финансовый университет, доцент, к.ф.-м.н.
korchaginser@gmail.com
Хороводова Н.Ю.
СГТУ, ассистент
Nkhorovodova@mail.ru
Селиверстов В.В.
СГТУ, аспирант
seliverstov_vitaly@mail.ru

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ СЕРТИФИКАТОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ WEB – РЕСУРСОВ УЧЕБНЫХ УЧРЕЖДЕНИЙ

За последний год и по настоящее время информатизация охватила все аспекты и направления образовательной деятельности [1,2]. В связи с переходом на дистанционный формат обучения создание и модернизация электронных образовательных ресурсов стало обязательным условием для построения высокого уровня взаимодействия между студентами и учебными заведениями.

Очевидно, что нельзя забывать о информационной безопасности при организации такого формата образования. Для реализации высокого уровня защищенности электронной информационной среды необходимо соблюдать меры по обеспечению целостности, достоверности и конфиденциальности образовательной информации [3,4].

Важнейшими аспектами при работе с образовательным ресурсом учреждения являются санкционированный доступ, защита электронных документов от копирования, модификации и подделки и обеспечение подлинности этих электронных документов [5,6]. За все эти параметры может отвечать цифровой сертификат безопасности.

Цифровой сертификат – это электронный документ, который однозначно идентифицирует владельца сертификата [7] по некоторым параметрам, такими как:

- Серийный номер сертификата;
- Имя центра сертификации;
- Имя держателя сертификата;
- Открытые ключи держателя сертификата;
- Идентификаторы алгоритмов открытых ключей;
- Электронная подпись, сгенерированная секретным ключом центра сертификации;
- Идентификатор алгоритма электронной подписи;
- Срок годности

Цифровой сертификат позволяет владельцу безопасным способом взаимодействовать с некоторой системой при помощи шифрования. Составную часть сертификата можно дополнять своими дополнительными параметрами, в зависимости от целей использования.

Электронная подпись является частью электронного сертификата, регламент которого определяется ст.2 Федерального закона «Об электронной подписи» от 06.04.2011 N 63 – ФЗ [8].

Электронная подпись является некой математической операцией над совокупностью битов, которую можно выполнить только при помощи определенного ключа [9].

Диапазон методов генерации таких ключей разнообразен и включает в себя такие алгоритмы шифрования, как:

- Алгоритм шифрования ГОСТ 28147-89;
- Функции хэширования ГОСТ Р 34.11-2012 для ключей длины 256 и 512 бит;
- Алгоритмы ГОСТ Р 34.10-2012 для ключей длины 256 и 512 бит;
- Алгоритмы Диффи-Хеллмана на базах потенциальной функции и эллиптической кривой для ключей длиной 256 и 512 бит;
- Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94

Сертификат может быть неподписанным (unsigned), самоподписанным (self-signed – подписанный самим владельцем) и подписанным специальным центром сертификации.

В зависимости от используемого стандарта существуют различные форматы сертификатов. В большинстве случаев бывает достаточно сертификатов в кодировках Distinguished Encoding Rules (DER) и Base-64. Файл, содержащий сертификат имеет расширение *.cer и соответствует стандарту X.509v3.

Правильная цепочка представляет собой последовательность из n сертификатов, в которой владелец сертификата x есть издатель сертификата x + 1, x = 1 – корневой самоподписанный сертификат центра сертификации, x = n – конечный сертификат. Процедура верификации сертификатов подразумевает, что цепочка считается правильной, если начинается с сертификатов, изданных одним доверенным центром сертификации.

Учебные заведения, в большинстве случаев, в наименьшей степени уделяют внимание информационной безопасности своих внутренних образовательных ресурсов. А ведь следует учесть, что на таких ресурсах выкладывается и хранится большой объем научной, научно – образовательной и научно-технической информации. И угрозы информационной безопасности может привести к нарушению целостности таких данных.

В таких случаях, крайне актуально является внедрение некой подсистемы, которая бы: во-первых, разграничивала доступ к основному ресурсу на основе параметра принадлежности держателя сертификата к определенной группе лиц – будь то обучающийся или преподаватель. И во-вторых, гарантировала подлинность и защиту образовательной информации от несанкционированной модификации, копирования и подделки на основе электронной подписи, проставляемой автором выкладываемой в ресурс информации.

Подсистема должна обеспечить как свободной доступ к основной системе, так и упростить процесс авторизации и разграничение доступа.

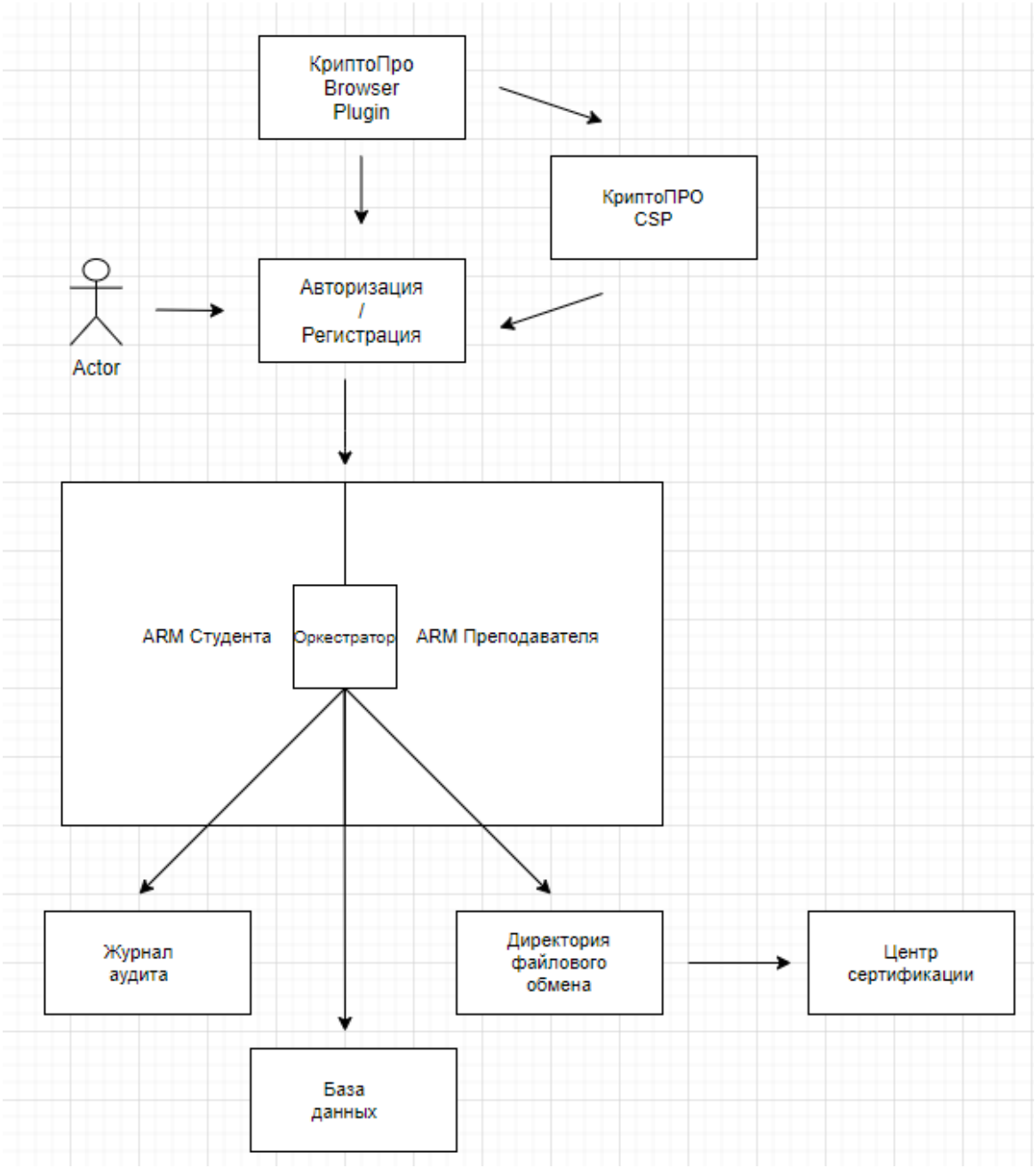


Рис. 1. Концепция подсистемы

Для аутентификации сервер потребует от клиента предъявления действительного и доверенного сертификата, причем логин и пароль запрашиваться не будут. В большинство браузеров можно установить сертификат и закрытый ключ непосредственно в сообственное хранилище сертификатов браузера. Атрибут CN (Common Name) сертификата сравнивается с запрашиваемым именением пользователя из базы данных, и, если они соответствуют, вход разрешается. Данная схема авторизации признана наиболее надежной и, в том или ином виде, широко используется в сфере предоставления банковских услуг.

Разграничение доступа достигается путем добавления в сертификат некоторого флага, по которому подсистема определит роль держателя сертификата и, в зависимости от этой роли, перенаправит подключение либо на ARM обучающегося, либо на ARM преподавателя.

Для подключения к образовательному ресурсу нового пользователя достаточно получить у администратора корневой сертификат центра сертификации. На основе корневого сертификата пользователь создает запрос на выпуск (файл с расширением *.rtm или *.pse) и закрытый ключ. Созданный файл запроса на получение сертификата необходимо передать администратору, который уже начнет взаимодействовать с центром сертификации. После получения сертификата пользователь должен внести сертификат в свое хранилище на локальном компьютере.

Очевидно, что подсистема должна отслеживать действительность сертификата. Недействительным сертификат может быть признан, если срок действия сертификата истек или не наступил, а также если сертификат отозван центром сертификации.

Плагин «КриптоПро ЭЦП Browser plug in» отвечает за проверку и формирование на web-страницах электронной подписи. Инструмент основан на механизме «КриптоПро CSP» и позволяет контролировать целостность и достоверность информации, объединяя подпись с заверяемым электронным документом или загруженным на компьютер файлом. Сама электронная цифровая подпись создается на стороне пользователя, что позволяет минимизировать риск ее перехвата.

В современном мире информационная структура один из главных компонентов образовательного процесса. Обеспечение безопасности образовательных ресурсов в учебных учреждениях – весьма серьезная задача, которой нужно уделять серьезное внимание, ведь качество знаний напрямую зависит от подлинности и достоверности информации. Предложенная концепция подсистемы в полном объеме учитывает эти факты и зависимости.

Помимо цифровых сертификатов безопасности широко применяются и другие методы обеспечения доступа и защиты информации, но на данный момент именно использование сертификатов позволяет наилучшим способом минимизировать риски угроз информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Mladenov, Vladislav, et al.: 1 Trillion Dollar Refund: How To Spoof PDF Signatures. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communica-tions Security, 1-14. ACM, London (2019).
2. Salah, Khaled, et al.: Blockchain for AI: Review and open research challenges. IEEE Access 7, 10127-10149 (2019).
3. Yadav A. K., Singh K.: Comparative analysis of consensus algorithms of blockchain technology. Ambient Communications and Computer Systems, 205-218 (2020).
4. Gupta, Brij B., et al.: A Comprehensive Survey on DDoS Attacks and Recent Defense Mechanisms. Handbook of Research on Intrusion Detection Systems, 186-218 (2020).
5. Nugroho, Herry Prasetyo, Muhammad Irfan, and Amrul Faruq: Software Defined Net-works: a Comparative Study and Quality of Services Evaluation. Scientific Journal of Informatics 6 (2), 181-192 (2019).
6. Tavares, Bruno, Filipe Figueiredo Correia, and André Restivo: A Survey on Blockchain Technologies and Research. Journal of Information 14 (2019), 118-128 (2019).
7. Marcus Schulzke: The politics of attributing blame for cyberattacks and the costs of uncertainty. Perspectives on Politics 16 (4), 954-968 (2018).

8. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ (последняя редакция) [Электронный ресурс]: дата обращения 22.11.2021
http://www.consultant.ru/document/cons_doc_LAW_112701/
9. Maurice Dawson: National Cybersecurity Education: Bridging Defense to Offense. Land Forces Academy Review 25(1), 68-75 (2020).

Байбурин В.Б.
СГТУ, заведующий кафедрой, д.ф.-м.н., профессор
baiburinvb@rambler.ru
Корчагин С.А.
СГТУ, доцент,
Финансовый университет, доцент, к.ф.-м.н.
korchaginser@gmail.com
Шелудяков Д.А.
СГТУ, ассистент
dimka.ice@yandex.ru
Смирнов Е.С.
СГТУ, аспирант
theproteks.business@gmail.com

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПРОТИВОДЕЙСТВИЯ DDOS-АТАКАМ НА ОБРАЗОВАТЕЛЬНЫЕ УЧРЕЖДЕНИЯ

Современные реалии требуют взаимодействия с информационными системами разного масштаба во всех сферах жизни человека и общества в целом. С ростом объема и значимости обрабатываемой информации приоритетными становятся проблемы обеспечения информационной безопасности, в частности политических институтов. Политические институты как объект информационной безопасности обладают рядом особенностей, среди которых можно выделить: широкий спектр DDoS-атак (100-500 Гбит / с), многоуровневые (L1-L7 по сети OSI). модель), сложность использования протоколов (NTP, DNS, SNTP, HTTP, Charden, SSDP и др.), масштаб воздействия и последствий [1].

Существует большое количество работ и прикладных инструментов, предназначенных для противодействия DDoS-атакам. Решения, позволяющие организовать скоординированный ответ на DDoS-атаки сетевыми силами, при этом разработка таких решений является активно развивающимся и перспективным направлением. Несмотря на большое количество традиционных средств защиты от DDoS-атак, количество жертв таких атак с каждым годом увеличивается [2]. В настоящее время растет интерес к разработке децентрализованных информационных систем для решения задач информационной безопасности образовательных учреждений [3]. В таких системах целостность и защита информации поддерживается с помощью технологии блокчейн, в отличие от традиционных систем, где каждый объект атаки имеет собственную систему защиты.

DDoS-атаки, как правило, происходят в сети с одним доменом, каждая из которых независимо раскрывает текущую атаку. системы защиты от DDoS-атак с использованием технологии блокчейн и смарт-контрактов, которые обеспечивают необходимый механизм без необходимости разработки нового протокола и позволяют обмениваться информацией о продолжающихся атаках в полностью распределенном и автоматическом режиме.

Сказанное определяет актуальность работы, а также ее цели и задачи.

Целью данной работы является разработка программного комплекса, основанного на технологии блокчейн, который защитит информационные сети образовательных учреждений от таких атак, как распределенный отказ в обслуживании (DDoS). В задачи

исследования входят: сравнительный анализ существующих алгоритмов блокчейна применительно к задачам информационной безопасности; моделирование системы защиты от DDoS-атак с использованием технологии блокчейн; разработка программы скоординированного реагирования на DDoS-атаки.

Предлагаемый в работе метод можно отнести к распределенному или гибридному механизму защиты от DDoS-атак [4,5]. Отличительной особенностью предлагаемого в исследовании метода является использование технологии блокчейн, в частности, использование децентрализованной платформы разработки приложений Stratis [6-8].

Предлагаемая модель смягчения воздействия DDoS-атак на сеть основана на сочетании преимуществ технологии блокчейн и программно-определяемых сетей (SDN) [9-11]. Гибкость в настройке решений SDN внутри доменов позволяет быстро вносить изменения в сетевую политику без ущерба для производительности, а возможности междоменного взаимодействия децентрализованных приложений на основе блокчейнов позволяют организовать достаточно быструю и эффективную сеть с автоматической реконфигурацией. для борьбы как с междоменными атаками, так и в пределах одного сетевого домена.

Рассмотрим следующий сценарий DDoS-атаки на образовательные учреждения (рис. 1). Веб-сервер, размещенный в автономной системе (АС) С, подвергается DDoS-атаке с устройств, расположенных в разных доменах.

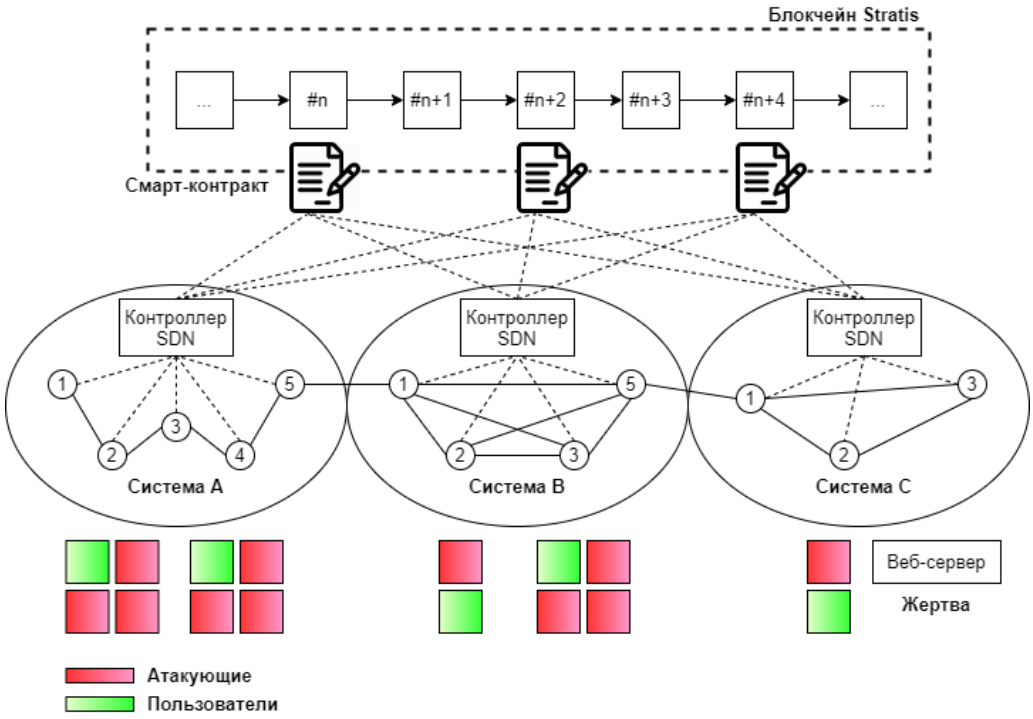


Рис. 1. Сценарий DDoS-атаки

При непоследовательном подходе к предотвращению DDoS-атак между домами веб-сервер полагается на механизмы защиты, которые реализованы в сети, в которой он расположен, которая в большинстве случаев расположена на расстоянии от источника паразитного трафика, как следствие перегрузки. сразу - сколько доменов.

Для организации согласованного противодействия DDoS-атакам между пользователями и АС необходимо разработать смарт-контракт и опубликовать его в сети

блокчейн с поддержкой смарт-контрактов. Таким образом, как только один из пользователей или АС обнаруживает DDoS-атаку в сети, он должен отправить IP-адрес, с которого отправляется паразитный трафик, в согласованный смарт-контракт. Как описано ранее, время на создание нового блока в сети Stratis занимает 16 секунд, и поэтому после обработки вызываемого смарт-контракта АС, подписанные на него, получат обновленный список адресов для черного списка и подтвердят факт. атаки, если полученный адрес совпадает с исходным паразитным трафиком.

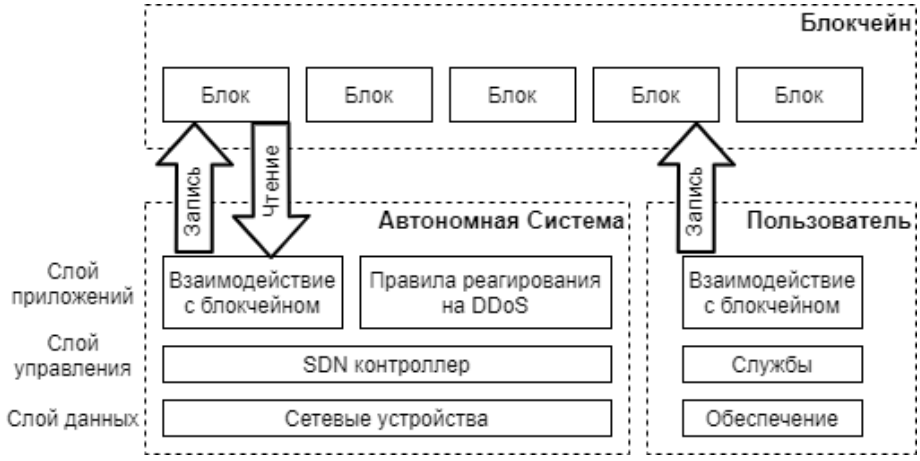


Рис. 2. Архитектура программного комплекса

Как только пользователи получают список злоумышленников и подтверждают, что атака происходит, каждый из них должен запустить различные стратегии смягчения в соответствии с политиками и механизмами безопасности, доступными в домене. Также АС может блокировать вредоносный трафик вблизи места его происхождения, что является лучшим решением для Интернета в целом, поскольку позволяет снизить общую стоимость пересылки трафика, пакеты в котором в случае DDoS-атак в основном состоят. бесполезной и тяжелой информации.

В ситуации междоменного взаимодействия узлы, участвующие в совместной защите, после получения информации об атаках могут принимать меры в соответствии со своими политиками безопасности. Однако в этом случае необходим механизм вознаграждения, помогающий предотвратить атаку, чтобы стимулировать каждого участника к совместной работе.

Архитектура построена с учетом следующих принципов:

1. Обнаружение DDoS и меры по его предотвращению предоставляются в виде услуг либо через механизмы, определенные в AS, либо через сторонние сервисы;

2. Чтобы передать или отправить информацию об атаке в домен, необходимо выбрать узел, который будет подключен к блокчейну. Это может быть выделенное оборудование исключительно для этой цели или виртуализированное с помощью SDN для уменьшения потребления ресурсов;

3. Для эффективного скоординированного ответа на атаки модули, подключенные к блокчейну, которые развернуты на клиентах и АС, должны регулярно обращаться к смарт-контракту на предмет изменений в списках IP-адресов;

4. Записи в списках смарт-контракта обновляются только участниками согласованного ответа посредством подтверждения права собственности (англ. Proof of Ownership);

5. После уведомления об атаке, в ходе которой клиент подтвердил свою личность, определяются меры противодействия в соответствии с установленными политиками безопасности домена.

В результате исследования была разработана система с использованием блокчейна для противодействия DDoS-атакам. Например, образовательные учреждения рассматривались как объект атак, имеющий ряд особенностей.

Stratis и программно-определяемые сети были предложены в качестве технологии для разработки интеллектуальной системы противодействия DDOS-атакам.

СПИСОК ЛИТЕРАТУРЫ

1. Dunn Cavelty M., Wenger A.: Cyber security meets security politics: Complex tech-nology, fragmented politics, and networked science. Contemporary Security Policy 41 (1), 5-32 (2020).
2. Canh, Nguyen Phuc, et al.: Systematic risk in cryptocurrency market: Evidence from DCC-MGARCH model. Finance Research Letters 29, 90-100 (2019).
3. Husain, Syed Omer, Alex Franklin, and Dirk Roep: The political imaginaries of block-chain projects: discerning the expressions of an emerging ecosystem. Sustainability Science, 1-16 (2020).
4. Conti, Mauro, et al.: A survey on security and privacy issues of bitcoin. IEEE Commu-nications Surveys & Tutorials 20 (4), 3416-3452 (2018).
5. Korchagin, S. A., et al.: Software and Digital Methods in the Natural Experiment for the Research of Dielectric Permeability of Nanocomposites. In: 2018 International Con-ference on Actual Problems of Electron Devices Engineering (APEDE), pp. 262-265. IEEE, Saratov (2018).
6. Apel, Sebastian, Florian Hertrampf, and Steffen Spathe: Towards a Metrics-Based Software Quality Rating for a Microservice Architecture. In: International Conference on Innovations for Community Services, pp. 205-220. Springer, Cham (2019).
7. Mladenov, Vladislav, et al.: 1 Trillion Dollar Refund: How To Spoof PDF Signatures. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communica-tions Security, 1-14. ACM, London (2019).
8. Salah, Khaled, et al.: Blockchain for AI: Review and open research challenges. IEEE Access 7, 10127-10149 (2019).
9. Yadav A. K., Singh K.: Comparative analysis of consensus algorithms of blockchain technology. Ambient Communications and Computer Systems, 205-218 (2020).
10. Gupta, Brij B., et al.: A Comprehensive Survey on DDoS Attacks and Recent Defense Mechanisms. Handbook of Research on Intrusion Detection Systems, 186-218 (2020).
11. Nugroho, Herry Prasetyo, Muhammad Irfan, and Amrul Faruq: Software Defined Net-works: a Comparative Study and Quality of Services Evaluation. Scientific Journal of Informatics 6 (2), 181-192 (2019).

Магомедов Р.М.
ДГТУ, ассистент,
indiansbobi@gmail.com
Качаева Г.И.
ДГТУ, заведующая кафедрой, к.э.н.
providetc@mail.ru

СИСТЕМЫ ЗАЩИТЫ БАЗ ДАННЫХ

Ключевые слова: база данных, защита базы данных, мониторинг активности.

Никто не будет спорить с утверждением, что тот, кто владеет информацией, тот управляет миром. По сути, информация — это самый дорогой актив любой компании, вне зависимости от ее специализации и масштаба. То есть, защита информации – ключевая задача, которую должны решать подразделения, несущие ответственность за состояние информационной безопасности.

Нет такой организации, которая не использует в своей работе базы данных (БД). Зачастую в них размещены конфиденциальные данные, относящиеся к финансам, клиентам, поставщикам и пр. это позволяет говорить о злободневности ее защиты.

Термин «защита БД» подразумевает методы предупреждения несанкционированного доступа (НСД) к данным занесенным в БД.

Длительное время под термином «защита БД» понимали охрану локальной компьютерной сети (ЛВС) от попыток проникновения со стороны злоумышленников. Но, как показало время, наиболее слабое место – люди, работающие в компании и имеющие доступ к информации. Другими словами, угрозы информационной безопасности исходят и снаружи, и изнутри компании, а источником угрозы можно назвать легитимных пользователей.

Базовые средства защиты баз данных

На первой линии защиты стоят сисадмины и администраторы БД. Сущность первой линии защиты заключена в формировании межсетевых экранов, они нужны для предотвращения попыток доступа к содержимому БД со стороны разных источников, настойка и поддержание в рабочем состоянии систем паролей и разграничения доступа. Это эффективные инструменты, которые требуют к себе особо внимательного отношения со стороны специалистов подразделения по защите информации.

Второй линией обороны можно назвать аудит пользовательских действий, по сути это и есть главная задача, решаемая в отделе информационной безопасности.

Важность аудита обусловлена тем, что в индустриальной системе довольно сложно выполнить настройку прав доступа к данным, хранящимся в БД компании.

Штатный аудит баз данных

Для выполнения вышеописанных мероприятий многие компании применяют инструменты «штатного аудита», входящим в состав многих существующих СУБД.

Штатный режим подразумевает ведение журнала подключения к СУБД, и выполнения запросов, инициированных пользователями. Проще говоря, сущность штатных мер защиты заключена в создании и настройке триггеров, определенных функций, срабатывающих при выявлении доступа к значимой информации, регистрации подобных запросов и сведение полученных сведений в единую таблицу.

Этих мер иногда хватает для исполнения отраслевых норм регулятора,

но они не принесут пользы при решении задач по обеспечению внутренней информационной безопасности, например, при расследовании периодически возникающих конфликтов.

Автоматизированные системы защиты баз данных

Но существует более результативный подход – применение специальных средств информационной безопасности в сфере защиты БД, решение типа DAM.

DAM (Database Activity Monitoring) – это инструмент независимого отслеживания действий пользователей. Под понятием независимость понимают отсутствие нужды в проведении дополнительных настроек СУБД. Системы этого типа могут осуществлять свои функции в пассивном режиме, при этом никак не влияя на бизнес-процессы, в состав которых входят БД.

Системы этого класса в состоянии разобрать поток данных, образованный между пользователями и БД, систематизировать SQL-запросы по их отношению к той или иной группе. Кроме этого эти системы могут вести полный аудит SQL-запросов и ответов на них. Системы оснащены технологией глубокой фильтрации, которая разрешает обнаружить вероятные конфликты и поддерживать полный архив, с зафиксированными действиями пользователей. Это нужно как для удовлетворения требований регулятора (ФСТЭК), так и для подробного анализа событий предшествовавших началу конфликта.

Система DAM позволяют выполнять синхронизацию с охраняемой БД. Это необходимо для:

Классификации – выявления местоположения небезопасных для компании сведений. Эта опция после сканирования БД позволяет увидеть наименования таблиц в которых могут быть размещены данные о клиентах. Такое решение упрощает дальнейшую настройку политики безопасности;

Проверки на уязвимость – определяет соответствие существующей конфигурации БД настройкам, выполненным на основании лучших практик.

Получение матрицы доступа к данным – решение этой задачи позволит выявить имеющиеся широкие права доступа, неиспользуемых привилегий, наличие «мертвых душ», т.е. неактивных учетных записей, которые могли остаться после, ухода сотрудника из компании.

К неоспоримым достоинствам подобных систем можно отнести – наличие гибкой системы формирования отчетности, возможность их встраивания в SIEM-системы для проведения глубокой оценки выполняемых запросов.

В перечень функций систем наблюдения активности БД входят:

Наблюдение за действиями привилегированных пользователей. Под привилегированными пользователями понимают – администраторов БД, сисадминов, внутренних и внешних разработчиков. Отслеживание пользователей этого уровня позволяет проследить за действиями сотрудников компании и установить подозрительную деятельность, проявляемую при работе с БД.

Задачу мониторинга привилегированных пользователей этого класса относят к достаточно трудоемким, это обусловлено в первую очередь тем, что сотрудники этого уровня обладают повышенными возможностями при проведении атак.

Отслеживание активности установленного ПО. Это позволяет установить работников, осуществляющих неразрешенные действия с программными приложениями, работающими с БД.

На российском рынке ПО существует решение DAM «Гарда БД» от компании "Гарда Технологии".

Это комплекс программ, осуществляющий постоянный мониторинг всех запросов, совершаемых к БД и веб-приложениям в текущем времени, и сохраняющий их в архиве в течении определенного времени.

Система проводит сканирование и выявление слабых мест в защите СУБД. К слабым местам можно отнести:

не заблокированные учётные записи, незатейливые пароли и пр.

Реакция на возникающие конфликтные ситуации происходит моментально, и соответствующие сообщения уходят на e-mail и в SIEM-систему.

Система защиты БД устанавливается в пассивном режиме и не влияет на работоспособность сети. При поддержке интеллектуальной системы хранения можно создать архив запросов и ответов к базам данных за установленный интервал времени. Этот архив нужен для оценки произошедших инцидентов и их расследования.

Это первый комплекс DAM, внесенный в реестр отечественного ПО. Он установлена во многих крупных банках России.

В настоящее время ИТ-рынок богат различными решениями программного обеспечения, и это затрудняет выбор среди них. Для получения оптимального программного решения для обеспечения безопасности вашей сети вы можете сначала рассмотреть такие факторы, как целевое решение, возможность обрабатывать объемные данные, возможность создавать различные отчеты о состоянии и безопасности системы, настраиваемость и, конечно же, простую в использовании функцию.

Рейтинг обеспечивается с помощью таких факторов, как особенности, удобство использования, производительность, поддержка, соотношение цены и качества и т.д. Поэтому, если вы заинтересованы в развертывании эффективного программного обеспечения и инструментов для вашей безопасности, вы должны более внимательно посмотреть на некоторые популярные рейтинги авторитетных рецензентов.

СПИСОК ЛИТЕРАТУРЫ

1. Увайсова З. М., Билалова И. М. Защита и безопасность баз данных // Студенческий научный форум : материалы VII Междунар. студ. электронной науч. конф. [Электронный ресурс]. URL: http://www. scienceforum.ru/ (дата обращения: 14.09.2019).
2. Лихоносов А. Г. Безопасность баз данных: интернет-курс по дисциплине [Электронный ресурс]. URL: http://www.e-biblio.ru/ (дата обращения: 12.09.2019).
3. Смирнов С. Н. Безопасность систем баз данных. М. : Гелиос АРВ, 2007. С.352-353.
4. [Электронный ресурс]. URL: https://gardatech.ru/ (дата обращения: 20.03.2021).

НАУЧНАЯ СЕКЦИЯ
«БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИЙ»

Место проведения:
г. Москва, ул. Авиамоторная, д. 8а, стр. 39 (конгресс-центр), 2-й этаж

Подсекция № 1

«Организационно-технические проблемы защиты телекоммуникаций»

Руководитель: **Кубанков Александр Николаевич**,
Московский технический университет связи и информатики,
заведующий кафедрой «Безопасность телекоммуникаций»,
доктор военных наук, профессор

Секретарь: **Симонов Павел Игоревич**,
Московский технический университет связи и информатики,
доцент кафедры «Безопасность телекоммуникаций»,
кандидат технических наук

Давлетова Д.Р.
БашГУ, студент
Davletova.dii@yandex.ru
Кормилец В.П.
БашГУ, студент
vkormilecz@bk.ru
Каримов А.И.
БашГУ, ассистент
aidar.karimov2015@yandex.ru

ОСОБЕННОСТИ СОВРЕМЕННЫХ КОММУНИКАЦИЙ

Потребность в телекоммуникации возникла и развивалась одновременно с развитием общества. Современная отрасль телекоммуникационных услуг требует новых решений, в свою очередь инновационные решения невозможны без грамотных технических специалистов, которые обладают знаниями в области последних новинок в сфере коммуникаций. С каждым годом, количество объема информации возрастает, возрастают и потребности в усовершенствовании технологий, позволяющие обеспечить передачу этой информации. Далее мы рассмотрим несколько особенностей, которые появились с развитием телекоммуникационных технологий.

Под телекоммуникациями принято понимать любые формы связи и передачи информации на расстоянии.

Телекоммуникационная сеть представляет собой сеть для обмена и обработки информации. Осуществляется с помощью средств телекоммуникации, представляющие совокупность сетевых устройств, которые реализуют передачу информации. Наиболее известная телекоммуникационная система - это Интернет.

В 1969 году появляется APRANet (Advanced Research Projects Agency Network) – прототип сети Интернет. Впоследствии данному проекту требовалось внедрения нового протокола передачи данных. Необходимо было установить набор правил, определяющий общий алгоритм обмена данными между двумя абонентами сети. В 1974 году группа инженеров Internet Network Working Group (INWG) представила универсальный протокол передачи данных и объединения компьютерных сетей. Протокол был назван Transmission Control Protocol/Internet Protocol (TCP/IP - Протокол управления передачей/Межсетевой протокол) - TCP/IP.

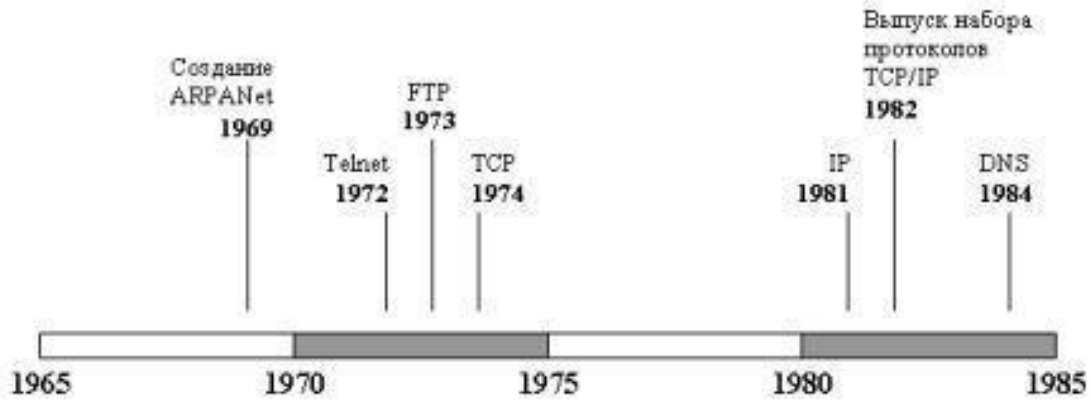


Рис. 1. Этапы возникновения TCP/IP

В глобальных и локальных сетях используется сеть TCP\IP, где главными достоинствами является масштабируемая система адресации и ее гибкость. Основные задачи адресации:

1. Согласованное использование адресов разных типов;
2. Конфигурирование сетевых интерфейсов и сетевых приложений;
3. Обеспечить уникальность адресов.

Стек TCP/IP состоит из иерархической, четырехуровневой структуры (Рис. 2).

Прикладной уровень	**Сетевой уровень**	**Транспортный уровень**	**Уровень сетевых интерфейсов**
FTP TFTP HTTP SNMP Telnet SMTP	IP RIP ICMP OSPF	TCP UDP	Не регламентируется

Рис. 2. Уровни TCP/IP

В сетке TCP/IP образовалась устоявшаяся терминология (Рис. 3).

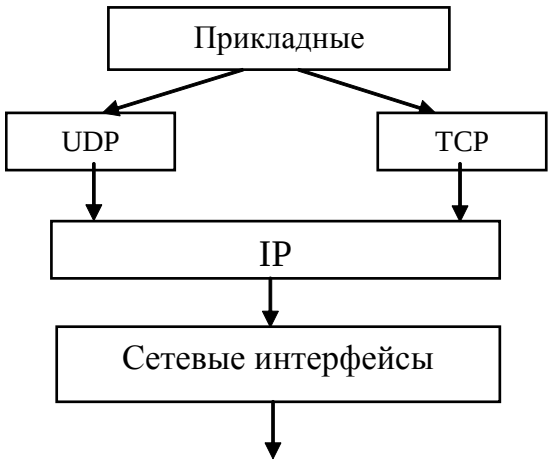


Рис. 3. Терминология TCP/IP

Так как в начале 90-х стек протоколов TCP/IP выявились серьезные проблемы и это поспособствовало к увеличению узлов сети, ужесточению требований, предъявляемых к качеству обслуживания сетью ее пользователей и ухудшению характера трафика. Вследствие этого был создан новый шестой версии протокол IPv6(RFC 8200). Система адресации привнесла важные изменения в старую систему, что привело за собой увеличения разрядности адреса. И вместо 4 байт IP-адреса в IPv4 в новой версии под адрес отведено 16 байт. Данные манипуляции решили проблему с нехваткой количества узлов сети.

Одна из первоочередных целей системы адресации выражалась в повышении эффективности работы стека TCP/IP.

В IPv6 три основных типа адресов (RFC 4291):

1. Индивидуальный адрес (unicast) – оригинальный идентификатор отдельного интерфейса конечного узла.

2. Групповой адрес (multicast) – идентифицирует группу интерфейсов, имеющих отношение к разным узлам.

3. Адрес произвольной рассылки (anycast) – определяет группу интерфейсов.

Также положительный эффект отразился на маршрутизаторах, а именно избавились от различных вспомогательных функций :

1. Перенос функций фрагментации с маршрутизаторов на конечные узлы.

2. Отказ от обработки необязательных характеристик заголовка.

3. Обширное использование маршрутизации от источников.

4. Отказ от подсчета контрольной функции.

5. Агрегирование адресов.

6. Прекращение использования технологии NAT.

7. Немаловажная вероятность использования в качестве номера узла его MAC-адреса.

Но протокол IPv6 не может работать без вспомогательных протоколов, которые выполняют функции отображения адресов, оповещения о произошедших ошибках (в IPv4 такую роль играют DNC, ICMP, ARP, DHCP). Для этого был создан протокол ND (Neighbor Discovery). Он представляет собой набор процессов и сообщений, которые определяют взаимоотношения между смежными узлами и выполняет следующие задачи:

1. Определение адреса маршрутизатора и префикса IPv6 (SLAAC).

2. Замена ARP для IPv6 (замена MAC-адресов).

3. Настройка маршрутизации (router redirect).

4. Проверка доступности узлов сети (соседей).

5. Определение конфликта IP-адресов.

Протокол NDP – расширение ICMP. Он задает новые типы сообщений, новые форматы пакетов для каждого типа. Этот протокол используется совместно с протоколом IPv6 и определен стандартом RFC 4861. Он используется в процессе автоматического конфигурирования, и благодаря именно этому протоколу хост, который использует IPv6 получает адрес маршрутизатора и префикс сети в которой он находиться, то есть маску подсети. Кроме этого протокол NDP используют так же и для других целей, одна из важнейших это определение MAC-адреса по известному адресу IPv6.

Типы сообщений NDP:

– 133 – Router Solicitation;

– 134 – Router Advertisement;

– 135 – Neighbor Solicitation;

– 136 – Neighbor Advertisement;

– 137 – Redirect.

Формулы:

1.Буферы.

По умолчанию ограничение буферной скорости передачи данных TCP составляет 2^16 байт (до 64 КБайт). Максимальная пропускная способность в данном случае (1.1):

$$\text{Throughput} \leq \frac{\text{RWIN}}{\text{RTT}} \tag{1.1}$$

2. Задержка и потеря пакетов.

Для более устойчивой передачи информации TCP дважды передает сегменты при потере пакетов в сети. Это, в первую очередь, приводит к понижению скорости. Соотношение скорости TCP к потере пакетов, определяется формулой Mathis-a (1.2):

$$\text{Throughput} \leq \frac{\text{MSS}}{\text{RTT}\sqrt{P_{\text{loss}}}}, \quad (1.2)$$

Подводя итоги, мы можем выделить несколько особенностей современных телекоммуникаций:

– внедрение IPv6

– создание протокола ND (Neighbor Discovery).

Необходимость в IPv6 возникла из-за нехватки адресов в IPv4. Протокол начал внедряться относительно недавно. Но так как протокол IPv6 не может работать без вспомогательных протоколов, был создан NDP.

Совместно эти протоколы выполняют важные задачи:

– автоматическая настройка адресов IPv6;

– замена ARP для IPv6 (определение MAC-адреса).

Особенности NDP в том, что вместо IPv4 широковещательных адресов используются групповые адреса:

1. FF02::1 – все узлы в канале связи;

2. FF02::2 – все маршрутизаторы в канале связи;

3. FF:02::1:FFXX:XXXX – все узлы, IPv6-адреса которых заканчиваются на XX:XXXX.

СПИСОК ЛИТЕРАТУРЫ

1. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер // Питер. - 2020. - 1008с. - ISBN 978-5-4461-1426-9
2. Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации. Учебное пособие / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко // КноРус. – 2019. – 372с. - ISBN 978-5-406-06790-1
3. Украинцев, Ю.Д. Основы телекоммуникаций. (СПО). Учебное пособие / Ю.Д. Украинцев // КноРус. – 2021. – 342с. - ISBN 978-5-406-06305-7
4. Калугин, Н.Г. Электропитание устройств и систем телекоммуникаций / Н.Г. Калугин // Academia. – 2011. – 192с. – ISBN 978-5-7695-6857-2
5. Крук, Б.И. Телекоммуникационные системы и сети. Том 1. Современные технологии. Учебное пособие / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов // Горячая линия-Телеком. -2003. - 647с. - ISBN 5-93517-088-4
6. Быховский, М.А. Развитие телекоммуникаций. На пути к информационному обществу. Развитие спутниковых телекоммуникационных систем. Учебное пособие / М.А. Быховский // Горячая Линия – Телеком. -2014. - 436с. - ISBN 978-5-9912-0405-7
7. Самуйлов, К.Е. Сети и телекоммуникации / К.Е. Самуйлов // ЮРАЙТ-Восток. - 2021. - 364с. - ISBN 978-5-9916-0480-2

8. Канев, В.С. Основы моделирования и управления операционными рисками в электронной коммерции и телекоммуникациях / В.С. Канев, Ю.В. Шевцова // Горячая линия-Телеком. -2015. - 278с. - ISBN 978-5-9912-0495-8
9. Замятина, О.М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей / О.М. Замятина // ЮРАЙТ-Восток. -2021. - 160с. - ISBN 978-5-534-00335-2
10. Фронтов, В.В. Регулирование телекоммуникаций в России и странах СНГ Учебное пособие для вузов / В.В. Фронтов, В. О. Тихвинский // Горячая линия-Телеком. -2006. - 368с. - ISBN 5-93517-300-X

Кутуев Т.М.
БашГУ, студент
ktm_tim22@mail.ru
Бочкарёв Д.В.
БашГУ, студент
fergust322@gmail.com
Каримов А.И.
БашГУ, ассистент
aidar.karimov2015@yandex.ru

ПРОБЛЕМА БЕЗОПАСНОСТИ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация: Защита сетей от атак является важным аспектом, который нельзя игнорировать. В данной статье освещаются некоторые важные проблемы безопасности современных телекоммуникационных сетей и рекомендуются контрмеры, которые могут быть реализованы для повышения безопасности от кибератак.

Abstract: Protecting these networks from attacks is thus an important aspect that cannot be ignored. This paper highlights some of the important security challenges to current telecommunication networks and recommends countermeasures that can be implemented to mitigate not only infrastructural insecurity but also the risk from cyber-attacks.

Ключевые слова: кибербезопасность; кибератака; телекоммуникационная инфраструктура; киберпреступность; взлом.

Keywords: cybersecurity; cyberattack; telecommunication infrastructure; cybercrime; hacking.

Телекоммуникационные сети представляют собой комплекс аппаратных и программных средств, обеспечивающих передачу информационных сообщений между абонентами с заданными параметрами качества. В телефонной сети общего пользования (ТСОП) используется технология коммутации каналов, которая быстро заменяется технологией мобильных беспроводных сетей. Технология беспроводных сетей - это технология коммутации на основе пакетов. Инфраструктура ТСОП состоит из цифровых коммутаторов, кабелей, таких как коаксиальные, надводные и подводные оптоволоконные кабели для передачи данных на большие расстояния, наземные микроволновые и спутниковые линии связи. Эта технология была разработана в первую очередь как сеть для передачи голосовых сигналов. Решение проблемы высокого спроса на услуги видео и передачи данных было найдено с появлением беспроводных мобильных технологий. Эта технология, основанная на пакетной коммутации, обеспечила тип сети, подходящий для тройной связи (т.е. голос, данные и видео). Эта технология, в отличие от технологии с коммутацией каналов, подходит для передачи голоса, данных и видеоинформации. Телекоммуникационные сети с глобальной точки зрения представляют собой конвергенцию нескольких технологий - ТСОП, 2G, 3G и 4G с жизненно важными сетевыми компонентами. Этими компонентами являются сеть доступа, базовая сеть, внутренние и внешние сети. Атаки на сеть одного оператора связи могут также распространяться на несколько сетей через межсетевое взаимодействие. Это подчеркивает

возможность получения злоумышленниками доступа к своим целям независимо от географического положения удаленного терминала.

В наше время безопасность в интернете является очень важным аспектом. Кибербезопасность предполагает снижение риска злонамеренных атак на программное обеспечение, компьютеры и сети. Сюда входят инструменты, используемые для обнаружения взломов, остановки вирусов, блокировки злонамеренного доступа, принудительной аутентификации, включения зашифрованной связи и так далее. По статистике МВД количество киберпреступлений за первую половину 2021 года поднялось на 25 процентов в сравнении с аналогичным периодом 2020 года. Вся связь, которая происходит через Интернет, осуществляется через порты. Каждый IP-адрес содержит два вида портов, TCP и UDP, и для любого данного IP-адреса может быть до 65 535 портов. Службы, подключающиеся к Интернету (например, браузеры, почтовые клиенты и службы передачи файлов), используют определенные порты для получения информации. TCP (Протокол управления передач) - самый популярный протокол транспортного уровня в Интернете. TCP протокол предназначен для управления передачей данных интернета. UDP (User Data Program) - транспортный протокол пользовательских датаграмм из набора правил TCP/IP. Позволяет отправлять информацию (датаграммы) по IP-сети без предварительного установления соединения и создания специального виртуального канала или путей данных.

Существует большое количество вирусов, которые злоумышленники могут использовать в незаконных целях. Некоторые вредоносные программные обеспечения работают по принципу открытия портов. Одним из таких вирусов является троян. Троян - это вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю (злоумышленнику), а также действия по удалению, изменению, сбору и пересылке информации. Троянский конь составляет около 58 процентов всех компьютерных вредоносных программ. Использование трояна в настоящее время больше относится к вредоносным программам, которые очень опасны из-за масштабных последствий, начиная от кражи данных и заканчивая изменениями прав доступа на ПК жертвы. Троян обычно выглядит как вредоносная программа, прикрепленная к электронному письму. Будь это файл, программа или приложение. Благодаря нужных утилит возможно спрятать троян даже в картинку. Когда вы нажмёте на просмотр картинки сервер принимает подключение, и закрывает порт для дальнейших подключений. С этого момента сервер и клиент начинают обмениваться данными и у злоумышленника появится доступ к вашему компьютеру.

Проблемы кибербезопасности в России являются актуальной по сей день. В пример можно привести общедоступный сервис Zoom. С начала пандемии спрос на услуги данного сервиса сильно вырос. Из-за пандемии многие компании постепенно переходить на удаленный режим работы, а в образовательных учреждениях стали вводить дистанционный формат обучения. Из-за высокого спроса на видеоконференции и другие подобные инструменты для совместной работы может возникнуть много лазеек для работы хакеров. Эксперты по безопасности, защитники персональных данных и даже ФБР (Федеральное бюро расследований) предупреждают, что настройки Zoom по умолчанию небезопасны. Основные уязвимости зума:

- Отсутствие сквозного шифрования E2E (информация хранится на серверах компании может попасть в руки злоумышленников).

- Прослушивание вызовов.

- Zoom строится вокруг службы Active Directory, где хранятся данные обо всех учетных записях пользователя (Подключаясь к звонку по ссылке, вы передаете верификационные данные так называемому Man in the Middle — провайдеру или оператору связи. Защита информации во время такой передачи в Zoom слабо проработана, и если в сети «посредника» есть зараженный участок, данные могут быть перехвачены мошенниками).

- Нет надёжной защиты аккаунта по типу 2FA (Двухфакторной защиты).

Следите за портами, которые используются в вашей сети, и исследуйте любые странности или необъяснимые открытые порты. Поймите, как выглядит ваше обычное использование порта, чтобы можно было идентифицировать необычное поведение. Выполняйте сканирование портов и тесты на проникновение.

Чтобы определить, действительно ли устройства в опасности, вам необходимо выяснить, что увидит злоумышленник, если выполнит сканирование портов на вашем устройстве. Один из способов сделать это - использовать сканер портов, который используют хакеры (но не опасен для вас на вашем собственном устройстве). Оттуда вы можете увидеть, какой из портов вашего компьютера отвечает как «открытый».

Если какие-либо из них открыты, возможно, что эти порты на самом деле не должны быть доступны извне вашей сети, и в этом случае вы должны приступить к работе, заблокировав их или отключив. Если вам действительно нужно открыть эти порты, вы можете начать применять исправления для защиты вашей сети от злоумышленников.

Кроме того, профессионалы в области кибербезопасности могут использовать тот факт, что хакеры обычно проверяют сети на наличие уязвимостей с помощью атак со сканированием портов, чтобы настроить свои сети для замедления работы злоумышленников. Используя брандмауэры для перенаправления открытых портов на «приманки» или пустые хосты, вы можете превратить сканирование портов, которое займет у хакеров всего несколько секунд, в 7-часовую работу. Использование частоты сканирования портов с помощью средств защиты от обмана, которые отправляют хакеров в «ловушки-приманки», может быть эффективным методом, требующим относительно небольших вложений.

Реализация инфраструктуры безопасности. Важные процессы и политики организации, принятые организацией, должны поддерживаться инфраструктурой безопасности, включающей несколько уровней безопасности. Эта стратегия позволяет использовать различные уровни безопасности таким образом, что компрометация только одного уровня безопасности не подвергает сеть атакам. Некоторые из мер безопасности, которые могут быть развернуты на различных уровнях, следующие:

- Брандмауэры на периметре сети для общедоступных систем

- Хост и сетевые системы обнаружения/защиты от вторжений (IDPS).

- Системы управления информацией и событиями безопасности (SIEM) для обработки событий безопасности и журналов, которые генерируются несколькими системами.

- Проведение проверок безопасности телекоммуникационного оборудования, периметров, критических компонентов сети и приложений.

- Регулярно обновлять операционные системы и приложения, которые являются частью инфраструктуры промышленной сети, и устанавливать патчи сразу, как только они выходят.

Телекоммуникационная инфраструктура является большой мишенью для кибератак. Это связано с тем, что они создают, контролируют и эксплуатируют критически важные сети, которые широко используются для передачи и хранения больших объемов конфиденциальных данных. Атаки могут нанести ущерб, например, привести к утечке конфиденциальной информации и обнародованию документов безопасности, что может поставить под угрозу как отдельных лиц, так и пострадавшие организации.

Открытые порты также увеличивают риск утечки данных. Однако, если правильно следить за безопасностью своих портов, можно избежать потерю данных. Поэтому, уделять внимание проблемам безопасности в области телекоммуникаций и информационных технологий необходимо.

СПИСОК ЛИТЕРАТУРЫ

1. Александровская Л.Н., Безопасность и надежность технических систем : Учебное пособие. / Александровская Л.Н., И.З. Аронов, В.И. Круглов, А.Г. Кузнецов, Н.Н. Патраков, А.М. Шолом - Москва. : Логос, 2017. – 376 с.
2. Ахмад Д.М., Защита от хакеров корпоративных сетей / Ахмад Д.М. и др. ; Пер. с англ. А.А. Петренко. - Второе издание. - Москва. : ДМК Пресс, 2016. - 864 с.
3. Байер, Д. Обеспечение безопасности: учебное пособие/ Доминик Байер. - Москва: Русская Редакция, 2013. - 430 с.
4. Бондарев В.В., Введение в информационную безопасность автоматизированных систем : учебное пособие / В.В. Бондарев - Москва.: Издательство МГТУ им. Н. Э. Баумана, 2018. - 250 с.
5. Грушо, А.А. Теоретические основы защиты информации: учебное пособие / Е. Г. Тимонина. - Москва: Яхтсмен, 2016. - 187 с.
6. Душкин А.В., Методологические основы построения защищенных автоматизированных систем : учеб. пособие / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий, А.П. Данилкин, А.А. Малышев - Воронеж : ВГУИТ, 2013. - 263 с.
7. Куприянов, А. И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений/ А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. - Москва: Издательский центр «Академия», 2014. – 35с.
8. Климентьев К.Е., Компьютерные вирусы и антивирусы: взгляд программиста / Климентьев К.Е. - Москва. : ДМК Пресс, 2013. - 656 с.
9. Малюк А.А., Защита информации в информационном обществе : Учебное пособие для вузов. / А.А. Малюк - Москва. : Горячая линия - Телеком, 2015. - 230 с.
10. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2015. - 352 с.

Сайфутдинова А.Р.
БашГУ, студент
alina.saifutdinova@list.ru
Каримов А.И.
БашГУ, ассистент
aidar.karimov2015@yandex.ru

АНАЛИЗ МНОГОФУНКЦИОНАЛЬНЫХ ПОИСКОВЫХ ПРИБОРОВ

Аннотация: в статье рассматривается многофункциональный прибор ST131.S ПИРАНЬЯ II, проводится анализ работы прибора в разных режимах и методах поиска закладочных устройств.

Ключевые слова: защита информации, закладочные устройства, многофункциональный прибор, локализация, режимы работы, радиозакладка, обнаружение, датчик.

Информации – это один из самых ценных ресурсов в современном мире, играет большую роль в жизни отдельной личности, так и всего общества. Пока одни стараются сохранить информацию в тайне, другие всеми средствами пытаются заполучить ее. Поэтому вопрос защиты информации на сегодняшний день стоит очень остро.

Есть множество способов несанкционированного съема данных, одним из самых распространенных способов считается применение всякого рода электронных устройств прослушивания. Их обнаружение весьма проблематично, для этого требуются профессиональный персонал и использование всевозможного оборудования. Тем не менее устройства работать в режиме нескольких приборов, процесс радиопоиска может быть автоматизирован, а в конце подробно анализируются все собранные сведения. Называются такие приборы многофункциональными средствами поиска устройств не сканкционированного съема информации. [1]

В большинстве случаев многофункциональные приборы обнаружения средств съема информации работают по одним и тем же принципам. Ради эксперимента исследуем и проведем анализ работы поискового устройства ST131.S ПИРАНЬЯ II (Рис. 1).

Рис.1 Многофункциональный поисковый прибор ST131.S ПИРАНЬЯ II

«Пиранья» изготовлена для проведения оперативно-розыскных мероприятий по нахождению и локализации технических средств негласного съема информации и возможных каналов утечки информации.

Это оборудование способно выявить и локализовать:

- радиоизлучающие технические средства, например, радиомикрофон.
- приборы, которые действующие в инфракрасном диапазоне;
- устройства съема сведений, применяющие проводные линии для их передачи. Например, они могут использовать абонентские телефонные линии;
- источники электромагнитных полей;
- уязвимые места, в которых возможно появление акустических КУИ.
- уязвимые места, в которых возможно появление виброакустических КУИ.

Перечислим возможности многофункционального прибора:

- Идентификация цифровых протоколов, которые применяются в найденных устройствах;
- Интерфейс прибора достаточно прост и удобен в эксплуатации;
- в устройстве есть четыре канала обнаружения, производящие поиск в разном диапазоне частот (Рис. 2).

Каналы обнаружения	Диапазон частот	Датчик	Назначение
РАДИО	0.01-30МГц	Телескопическая антенна	Прием и обработка радиосигналов
	30-6000МГц	УВЧ антенна «ST131.S.A».	
	4000-18000МГц	СВЧ детектор «ST131.S.SHF».	
ПРОВОДНОЙ	0.3-15КГц 0.01-30МГц	Адаптер проводных линий «ST131.S.AWL»	Приём и обработка сигналов, передаваемых по проводным линиям различного назначения (силовые, телефонные, коаксиальные, вычислительных сетей, пожарной, охранной сигнализации и т.п.).
	30-3870МГц	Радиочастотный адаптер «ST131.S.RAWL»	
ОПТИЧЕСКИЙ	770-1650нМ (полоса 0.001-5МГц)	Датчик инфракрасного излучения «ST131.S.IF»	Приём и анализ излучений в инфракрасном диапазоне частот.
АКУСТОЭЛЕКТРИЧЕСКИЙ	0.01-125кГц	Датчик магнитного поля «ST131.S.MF» Микрофон	Прием и анализ сигналов - низкочастотного магнитного поля - акустического и ультразвукового диапазона

Рис. 2 Каналы обнаружения ST131.S ПИРАНЬЯ II

Для обнаружения и локализации радиоизлучающих технических средств, создающих опасные радиосигналы, применяется метод акустической завязки. Появляется положительная акустическая связь между динамиком прибора и микрофоном закладки. При обнаружении средства съема информации прибор начинает «пищать». Этот метод применим только к амплитудной и частотной модуляции. [2]

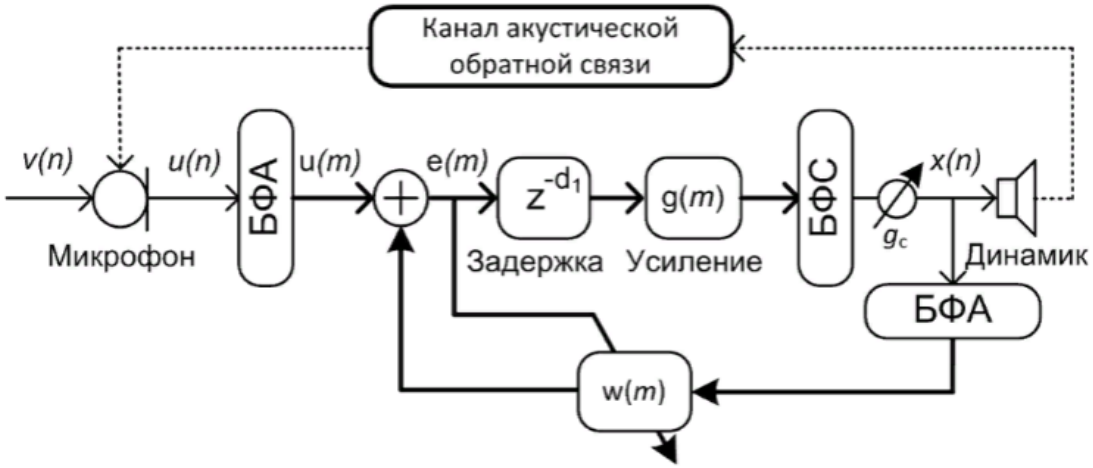


Рис. 3 Сема принципа работы метода акустической завязки

В устройстве есть блок управления, набор преобразователей, благодаря которым можно работать в разных режимах.

В приборе имеется режим высокочастотного детектора, весь принимаемый сигнал колеблется в пределах от 30 до 2500 МГц.

Во время своей работы радиозакладка излучает радиоволны, которые фиксирует антенна детектора и они попадают на транзистор, проходя через высокочастотный фильтр. Усиленный биполярным транзистором, сигнал идет на высокочастотный диод. Как только появляется излучение, усиленный сигнал с этого выхода идет на генератор звуковой частоты, который регулируется напряжением, а дальше сигнал поступает на динамик прибора.

«Пиранья» способна работать как детектор низкочастотных магнитных полей. Сигнал, наводимый в магнитной антенне, идет на широкополосный усилитель, проходя сквозь фильтр высокой частоты, а дальше поступает на диодный детектор. Выходя их усилителя, сигнал идет на устройство, которое показывает уровень сигнала и на генератор звука.

Прибор по принципу работы опирается на широкополосное детектирование электромагнитного поля. Это способствует определению радиоизлучающих средств при всех видах модуляции, будь то частотная, амплитудная или фазовая модуляция. От излучаемой радиозакладкой мощности учитывается радиус ее обнаружения, обычно это один метр.

Для уязвимы мест, в которых могут возникнуть акустические и виброакустические каналы утечки информации применяется режим приемника. Во время действия получает выносным микрофоном акустических и виброакустических сигналов в пределах 300-6000 Гц. Применяют данный режим для того, чтобы определить состояние звукоизоляции помещений, а также для создания маскирующих шумовых помех в пространстве, элементах ограждающих конструкций.

Необходимо выделить, что новая версия прибора «Пиранья» обладает режимом нелинейного локатора в проводных линиях. Особенность этого режима в том, что абсолютно все закладки строятся на основе полупроводниковых материалов, это могут быть микросхемы, диоды, транзисторы. А они в свою очередь являются «отражателями» для прибора.

В процессе работы, прибор облучает закладное устройство зондирующим сигналом, дальше в устройстве наводится переменная электродвижущая сила. Полупроводниковые материалы превращают появившуюся ЭДС в высокочастотные сигналы кратных частот, которые переизлучаются в пространство. По наличию в спектре принимаемого прибором сигнала высших гармоник частоты собственного передатчика делается вывод о наличии закладного устройства. Схематично показан принцип работы «Пираньи» в этом режиме на рис. 3.

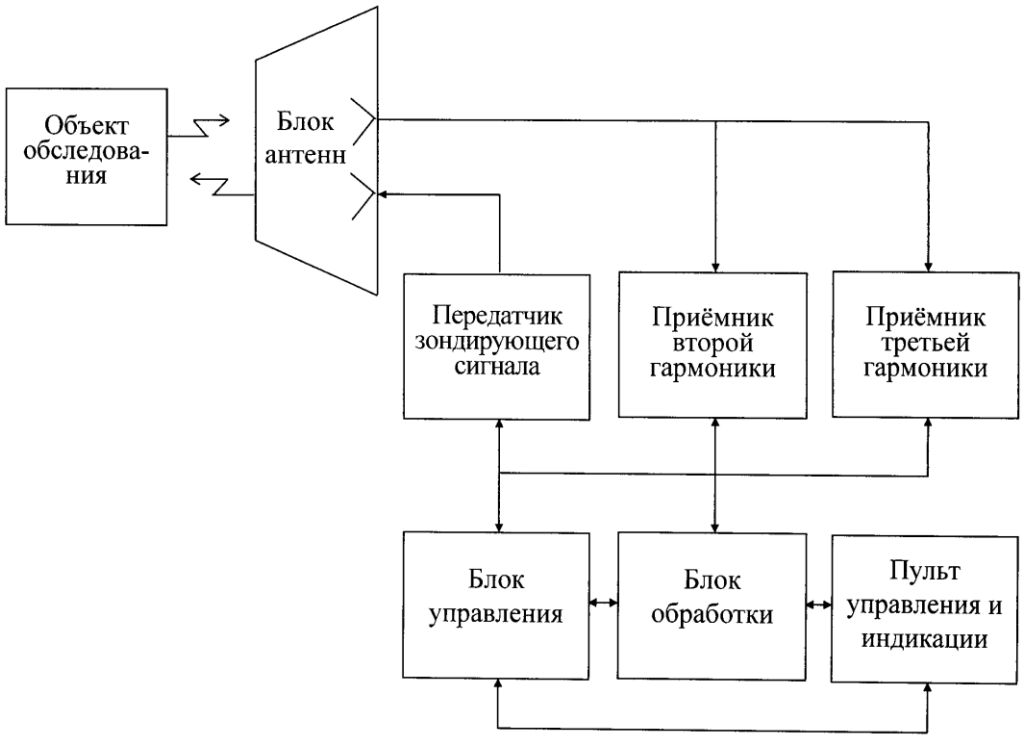


Рис. 4 Схема работы прибора в режиме нелинейного локатора.

Метод нелинейного локатора в отличие от остальных режимов способен обнаружить:

- закладки, у которых отсутствует подключение к электропитанию;
- устройство съема информации, управление которым происходит дистанционно и в данный момент оно находится в режиме ожидания.
- закладки, применяющие технологии передачи сведений с повышенной скрытностью их деятельности, например разные виды модуляции, несколько несущих частот, передача данных частями после их накопления.

Смена одного режима на другой происходит автоматически при подключении соответствующего преобразователя.

Злоумышленники привыкли использовать различные виды закладных устройств, отличающихся по их построению, наполнению и принципу работы. Поиск этих передатчиков с применением только одного метода или оборудования на сегодняшний день не актуален. Эффективнее использовать многофункциональные приборы поиска, которые включают в себя методы работы нескольких устройств и используют комплексный подход к решению этой проблемы.

СПИСОК ЛИТЕРАТУРЫ

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Техническая защита информации: Лабораторный практикум / Под редакцией Ю.Ф. Каторина - СПб: НИУ ИТМО, 2013 – 112 с.

2. Ананский Е.В. Служба безопасности: научный журнал / Е.В. Ананский – М: 2005 – 20 с.

3. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации / А.А. Хорев - М.: МО РФ, 1998. - 224 с.

4. Скрипник, Д. А. Общие вопросы технической защиты информации / Д. А. Скрипник - Москва: Национальный Открытый Университет "ИНТУИТ", 2016 – 293 с.

5. Кудряшова, Н.Ю. Системный анализ в науке и образовании / Н.Ю. Кудряшова, А.С. Минзов – М: 2016. № 3. С. 11-23

6. Даньшин, И.В. Методика измерений и оценка погрешностей при исследовании многофункционального поискового прибора ST 031 «Пиранья»: научная статья / - СПб: 2020 – 320 с.

7. Приданцева, Д.И. Применение многофункционального поискового прибора «ST033 ПИРАНЬЯ» для проведения оперативных мероприятий по обнаружению и локализации радиоизлучающих средств негласного получения информации: научная статья / - М: 2015 – 311с.

8. Нам, Г.Е. Технические средства поиска каналов утечки информации: научная статья / 2017 – 169 с.

9. http://www.confident.org.ua/index.php/stati-po-teme/85-statya-po-teme-1.html

10. http://samzan.ru/211598

Мирзагитов Ильшат Радикович
БашГУ, студент
nf.mir01@gmail.com
Шагапов Илдар Ахняфович
БашГУ, доцент, к.ф.-м.н.
shagapovia@mail.ru

МОБИЛЬНЫЙ ПОДХОД В ЗАЩИТЕ ИНФОРМАЦИИ

В данной работе анализируются и приводятся предложения по повышению эффективности (надежности) систем защиты информации за счет смены месторасположения, отказа от стационарности, предлагается использование мобильных передвижных пунктов системы защиты информации.

Найден не исследованный в защите информации путь использования внутренних скрытых возможностей множества компонентов известных недорогих подсистем защиты информации, каждая из которых в свою очередь построена и функционирует на разных принципах, типах, платформах и т.д. Данный подход позволит существенно повысить эффективность и надежность системы защиты информации [3].

На текущий момент времени, существует много разных систем ЗИ, но все же часть из них, малоэффективна и довольно дорого обходится каждой компании. Учитывая такие недостатки систем защиты информации, предлагается создание мобильных систем защиты информации, для повышения надежности существующих систем.

Понятие "мобильность", как правило, ассоциируется с динамикой и изменениями, свободой действий. Говоря о мобильности в применении к защите информации как правило, под этим словом понимают возможности работы специалистов с информационными ресурсами без привязки к конкретной точке пространства.

С точки зрения применения такой СЗИ, значительно повысить надежность системы можно и с применением отказоустойчивых подходов.

Под отказоустойчивостью технических систем будем понимать их способность выполнять предусмотренные функции в реальных условиях эксплуатации при наличии внутренних возмущающих воздействий – отказов, сбоев составных технических средств, программных ошибок. По нашему мнению, требуется изменить подход к построению и функционированию систем защиты информации [11].

Такая система предполагает проведение конфиденциальных переговоров, обработку персональных данных и засекреченной информации в разных местах страны, где это все можно будет защитить. То есть, если на текущий момент времени вся эта процедура проходит только в одном закрепленном месте, то мобильность систем защиты предполагает сделать (провести) это на разных помещениях, к примеру, арендуемом. Все это будет осуществлено и выглядеть точно также, как и в выделенных и защищаемых помещениях [5]. Лицо, которому необходимо обезопасить важную информацию от утечек, может снять помещение, провести комплекс организационных и технических работ, направленных на обнаружение, отражение и ликвидацию различных видов угроз арендуемому помещению, помимо всего этого свою безопасность может закрепить аттестацией [2]. К тому же мобильность систем может реализовать IT компаниям, которые будут арендовать помещения на определенный срок по обращению клиентов, провести

организационные мероприятия по защите информации помещения, то есть развернуть систему защиты, провести обработку конфиденциальных сведений и завершить. Помимо всего этого мобильные СЗИ можно сделать так, чтобы она могла перемещаться в любой точке на Земле. Отличие мобильности от других систем ЗИ в том, что она не находится постоянно в определенном месте, а при необходимости может поменять траекторию своего местоположения.

Любой злоумышленник, прежде чем получить доступ к той или иной информации, в первую очередь добывает всевозможные сведения о ее местонахождение. В мобильных системах этого сделать не получится, потому что как только он сможет узнать, что, та или иная система находится там, в определенном месте, то в последующих попытках добыть информацию поподробнее, у него этого не получится, ибо ее свернут и уйдут в неизвестное злоумышленнику место. Следует понимать, что злоумышленник тоже подвергается к затратам для того, чтобы найти информацию, и учитывая то, что при каждых таких попытках его труд сведется безуспешностью, то «копать» информацию на такие системы ЗИ у него нет смысла. Неизвестность месторасположения помешает ему [6].

Для большей эффективности предложено ввести отдельную подсистему управления. Большое количество вариантов вместе с соответствующим механизмом переключения создает «непредсказуемое» для нарушителя функционирование системы. Подход позволяет без особых усилий модернизировать систему, например, внедрить в работу новую подсистему или вывести из эксплуатации подсистему, не удовлетворяющую тем или иным требованиям [10].

Следовательно, к данным новшествам нужно приручить и самих специалистов, проведение регулярных ИБ тренинги для повышения осведомленности персонала в вопросах защиты информации. Учитывая эти факты, необходимо помнить, что такая система должна быть сама защищена от различных видов уязвимостей. Её уязвимость может заключаться демаскирующих признаках, то есть она должна иметь ряд признаков, не отличающихся от повседневного вида.

В качестве аналогии мобильных систем защиты информации, можно учесть IT аутсорсинг, то есть данную систему могут использовать любые IT компании [4]. Все те, кому необходимо обезопасить обработку, получение, передачу конфиденциальной информации, смогут обратиться в такие компании. Всю работу по защите выполнят специалисты IT компаний. Также они смогут проводить мероприятия по защите информации в состоянии движения. То есть, оснастить всеми необходимыми устройствами передвижной транспорт, провести работы по защите.

Мобильность систем ЗИ представляет собой комплекс тех же мероприятий, что и стационарные защищаемые помещения, но она отличается тем, что она защищает информацию в разных помещениях. Смысл же в том, чтобы защитить информацию нужно ее обезопасить, чтобы ее обезопасить нужны средства, если помещение будет одним и тем же, то вся конфиденциальная информация, будет проводиться только в одной точке, то данное место рано или поздно смогут узнать злоумышленники. А в мобильных системах ЗИ необходимы начальные средства для обеспечения безопасности, систему ЗИ развернут и смогут приступить к конфиденциальным сведениям, если же им дальше нет необходимости больше защищать информацию от утечки, то в таком случае могут свернуть систему и покинуть это помещение.

Преимущества такой мобильной системы защиты информации именно в этом, она не имеет стационарности. Такая система в отличие от существующих не требует дополнительных затрат на предотвращение уязвимости, потому что при обнаружении ее нарушителем, она меняет свое место. Возможности пути использования внутренних скрытых возможностей множества компонентов известных недорогих(классических) подсистем защиты информации, каждая из которых в свою очередь построена и функционирует на разных принципах, типах, платформах и т.д. [1]. Мобильность системы ЗИ можно развернуть (оборудовать) на транспортном средстве, в ней также будет проведены комплекс организационных мероприятий от утечек и уязвимостей. За счет передвижения, в частности при работе с секретной информацией позволяет сократить время на выполнение необходимых процедур обработки секретной информации, находясь непосредственно на объекте и работая в автономном режиме, что является выгодным вариантом [9]. Помимо этого, природные условия играют роль преимущества. Так, например, если развернуть такую систему защиты где-то в лесной глуши, где нет мобильной сети, ей не будет грозить утечка информации исходя из мобильной сети.

Данное свойство предложенной системы защиты обеспечивает и экономическую привлекательность: имея небольшое количество недорогих подсистем, можно построить существенно большее количество функционирующих различных систем защиты информации, причем приобретать и внедрять новые подсистемы можно по необходимости и финансовой возможности [8].

Не смотря на эти плюсы, она имеет недостатки, что в первую очередь является постоянное перемещения из-за обнаружения злоумышленником, лицу, которому необходимо будет обезопасить важную для него информацию, обойдется дороже, чем обезопасить ее в стационарном помещении. Но все же учитывая современные методы ЗИ, такой вариант развитий событий может быть в редких случаях. Мобильную систему ЗИ нельзя использовать для всех СЗИ, в частности в правовой защите. Учитывая если такая система будет реализована (развернута) на транспортном средстве, за счет передвижения, могут возникнуть угрозы от неизвестности.

Сравнивая преимущества и недостатки, можно определенно утвердить, что данная разработка будет эффективной системам ЗИ. Поэтому мобильность СЗИ предполагает метод, который будет являться уникальном на текущий и будущий момент времени, перемещение из одной точки в другую, где развернув и свернув можно будет защититься от угроз злоумышленника.

Говоря о применимости, следует подчеркнуть, что такой способ ЗИ от угрозы ее утечек отлично подойдет коммерческим предприятиям [7], которые обрабатывают коммерческую тайну, предприятиям, которые взаимодействуют с персональными данными (например, частные клиники).

Стоит отметить, что мобильную систему защиты информации, без ее тестирования на практике нет смысла применять в государственных органах и целях. Применить в организациях, созданные в организационно-правовой форме государственного или муниципального учреждения не получится без разрешения, к ним относится многофункциональный центр. В таком случае невозможно будет избавиться от демаскирующих признаков. Мобильные системы ЗИ, не предназначены для больших количеств лиц.

СПИСОК ЛИТЕРАТУРЫ

1. SERCHINFORM. Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 год. – URL: https://searchinform.ru/survey/global-2020/ (дата обращения: 18.11.2021). – Текст: электронный.
2. Гафнер, В.В. Информационная безопасность: учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.
3. Исмагилова А.С. Информационная безопасность в цифровом обществе / А.С. Исмагилова, И.А. Шагапов, А.А. Султанова (Корнилова), И.В. Салов // – Уфа: РИЦ БашГУ, 2019. - 128 с.
4. Карганов, В. В. Методология безопасности информации в текущих информационных системах / В. В. Карганов // Национальная безопасность России : актуальные аспекты : Сборник избранных статей Всероссийской научно-практической конференции. – Санкт-Петербург, 2020. – С. 21–27
5. Когутенко, А. А. Исследование организации кроссплатформенной рабочей среды с облачным хранилищем данных / А. А. Когутенко, С. В. Плотникова // Информатика и кибернетика. – 2018. – № 2 (12). – С. 20–24.
6. Маляревский, А. Тренды 2021 года : рельеф киберугроз становится сложнее. – URL: https://www.crn.ru/news/detail.php?ID=150817 (дата обращения: 18.11.2021). – Текст: электронный.
7. Москвитин, Г.И. Комплексная защита информации в организации / под ред. Г.И. Москвитин. - М.: Русайнс, 2017. - 400 с.
8. Муромцев, Д. Ю. Усовершенствование подсистемы обеспечения работоспособности средств защиты информации в системе мониторинга инцидентов информационной безопасности банка / Д. Ю. Муромцев, С. В. Попов, В. Н. Шамкин // Вестник Тамбовского государственного технического университета. – 2020. – Том 26. – № 2. – С. 176–187.
9. Шабанов, А. Применение технологий искусственного интеллекта в информационной безопасности / А. Шабанов. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/using-articial-intelligence-technologies-in-information-security (дата обращения: 18.11.2021). – Текст: электронный.
10. Шагапов, И.А. Рекомпозиционный подход в защите информации / И.А. Шагапов, А.С. Исмагилова, И.В. Салов. // Международный форум KAZAN DIGITAL WEEK – 2021: сборник материалов / Сост.: Р.Ш. Ахмадиева, Р.Н. Минниханов; Под общей ред. член-корр. Академии наук Республики Татарстан, д-ра техн. наук, проф. Р.Н. Минниханова. – Казань: ГБУ «НЦБЖД», 2021. – Ч. 1. – С. 275 – 282.
11. Шубинский, И. Б. Функциональная надежность информационных систем: методы анализа. Монография / И. Б. Шубинский. – Ульяновск: Печатный двор, 2012. – 296 с.

Гришина Н.В.
РГГУ, доцент, к.т.н, доцент,
grnat@rambler.ru

ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Информационно-телекоммуникационные системы относятся к одному из восьми приоритетных направлений развития науки, технологий и техники в Российской Федерации в соответствии с Указом Президента Российской Федерации от 7 июля 2011 г. № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня технологий Российской Федерации» [1].

Любое современное предприятие представляет собой объект информатизации, включающий в себя целый ряд компонентов: совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Одним из неотъемлемых элементов объекта информатизации являются телекоммуникационные системы.

Данная работа направлена на раскрытие сущности управления информационной безопасностью объекта информатизации и информационно-телекоммуникационных систем как элемента объекта информатизации.

С момента начала пандемии в мире особенно актуальной стала удаленная работа, поэтому именно аспекту надежного взаимодействия при передаче информации сегодня уделяется наиболее пристальное внимание.

К сожалению, традиционно при решении вопросов обеспечения информационной безопасности основное внимание уделяется главным образом технической стороне вопроса. Однако научными исследованиями и практическим опытом доказано, что только системный подход позволяет обеспечить максимальную эффективность работы любого организованного механизма, в том числе системы защиты информации [6,9] .

В то же время для успешной работы такого рода системы необходимо не просто создать целесообразные и надежные механизмы, обеспечивающие требуемый уровень защиты информации, а также обеспечить грамотное управление этими механизмами [7].

Традиционно управление включает в себя ряд функций: планирование, организация, учет и контроль. Схема, представленная на рис. 1 показывает, что в основе управления лежит планирование (как перспективное, так и текущее).

Еще на этапе планирования будущей системы защиты или в процессе ее совершенствования необходимо выработать стратегию и политику защиты информации.

Стратегия защиты информации формируется на основе целого ряда факторов: условия, в которых происходит деятельность, возможности организации, объективные потребности в данном виде деятельности и т.д.

Рис. 1. Схема связи и взаимодействия функций управления

По теории Г. Минцберга стратегическое управление может быть реализовано по принципу 5-Р, который предполагает [10]:

-план;

-прием;

-модель поведения;

-позицию по отношению к другим;

-перспективу.

Для реализации систем защиты информации можно выделить три основных стратегии: оборонительная, наступательная, упреждающая.

Стратегия реализации системы защиты информации должна быть направлена на нейтрализацию дестабилизирующего воздействия на систему окружающей среды (внешних факторов), установление баланса между внешними требованиями и внутренними возможностями, обеспечение непрерывности бизнес-процессов, а также на создание преимущества по отношению с другими системами защиты информации.

Какой бы не была выбранная стратегия защиты информации, она может быть реализована в соответствии с обозначенными принципами.

Следующий шаг - разработка политики информационной безопасности.

Политика информационной безопасности определяется мероприятиями по обеспечению защиты информации и особенности процессов ее обработки, которыми обязаны руководствоваться в своей деятельности предприятия и организации. Она должна применяться к системе на всех этапах ее жизненного цикла.

Реализация политики информационной безопасности базируется на организационных мерах и программно-технические средствах, которые определяют структуру системы.

Политика безопасности должна иметь индивидуальные признаки, которые зависят от особенностей работы конкретной организации: используемых программно-технических средств и их расположения, технологии обработки информации, руководящих документов, процедур и практических механизмов защиты информации, а также средств управления этими механизмами и т. д.

Из числа процессов, связанных с проектированием и реализацией политики безопасности, можно выделить перечисленные ниже действия и мероприятия.

1. Комплекс мероприятий по анализу рисков информационной безопасности, к которому можно отнести:
   - проведение инвентаризации информационных активов;
   - моделирование угроз системы защиты информации;
   - анализ рисков с использованием различных вариантов методики их исследования, например, анализ рисков на основании стоимостных характеристик.
2. Оценка соответствия обеспечиваемых системой мер по защите информации определенному эталону, в качестве которого может использоваться стандарт, профиль защиты и т. п.
3. Действия по разработке различных документов, предусматриваемых политикой безопасности: профилей защиты, отчетов, диаграмм.
4. Действия по сбору, обработке и хранению статистических данных, относящихся к событиям информационной безопасности для организации.

С целью обеспечения единого подхода к организации управления информационной безопасностью в нашей стране продолжаются работы по разработке новых стандартов.

30 ноября 2021 приказом Росстандарта вводятся в действие новые национальные стандарты: ГОСТ Р ИСО/МЭК 27002-2012 отменяется с 30.11.2021. Заменен ГОСТ Р ИСО/МЭК 27002-2021; ГОСТ Р ИСО/МЭК 27003-2012 отменяется с 30.11.2021. Заменен ГОСТ Р ИСО/МЭК 27003-2021; ГОСТ Р ИСО/МЭК 27004-2011 отменяется с 30.11.2021. Заменен ГОСТ Р ИСО/МЭК 27004-2021.

Указанные стандарты содержат руководство по реализации требований к системе менеджмента информационной безопасности и описывают рекомендации, возможности и допустимые действия по реализации этих требований. Важно, что представленные стандарты идентичны международным.

Действующие нормативные документы раскрывают основные виды угроз информационной безопасности, которые можно разделить на преднамеренные и случайные. При этом в случае реализации угрозы может произойти незаконный доступ к информационным ресурсам, утечка информации, несанкционированный доступ, нарушение целостности данных, непризнание авторства, подлог информации или отказ в обслуживании.

В результате проведенного исследования показано, что для эффективной работы системы защиты информации необходимо уделять самое пристальное внимание вопросам управления этой системой, то есть планированию, организации и контролю.

С целью обеспечения информационной безопасности объекта информатизации необходимо: понимать необходимость широкого понимания проблемы - внедрения политики информационной безопасности как комплекса мер по обеспечению защиты

информации; реализовать непрерывность управления системой защиты информации; система управления должна включать правовые, инженерно-технические, административные, социально-психологические, экономические методы.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 07.07.2011 N 899 (ред. от 16.12.2015) "Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации".
2. ГОСТ Р ИСО/МЭК 27002-2021//НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Информационные технологии МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Свод норм и правил применения мер обеспечения информационной безопасности.
3. ГОСТ Р ИСО/МЭК 27003-2021//НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Информационные технологии. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Системы менеджмента информационной безопасности. Руководство по реализации.
4. ГОСТ Р ИСО/МЭК 27004-2021 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Информационные технологии МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание.
5. ГОСТ Р ИСО/МЭК 27005-2010//НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Менеджмент риска информационной безопасности.
6. Гришина, Н. В. Комплексная защита информации на предприятии: учеб. пособие. - М.: ФОРУМ, 2009.
7. Гришина Н.В., Русецкая И.А. Анализ взаимодействия субъектов информационных отношений // Прикладная информатика. —2012. —№ 3 (39). —С. 95-99.
8. Гришина Н.В. Этические аспекты взаимодействия персонала системы защиты информации // Информационная безопасность: вчера, сегодня, завтра : сборник статей по материалам IV Международной научно-практической конференции, Москва, 22 апреля 2021 г. / М-во науки и высш. образования Рос. Федерации, Гос. образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" ; - Москва : РГГУ, 2021. - С. 27-32.
9. Гришина Н.В. Основы информационной безопасности предприятия. - Москва : ИНФРА-М, 2021. - 216 с.
10. Гришина Н.В. Использование стратегии "5-Р" для повышения эффективности управления персоналом системы защиты информации // Информационная безопасность: вчера, сегодня, завтра. - Москва : РГГУ, 2018. - С. 163-167.

Чернов Д.В.
АО «Центральное конструкторское бюро аппаратостроения», начальник сектора,
ТулГУ, старший преподаватель,
cherncib@gmail.com

НАУЧНЫЕ РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ ПРОЕКТА «РАЗРАБОТКА МЕТОДОВ И АЛГОРИТМОВ МОДЕЛИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ»

В соответствии с положениями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» АСУ ТП относятся к объектам критической информационной инфраструктуры Российской Федерации, в отношении которых владелец АСУ ТП обязан выполнить комплекс организационных и технических мер, направленных на обеспечение ИБ. В целях эффективной защиты АСУ ТП необходимо создание комплексной системы обеспечения ИБ, которая должна отвечать следующим принципам: законность, непрерывность и комплексность обеспечения безопасности, а также приоритет предотвращения компьютерных атак [1].

Важное значение при разработке, построении и поддержании работоспособности промышленных систем имеет моделирование угроз ИБ АСУ ТП. Под моделированием угроз ИБ понимается физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [2]. Техническая и методическая база построения актуальных моделей угроз промышленных систем имеет в своем составе большое количество программных средств автоматизации процессов моделирования угроз безопасности информации [3,4]. Вместе с тем, основным драйвером повышения качества моделей угроз информационной безопасности АСУ ТП выступают научные разработки новых методик, алгоритмов и программных продуктов моделирования угроз информационной безопасности.

Выполнение вышеуказанных научных разработок проводилось автором в рамках проекта, поддержанного грантом ИБ РТУ МИРЭА № 15/2020.

Выполнение проекта преследовало своей целью повышение уровня ИБ АСУ ТП за счет разработки автоматизированной системы определения актуальных угроз информационной безопасности, реализация которых может привести к нарушению штатного режима функционирования АСУ ТП, а также набора мер защиты, необходимых и достаточных для минимизации рисков реализации актуальных угроз. Для достижения поставленной цели были сформулированы основные и вспомогательные задачи, представленные в графической форме на рисунке 1.

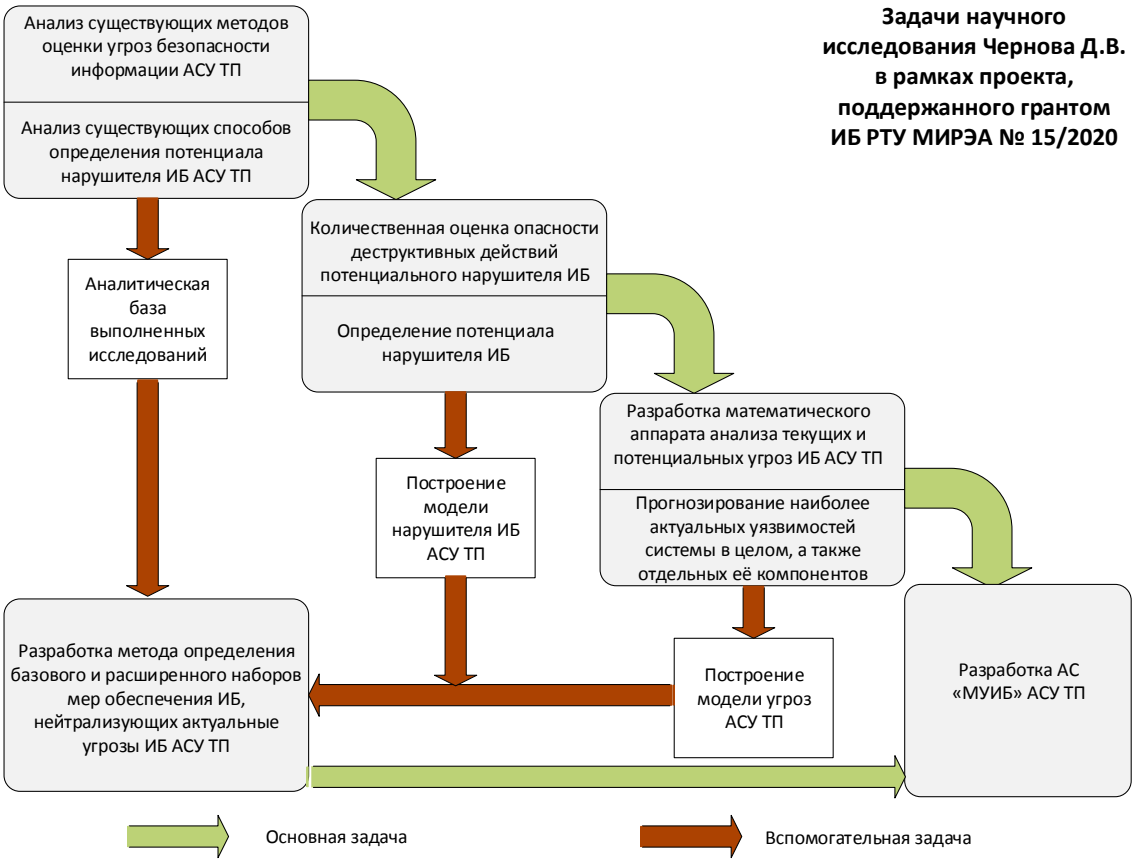


Рис. 1. Задачи проекта

Реализация поставленных задач выполнена на основе анализа современного состояния проблемы моделирования угроз ИБ АСУ ТП. Рассмотрены задачи построения модели нарушителя и модели угроз информационной безопасности. Выделены основные метрики квалификации и мотивации потенциальных нарушителей ИБ АСУ ТП. Выполнен анализ нормативно-правовой и терминологической базы обеспечения информационной безопасности АСУ ТП. Проведена аналитика наиболее крупных атак на критическую информационную инфраструктуру. Описана многоуровневая структура АСУ ТП [5].

По результатам проведения анализа предметной области формализованы следующие задачи:

- задача построения модели нарушителя ИБ АСУ ТП;
- задача оценки нарушителей информационной безопасности АСУ ТП, учитывающей возможные негативные последствия от атак на различные уровни АСУ ТП;
- задача моделирования угроз ИБ АСУ ТП;
- задача выбора защитных мер ИБ АСУ ТП.

В целях решения поставленных и формализованных задач реализации проекта разработан алгоритм формирования модели нарушителя АСУ ТП с использованием предположений о его потенциале и возможных последствиях реализации угроз ИБ. Также был предложен алгоритм решения задачи определения потенциала нарушителя информационной безопасности АСУ ТП на основе наборов оцениваемых характеристик, которые могут динамически изменяться в зависимости от условий функционирования,

исполняемых технологических процессов, а также технологического процесса обработки информации в АСУ ТП [6].

В процессе выполнения проекта дополнительно разработан алгоритм работы сканера безопасности, предназначенного для определения фактических уязвимых звеньев в общей структуре определения и оценки защищенности уязвимых звеньев АСУ ТП.

В ходе решения задачи построения модели нарушителя ИБ АСУ ТП предложен метод количественной оценки потенциалов нарушителей ИБ многоуровневых АСУ ТП, имеющий в своей основе сформированные в виде матриц идентификаторов угроз предположения о нарушителях ИБ (1) в соотношении со сложностью реализации угрозы и возможностью получения нарушителем доступа к системе. Сформулирована и решена задача субъективности индивидуальной оценки потенциалов нарушителей ИБ.

$$C_i = \begin{pmatrix} c_{11} & \Lambda & c_{1j} \\ \text{M} & \text{O} & \text{M} \\ c_{m1} & \Lambda & c_{mj} \end{pmatrix}. \qquad (1)$$

Каждый технологический процесс в АСУ ТП содержит в себе конечное количество подпроцессов, характеризуемых набором оценок вероятностей наступления тех или иных событий в системе. Для оценки защищенности технологических процессов разработан и формализован метод оценки опасности деструктивных действий нарушителя ИБ на каждом уровне АСУ ТП на основании критичности и защищенности технологических процессов и их подпроцессов. В данных целях была использована методика анализа видов и последствий потенциальных дефектов Potential Failure Mode and Effects Analysis, FMEA, представленная выражением 2. Методика FMEA позволила минимизировать экспертное участие в оценке возможностей нарушителя при реализации угрозы ИБ в разработанном методе [7].

$$C_j(t) = \prod_{n=1}^{3} B_{nj}(t), \qquad (2)$$

где $C_j(t)$ — критичность нарушения j-го подпроцесса; $B_{1j}(t)$ — оценка частоты (вероятности) нарушения j-го подпроцесса; $B_{2j}(t)$ — оценка вероятности выявления нарушения j-го подпроцесса до его появления; $B_{3j}(t)$ — оценка тяжести последствий нарушения j-го подпроцесса.

По результатам решения задачи прогнозирования актуальных уязвимостей АСУ ТП предложен метод определения и оценки защищенности уязвимых звеньев АСУ ТП. Метод ориентирован на многоуровневую архитектуру АСУ ТП и отличается тем, что основан на вычислении показателей актуальности и вероятностей использования уязвимых звеньев системы. К преимуществам предложенного метода определения и оценки уязвимых звеньев относится возможность уменьшения общего количества субъективных оценок экспертных групп за счет определения вероятности использования уязвимого звена на основе Марковских моделей, а также возможности использования

результатов работы сканеров безопасности и открытых банков данных уязвимостей АСУ ТП.

В целях разработки математического аппарата анализа текущих и потенциальных угроз ИБ АСУ ТП рассмотрен вариант применения теории игр с неполной информацией. Для решения поставленной задачи был предложен метод оценки актуальности угроз ИБ АСУ ТП, основанный на применении результатов моделирования игры Штакельберга с различными коэффициентами выигрышей. Метод позволяет выделить наиболее подверженные угрозам ИБ уровни АСУ ТП, а также наборы актуальных угроз ИБ АСУ ТП, в том числе группировать угрозы по уровням и типам нарушителей ИБ [8].

В рамках решения задачи выбора защитных мер ИБ АСУ ТП определены [9,10]:

- минимальный набор мер защиты;
- базовый набор мер защиты;
- адаптированный базовый набор мер защиты;
- уточненный адаптированный базовый набор мер защиты.

Дополнительно в работе [11] выведена дефиниция «адаптация базового набора мер защиты АСУ ТП». Описан переход к адаптированному базовому набору мер защиты и его уточнению, а также наглядно продемонстрирована взаимосвязь потенциалов нарушителей и базового набора мер защиты АСУ ТП.

В рамках разработки структуры и интерфейсов компонент, согласования функций и технических требований к компонентам АС «МУИБ» АСУ ТП, а также в целях определения информационных потоков между основными компонентами моделирования, связей между ними и внешними объектами проведено функциональное моделирование системы оценки актуальных угроз безопасности информации с декомпозицией отдельных функциональных блоков на основе методологии функционального моделирования IDEF0 [12].

Полученные результаты

Разработанная на базе описанных в проекте методов, моделей и алгоритмов АС «МУИБ» АСУ ТП позволяет автоматизировать этапы построения моделей угроз АСУ ТП с учетом специфики исполняемых технологических процессов и нормативных документов в области защиты АСУ ТП. Автоматизированная система объединяет подсистемы «Формирования предположений о квалификации и мотивации нарушителей информационной безопасности АСУ ТП», «Оценки потенциала нарушителя», «Построения модели нарушителя», «Определения и оценки защищенности уязвимых звеньев», «Оценки актуальности угроз ИБ АСУ ТП», «Выбора мер защиты на всех уровнях АСУ ТП». Графическое отображение пользовательского интерфейса АС «МУИБ» АСУ ТП приведено на рисунке 2.

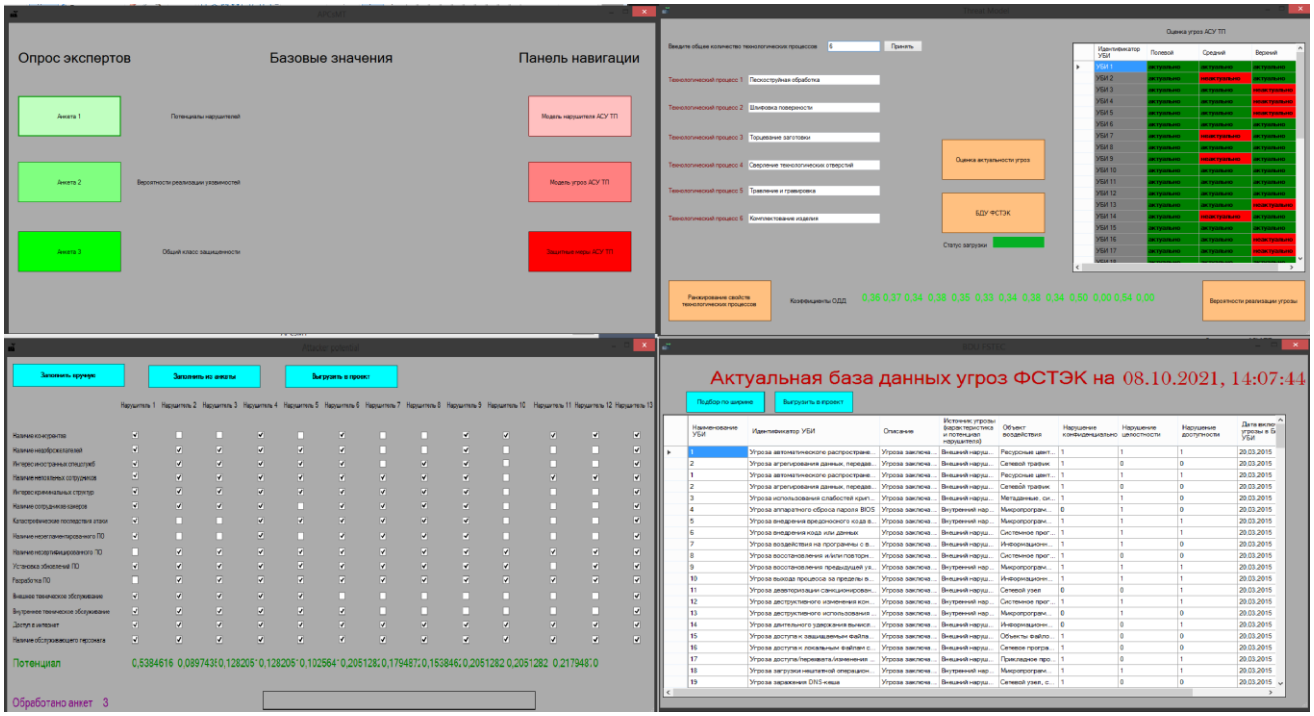


Рис. 2. Пользовательский интерфейс АС «МУИБ» АСУ ТП

В целях апробации АС «МУИБ» был проведен ряд вычислительных экспериментов с применением разработанной автоматизированной системы в АСУ ТП субъектов критической информационной инфраструктуры, относящихся к различным сферам деятельности. По результатам экспериментов получены данные о повышении эффективности моделирования угроз информационной безопасности АСУ ТП с применением разработанной АС «МУИБ» на 14 % по сравнению с применяемыми методиками моделирования угроз. В качестве оценки эффективности моделирования угроз ИБ использован метод интегральной оценки эффективности на основании качественных и количественных критериев.

Заключение

В рамках выполнения проекта, поддержанного грантом ИБ РТУ МИРЭА № 15/2020, автором поставлена и решена задача разработки методического, алгоритмического и программного обеспечения процесса моделирования угроз информационной безопасности многоуровневых АСУ ТП. Полученные результаты научных исследований внедрены на различных производствах Тулы и Тульской области и продемонстрировали положительные результаты при разработке моделей угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон №187-ФЗ от 26.07. 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ, 31.07.2017, № 31 (часть I), ст. 4736.

2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 8 с.

3. Чернов Д. В., Методики оценки угроз безопасности информации автоматизированных систем управления технологическими процессами // Современная

наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. Научный журнал. —2021, —№ 9. —81-88.

4. Чернов Д.В. Анализ современных требований и проблем обеспечения информационной безопасности автоматизированных систем управления технологическими процессами / Чернов Д.В., Сычугов А.А. // Нейрокомпьютеры. Разработка, применение. М.: Радиотехника, —2018, —№8, —38-46.

5. Чернов Д.В. О комплексном подходе к построению системы информационной безопасности АСУ ТП / Чернов Д.В., Сычугов А.А. // Технологические инновации и научные открытия. Сборник научных статей по материалам IV Международной научно-практической конференции. Уфа: Изд. НИЦ Вестник науки, —2020, —53-57.

6. Chernov D. Method of determining the danger coefficient of actions of the information security offender of APCS / Chernov D., Sychugov A. // International scientific conference CAMSTECH-2020: Advances in material science and technology, Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. Krasnoyarsk, Russia, —2020.

7. Чернов Д.В. Определение коэффициента опасности деструктивных действий нарушителя информационной безопасности АСУ ТП / Чернов Д.В., Сычугов А.А. // Информационно-измерительные и управляющие системы. М.: Радиотехника, —2020, —№4. —49-57.

8. Chernov D. Application of the method of determining the degree of danger of destructive actions to solve the problem of information security of APCs / Chernov D., Sychugov A. // 2020 International Conference on Electrotechnical Complexes and Systems (ICOECS), Ufa, —2020, —1-4.

9. Chernov D. Definition of Protective Measures of Information Security of Automated Process Control Systems // 2021 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Sochi, Russia, —2021, —1-5.

10. Чернов Д.В. О выборе мер обеспечения информационной безопасности автоматизированных систем управления технологическими процессами / Чернов Д.В., Сычугов А.А. // Моделирование, оптимизация и информационные технологии. Научный журнал. —2021, —№9(2), —1-9.

11. Чернов Д. В., Применение диаграмм Эйлера-Венна при решении задачи выбора мер защиты АСУ ТП // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. Научный журнал. —2021, —№7, —127-131.

12. Chernov D. Application TRIKE methodology when modeling threats to APCs information security // 2021 International Russian Automation Conference (RusAutoCon), Sochi, Russia, —2021, —1-5.

Палютина Г.Н.
РГЭУ (РИНХ), аспирант
hello616@yandex.ru

АНАЛИЗ И ОЦЕНКА УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЛАСТИ ФИНАНСОВОЙ ДЕЯТЕЛЬНОСТИ

Вопрос обеспечения безопасности финансовой деятельности всегда востребован и требует выполнения всех необходимых требований по применению защитных мер. Любая неосторожность со стороны организации системы защиты информации, позднее реагирование на обнаруженные уязвимости могут привести к большому кризису в виде утечек информации, совершению операций без согласия клиентов и другим атакам, приводящим к финансовым убыткам как клиентов банка, так и самого банка.

Обратимся к актуальной статистике, собранной экспертами Финансового центра мониторинга [1] за II квартал 2021 года.

Согласно данной статистики значительно увеличилось количество операций без согласия клиентов (ОБС) по сравнению со II кварталом предыдущего года (Рис. 1).

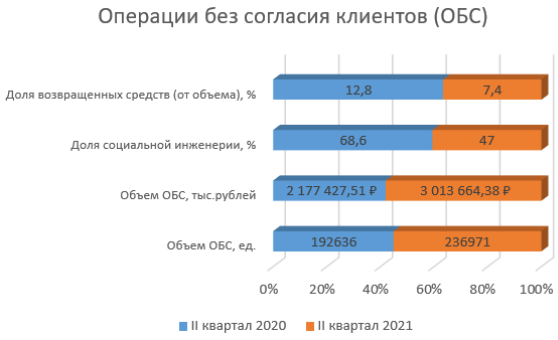


Рис. 1. Операции без согласия клиентов.

Количество ОБС за счет социальной инженерии также возросло (Рис. 2).

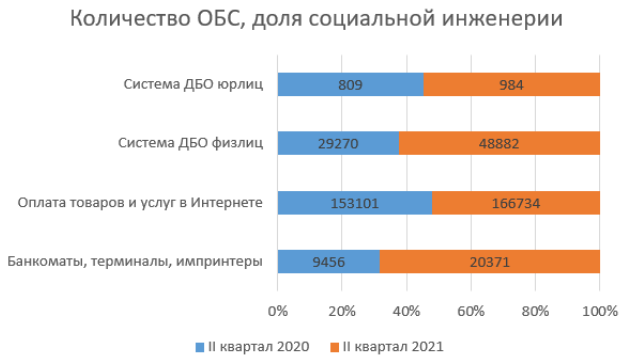


Рис. 2. Количество ОБС, доля социальной инженерии.

Среди инцидентов Финцерт выделяет атаки, направленные непосредственно на клиентов или на саму финансовую организацию, и среди самых распространенных инцидентов выделяет эксплуатацию уязвимостей ПО, атаки с использованием ВПО, с использованием методов социальной инженерии, фишинговые атаки (Рис.3).

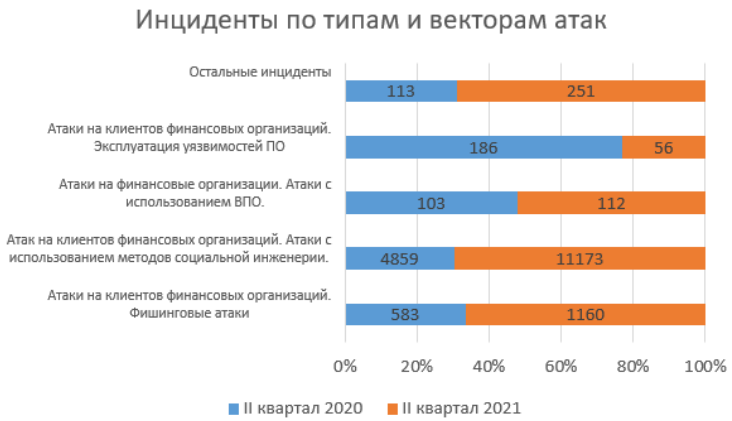


Рис. 3. Инциденты по типам и векторам атак.

Возросло и количество мошеннических телефонных номеров (Рис.4) и мошеннических интернет-ресурсов (Рис.5).

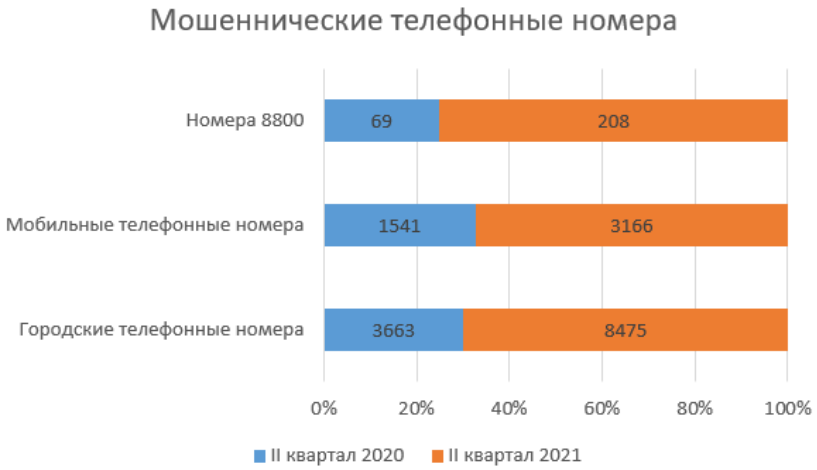


Рис. 4. Мошеннические телефонные номера.

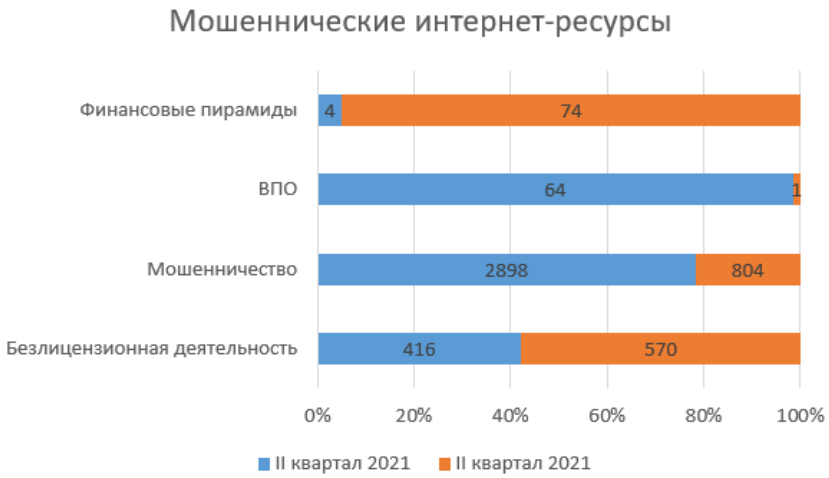


Рис. 5. Мошеннические интернет-ресурсы.

Таким образом, видим, что количество преступлений в области финансовой деятельности возрастает. В связи с этим, становится очевидным совершенствование требований и метод защиты информации в этом секторе.

Среди существующих требований на данный момент основными являются требования Банка России 683-П [2], 382-П [3] (в новой и старой редакции) для кредитных организаций, также требования к организации защиты информации этой сферы прописаны и в ГОСТ Р 57580.1-2017 [4].

Проанализировав эти документы, можно выделить два основных требования:

1. Использование сертифицированного прикладного ПО или ПО, в отношении которого проведен анализ уязвимостей к ОУД4.
2. Проведение ежегодного тестирования на проникновение и анализ уязвимостей ИБ объектов информационной инфраструктуры (проведение пентестов).

Анализ уязвимостей представляет собой оценку с целью сделать заключение, могут ли потенциальные уязвимости позволить нарушителям нарушить функциональные требования безопасности.

Поиск и устранение уязвимостей — это совместная работа разработчиков ПО и экспертов по ИБ.

Выделим объекты, подвергаемые анализу на наличие уязвимостей:

- Прикладное ПО и приложения, распространяемое клиентам для осуществления банковских операций.
- Прикладное ПО и приложения, обрабатывающие защищаемую информацию при приеме электронных сообщений к исполнению с использованием сети Интернет.

Проведение анализа уязвимостей необходимо для каждого обновления ПО (или в отношении всего процесса разработки ПО для релизов, затрагивающих существенные изменения в части функционирования ядра, обеспечения ИБ) не менее 1 раза в год в соответствии с ГОСТ Р 57580.1-2017 (п 9.7 ЖЦ.20).

В (Табл. 1) приведены исходные данные для проведения анализа ИС на наличие уязвимостей.

Табл. 1. Исходные данные для проведения анализа ИС на наличие уязвимостей.

Описание архитектуры безопасности	Обоснование безопасности процесса инициализации и невозможности обхода ФБО, обеспечения собственной защиты объекта оценки от вмешательства.
Функциональная спецификация	Описание назначения и методов использования интерфейсов ФБО, их параметров, связанных с ними действий для выполнения ФТБ и формируемых сообщений об ошибках.
Руководство пользователя по эксплуатации	Описание доступных пользователям функций, интерфейсов прав и обязанностей, описание принципов безопасной работы пользователей с интерфейсами ОО.
Представление реализации ФБО	Процессы внутреннего содержания ФБО в виде исходного текста программ, микропрограмм, схем аппаратных средств и/или программного кода модели интегральных схем или размещения данных.

Проект ОО	Описание структуры ОО на уровне подсистем и модулей, их назначение и взаимодействие
Задание по безопасности / Профиль защиты	Изложение потребности в безопасности

В (Табл.2) представлены этапы проведения анализа уязвимости объектов информационной инфраструктуры.

Табл. 2. Этапы проведения анализа уязвимости отражены в таблице.

1.Подготовительный			
1.1	Сбор исходных данных		
1.2.2	Исследование объекта оценки	Анализ ЗБ: согласуется ли тестируемая конфигурация с оцениваемой (определенной в ЗБ)	
1.2.3		Анализ конфигурации: соответствует ли реальное состояние ОО известному (правильно ли установлен)	
2. Анализ			
2.1.1	Идентификация потенциальных уязвимостей	Исследование общедоступных источников	специальные публикации (журналы, книги), исследовательские статьи, материалы конференций
2.1.2		Фокусированный поиск в документации на ОО. Классификация уязвимостей по:	*по области происхождения:*
			уязвимости кода
			уязвимости конфигурации
			уязвимости архитектуры
			организационные уязвимости
			многофакторные уязвимости
			по типу недостатка ОО:
			неправильная настройка параметров ПО
			неполнота проверки входных данных
			прослеживание пути доступа к каталогам
			внедрение команд ОС
			межсайтовый скриптинг
			внедрение разметки
			внедрение произвольного кода
			неконтролируемая форматная строка
			недостатки в вычислениях
			утечка/раскрытие информации ограниченного доступа
			управление привилегиями и доступом
			недостатки шифрования
			подмена межсайтовых запросов
			недостатки, связанные с управлением ресурсами
			по месту возникновения:
			в общесистемном ПО
			в прикладном ПО

			в специальном ПО
			в технических средствах
			в портативных ТС
			в сетевом оборудовании
2.1.3		Документирование перечня кандидатов на тестирование в Техническом отчете	
2.2.1	Тестирование на проникновение	Разработка тестов проникновения и тестовой документации	*Тестовая документация содержит:*
			идентификацию тестируемой потенциальной уязвимости оцениваемого ОО
			инструкции по подключению и настройке тестового оборудования и установке начальных условий
			инструкции по инициированию и наблюдению режима выполнения ФБО
			описание ожидаемых результатов и дальнейшего анализа
2.2.2		Тестирование на проникновение	*Факторы анализа потенциала нарушителя:*
			Время, затрачиваемое на идентификацию уязвимости и её использование.
			Компетентность специалиста в области общих знаний, основополагающих принципов, типа продукта или методов нападения.
			Знание проекта ОО и его функционирования
			Возможность доступа к ОО: временной интервал или количество образцов ОО, необходимые для использования уязвимостей
			Аппаратные средства/программное обеспечение ИТ или другое оборудование
2.2.3		Фиксация фактических результатов	
3. Формирование результатов			
3.1	Разработка Технического отчета об оценке		

Как видно из вышеприведенной таблицы во время анализа большая часть работ выполняется с помощью ручного труда и на основе компетенций специалистов.

Эту же проблему поднимает руководитель отдела систем мониторинга и реагирования группы компаний Angara А. Носарев [5], отмечая наличие большого количества ручного труда при принятии архитектурных решений, адаптации систем безопасности к новым условиям работы и изменениям IT-инфраструктуры, трендам угроз и усложняющимся техникам злоумышленников. К компетенции специалистов в данной сфере с каждым годом предъявляются все более жесткие требования.

Таким образом, важно понимать, что процессы анализа и оценки уязвимостей объектов информационной инфраструктуры требуют совершенствования и постоянной модернизации, в том числе в виде автоматизации ручных процессов.

Существуют различные направления в данном вопросе, в том числе в виде автоматизации анализа уязвимостей программного обеспечения на основе технологии Text Mining [6]. Исследователи данного метода изучают возможности сопоставления множества выявленных уязвимостей ПО и релевантных угроз безопасности информации путем оценки метрик семантической близости их текстовых описаний.

Дальнейшее изучение методов автоматизации процессов анализа уязвимостей может способствовать повышению достоверности оценки степени критичности уязвимостей ПО, значительно сокращая затраты времени на поиск и сопоставление уязвимостей и угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. II квартал 2021 года – URL: https://www.cbr.ru/analytics/ib/review_2q_2021/
2. Положение Банка России от 17 апреля 2019 г. N 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» – URL: https://base.garant.ru/72246408/
3. Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» – URL: https://cbr.ru/psystem/acts/382-p/
4. ГОСТ Р 57580.1-2017. Национальный стандарт российской федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер – URL: https://files.stroyinf.ru/Data2/1/4293744/4293744380.pdf
5. Александра Крылова. SOC и SIEM уперлись в облака // Финансовая сфера, Банковское обозрение – 2021 – URL: https://bosfera.ru/bo/soc-i-siem-uperlis-v-oblaka
6. Васильев В.И. Автоматизация анализа уязвимостей программного обеспечения на основе технологии Text Mining / Вульфин А.М., Кучкарова Н.В. // Вопросы кибербезопасности. – 2020 г. – №4 (38) – 22-29 стр. URL: https://cyberleninka.ru/article/n/avtomatizatsiya-analiza-uyazvimostey-programmnogo-obespecheniya-na-osnove-tehnologii-text-mining

Корх И.А.
КубГТУ, младший научный сотрудник,
Aia2004@inbox.ru

ИНСТРУКТАЖ, КАК МЕТОД ПОВЫШЕНИЯ ДОВЕРИЯ К ПЕРСОНАЛУ

Аннотация:
Исследование посвящено методу повышению уровня осведомленности сотрудников в вопросах информационной безопасности (ИБ) с учетом возможных атак социальной инженерии. Осведомленность и сознательность сотрудников представляется методом повышения доверия к персоналу организации. Цель достигается за счет индивидуального подхода к проведению инструктажа и автоматизации процесса обучения. Результатом работы является программный комплекс, позволяющий генерировать рекомендации сотруднику службы защиты информации об особенностях личности инструктируемого лица, проводить персонифицированный инструктаж на рабочем месте, формировать отчет о прохождении инструктажа по утвержденной в организации форме.
Ключевые слова: доверие к персоналу, информационной безопасности, инструктаж, акцентуация характера

В соответствии со Стратегией научно-технологического развития, для направления информационной безопасности интерес представляют исследования по противодействию социокультурным угрозам, киберугрозам и иным источникам опасности для общества, экономики и государства, а также обеспечению возможности эффективного ответа общества на большие вызовы с учетом взаимодействия человека и технологий, в том числе применяя методы гуманитарных и социальных наук.

Таким вызовом представляется доверие к безопасности объектов в критических информационных инфраструктурах и в частности, доверие к персоналу организации или учреждения.

Исследование направлено на разработку организационных решений по обеспечению информационной безопасности, что является одной из актуальных задач защиты информации.

В соответствии с аналитическими обзорами специалистов компании InfoWatch [1], Positive Technologies [2], за второй квартал 2021 год возросло количество атак с применением методов социальной инженерии (с 36% в I квартале 2021 года до 53% во II квартале). Основным способом распространения вредоносов в атаках на организации (58%) остается электронная почта. Аналитические данные представлены на рисунке 1.

Все большую роль для поддержания защищенности данных организации играет понимание сотрудниками компаний важности знаний основ информационной безопасности, а для компаний – доверие к персоналу в вопросах безопасности. В связи с вышесказанным, работа представляется актуальной.

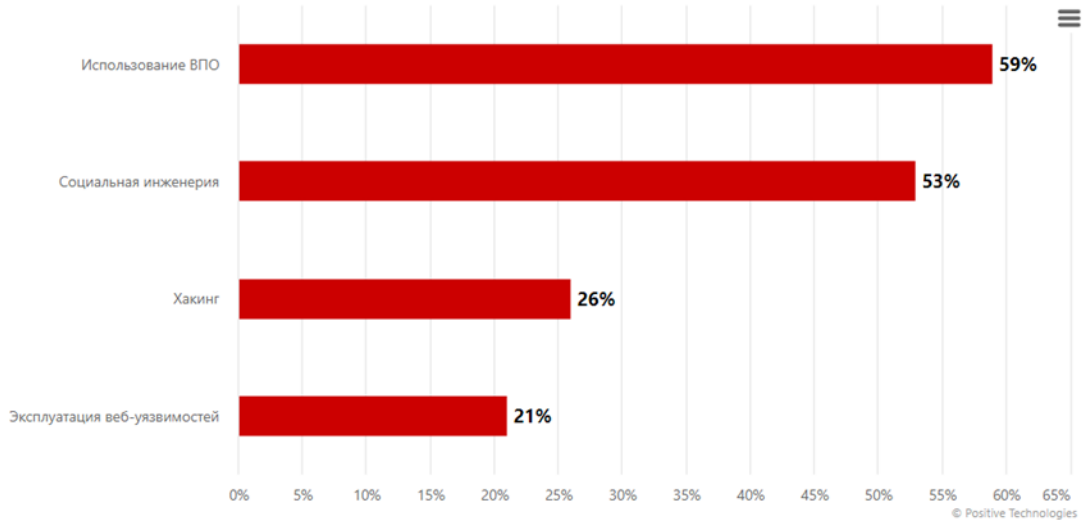


Рис. 1 Аналитические данные эксплуатируемых методов

Проблемой, решение которой предлагается в работе, является необходимость обеспечения доверия к персоналу внутри организации с одной стороны и необходимость обеспечения непрерывности бизнес-процессов организации, с другой. Существующие методики повышения осведомленности основаны на тренингах, использовании информационных материалах, что дает хорошие результаты только в крупных корпорациях мирового значения. Организации на уровне муниципалитетов не имеют возможности занимать рабочее время сотрудников более, чем на 10 минут в день из-за загруженности последних и не оптимизированной логики бизнес-процессов, а также из-за банального отсутствия должного финансирования. Внедрение DLP-систем так же не представляется решением поставленной проблемы, поскольку это средство аудита и анализа, но не обучения. Поддержание доступности сервисов напрямую влияет на репутацию организации, потому слаженная работа сотрудников – залог высокого уровня доверия клиентов.

В литературных источниках существуют описания информационных и автоматизированных систем обработки персональных данных, подробно изучены угрозы и нарушители, составлены частные модели угроз. Техническое направление достаточно изучено, но по опыту работы, наибольшую угрозу представляют собственные сотрудники вне зависимости от мотива действий.

В связи с вышесказанным, предлагается модифицировать проведение инструктажей на рабочем месте. До внедрения разработанного метода, процедура повышения осведомленности представлялась схемой на рисунке 2.

Рис. 2 Процедура классического инструктажа

В реалиях современной действительности, классический инструктаж проводится в формате личной беседы или дистанционного ознакомления с действующими нормативными документами организации. Обучение сотрудников работе со средствами криптографической защиты информации (СКЗИ) производится в соответствии с Инструкцией [3] в очном формате с прохождением проверки знаний и выдачей Заключения о возможности самостоятельной работы со средствами СКЗИ. Классический инструктаж не учитывает характерологических особенностей личности и не позволяет специалистам кадровых служб и подразделений по защите информации сделать предположения о возможности воздействия на сотрудника конкретными методами социальной инженерии. Взаимосвязь методов социальной инженерии и противодействия им представлена в более ранних работах автора и материалах исследователей [4].

В рамках исследования, предложено модифицировать представленную схему, добавив в нее Модуль анализа и принятия решения (Sk), формирующий рекомендации специалисту подразделения информационной безопасности и персонифицированный текст инструктажа, построенный на анализе характерологических особенностей личности, подверженности человека конкретному методу социальной инженерии, обработанный методами многозначной логики и нейросетевым алгоритмом. Для проверки работоспособности метода аппарат многозначной логики использовался в сравнении с результатами работы нейронной сети. После внедрения инструктирование производится по схеме на рисунке 3.

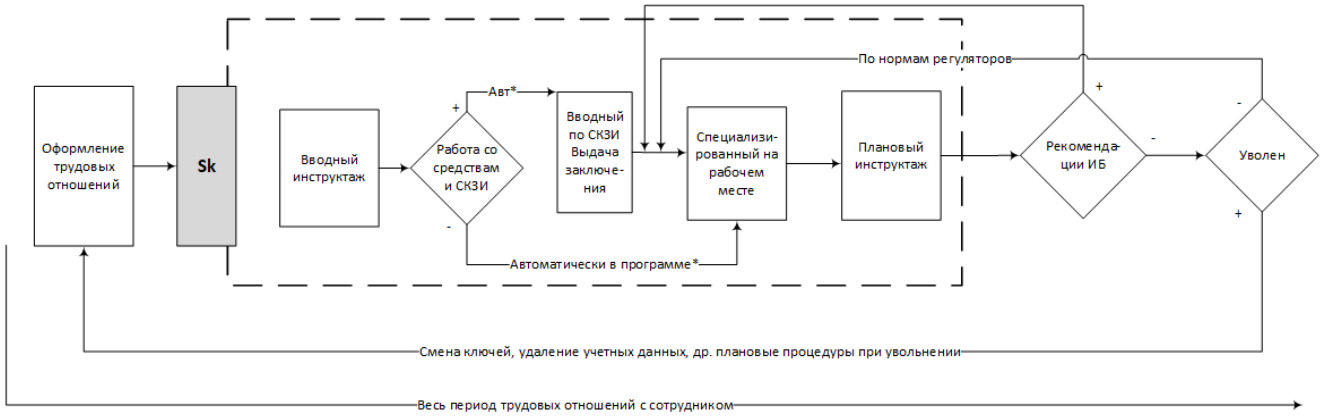


Рис. 3 Процедура автоматизированного инструктажа

При разработке модуля (Sk) применялся подход «7 радикалов» [5], проанализированные методы атак социальной инженерии [6], математический аппарат многозначной логики [7], нейронная сеть на языке Python, обучаемая на платформе [8].

С целью снижения времени на обработку результатов характерологического тестирования и определения подверженности индивида атакам социальной инженерии, было принято решение разработать нейронную сеть. Готовых наборов данных для обучения нейронной сети по заданным требованиям в сети Интернет, а также в работах других исследователей нет, поэтому следующим этапом проводился психологический эксперимент, результаты которого были обезличены и легли в основу дальнейшей разработки. В эксперименте принимали участие 250 человек в возрасте от 20 до 55 лет, без привязки к полу, возрасту, социальному и семейному положению, хотя такие данные сохранены и планируются к использованию в дальнейшем для повышения точности работы программы. Первичная обработка данных эксперимента проводилось в

обезличенном виде средствами табличного процессора и математическим аппаратом многозначной логики. При этом, для представления данных матричным способом, были выбраны следующие параметры:

1. Радикалы (выборки наиболее приемлемых акцентуаций характера личности) –

$$R = \{r_1, r_2, r_3, r_4, r_5, r_6, r_7\} \quad (1)$$

2. Методы атак социальной инженерии (выборки наиболее часто применяемых, на основе собственных аналитических исследований) –

$$C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7\} \quad (2)$$

3. Сводная матрица такая, что

$$M = R \leftrightarrow C: f(R, C) \quad (3)$$

Фрагмент первичной обработки данных представлен на рисунке 4.

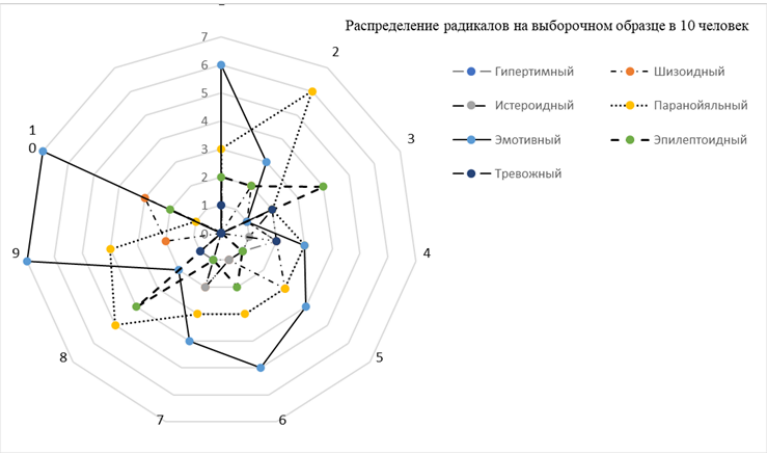


Рис. 4 Фрагмент первичной обработки данных в выборке 10

Выбор вида нейронной сети основывался на необходимости иерархического анализа каждого ответа сотрудника, в результате наиболее подходящей под задачу архитектурой явилась рекуррентная [9]. Такая сеть представляется более предпочтительной, в связи с особенностями построения вопросов при тестировании и невозможностью полного исключения какой-либо атаки из выборки. Необходима градация не только текущего вопроса и атаки, но и предыдущего, а также последующего. Только так получилось реализовать анализ эмоциональной семантики отдельных слов, а также и эмоциональное значение цельного предложения. Нейросеть обучалась на платформе Google Colab с использованием библиотеки TensorFlow [8]. Для оценки качества обучения была выбрана метрика Accuracy (точность). При прекращении роста параметра точности процесс обучения приостанавливался, поскольку далее имеет место переобучение модели. Обучение выбранных моделей происходило по схеме обучения с учителем.

Выборка данных составлял 25% от общего количества данных для обучения.

Структура выбранной сети представлена на рисунке 5 [9]

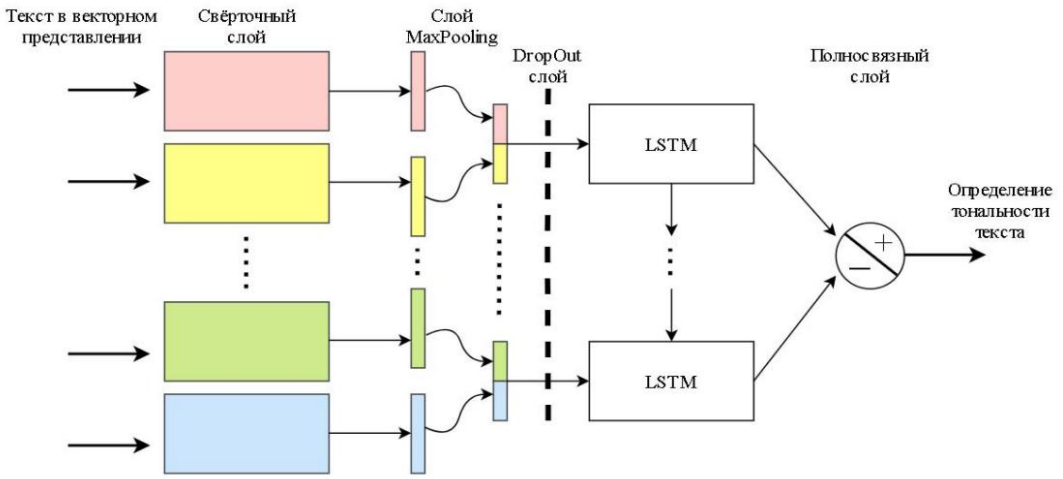


Рис. 5. Структура сети

Работа модуля подразумевает выполнение всех необходимых операций при проведении инструктажа. Важным представляется соблюдение требований регуляторов в части контроля уровня осведомленности.

Алгоритм работы модуля анализа представлен на рисунке 6.

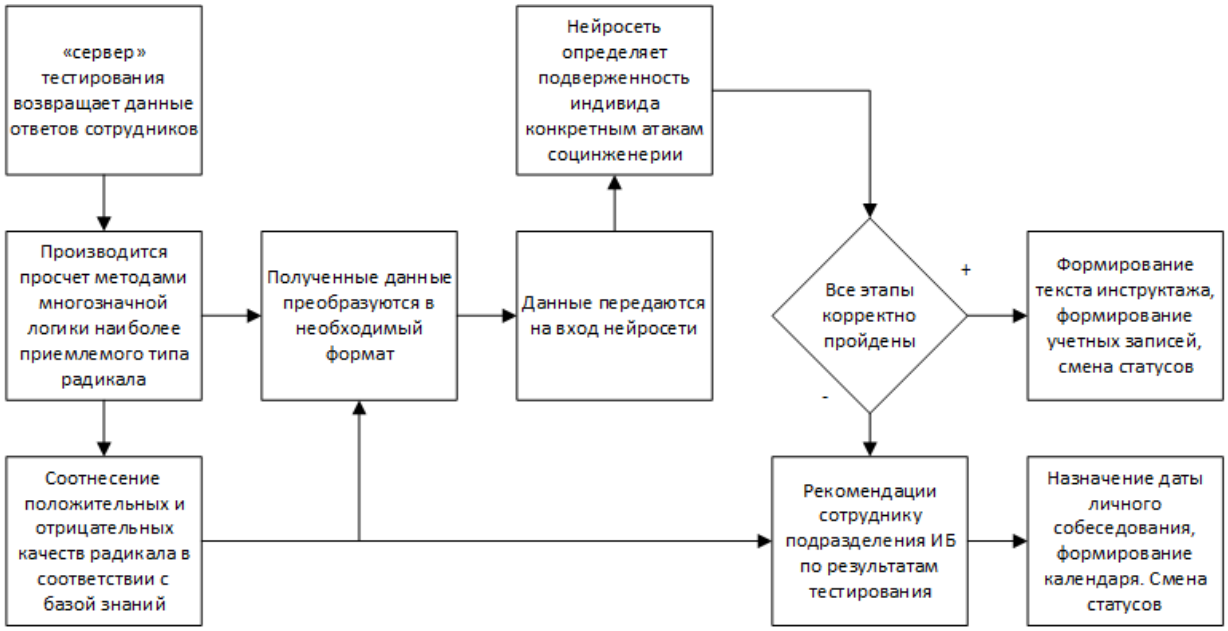


Рис. 6 Алгоритм работы модуля анализа

Разработка программного модуля включала в себя несколько этапов:

1 Разработка алгоритма работы ПО;

2 Разработка графического интерфейса;

3 Написание логики работы программы;

4 Тестирование работоспособности.

Перечень программных продуктов, используемых при разработке программной реализации, представлен в Таблице 1.

Таблица 1 Программные средства разработчика

№ п/п	Наименование	Описание	Применение
1	Python	Язык программирования	Реализация ПО
2	PyCharm	Интегрированная среда разработки для языка программирования Python.	Написание логики работы программы
3	PyQt5	Набор Python библиотек для создания графического интерфейса	Создание графического интерфейса

Первоначальная настройка программы состоит из нескольких обязательных шагов:

1. Привязка логина администратора к базе данных и загрузка обновленных табельных номеров сотрудников (используется в качестве логинов и паролей на вход). Дальнейшее обновление учетных данных производится автоматически при подключении к сети организации.
2. Выбор фрагментов инструктажей для работы (программа позволяет настраивать дополнительные модули и модифицировать вводный инструктаж по требованиям организации.
3. Задание пути сохранения результатов инструктажа и средств связи со специалистом подразделения ИБ.

Этапы установки административной части разработанного программного обеспечения стандартные, через запуск Установщика (Setup.exe), Выбор языка установки (По умолчанию язык русский), Выбор дополнительных задач (рекомендуется создать значок на рабочем столе).

В дальнейшем для включения/отключения процедуры аутентификации администратора необходимо пользоваться главным меню программы.

Вход пользователя подразумевает отсутствие любых настроек программы. Выбор режимов входа производится при запуске программы. После прохождения вводного тестирования, программа предоставляет текст инструктажа с последующей проверкой остаточных знаний в форме опроса.

Экономическая эффективность предложенного решения проблемы повышения доверия к персоналу должна учитывать:

1. оценку ущерба от реализации атак методами социальной инженерии до и после внедрения;
2. расчет затрат на разработку;
3. расчет окупаемости.

По п.1 расчет не завершен, поскольку содержит необходимость внедрения и опытной эксплуатации продукта.

Расчет общих затрат на разработку программного продукта осуществляется согласно формуле:

$$К = C_1+C_2+C_3+C_4, \quad (4)$$

где C_1 – разработка программного продукта;

C_2 – разработка документации;

C_3 – установка и настройка ПО;

C_4 – тестирование системы.

Стоимость разработки программного модуля представлена в таблице 2.

Таблица 2- Стоимость разработки системы защиты информации

№	Наименование	Цена, руб.
1	Разработка программного модуля	150 000
2	Разработка документации	10 000
3	Установка и настройка ПО	20 000
4	Тестирование системы	10 000
Итого:		190 000

По аналогии с пунктом 1, расчет окупаемости можно будет произвести только после внедрения и опытной эксплуатации.

По результатам проведенного исследования, можно сделать следующие выводы:

1. Анализ нормативной базы в части обеспечения доверия к безопасности в организации показал рассмотрение этого направления только на уровне разработки программного обеспечения. Вопросы доверия к персоналу при выполнении им должностных обязанностей, регламентированы только требованиями трудового договора.

2. Определение уровня доверия носит качественный, приближенный характер ввиду отсутствия утвержденной стандартизированной методики оценки. В большинстве организаций, доверие определяется по уровню риска.

3. Анализ влияния атак социальной инженерии на уровень доверия к персоналу показал функциональную связь акцентуаций характера с конкретными видами атак, поскольку метод воздействия выбирается исходя из слабостей человеческой природы.

4. Разработана методика формирования текста инструктажа и рекомендаций специалисту по безопасности для принятия решения при невозможности правильной программной идентификации. Такой подход позволяет снизить нагрузку на специалиста, повысить его вовлеченность в процесс обучения и избежать халатности со стороны лица, проводящего инструктаж.

5. Построена архитектура и произведена реализация программного продукта по автоматизации инструктажей по информационной безопасности на базе математического аппарата многозначной логики и алгоритмов рекуррентных нейронных сетей.

6. Проведена частичная оценка эффективности внедрения продукта.

СПИСОК ЛИТЕРАТУРЫ

1. Бывшие сотрудники как угроза информационной безопасности [Электронный ресурс] https://www.infowatch.ru/analytics/utechki-informatsii/byvshie-sotrudniki-kak-ugroza-informatsionnoy-bezopasnosti (дата обращения 12.10.2021)

2. Актуальные киберугрозы: II квартал 2021 года [Электронный ресурс]: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/ (дата обращения 15.09.2021)

3. Приказ ФАПСИ от 13 июня 2001 г. N 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну"

4. Моторина В. О., Полякова Е. Н. Методы социальной инженерии в обеспечении информационной безопасности в организации. // Сборник материалов всероссийской научно-практической конференции «Актуальные проблемы правового обеспечения национальной безопасности в России». – 2019. С. 119-123.

5. Практическая характерология: методика 7 радикалов / В.В. Пономаренко. – Москва : Издательство АСТ, 2019. -224с. – (Практический тренинг).

6. Чернецова Т.В., Корх И.А., Зангиев Т.Т. Атака на человека // Социотехнические и гуманитарные аспекты информационной безопасности». Материалы II Всероссийской научно-практической конференции. Пятигорск: ПГУ, 2020. – 160-165.

7. А. С. Карпенко. — Логики многозначные / Гуманитарный портал: Концепты [Электронный ресурс] // Центр гуманитарных технологий, 2002–2021 (последняя редакция: 22.03.2021). URL: https://gtmarket.ru/concepts/6940

8. Colaboratory - URL: https://colab.research.google.com (дата обращения: 12.06.2021).

9. Черкасов А.Н., Туркин Е.А. Выбор оптимальной архитектуры искусственной нейронной сети для задачи классификации текстов // Вестник Адыгейского государственного университета. Серия «Естественно-математические и технические науки». – Майкоп: Изд-во АГУ, 2021. – Вып. 1 (276). – с. 62-67.

Сердечный А.Л.
ВГТУ, старший преподаватель
к.т.н.
alex-voronezh@mail.ru
Гончаров А.А.
ВГТУ, аспирант
zzzsuprema@gmail.com

МЕТОДЫ КАРТОГРАФИРОВАНИЯ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА

Настоящий доклад посвящён результатам разработки системы методов картографии защищаемого киберпространства. С помощью данных методов реализуется подход, позволяющий по-новому взглянуть на киберпространство как объект защиты и исследований [1, 2]. В основе такого подхода лежит идея изображения киберпростарнства в виде системы информационных карт (Рис. 1).

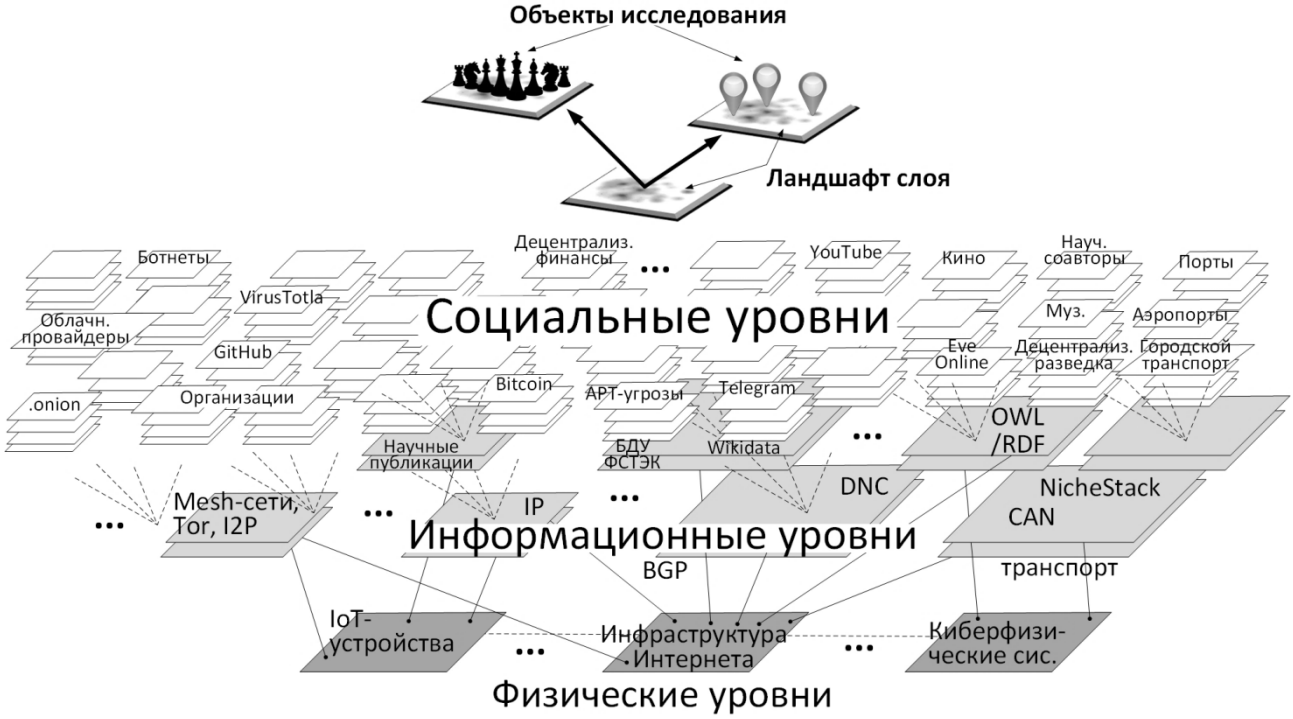


Рис. 1. Многоуровневое представление киберпространств в виде системы информационных карт

Термин «информационная карта» введён в [2] и обозначает цифровой объект, позволяющий представить в двухмерном или трёхмерном пространстве информационные объекты подобно тому, как географические карты изображают земные объекты.

Одним из важнейших принципов, который заложен в данном понятии, является принцип близости изображения схожих информационных объектов. Это позволяет использовать информационные карты для наглядного представления большого объёма данных об объекте исследования таким образом, чтобы аналитик мог использовать возможности своего мозга по обработке визуальной информации для более быстрого и всестороннего изучения объекта с учётом контекста, в котором такой объект

рассматривается. Данный подход был успешно апробирован при решении задач в области защиты информации и обеспечения информационной безопасности, некоторые из которых подробно рассмотрены в работах [3, 4, 5, 6, 7].

Эффективность исследований, проводимых с помощью информационных карт, существенным образом зависят от применяемых методов и средств картографирования защищаемого киберпространства. В настоящем докладе основное внимание уделено методам картографирования защищаемого киберпространства, система которых была сформирована в ходе практической проработки рассмотренного подхода.

Прежде чем перейти к изложению результатов разработки системы методов картографии защищаемого киберпространства необходимо отметить ключевые аспекты информационно-картографического исследования и средств автоматизации, которые используются для его проведения.

Информационно-картографическое исследование представляет собой процесс получения нового знания, показанный на Рис. 2. Это циклический процесс, в ходе которого осуществляется построение и анализ информационных карт на основании собранных исходных данных, удовлетворяющих заданной модели, которая определяется исходя из задач исследований. В ходе анализа эксперт анализирует визуальные образы, с помощью которых изображается объект исследований на ландшафте информационной карты. При этом в процессе исследования по мере получения новых знаний или выявления противоречий в имеющихся данных могут быть уточнены источники исходных данных, их модель, сами исходные данные, а также информационная карта.

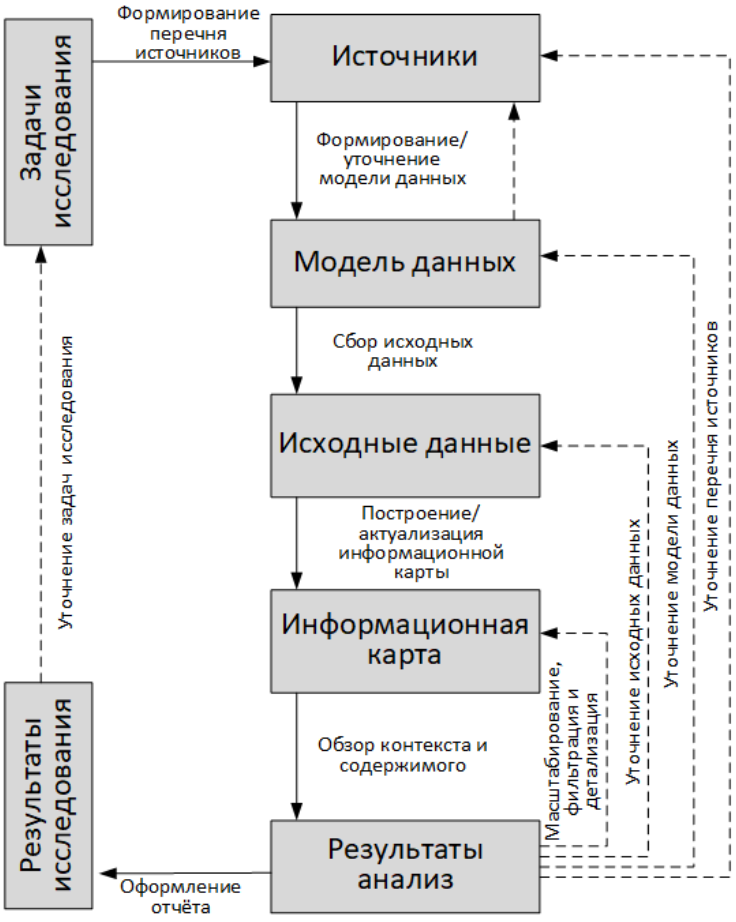


Рис. 2. Процесс информационно-картографического исследования

Данный процесс (Рис. 2) реализуется с помощью специализированных средств автоматизации, названных информационно-картографическими системами (Рис. 3). Такие программные средства подобны геоинформационным системам, а основное отличие от них заключается в том, что в информационно-картографической системе помимо функций работы с пространственными данными заложены возможности сетевого анализа (визуализации и анализа графов, с помощью которых представлены информационные объекты).

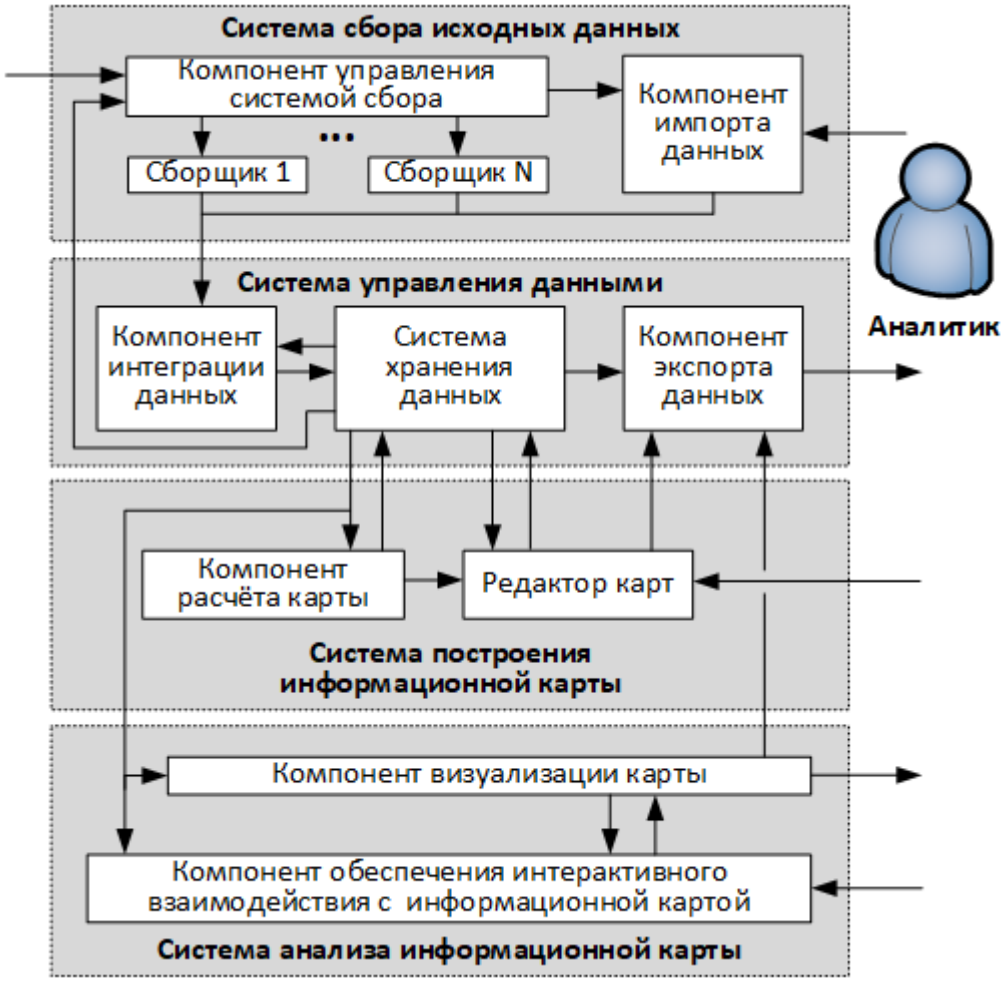


Рис. 3. Состав основных компонентов информационно-картографической системы

Информационно-картографическая система обеспечивает применение *методов картографирования защищаемого киберпространства*, которые разделены на следующие категории:

а) методы построения информационных карт:

- методы подготовки данных для информационной карты;
- методы визуализации информационной карты;
- методы актуализации информационной карты.

б) методы анализа информационных карт:

- традиционные картографические методы;
- сетевые методы.

Категория *методов подготовки данных для информационной карты* включает:

- методы моделирования данных информационной карты (моделирование данных на основе источников, моделирование данных на основе онтологий);

- методы сбора исходных данных (веб-скрапинг; зондирование информационного ресурса; извлечение текстовой информации; извлечение геопространственной информации; анализ сцен и извлечение мультимедийных данных; очистка данных);

- методы генерализации данных (экспертная генерализация данных; автоматическая генерализация данных; автоматизированная генерализация данных).

Методы моделирования данных имеют ключевое значение, так как с помощью них формируется основа для построения информационной карты. От того, насколько точно и полно будут описаны исходные данные, зависит качество и скорость построения информационной карты. Моделирование данных может осуществляться как на в результате анализа неструктурированных или частично структурированных информационных источников, так и на основании онтологий соответствующих предметных областей.

Методы автоматизированного сбора исходных данных связаны с поиском, получением доступа и предварительной обработкой данных. На реализацию данных методов уходит большая часть времени построения информационных карт. Для некоторых типов данных существуют специализированные методы извлечения фактов. Так, например, для автоматического извлечения ключевых слов и терминов из текстовой информации существует отдельная задача в рамках компьютерной лингвистики. Анализ сцен в потоке видео также требует особых методов, связанных с анализом изображений и сопоставлением их содержимого с текстовой информацией.

Методы генерализации данных применяются для многослойных информационных карт и заключаются в отображении или скрытии её деталей в зависимости от необходимости фокусирования внимания аналитика на определённых объектах.

Категория *методов визуализации информационных карт* включает:

- методы укладки графов (укладка графа на плоскости);

- методы формирования ландшафта информационной карты (построение тепловой карты; построение диаграммы Вороного);

- методы визуализации объектов на информационной карте (визуализация точечных объектов; визуализация протяжённых объектов; визуализация вложенных объектов; визуализация динамических объектов; визуализация вспомогательных объектов).

Методы укладки графов позволяют на основании подготовленных исходных данных сформировать сетевую основу для ландшафта информационной карты. Выбор конкретного метода укладки графа определяется в первую очередь размерностью пространства, в котором изображается информационная карта. Возможны следующие варианты укладки графа:

- укладка графа на плоскости;

- укладка графа на поверхности сферы;

- укладка графа в трёхмерном пространстве.

Наиболее распространёнными являются алгоритмы силовой укладки, основанные на аналогиях с физическими силами, действующими на материальные объекты. Чаще всего используется алгоритм ForceAtlas2 [8], основанный на пружинной модели.

Методы формирования ландшафта информационной карты предназначены для визуализации контекста, в котором рассматривается исследуемый объект. Ландшафт представляет собой фон, на который наносятся отметки, необходимые для исследования

объекта. Ландшафт информационной карты, представленный с помощью графа, уложенного в соответствующем пространстве, назван *сетевым*. Для графов, размер которых превышает критическое значение (обычно более 30 тыс. узлов), отображение всех его рёбер и узлов не является оптимальным выбором, так как избыточная информация отвлекает исследователя и требует нерациональное потребление вычислительных ресурсов. В этом случае ландшафт может быть сформировано с помощью следующих методов:

- построения тепловой карты;
- построения диаграммы Вороного.

На сформированном ландшафте можно проводить исследования объектов, которые должны быть представлены наглядным образом. Методы визуализации таких объектов зависят от их типов, к которым относятся: точечные объекты, протяжённые объекты, вложенные объекты, динамические объекты, вспомогательные объекты (навигационные и справочные).

Визуализация точечных объектов реализуется с помощью геометрических фигур разной формы, цвета и размера, пиктограмм, выносок с названием, анимированных объектов, тепловых карт. Визуализация протяжённых объектов, как правило, представляется в виде линий или полигонов. Обычно это маршруты, границы территорий или зон распространения. Для интерактивных информационных карт появляется возможность быстрого перемещения (навигации) по карте, а также отображения дополнительной информации по представляющему интерес объекту или группе объектов. Возможности визуализации навигационных и справочных объектов карты зависят от средств ввода/вывода, а также наличия соответствующей вычислительной мощности.

Категория *методов актуализации информационной карты* включает:

- метод совмещения графов;
- метод трансформации ландшафта.

Актуализация информационной карты может потребоваться, если изменился объект исследования или же контекст, в котором этот объект исследуется. В первом случае перестройка ландшафта не требуется, а актуализация информационной карты заключается лишь в адаптации некоторых слоёв (на которых был изображён объект исследования). Второй случай является более сложным и требует больших затрат, так как изменение основы информационной карты требует её полной перестройки.

Метод совмещения графов предполагает объединение двух и более информационных карт на уровне графов, лежащих в основе их ландшафтов. Метод трансформации ландшафта основан на изменении лишь формы информационной карты без перестройки графа, лежащего в её основе. Реализация метода связана только с геометрическими преобразованиями векторного или растрового изображения ландшафта. Применить данный метод легче, чем осуществить полный цикл операций совмещения графов, однако его результаты имеют низкую точность интеграции данных с совмещённой карты (трансформация ландшафта сохранят связь между объектами только в рамках координат двухмерного или трёхмерного пространства).

К *традиционным картографическим методам* относятся [9]:

- графический оверлей;
- разметка областей карты;
- навигация и интерактивное взаимодействие с картой.

Графический оверлей является картографическим методом, направленным на получение знаний в результате анализа совмещённых карт. Для реализации метода необходимо приведение карт к единой проекции. Разметка областей карты выполняется над её ландшафтом и может осуществляться как в ручном, так и в автоматическом режиме. Для перемещения по карте, представленной в трёхмерном пространстве, могут быть использованы специализированные устройства-манипуляторы.

Категория сетевых методов включает:

- методы расчёта метрик графа (метрик узлов, рёбер, а также графа в целом или его компонентов);

- методы кластеризации графа (кластеризация на основе показателя модулярности; спектральная кластеризация; кластеризация на основе стохастической блочной модели; кластеризация с использованием искусственных нейронных сетей; кластеризация на основе разложения матрицы; потоковая кластеризация);

- методы решения типовых задач на графах (поиск минимального пути, задача коммивояжёра, задача о канадском путешественнике и др.).

Методы сетевого анализа являются базовыми аналитическими методами информационной картографии и применяются для решения задач построения ландшафтов информационных карт, а также анализа объектов исследования, отображаемых на таких ландшафтах. Сетевые методы подробно рассмотрены в [10, 11] и применяются для выявления типовых структур графа, определения его особых узлов и рёбер, анализа маршрутов между информационными объектами (представленными в виде узлов графа), анализ изменений графа (ландшафта информационной карты) и др.

Таким образом, предлагаемая система методов формирует методическую основу процесса информационно-картографического исследования защищаемого киберпространства. Их эффективность зависит от конкретных алгоритмов, реализуемых в информационно-картографических системах, и является направлением дальнейших исследований в рамках рассмотренной темы.

СПИСОК ЛИТЕРАТУРЫ

1. Сердечный А.Л. Киберпространство как объект исследования и защиты. Часть 1 // Информация и безопасность». Том 24. Ч.3. — Воронеж: ВГТУ. — 2021. —Т. 23. № 3 (4). — С. 309-326.
2. Сердечный А.Л. Концептуальные основы картографии защищаемого киберпространства. Часть 1 // Информация и безопасность». Том 24. Ч.3. — Воронеж: ВГТУ. — 2021. —Т. 23. № 3 (4). — С. 373-386.
3. Сердечный А.Л. Карты источников, содержащих сведения об уязвимостях программного обеспечения / А.Л. Сердечный, М.А. Тарелкин, А.А. Ломов и др. // Информация и безопасность». Том 21. Ч.3. — Воронеж: ВГТУ. — 2019. — С. 411-422.
4. Калашников А.О. Картографический подход в библиометрическом исследовании отечественных научных школ, сложившихся в области защиты информации и обеспечения информационной безопасности / А.О. Калашников, А.Л. Сердечный, А.Г. Остапенко // Информация и безопасность. — 2019. — Т. 22. — № 4. — С. 455-484.

5. Serdechnyi A.L. Mapping retrieval method for academic publications in the field of aerospace technology safety / A.L. Serdechnyi, A.A. Goncharov, A.G. Ostapenko, I.L. Bataronov // IOP CONFERENCE SERIES: MATERIALS SCIENCE AND ENGINEERING. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. — 2020. — P. 52028
6. Москалева Е.А. Картографическое исследование деятельности киберпреступных группировок в контексте повышения эффективности мер защиты / Е.А. Москалева, Н.И. Баранников, Д.С. Каребин и др. // Информация и безопасность. — 2020. —Т. 23. № 3 (4). — С. 431-446.
7. Сердечный А.Л. Картографический подход исследования процессов распространения деструктивного контента в сообществах единой тематики социальной сети «Вконтакте» / А.Л. Сердечный, Р.В. Марков И.В. Герасимов и др. // Информация и безопасность. — 2020. —Т. 23. № 2 (4). — С. 203-214.
8. Jacomy M. ForceAtlas2, a continuous graph layout algorithm for handy network visualization designed for the Gephi software / M. Jacomy, T. Venturini, S Heymann b и др. // PloS one. — 2014. — Т. 9. — №. 6. — С. e98679.
9. Берлянт А.М. Картографический метод исследования // Изд-во Моск. ун-та. — 1978. — 257 с.
10. Остапенко А.Г. Социальные сети и психологическая безопасность / А.Г. Остапенко, Е.Б. Белов, А.О. Калашников и др.; Под ред. чл.-корр. РАН Д.А. Новикова. — М: Горячая линия — Телеком, 2021. — 232 с.: ил. — (Серия «Теория сетевых войн»; Вып. 5).
11. Fortunato S. Community detection in graphs // Physics reports. — 2010. — Т. 486. — №. 3-5. — С. 75-174.

Вульфин А.М.
УГАТУ, доцент

МОДЕЛИ И АЛГОРИТМЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В НАКАПЛИВАЕМЫХ ДАННЫХ МОНИТОРИНГА СОСТОЯНИЯ КИБЕРФИЗИЧЕСКОГО ОБЪЕКТА

Аннотация: Рассмотрены вопросы совершенствования моделей и алгоритмов обнаружения аномалий в накапливаемых параметрах состояния киберфизического объекта в составе критической информационной инфраструктуры в рамках концепции расширенного обнаружения и устранения угроз на основе технологий интеллектуального анализа данных и методов машинного обучения.

Ключевые слова: обнаружение аномалий, киберфизические объекты, критическая информационная инфраструктура, методы и алгоритмы интеллектуального анализа данных.

Введение

На современном этапе цифрой трансформации индустрии актуальными являются вопросы поддержания работоспособности киберфизических систем (КФС), т.е. обеспечения устойчивости протекающих в них физических процессов и непрерывности управления в условиях возможных внутренних и внешних целенаправленных деструктивных воздействий. Основным направлением развития систем защиты информации для обеспечения киберустойчивости КФС является реализация опережающей стратегии защиты (проактивная защита), основанной на предсказании угрозы (предиктивный анализ) и раннем обнаружении атак с целью адаптации системы к предполагаемому деструктивному воздействию.

Одним из современных подходов к построению систем защиты является концепция расширенного обнаружения и устранения угроз (XDR [1], Extended Detection and Response) – рис. 1, где *X* – это любой источник данных (информационно-телекоммуникационная инфраструктура, конечные системы, пользователи, киберфизические объекты (КФО)), *D* и *R* – обнаружение и реагирование. Подобные системы обеспечивают видимость и контекст на этапе анализа сложных угроз с возможностью приоритезации мер по их устранению на основе агрегации и анализа данных из множества источников.

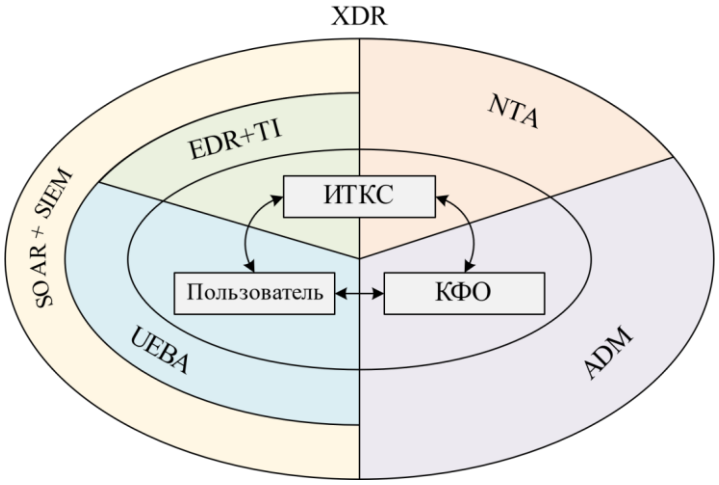


Рис. 1. Концепция расширенного обнаружения и устранения угроз (ИТКС – информационно-телекоммуникационная система)

Источниками данных для XDR являются:

- системы анализа сетевого трафика (NTA, Network Traffic Analysis) информационно-телекоммуникационной среды КФС;
- системы оркестровки безопасности и автоматизации реагирования (SOAR, Security Orchestration and Automated Response), объединяющие анализ контекста и контента в виде структурированных и неструктурированных данных в системах управления информацией и событиями безопасности (SIEM, Security Information and Event Management), реализуемый с помощью:
    - системы анализа безопасности поведения пользователей и сущностей (UEBA, User and Entity behavior Analytics);
    - системы обнаружения и реагирования на угрозы для конечных точек (EDR, Endpoint Threat Detection and Response);
    - системы обмена данными об угрозах (TI, Threat hunting);
- системы обнаружения и устранения аномалий (ADM, Anomaly Detection and Mitigation) производственных и технологических процессов КФО.

В концепции расширенного обнаружения и устранения угроз XDR важная роль отводится предиктивному анализу, выступающему в качестве одного из методов обеспечения кибербезопасности КФС. Методы предиктивного анализа направлены на выявление предпосылок неполадок и сбоев функционирования, ведущих к деградации КФО в составе КФС, на основе анализа накапливаемых параметров их состояния. Основным инструментом предиктивного анализа является выявление аномалий в технологических временных рядах (ТВР) накапливаемых параметров состояния КФО. Под аномалией при этом понимается отклонение в функционировании КФО или отклонения, связанные с нарушением взаимодействия устройств при обмене данными в составе КФО [2, 3].

Целью работы является совершенствование моделей и алгоритмов обнаружения аномалий в накапливаемых данных мониторинга состояния киберфизического объекта (сетевой трафики, технологические временные ряды параметров, характеризующих состояние объекта, поведение пользователей конечных систем) критической информационной инфраструктуры (КИИ) в рамках концепции расширенного обнаружения и устранения угроз на основе технологий интеллектуального анализа данных и методов машинного обучения.

Анализ систем обнаружения аномалий в рамках концепции расширенного обнаружения и устранения угроз кибербезопасности

Одна из возможных [4-6] классификаций методов обнаружения аномалий и направлений их использования в задачах обеспечения кибербезопасности КФС представлена на рис. 2.

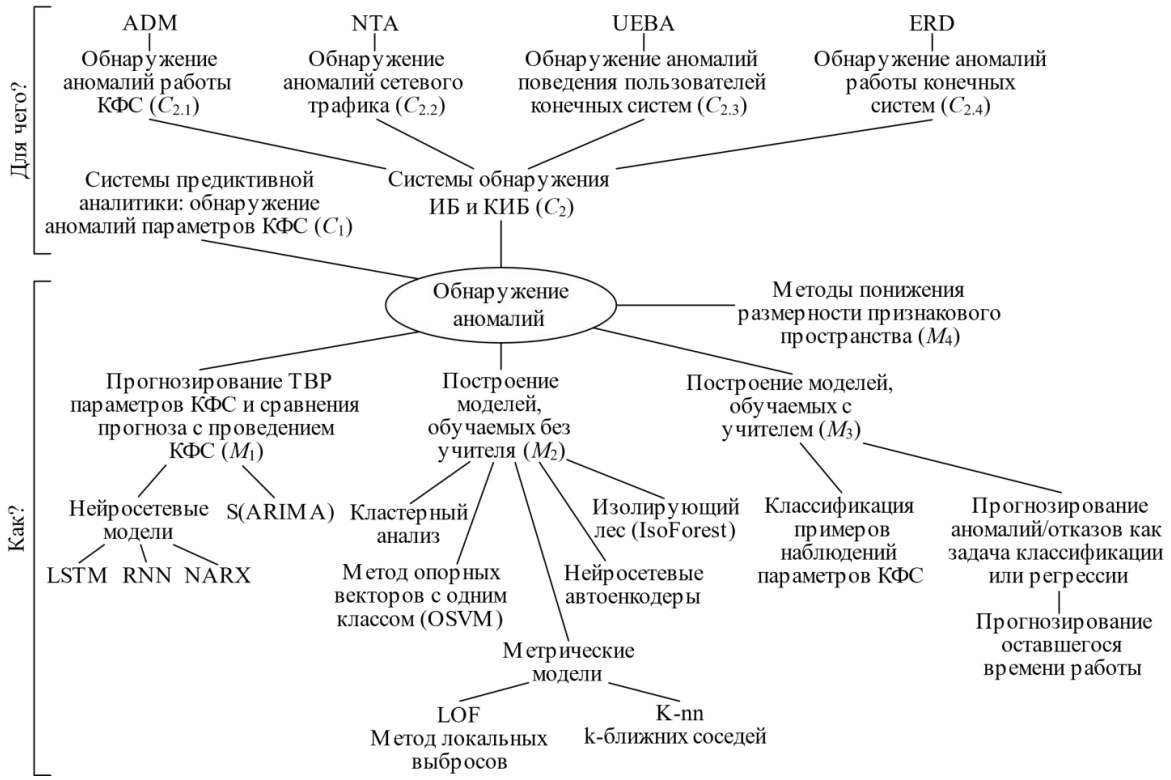


Рис. 2. Методы обнаружения аномалий в рамках концепции расширенного обнаружения и устранения угроз

При построении подобных систем возникает необходимость сбора и обработки значительных объемов структурированных и слабоструктурированных данных со всех уровней КФС для формирования набора параметров, пригодных для оперативного анализа и выявления аномалий, возникающих в результате возможных действий злоумышленника. Ведущую роль при решении этой задачи играют методы интеллектуального анализа данных (ИАД) временных рядов параметров, характеризующих состояние КФО, и методы машинного обучения.

Применение подобных решений при обнаружении аномалий функционирования ИТКС, аномалий в поведении пользователей и аномалий параметрах КФО нашло свое отражение в ряде публикаций (таблица 1).

Таблица 1 – Применение методов ИАД и машинного обучения в задачах обнаружения аномалий в рамках концепции расширенного обнаружения и устранения угроз кибербезопасности

Тип системы	Пример
Системы анализа аномалий сетевого трафика на основе методов ИАД и машинного обучения	- Модель обнаружения гибридных аномалий в высоконагруженных сетях связи на основе методов ИАД [7]; - Платформа обнаружения аномалий для выявления кибератак на облачные вычислительные среды [8]; - Комплексная система контроля и обеспечения безопасности сбора данных, реализующая мониторинг трафика в реальном времени, обнаружение аномалий, анализ воздействия, стратегии смягчения последствий [9, 10]; - Система обнаружения аномалий на основе алгоритмов

Тип системы	Пример
	машинного обучения для устранения угроз кибербезопасности сетей Интернета вещей в умном городе [11]; - Подход на основе кластерного анализа сетевого трафика для обнаружения кибератак, вызывающих аномалии в сетях критической информационной инфраструктуры газокомпрессорных станций [12]; - Распределенная система обнаружения вторжений для систем диспетчерского управления и сбора данных [13]; - Алгоритм обнаружения аномалий и система обнаружения вторжений с фильтрацией ложных срабатываний и возможностью подтверждения атаки [14]; - Система обнаружения аномалий для обнаружения утечек конфиденциальной информации в сетевом трафике энергосистем [15]; - Методология создания надежных наборов данных для обнаружения аномалий в АСУ ТП [16]
Анализ состояния конечных систем и поведения пользователя в задаче обнаружения аномалий	- Программная платформа для обнаружения аномалий работы конечной системы в режиме реального времени на основе анализа и оценки значимых выбросов наблюдаемых параметров [17]; - Детектор аномалий для обнаружения атак на конечные системы и подсистема объяснения решения [18]; - Фильтр событий для последующего анализа на основе метода глубокого обучения для обнаружения аномальной сетевой активности из журналов конечных систем в режиме реального времени [19]; - Модели сетевых вторжений, основанных на учете человеческого фактора при реализации сложных сетевых атак [20]
Обнаружение аномалий работы КФО	- Алгоритм, основанный на гауссовском процессе (метод непараметрического машинного обучения) для мониторинга состояния установок ветрогенераторов и выявления эксплуатационных аномалий [21]; - Двухэтапная методология обнаружения аномалий в промышленных процессах [22]; - Стратегия выбора датчика и обнаружение аномалий данных с помощью методов теории информации [23]; - Компоненты онлайн-системы для диагностики и обнаружения аномалий трансформаторов силовой подстанции [24]; - Анализ отклонения прогноза нейронной сети от параметров реального объекта для выявления аномалий на водоочистной станции [25]; - Обнаружение аномального поведения с помощью метода контролируемой классификации на основе частично

Тип системы	Пример
	определенной логической функции, позволяющий извлекать закономерности из исторических измерений датчиков [26]

Основной задачей обнаружения аномалий работы КФО является разработка механизма, который не только позволяет выявлять аномалии состояния КФО, но и способен отличать имеющий место фактический отказ от проводимой кибератаки [25-27].

Рассмотрим возможную классификацию методов и алгоритмов обнаружения аномалий на основе интеллектуального анализа временных рядов параметров состояния КФО. Группа методов M_1 (рис. 2) основана на построении прогностической модели одномерных и многомерных временных рядов и дальнейшем пороговом сравнении прогноза модели и реальных данных, характеризующих состояние КФО:

- модели авторегрессии (ARIMA, Auto Regressive Integrated Moving Average) и нейросетевой регрессии NARX;
- нелинейные предикторы на основе рекуррентных нейронных сетей (Recurrent Neural Network, RNN) и сетей с долгой краткосрочной памятью (Long Short-Term Memory, LSTM).

Группа методов M_2 (рис. 2) основана на применении моделей, обучаемых без учителя:

- метод опорных векторов с одним классом (One-Class SVM) – модель обучается на данных, не содержащих аномалий. Для задания порога отделения нормальных и аномальных данных необходимо иметь оценку их соотношения;
- метод изолирующего леса (Isolation Forest): ансамбль случайных деревьев решений на первых уровнях построения модели выделяет наиболее значимые аномальные данные;
- метрические методы (k-ближайших соседей, LOF (Local Outlier Factor)) основаны на оценке относительного взаимного положения данных в пространстве признаков;
- методы, основанные на кластерном анализе, оценивают удаленность точек в пространстве признаков от выделенных центров кластеров;
- методы, использующие нейросетевые автоенкодеры, строят модели, обучаемые на нормальных данных.

Группа методов M_3 (рис. 2) основана на построении моделей, обучаемых с учителем:

- классификация отдельных примеров наблюдений с помощью моделей, обучаемых с учителем, требует наличия размеченных исторических данных;
- методы предсказания дефектов и сбоев на основе специфических предвестников (классификация);
- прогнозирование оставшегося времени безотказной работы системы (задача регрессии).

Группа методов M_4 (рис. 2) понижает размерность признакового пространства описания состояния системы:

- метод главных компонент;
- вероятностный метод главных компонент.

Система и алгоритмы обнаружения аномалий состояния объектов и сущностей КИИ на основе методов машинного обучениям

Предложена архитектура системы (рис. 3) обнаружения аномалий состояния киберфизического объекта [28-33], основанная на применении методов машинного обучения и интеллектуального анализа собираемых данных телеметрии, позволяющая выявить действия злоумышленника, получившего доступ в промышленную сеть управления технологическим процессом.

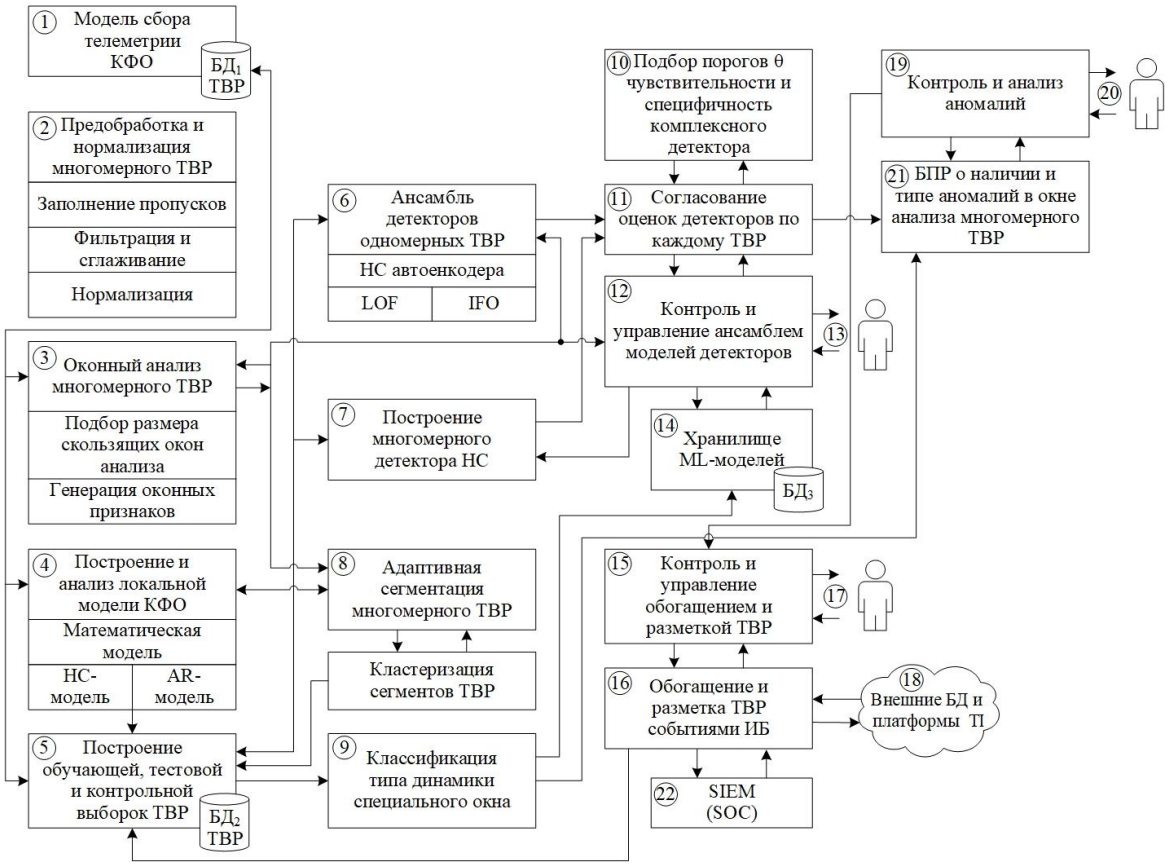


Рис. 3. Архитектура системы обнаружения аномалий состояния киберфизического объекта

Технологические временные ряды представляют собой последовательность измерений, собранных с датчиков промышленных объектов. Аномалии представляют собой отрезки временного ряда. На этапе предварительной обработки (2) входные данные подвергаются процедурам заполнения пропусков, сглаживающей фильтрации и нормализации.

Применение адаптивных опорного, тестового и расширяющегося скользящих окон (3) позволяет рассматривать непрерывные подпоследовательности ВР, для которых выполняется процедура построения признакового описания на основе статистических функций (среднее, отклонение от среднего, минимальное и максимальное значение и пр.), параметрических моделей, приближающих сегмент ВР, семейства регрессионных моделей (линейных и авторегрессионных) и нелинейных нейросетевых авторегрессионных моделей.

ТВР несут в себе признаки происходящих на КФО событий. Анализ ТВР требует идентификации фрагментов, связанных с отдельными событиями, и исследования соответствующих событий путем сегментации исходного технологического временного ряда и последующего анализа соответствующей параметров сегментов. Анализ ТВР

представляет собой задачу идентификации дискретных эпох и соотнесения их с событиями и инцидентами, характеризующими состояние объектах (16). Блок адаптивной нейросетевой сегментации ВР (8) с последующей кластеризацией выделенных сегментов со схожим типом динамики используется для построения ансамбля нейросетевых предикторов ВР с классификацией типов выделенных сегментов по заданным типам событий.

Гетерогенная модель ансамбля детекторов для обнаружения аномалий в многомерном технологическом временном ряду параметров, характеризующих ход технологического процесса КФО, включает:

- группа детекторов для одномерных ТВР (6) на основе нейросетевых автоенкодеров (7), модели оценки выбросов с автоподстройкой порога (LOF-детектор) и модели обнаружения аномалий на основе изолирующего леса (IFO-детектор);
- детектор для многомерного ТВР на основе нейросетевого автоенкодера с долгой-краткосрочной памятью (LSTM);
- детектор на основе порогового сравнения прогноза нейросетевого предиктора ВР (9) и исходного ВР.

Для создания гетерогенной модели ансамбля детекторов аномалий используются данные о нормальном состоянии для построения модели нормального функционирования КФО. Обучающая выборка содержит только данные о штатном функционировании системы, тестовая – содержит данные как нормального класса, так и класса аномалий (одиночные атаки и их комбинации).

Система и алгоритмы обнаружения аномалий функционирования ИТКС на основе методов машинного обучениям

Для повышения защищенности гетерогенной промышленной сети КФС разработана модель и алгоритм интеллектуального анализа сетевого трафика с последующей оценкой эффективности на общедоступных размеченных по типам атак и режимам работы базах сетевого трафика (NSL-KDD, CICIDS-2017, UNSW-NB15, сети промышленного интернета вещей – WUSTL-IIOT-2018; беспроводные промышленные сенсорные сети – WSN-DS-2016) и полусинтетических наборов, собранных с использованием полунатурного стенда, моделирующего сегмент корпоративной и промышленной сети. Особенностью наборов данных является акцент на использование промышленных протоколов (например, Modbus). Разведывательные сетевые атаки, при которых сеть сканируется злоумышленником для выявления возможных уязвимостей, эксплуатация которых позволит ему закрепиться в сегменте промышленной сети. Часть атак, при реализации которых существенно возрастает количество пересылаемых пакетов, уверенно обнаруживаются стандартными сигнатурными методами. Значительная часть сетевых атак с использованием эксплоитов практически не изменяет основные характеристики сетевого трафика, что делает очень затруднительным подбор сигнатур для их обнаружения. Применение методов машинного обучения и интеллектуального анализа позволяет выявить особенности аномального вредоносного трафика и построить соответствующий детектор.

Структурная схема системы обнаружения сетевых атак [34-39] на основе методов интеллектуального анализа данных приведены на рис. 4.

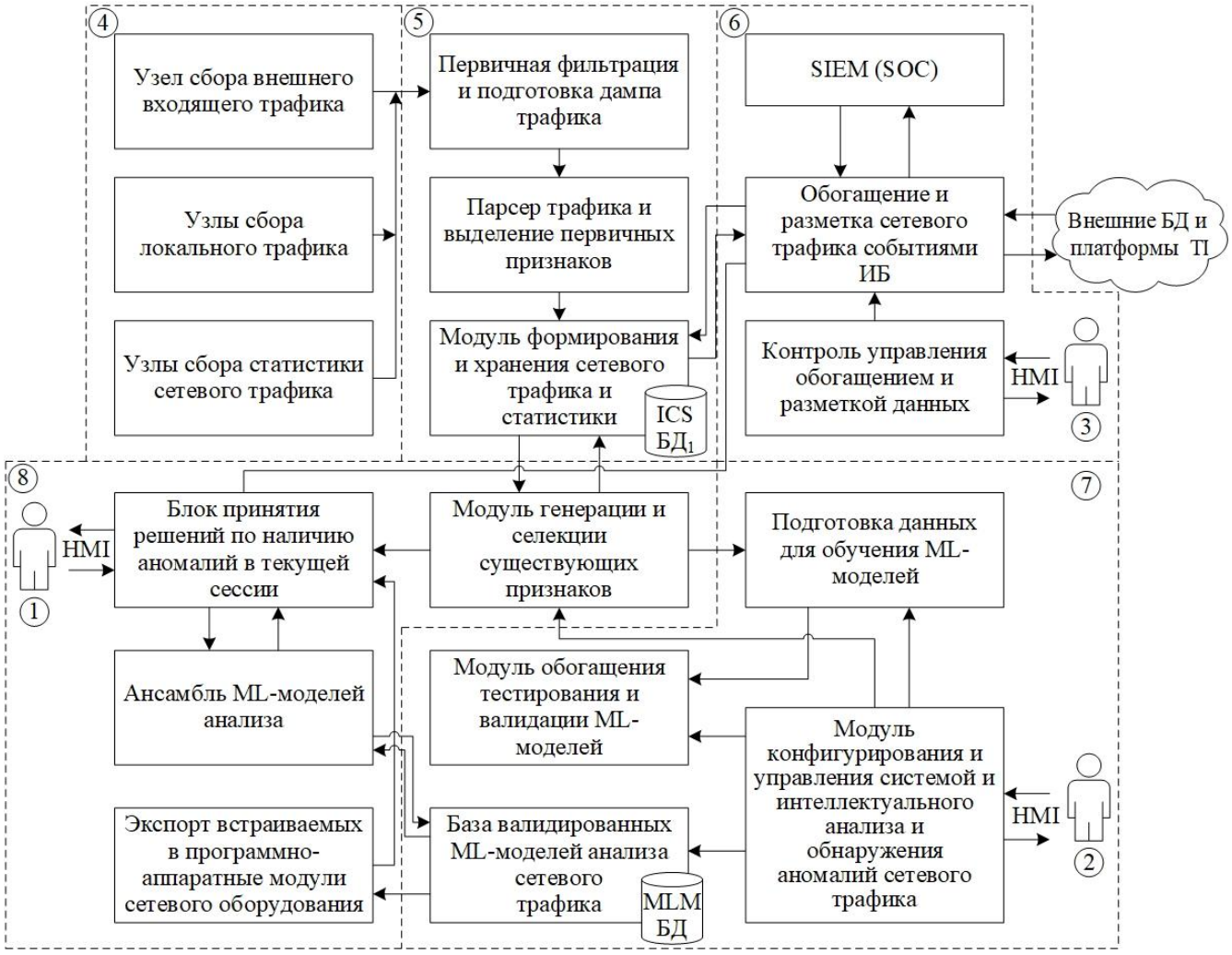


Рис. 4. Структурная схема системы обнаружения сетевых атак на основе методов интеллектуального анализа

Коллектор (4) сетевых сессий собирает параметры трафика с агентов, установленных в ключевых точках сетевой инфраструктуры: агрегирующих коммутаторах, пограничном межсетевом экране, с точек доступа в виде дампа трафика канального уровня и в формате семейства протоколов xFlow (netFlow или OpenFlow).

Модули (5) предобратки, выделения признаков и хранения статистики сетевого трафика позволяют фиксировать в долгосрочном хранилище (ICS БД) компактное описание сетевых сессий, что позволяет проводить ретроспективный анализ накопленных данных и оперативное обновление индикаторов компрометации при взаимодействии (6) с внешними платформами кибербразведки.

Модуль анализа и генерации признаков (8) используется при подготовке размеченных данных для построения и обучения моделей машинного обучения (ML-моделей), сохраняемых в БД (MLM БД) для дальнейшего использования при оперативном анализе входящего и внутреннего сетевого трафика.

Модуль обогащения, тестирования и проверки ML-моделей позволяет провести дополнительную разметку сетевого трафика, связав определенные события ИБ с соответствующими сетевыми сессиями.

Оперативное двухстороннее взаимодействие системы с системой управления событиями безопасности и центром мониторинга информационной безопасности и

реагирования на инциденты (SIEM / SOC) позволяет передавать метрики и дополнительную информацию о параметрах текущего состояния сети для последующей агрегации и анализа. Процессом разметки (обогащения) записей сетевых сессий управляет специалист (3) по сетевой безопасности текущего сегмента.

Специалист по ИАД (2) управляет работой ансамбля ML-моделей, выполняет задачи по корректировки параметров его работы и своевременного обновления банка моделей.

Итоговый блок принятия решений по обнаружения атак взаимодействует с специалистом (1) по сетевой безопасности и визуализирует результаты анализа ансамбля ML-моделей.

Обобщенный алгоритм интеллектуального анализа сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности изображен на рис. 5.

Проанализированы варианты построения ансамблей и комитетов классификаторов на основе традиционных моделей машинного обучения (модели случайного леса, рандомизированные деревья решений и пр.) и гетерогенных нейросетевых моделей (глубокие нейронные сети, сверточные нейронные сети и модели на основе автоэнкодеров с долгой-краткосрочной памятью). Оценка F1-меры при работе с тестовыми выборками достигает 96%.

Рассмотрена возможность встраивания полученных моделей в качестве модулей сетевого оборудования (МСЭ) для повышения оперативности анализа сетевого трафика промышленных систем или использования в составе сетевой системы обнаружения вторжений.

Наиболее перспективным для реализации модулей на специализированных сигнальных процессорах сетевого оборудования является классификатор на основе комитета случайных деревьев, т.к. обеспечивает приемлемое качество обнаружения сетевых атак (по сравнению с лучшими ML-моделями) и не требует значительных вычислительных ресурсов при запуске модели с подобранными в процессе обучения коэффициентами.

Система и алгоритмы обнаружения аномалий поведения пользователей на основе методов машинного обучения и интеллектуального анализа данных

С целью параметризации и оценки угрозы нарушения конфиденциальности и целостности информации и оценки соблюдения требований политики информационной безопасности объекта КИИ предложен комплекс моделей поведения пользователей конечной системы на основе методов интеллектуального анализа, включающий:

- построение цифрового отпечатка пользователя (модель пользовательского окружения конечной системы и модель динамического профиля взаимодействия пользователя с конечной системой);
- оценку психоэмоционального состояния пользователя.

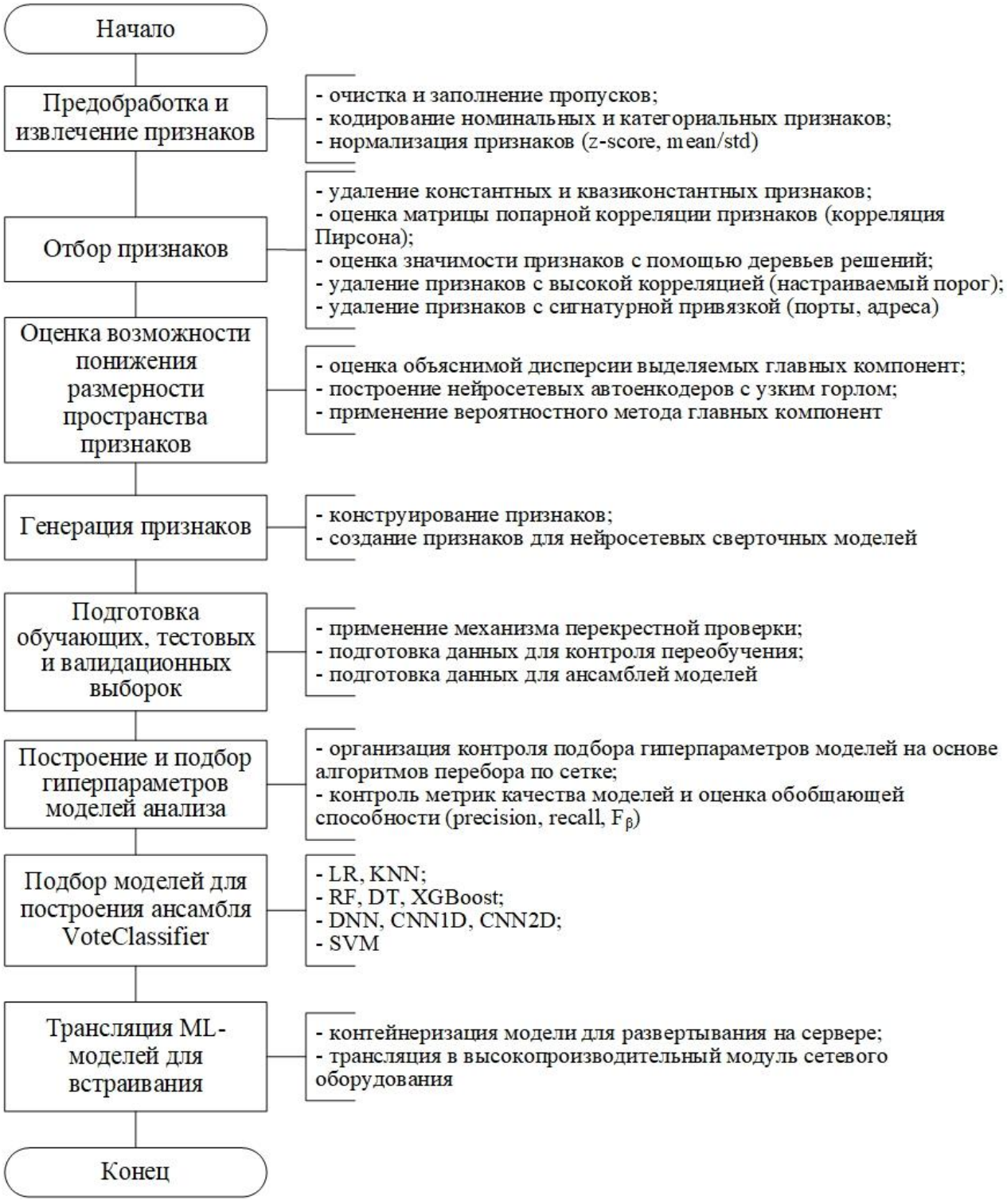


Рис. 5. Обобщенный алгоритм интеллектуального анализа сетевого трафика в задаче обнаружения аномалий и вредоносной сетевой активности

В составе системы [40-42] противодействия кибермошенничеству (антифрод-системы) предложен алгоритм сбора, обработки данных, характеризующих пользовательское окружение конечной системы, и алгоритм анализа изменения паттернов динамических биометрических признаков в случае удаленного управления пользовательским сеансом. С помощью алгоритмов кластерного анализа на основе карты самоорганизации Кохонена и иерархических алгоритмов кластеризации выявлена устойчивая структура образов, характеризующая совокупность отпечатков

пользовательских окружений со следами и без следов удаленного управления. Предложена гетерогенная модель ансамбля классификаторов для обнаружения удаленного управления пользовательским сеансом при работе с банковской системой с группой признаков, состоящих из временных интервалов между событиями движения курсора компьютерной мыши. Проведен вычислительный эксперимент на натурных данных. Доля корректного определения удаленного подключения составила 93 %.

С целью осуществления мониторинга и обмена данными об инцидентах информационной безопасности в финансовой сфере разработана структурная схема системы мониторинга банковских транзакций в составе антифрод-системы, которая включает модуль интеллектуального анализа текстовых меток назначения платежа. Внедрение модуля позволяет делать выводы о принадлежности транзитной операции к одному из предложенных классов, и строить динамический профиль пользователя и повысить обоснованность рекомендаций системы мониторинга.

Предложен алгоритм поэтапного анализа текстовой метки назначения платежа, включающий этапы предобработки, фильтрации, нормализации и построения классификатора на основе комплекса регулярных выражений и технологий интеллектуального анализа слабоструктурированных текстовых данных. Отличие алгоритма заключается в использовании адаптивных словарей категорий, построении векторного представления текстовых описаний и многопроходном применении гетерогенных нейросетевых классификаторов, что позволяет повысить обоснованность принимаемого решения о принадлежности транзакции к одному из выделенных классов.

Разработаны инструменты разметки и предобработки текстовых данных и наполнения словарей для формирования семантического пространства категорий. Результаты оценки показали, что с использованием композиции классификаторов достигнута точность классификации 81%.

В составе системы автоматического профайлинга предложена обобщенная схема модуля видеоаналитики, позволяющего:

1. Анализировать тип двигательной активности оператора – использование интеллектуальных камер и датчиков в системах видеоаналитики в сочетании с человеком-оператором, с которого снята большая часть аналитической и зрительной нагрузки, позволяет увеличить эффективность видеонаблюдения и, как результат, повысить безопасность на производстве. Рассмотрено совершенствование алгоритмов интеллектуального анализа видеоданных в системе контроля соблюдения правил промышленной безопасности (анализ типа динамики пользователей и контроль «свой-чужой») за счет использования нейросетевых технологий обработки видеоданных. Оценка эффективности программной реализации показала корректность классификации в 97 % случаев.
2. Оценивать психоэмоциональное состояние оператора – предложен алгоритм оценки и выявления неустойчивого психоэмоционального состояния оператора АСУ ТП в режиме мягкого реального времени с помощью методов интеллектуального анализа данных видеопоследовательности с целью снижения риска потери внимания и концентрации и снижения роли человеческого фактора в обеспечении безопасности промышленного объекта. Оценка программной реализации показала корректность выявления нестабильных психоэмоциональных состояний в 75 % случаев.

3. Выполнять функции нейросетевой криптографической системы идентификации и аутентификации – предложен подход на основе интеграции биометрической системы и криптографического модуля, что обеспечивает распределенное хранение базы биометрических образов и позволяет использовать в качестве выхода нейронной сети генерируемый на основе образа секретный криптографический ключ. Алгоритм выделяет биометрические признаки двухмерного изображения лица из видеопоследовательности путем применения алгоритмов цифровой обработки изображений, отличающейся способом формирования и сжатия выделяемых первичных признаков биометрических образов с помощью самоорганизующейся карты Кохонена, вероятностного алгоритма главных компонент, двунаправленной гетеро-ассоциативной памяти и многослойной нейронной сети, что позволяет порождать уникальные приватные ключи для легитимных пользователей в процессе аутентификации без возможности компрометации сжатого устойчивого вектора биометрических признаков. Наиболее эффективным на тестовых данных является подход с использованием глубоких свёрточных сетей и нейросетевой двунаправленной гетероассоциативной памяти. Для оценки защищенности разработанной подсистемы проведен анализ актуальных угроз, уязвимостей и потенциальных векторов атак на системы, использующие модели машинного обучения, построена нечеткая серая когнитивная карта для оценки локальных относительных рисков обеспечения информационной безопасности и кибербезопасности в случае воздействия злоумышленника без использования и с использованием нейросетевого преобразования «биометрия-ключ». Сценарии моделирования воздействия злоумышленника с помощью когнитивной модели позволяют оценить эффективность применяемых средств защиты и выбрать оптимальное сочетание применяемых решений с учетом выявленных угроз и потенциальных векторов атак на НСБИА, включающей модели на основе машинного обучения для обработки биометрических данных.

На рис. 6 блок формирования последовательности видеокадров с привязкой к временным отметкам (1) передает выделенные кадры для предобработки видеоряда (2) с применением нормализации и цифровой фильтрации с построением последовательности изображений в различных цветовых моделях. Поиск на отдельном изображении области интереса (ROI), включающей анализируемый объект (силуэт человека, лицо человека с привязкой ко временной метке), реализован (3) с помощью алгоритма Виолы-Джонса и сверточной нейронной сети (CNN).

Предложен алгоритм построения дескрипторов распознаваемых образов, включающий три этапа построения вектора признаков. Для выделения признаков первого уровня (4) из подготовленных изображений применяются: метод главных компонент (вариант PCA Eigenfaces), метод ориентированных градиентов (HOG), метод построения локальных бинарных шаблонов (LBP), двумерное дискретное вейвлет-преобразование (Wavenet), нейросетевое проецирование с помощью двумерной карты Кохонена (SOM), нейросетевое проецирование с помощью сверточной нейронной сети.

Для выделения признаков второго уровня (6) применяются сверточные нейронные сети, позволяющие получить описание изображения в виде ключевых точек (скелета и изображения лица).

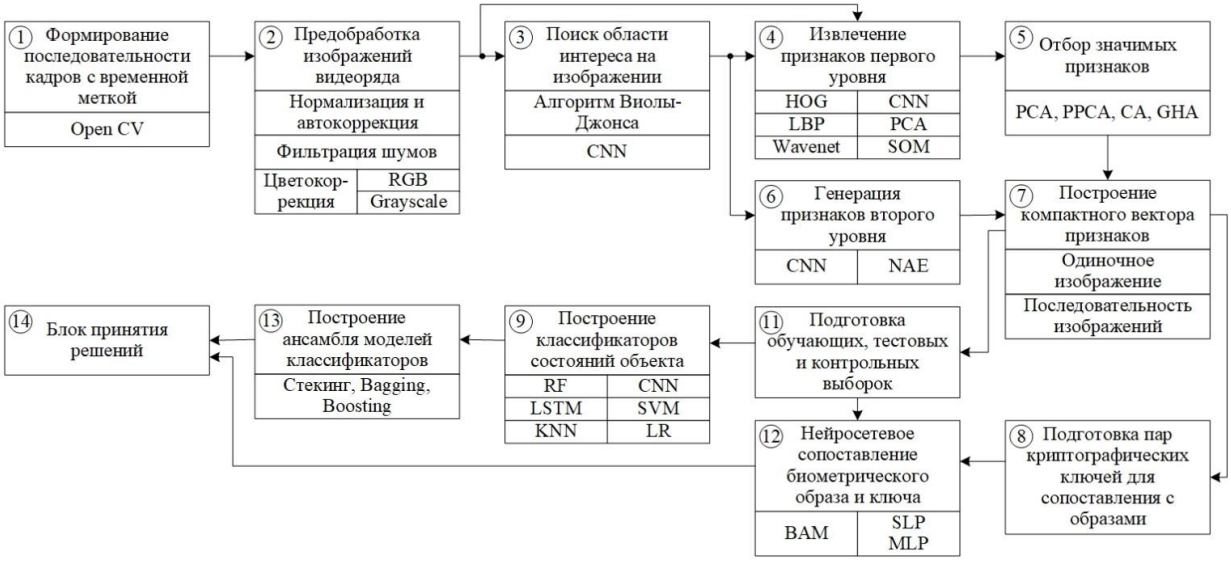


Рис. 6. Структура системы автоматического профайлинга

Для унификации (приведение к заданной длине), стандартизации и отбора наиболее значимых признаков (сокращения признакового размерности признакового пространства) используются (5): метод главных компонент, вероятностный метод главных компонент, нейросетевой фильтр Хебба, нейросетевой автоэнкодер.

На следующем этапе (7) выполняется генерация признаков для одиночного изображения и/или для последовательности кадров из сформированных векторов признаков первого или второго уровня.

Далее формируются обучающие, тестовые и контрольные выборки (11) для построения моделей классификаторов (9) на основе: случайного леса (RF), классификатора k-ближайших соседей (KNN), логистической регрессии (LR), метода опорных векторов (SVM), сверточной нейронной сети и нейронной сети с долгой-краткосрочной памятью (LSTM). Следующий этап позволяет строить (13) ансамбли классификаторов для повышения эффективности классификации на основе взвешенного усреднения и адаптивных композиций моделей.

При реализации функций нейросетевой криптографической системы аутентификации в блок (12) с помощью двунаправленной гетеро-ассоциативной памяти и/или полносвязной нейронной сети прямого распространения выполняется преобразование биометрического образа в секретный криптографический ключ.

Итоговый блок принятия решений (14) позволяет оценить степень уверенности композиции классификаторов в типе распознаваемого образа (аутентификация на основе изображения лица), динамике движений объекта (распознавание типа движений, жестов), типе психоэмоционального состояния и передать сформированный закрытый ключ в блок криптографической системы.

В составе подсистемы автоматического профайлинга предложена схема модуля анализа информационного почерка пользователя (динамический профиль пользователя на основе анализа клавиатурного почерка), позволяющего выполнять процедуру непрерывной скрытой аутентификации и оценки психоэмоционального состояния пользователя.

Разработан алгоритм кодирования вектора признаков, характеризующих клавиатурный почерк пользователя, на основе нормализованного представления вектора

временных интервалов удержания клавиш (ВУК) и временных интервалов между нажатиями клавиш (ВМН) для типовых N-графов, с последующей унификацией пользовательских шаблонов на основе применения вейвлет-преобразования Хаара. Предложена модульная структура нейросетевого классификатора, корректно определяющая пользователя в 98 % случаев.

Заключение

Для выявления сложных атак злоумышленников, получивших доступ с сеть промышленного объекта, необходимо применение методов и инструментов расширенной аналитики данных, позволяющих выполнять оперативный анализ и выявление скрытых признаков злонамеренной активности на основе модели наблюдаемого КФО.

Применение методов интеллектуального анализа данных в составе системы сбора и корреляции событий ИБ позволит автоматизировать анализ больших массивов гетерогенных данных о состоянии объекта и событиях безопасности. Данная задача является основной, наиболее ресурсоемкой и трудно формализуемой операцией, которая выявляет причинно-следственные связи между поступающими на обработку событиями, представляемыми в виде многомерных временных рядов. Операция корреляции позволяет выявлять вредоносную и аномальную активности, определять источник и цель атаки. Для анализа многомерных технологических временных рядов предложено использовать комплекс адаптивных нейросетевых модулей для представления паттернов состояний, что позволит повысить эффективность поиска скрытых зависимостей в накапливаемых данных.

Основные преимущества данных методов заключаются в возможности учета реальных статистических данных, а также знаний и опыта экспертов применительно к сложным организационно-техническим объектам, какими являются объекты КИИ, возможности прогнозирования потенциальных рисков ИБ (проактивный мониторинг) и принятия упреждающих защитных контрмер (повышение осведомленности о процессах объекта КИИ) с учетом множества потенциально существующих угроз и уязвимостей программно-аппаратного обеспечения объектов КИИ.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта № 1/2020.

СПИСОК ЛИТЕРАТУРЫ

1. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях // Горячая Линия – Телеком, 2021. 432 с.

2. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic control and computer sciences. 2016. Vol. 50. № 8. P. 673-681.

3. Зегжда Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам // Горячая Линия – Телеком, 2020. 560 с.

4. Pang G. et al. Deep learning for anomaly detection: A review // ACM Computing Surveys (CSUR). 2021. Vol. 54. № 2. P. 1-38.

5. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование // Горячая Линия – Телеком, 2020. 448 с.

6. Современные технологии аналитики в кибербезопасности // Газинформсервис [Электронный ресурс]. – URL: https://habr.com/ru/company/gaz-is/blog/480980/ (дата обращения 24.08.2021).

7. Monshizadeh M. et al. Performance evaluation of a combined anomaly detection platform // IEEE Access. 2019. Vol. 7. P. 100964-100978.

8. Moustafa N. et al. Collaborative anomaly detection framework for handling big data of cloud computing // 2017 military communications and information systems conference (MilCIS). IEEE. 2017. P. 1-6.

9. Ten C.W., Manimaran G., Liu C. C. Cybersecurity for critical infrastructures: Attack and defense modeling // IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. 2010. Vol. 40. № 4. P. 853-865.

10. Ten C.W., Hong J., Liu C. C. Anomaly detection for cybersecurity of the substations // IEEE Transactions on Smart Grid. 2011. Vol. 2. № 4. P. 865-873.

11. Alrashdi I. et al. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning // 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE. 2019. P. 305-310.

12. Kiss I. et al. Data clustering-based anomaly detection in industrial control systems // 2014 IEEE 10th International Conference on Intelligent Computer Communication and Processing (ICCP). IEEE. 2014. P. 275-281.

13. Cruz T. et al. A cybersecurity detection framework for supervisory control and data acquisition systems // IEEE Transactions on Industrial Informatics. 2016. Vol. 12. № 6. P. 2236-2246.

14. Tartakovsky A.G., Polunchenko A. S., Sokolov G. Efficient computer network anomaly detection by changepoint detection methods // IEEE Journal of Selected Topics in Signal Processing. 2012. Vol. 7. № 1. P. 4-11.

15. Keshk M. et al. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems // IEEE Transactions on Sustainable Computing. 2019. Vol. 6. № 1. P. 66-79.

16. Gómez Á.L.P. et al. On the generation of anomaly detection datasets in industrial control systems // IEEE Access. 2019. Vol. 7. P. 177460-177473.

17. Hariharan A., Gupta A., Pal T. Camlpad: Cybersecurity autonomous machine learning platform for anomaly detection // Future of Information and Communication Conference. Springer, Cham. 2020. P. 705-720.

18. Siddiqui M.A. et al. Detecting cyber attacks using anomaly detection with explanations and expert feedback // ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE. 2019. P. 2872-2876.

19. Tuor A. et al. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams // Workshops at the Thirty-First AAAI Conference on Artificial Intelligence. 2017.

20. Chen S., Janeja V. P. Human perspective to anomaly detection for cybersecurity // Journal of Intelligent Information Systems. 2014. Vol. 42. № 1. P. 133-153.

21. Pandit R.K., Infield D. SCADA-based wind turbine anomaly detection using Gaussian process models for wind turbine condition monitoring purposes // IET Renewable Power Generation. 2018. Vol. 12. № 11. P. 1249-1255.

22. Quatrini E. et al. Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities // Journal of Manufacturing Systems. 2020. Vol. 56. P. 117-132.

23. Liu L. et al. Effective sensor selection and data anomaly detection for condition monitoring of aircraft engines // Sensors. 2016. Vol. 16. № 5. P. 623.

24. Catterson V.M. et al. On-line transformer condition monitoring through diagnostics and anomaly detection // 2009 15th International Conference on Intelligent System Applications to Power Systems. IEEE. 2009. P. 1-6.

25. Goh J. et al. Anomaly detection in cyber physical systems using recurrent neural networks // 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE). IEEE. 2017. P. 140-145.

26. Das T.K., Adepu S., Zhou J. Anomaly detection in industrial control systems using logical analysis of data // Computers & Security. 2020. Vol. 96. P. 101935.

27. Karimipour H. et al. Intelligent anomaly detection for large-scale smart grids // 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). IEEE. 2019. P. 1-4.

28. Vulfin A.M., Frid A.I., Giniyatullin V.M. Neuralbase model for detection and recognition of technological situations within the scope of data mining strategy // Optical Memory and Neural Networks (Information Optics). 2010. Vol. 19, № 3. P. 207-212.

29. Вульфин А.М., Фрид А.И. Нейросетевая модель анализа технологических временных рядов в рамках методологии Data Mining // Информационно-управляющие системы. 2011. № 5(54). С. 31-38.

30. Вульфин А.М., Фрид А.И. Алгоритмы нейросетевой обработки информации в задачах диагностирования инженерной сети нефтедобывающего предприятия // Нейрокомпьютеры: разработка, применение. 2013. № 3. С. 36-39.

31. Vulfin A.M., Frid A.I. Safety Increasing of Oil Companies Engineering Networks Operation with Use of Artificial Intelligence Systems // Proceedings of the 16th International Workshop. Computer Science and Information Technologies (CSIT'2014). Sheffield, England, 17–22 September 2014. Vol. 3. P. 167-171.

32. Arpishkin M.I., Vulfin A.M., Vasilyev V.I., Nikonov A.V. Intelligent integrity monitoring system for technological process data // Journal of Physics: Conference Series. IOP Publishing, 2019. Т. 1368, № 5. P. 1-16. https://iopscience.iop.org/article/10.1088/1742-6596/1368/5/052029/meta

33. Berkholts V.V., Vulfin A.M., Frid A.I. Telemetry data integrity monitoring system // IOP Conf. Series: Materials Science and Engineering, 2nd Scientific Conference on Fundamental Information Security Problems in terms of the Digital Transformation (FISP 2020) 30 November 2020, Stavropol, Russian Federation. 2021. Vol. 1069. 012003. doi:10.1088/1757-899X/1069/1/012003

34. Sapozhnikova M.U., Nikonov A.V., Vulfin A.M. Intrusion detection system based on data mining technics for industrial networks // International Conference on Industrial Engineering, Applications and Manufacturing, (ICIEAM). IEEE, 2018. P. 1-5. URL: https://ieeexplore.ieee.org/abstract/document/8728771

35. Gurin M.A., Vulfin A.M., Vasilyev V.I., Nikonov A.V. Intrusion detection system on the basis of data mining algorithms in the industrial network // 5th International Conference on

Information Technology and Nanotechnology: CEUR Workshop Proceedings. 2019. P. 553-565. URL: http://ceur-ws.org/Vol-2416/paper68.pdf

36. Emil Hajrullin, Alexey Vulfin, Konstantin Mironov, Arkadij Frid, Murat Guzairov and Anastasia Kirillova Secure Data Exchange in the Industrial Internet of Things Network of the Fuel and Energy Complex // Proceedings ICOECS 2020 International Conference on Electrotechnical Complexes and Systems. Ufa State Aviation Technical University Ufa, Russia 27 - 30 October 2020. IEEE, 2020. P. 353-358.

37. Vulfin A.M., Vasilyev V.I., Kuharev S.N., Homutov E.V., Kirillova A.D. Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms // International Scientific and Practical Conference "Information Technologies and Intelligent Decision Making Systems (ITIDMS-II 2021) 1 July 2021, Moscow, Russia. Journal of Physics: Conference Series. 2021. Vol. 2001. 012004

38. Vulfin A. M. et al. Network traffic analysis based on machine learning methods //Journal of Physics: Conference Series. IOP Publishing, 2021. Vol. 2001. № 1. P. 012017.

39. Khayretdinov R.I., Dautov D.Sh., Vulfin A.M., Mironov K.V., Frid A.I. Secure data exchange system in software-defined networks of energy complex facilities // 2021 International Conference on Electrotechnical Complexes and Systems (ICOECS 2021) (в печати)

40. Sapozhnikova M.U., Nikonov A.V., Vulfin A.M., Gayanova M.M., Mironov K.V., Kurennov D.V. Anti-fraud system on the basis of Data Mining technologies // 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2017). IEEE, 2017. P. 243-248. URL: https://ieeexplore.ieee.org/abstract/document/8388649

41. Sapozhnikova M.U., Nikonov A.V., Vulfin A.M. Intrusion detection system based on data mining technics for industrial networks // International Conference on Industrial Engineering, Applications and Manufacturing, (ICIEAM). IEEE, 2018. P. 1-5. URL: https://ieeexplore.ieee.org/abstract/document/8728771

42. Startseva A.S., Vulfin A.M., Vasilyev V.I., Nikonov A.V., Kirillova A.D. Analysis of Financial Payments Text Labels in the Dynamic Client Profile Construction // 2020 International Conference on Information Technology and Nanotechnology (ITNT). Samara, Russia, 26-29 May 2020. IEEE, 2020. P. 1-10. (DOI:10.1109/ITNT49337.2020.9253280)

Башмаков Н.М.
УГАТУ, аспирант,
nail.bashmakov@gmail.com
Картак В.М.
УГАТУ, заведующий кафедрой, д. ф.-м.н., профессор,
kvmail@mail.ru

ИСПОЛЬЗОВАНИЕ ФИДОВ ПРИ ВНЕДРЕНИИ ПРОЦЕССА КИБЕР-РАЗВЕДКИ

Громкие заголовки новостей об очередных успешных компьютерных атаках уже стали привычным явлением. Именно поэтому обеспечение информационной безопасности обсуждается на самых высших уровнях, например, в 2021 году одной из важнейших тем, которые обсуждались между Путиным и Байденом, был именно вопрос взаимодействия по противодействию киберугрозам [1]. Это свидетельствует о том, что в нашем мире, подверженном стремительной цифровизации, обеспечение информационной безопасности данных остается очень важным и нужным направлением. В России же, в связи с курсом на цифровизацию, направление информационной безопасности становится даже более актуальным и востребованным [2]. Государству приходится задумываться об обеспечении информационной безопасности в том числе и потому, что целями атак APT-группировок часто становятся различные научные центры, занимающиеся инновационными разработками [3].

APT-группировками обычно называют группы высококвалифицированных хакеров, проводящих сложные многоэтапные компьютерные атаки. Изначально это так обозначались хакерские группировки, действующие в интересах какого-либо государства, однако позже оно стало относится ко всем группировкам, производящим многоуровневые атаки [4]. Для того, чтобы действовать успешно злоумышленникам приходится адаптироваться и развиваться – именно поэтому массовые атаки начала века сменились сложными спланированными действиями [5].

Для эффективного противодействия профессионалам-взломщикам специалисты в области информационной безопасности вынуждены развиваться, предлагать новые решения и стараться быть на шаг впереди своих оппонентов.

Одним из инструментов, который призван дать специалистам по информационной безопасности возможность быть лучше осведомленными о предполагаемых действиях злоумышленников, стала разведка кибер-угроз (cyber threat intelligence).

Разведка кибер-угроз представляет собой информацию об актуальных угрозах, способах которыми злоумышленники осуществляют атаки. Выделяют 2 уровня threat intelligence – стратегический и тактический. К стратегическому относят информацию о трендах и статистике, тактиках и техниках. К тактическому – фиды, правила и индикаторы компрометации [6].

Индикаторами компрометации (indicators of compromise, IOCs) называют некоторые признаки, указывающие на возможную вредоносную активность в инфраструктуре [7]. Обычно это ip-адреса, доменные имена, хэши файлов, url [8,9]. Выделяют следующие сценарии применения индикаторов компрометации: детектирование, блокирование, ретроспективный анализ, расследование. Подобные индикаторы зачастую группируют в списки, называемые фидами (feeds).

Фиды формируются как признанными экспертами в области информационной безопасности, такими как ESET NOD и Kaspersky, так и энтузиастами, а кроме того некоторыми сообществами, участники которых обмениваются обнаруженными индикаторами компрометации. Компании, занимающиеся информационной безопасностью, редко предоставляют фиды на безвозмездной основе, в отличие от любителей. Бесплатные фиды обычно размещаются в интернете и доступны для скачивания.

При любом из сценариев использования индикаторов компрометации, сгруппированных в фиды, существует несколько проблем, важнейшими из которых можно назвать устаревание индикаторов компрометации и отсутствие гарантии их качества. Первая проблема возникает из-за того, что скомпрометированная инфраструктура, используемая злоумышленниками, редко проявляет свою активность в течение продолжительного времени. Соответственно, информация об ip-адресе, с которого осуществлялись попытки эксплуатации уязвимости, может вскоре стать не актуальной [9]. Вторая проблема проистекает из различных способов сбора индикаторов компрометации и человеческого фактора – в фиды могут попасть такие сущности, которые на самом деле никакой вредоносной активности не проявляли, так называемые false positive. Еще можно выделить трудности, возникающие при реализации сценария блокирования – заблокированные ip-адреса и доменные имена могут оказаться вполне легитимными и более того, необходимыми для реализации бизнес-процессов.

Следовательно, при принятии решения об использовании свободно распространяемых фидов в процессе кибер-разведки прежде всего стоит задача выбора тех из них, что содержат наибольшее число действительно вредоносных индикаторов и минимальное число false positive.

Исследователи в статье [8] направили свои усилия на снижение количества false positive, которые могут встречаться в фидах. В своем исследовании она изучили 4 фида, поставлявших ip-адреса. Сперва они рассмотрели такую особенность, что некоторые фиды могут брать индикаторы из других фидов, а затем убедились, что исследуемые ими фиды являются независимыми. Предполагая, что они не могут заранее знать, насколько качественные данные будет предоставлять фид, авторы статьи предложили оценивать фид по следующим характеристикам: Экстенсивность (Extensiveness), Своевременность (Timeliness), Полнота (Completeness), Оценка пересечений с белым списком (Whitelist Overlap Score). Экстенсивность понимается как дополнительный контекст, предоставляемый фидом для каждого индикатора. Своевременность –время, за которое в фидах появился индикатор, уже замеченный одним из фидов. Полнота – это доля индикаторов конкретного фида из всего количества индикаторов, используемых в исследовании. Оценка пересечений с белым списком должна показывать, насколько пересекаются множества индикаторов фида и множество сущностей, для которых принято, что они не могут являться индикаторами компрометации. В случае ip-адресов к таким относят ip-адреса крупных компаний и провайдеров. Авторы вычислили оценки характеристик по соответствующим формулам и провели анализ изучаемых фидов [8].

После этого исследователи на основе частных оценок вычислили агрегированные оценки для фидов. При этом исследователи пришли в числе прочих к следующему выводу - характеристика Полнота не играет никакой роли, прочие характеристики могут применяться для оценивания фидов.

При выборе фидов, которые будут использоваться при построении процесса кибер-разведки, предлагаем основываться на характеристиках Экстенсивность, Своевременность, Пересечения с белым списком. Кроме того, мы хотим заметить, что даже среди фидов, поставляющих индикаторы компрометации одного типа, в данном случае ip-адреса, характер вредоносной активности, проявляемый индикаторами, может различаться и необходимо это учитывать при сравнении фидов, Такой индикатор компрометации как ip-адрес может быть, например, сервером управления ботнета, осуществлять попытки перебора паролей, пытаться проэксплуатировать уязвимость веб-сервисов. Соответственно, сравнивать их напрямую представляется нам некорректным, более целесообразным кажется выявление типов вредоносной активности, проявляемых индикаторами из фида и прямое сравнение только тех фидов, чьи индикаторы замечены за однотипной активностью.

В дополнение к предложенным характеристикам из вышеописанного исследования предлагаем для выбора фидов также следующие 2 характеристики: Оценка новых индикаторов в фиде и Оценка удаления неактуальных индикаторов. Первая обусловлена тем, что свободно распространяемые фиды могут в какой-то момент перестать поддерживаться и они будут содержать тот список индикаторов, что был на момент последнего обновления, очевидно, что вскоре этот список станет совершенно не акутальным. Вторая же предлагается потому, что в некоторых фидах есть индикаторы, которые попали в них месяцы и даже годы назад и продолжают в них присутствовать, хотя новой информации об их активности не поступало.

Для реализации процесса кибер-разведки требуется загружать и хранить индикаторы компрометации поставляемые фидами, при этом каждому индикатору должны ставиться в соответствие значения first_seen и last_seen – время первого и последнего появления индикатора в фиде. Значения first_seen и last_seen назначаются в момент загрузки индикаторов из фида, который производится раз в сутки. Для того, чтобы вычислить предложенные оценки требуется некоторое время хранить те индикаторы, которые присутствовали в фиде, но были удалены, поскольку стали считаться не актуальными. Оценки требуется пересчитывать после каждой загрузки индикаторов, поскольку характеристики фидов в этот момент изменяются.

Так же мы предлагаем не вычислять агрегированную оценку на основе частных оценок характеристик, а рассматривать каждую оценку по отдельности. Если оценка какой-либо характеристики фида окажется низкой это будет поводом разобраться в причинах этого и принять решение о том, стоит ли продолжать использовать фид в процессе кибер-разведки в дальнейшем.

Еще одной разумной рекомендацией представляется следующее – выявить в журналах событий инфраструктуры индикаторы компрометации, связанные с вредоносной активностью и осуществить поиск пересечений этих индикаторов с предполагаемыми к использованию фидами – те, которые покажут наибольшее число пересечений с высокой вероятностью будут наиболее полезными при построении процесса кибер-разведки.

СПИСОК ЛИТЕРАТУРЫ

1. Шакиров О. Киберсаммит Путина и Байдена [Электронный ресурс]. — Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/kibersammit-putina-i-baydena/
2. Кайгородцев А. А. Проблемы обеспечения информационной безопасности России в условиях цифровизации / А. А. Кайгородцев, Т. Ф. Кайгородцева // *Society and Security Insights*. – 2020. - *3*(3). - 79-89.
3. Новый дроппер группы APT31. Пункты назначения: Монголия, Россия, США и не только [Электронный ресурс]. — Режим доступа: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/apt31-new-attacks/
4. Васильков А. WTF is APT? Продвинутые атаки, хитрости и методы защиты/А. Васильков // Хакер. – 2018. – 232. - 15.
5. Friedman J. Definitive Guide to Cyber Threat Intelligence, J. Friedman, M. Bouchard. - 2015.
6. Новиков А. Threat Intelligence: куда и как его «прикладывать» / А. Новиков // Журнал "Information Security/ Информационная безопасность" – 2020. – 6. - 38-39.
7. Сергеев Ю. Особенности сбора, агрегации и ранжирования индикаторов компрометации / Ю. Сергеев // Журнал "Information Security/ Информационная безопасность" – 2020. – 5. - 22-23.
8. Ermerins J. Scoring model for IoCs by combining open intelligence feeds to reduce false positives / J. Ermerins, N.van Noort L. Velasco // 2020.
9. Пирожков А. Фиды для SOC. Осведомлен – значит вооружен/ А. Пирожков // Журнал "Information Security/ Информационная безопасность" – 2020. – 5. - 24-25.
10. Iklody A. Decaying Indicators of Compromise / A. Iklody, G. Wagener, A. Dulaunoy, S. Mokaddem. // 2018.

Волостных В.А.
Военная академия связи, научный сотрудник, к.в.н., доцент
ra1alo@mail.ru
Кононов П.А.
СПбГУТ, начальник отдела
kononov.pa@spbgut.ru

ФОРМИРОВАНИЕ СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

В современной образовательной организации информационная инфраструктура - одна из главных компонентов образовательного процесса. Современная высшая образовательная организация представляет собой сложную систему, для которой присуще концентрация большого объема информационных ресурсов, многообразие применяемых технологий и систем, сетевое взаимодействие компонентов в образовательном пространстве. Особенности образовательной организации высшего образования связаны с множеством направлений и форм учебной работы, пространственной распределенностью инфраструктуры (колледжи, филиалы), наличием многопрофильной структуры вспомогательных служб и подразделений. Актуальность проблемы защиты информационной среды и информационных потоков образовательной организации непосредственно обусловлена потенциальными и реальными угрозами в сфере информационной безопасности, что вызывает необходимость создания эффективной системы технической защиты информации.

Под системой технической защитой информации предлагается понимать совокупность технических средств охраны, технических средств защиты информации и обслуживающего персонала. Под техническими средствами охраны понимаются технические средства, предназначенные для использования силами охраны с целью обнаружения несанкционированных действий, информирования о попытках и фактах совершения таких действий, локализации и задержки продвижения нарушителей до прибытия сил реагирования. Под техническими средствами защиты информации понимается обеспечение некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [4].

Предлагается формирование системы технической защиты информации образовательной организации осуществлять на основе следующих принципов.

Принципы формирования системы технической защиты информации:

1. многорубежность системы защиты;
2. комплексный подход к защите информации;
3. применение высокоэффективных средств защиты информации;
4. подготовка специалистов соответствующей квалификации;
5. экономическая целесообразность.

Отличительной особенностью в деятельности образовательной организации является применение информационного ресурса и информационных систем для достижения целей обучения [1]. Можно предполагать, что несанкционированное

воздействие на информационные ресурсы и информационные системы приведет к снижению эффективности образовательного процесса, что вызывает необходимость создания системы технической защиты, соответствующей возможным угрозам.

К числу известных угроз информационной безопасности в образовательной организации необходимо учесть угрозу воздействия на информацию и информационные процессы со стороны обучаемых как умышленно, так и неумышленно [10].

Система защиты должна предусматривать защиту от физического доступа нарушителя к материальным носителям информационных ресурсов и к средствам ее обработки, так и защиту от несанкционированного доступа нарушителя по техническим каналам.

Основными методами защиты материальных носителей информационных ресурсов от физического доступа является:

1. организация пропускного режима в образовательной организации;

2. организация контролируемого доступа в здание (помещение), где располагаются носители информации и средства ее обработки;

3. организация защищенного хранения носителей информации;

4. обеспечение резервного копирования информационных ресурсов.

Тогда, основными средствами защиты будут:

1. инженерные заграждения (заборы, системы контроля и управления доступом);

2. система видеонаблюдения;

3. система охранной сигнализации;

4. средства контроля доступа в помещения;

5. средства инженерной укрепленности дверей и окон;

6. закрываемые металлические шкафы, сейфы.

Основными методами защиты информационных ресурсов от доступа по техническим каналам является:

1. локализация систем и средств обработки информации;

2. разграничение и контроль доступа лиц к информационных ресурсам и технологическим процессам;

3. управление информационными процессами в информационных системах;

4. применение защищенных линий и каналов связи, выходящих за пределы контролируемой зоны организации.

Основными средствами защиты от доступа нарушителя по техническим каналам является:

1. применение средств межсетевого экранирования;

2. применение средств разграничения доступа (СЗИ от НСД);

3. применение средств антивирусной защиты;

4. применение средств криптографической защиты информации.

Формирование системы технической защиты информации должно основываться на законодательстве Российской Федерации:

- законодательство об образовательной деятельности;

- законодательство о научной деятельности;

- законодательство об информации, информационных технологий и защите информации [2];

- законодательство о персональных данных [3];

- законодательства об информации ограниченного доступа и распространения;

- законодательство о техническом регулировании.

В информационном ресурсе образовательной организации можно выделить следующие категории информации, обрабатываемые техническими средствами и подлежащие защите:

- персональные данные обучающихся, работников, посетителей;

- структурированная учебная информация, обеспечивающая образовательный процесс, обрабатываемая техническими средствами;

- информация и информационные процессы, необходимые для функционирования образовательной организации.

- интеллектуальная собственность, ноу-хау.

Формирование системы технической защиты информации в образовательной организации должно осуществляться по следующим этапам:

1. анализ образовательных и управленческих процессов;
2. анализ информационных систем с учетом их предполагаемой модернизации [7].
3. моделирование угроз информационной безопасности;
4. моделирование и описание потенциальных возможных нарушителей и их действий;
5. проектирование системы технической защиты информации;
6. оценка эффективности спроектированной системы защиты информации как с учетом правовых и организационных мероприятий, так и без их учета;
7. приобретение и установка средств технической защиты информации и технических средств охраны;
8. подготовка персонала для эксплуатации системы технической защиты информации;
9. внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта.
10. тестирование и проведение оценки соответствия системы технической защиты информации требованиям по информационной безопасности;
11. ввод в эксплуатацию системы технической защиты информации;
12. техническое сопровождение функционирования системы технической защиты информации.

Будем считать, что $С_{уи}$ - система угроз информационной безопасности, а $С_{зи}$ - система технической защиты информации.

Тогда, последовательность действий по формированию системы защиты информации можно представить в виде упрощенного алгоритма (Рис. 1).

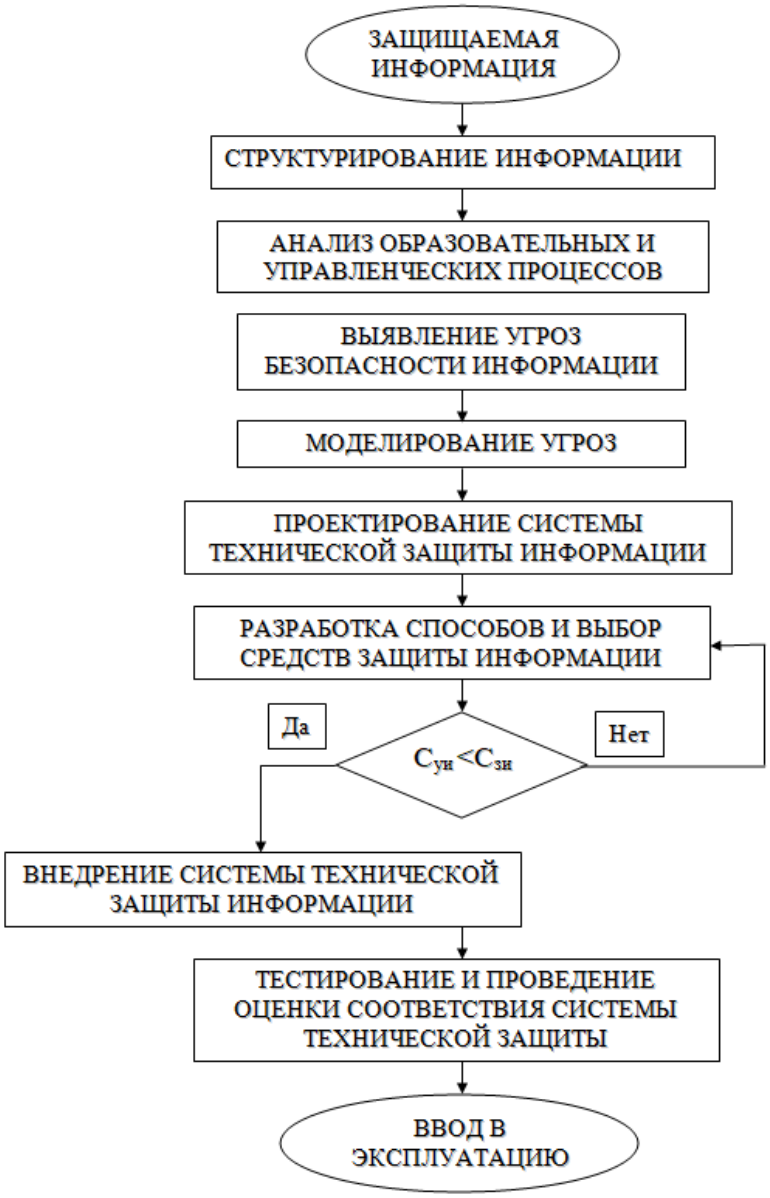


Рис. 1. Алгоритм последовательность действий по формированию системы технической защиты информации

Выводы:

При формировании технической защиты информации следует придерживаться определенных правил:

1. создание и эксплуатация системы защиты информации является сложным и ответственным процессом, поэтому необходимо систематически обучать персонал правилам работы со средствами защиты информации;
2. мероприятия по защите информации должны носить комплексный характер, то есть объединять правовые, организационные и технические мероприятия;
3. система технической защиты информации должна быть достаточной, надежной и эффективной, поэтому требуется оценивать экономическую целесообразность при ее формировании и проводить стоимостной анализ применения мер по защите информации;
4. в связи с тем, что угрозы безопасности информационных систем могут исходить от обучаемых, работников, посетителей как умышленно, так и не умышленно,

необходимо в целях снижения рисков реализации непреднамеренных угроз производить систематический контроль за действиями персонала и работоспособностью технических средств;

5. при оценке значимости информационных ресурсов и степени опасности угроз может применяться метод экспертных оценок.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон РФ от 29.12.2012 N 273-ФЗ «Об образовании Российской Федерации».
2. Федеральный закон РФ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон РФ от 27 июля 2006 г. N 152-ФЗ «О персональных данных».
4. ГОСТ Р 50922-2006 Защита информации ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.
5. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
6. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
7. Статья «Обобщенная модель информационной системы образовательной организации», Волостных В.А., Гвоздев Ю.В., Кононов П.А.В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сборник научных статей. Санкт-Петербург, 2020. С. 285-289.
8. Костарев С.В., Карганов В.В., Липатников В.А. Технологии защиты информации в условиях кибернетического противоборства: Науч. Монография/ Под общ.ред. В.А. Липатникова. – СПб.: ВАС, 2020, - 716 с.6 ил.
9. Жук А.П., Жук Е.П., Лепешкин О.М. и др. Защита информации. Учеб. Пособие – М. РИОР; ИНФРА-М, 2013. – 392 тс.
10. Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.
11. Информационная безопасность телекоммуникационных систем В.А. Липатников, В.А. Малютин, Ю.И. Стародубцев. СПб.: ВУС, 2002.-476с.

Алейников В.В.
РЭУ им. Г.В. Плеханова, доцент,
Aleynikov.VV@rea.ru
Бутенко А.А.
РЭУ им. Г.В. Плеханова, студент,
azrailovi@gmail.com

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С РАЗВИТИЕМ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Использование биометрии для удостоверения личности человека становится все более реальным. Российские банки уже 3 года широко используют биометрические данные своих клиентов для их аутентификации [1]. В октябре 2021 года ГУП Московский метрополитен запустило систему оплаты проезда по биометрии [2]. Биометрию используют вместо магнитных пропусков в школах [3] и на производстве [4]. С 2018 года в России действует Единая биометрическая система (ЕБС), которая агрегирует биометрические данные из разных организаций, составляя тем самым единое информационное пространство [5].

Сферы использования биометрии расширяются: ЕБС сообщает, что свои биометрические данные можно использовать вместо всех других документов для получения банковских, медицинских и образовательных услуг, для оплаты покупок, для удостоверения личности в государственных органах [6].

Биометрия становится актуальной и важной темой в России. Государство и частные компании работают над развитием и широким внедрением этой технологии. Аутентификация с использованием лица и голоса становится обычной практикой для все большего числа россиян – действующий профиль в ЕБС есть у 200 000 человек [7]. При этом возможностей применения этой технологии тоже становится все больше. Однако возрастает и количество угроз информационной безопасности, связанных с использованием биометрии.

Повсеместное внедрение и применение биометрии наравне с физическими документами имеет как свои преимущества, так и недостатки. Преимущества связаны с удобством использования и ускорением аутентификации человека в различных ситуациях. Недостатки – в части обеспечения информационной безопасности и соблюдения морально-этических норм.

В данной статье будут рассмотрены основные проблемы, которые могут возникнуть в связи с распространением и использованием биометрической аутентификации наравне с физическими документами. Будут сделаны предположения о том, с какими рисками придется столкнуться государству, бизнесу, обществу и отдельным людям в связи с широким применением биометрии в различных сферах жизни. Также будут предложены меры, которые помогут решить часть названных проблем.

Использование биометрических данных граждан России регулируется статьей 11 Федерального закона от 27.07.2006 N 152-ФЗ о персональных данных [8]. Согласно закону, биометрические данные – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются для установления личности. Биометрические данные

могут использоваться только с согласия их субъекта, за исключением случаев, описанных во второй части статьи 11 Федерального закона 152-ФЗ.

Единая биометрическая система хранит и обрабатывает биометрические данные россиян. Эта система создана Банком России совместно с ПАО Ростелеком. Компания имеет статус оператора Единой биометрической системы. Также к системе подключен ряд вендоров, которые распределенно аутентифицируют пользователей системы.

Основная проблема заключается в обеспечении должного уровня безопасности данных пользователей системы. Утечка биометрических данных граждан может привести к их несанкционированному и неконтролируемому использованию. При этом чем больше действий можно совершать с использованием биометрии, тем больше риски, которые она в себе несет.

Широкое применение биометрии ожидается не в ближайшее время, но в недалеком будущем. Вопрос информационной безопасности в будущем осложняется перспективой создания более продвинутых нейросетевых алгоритмов и более производительных компьютеров, в том числе квантовых [9]. Использование этих технологий может привести к тому, что современные алгоритмы шифрования и защиты данных будут легко взломаны. Таким образом, необходимо разрабатывать новые методы защиты данных, в том числе новые алгоритмы шифрования, которые будут устойчивы ко взлому с использованием новых технологий. Это позволит сохранить биометрические данные в безопасности.

Отдельную проблему составляет человеческий фактор. Оператор Единой биометрической системы и отдельные его сотрудники имеют доступ к биометрическим данным, находящимся в системе. В связи с этим возникает угроза использования этих данных в противоправных целях. Злоумышленники могут получить доступ к биометрическим данным в результате противоправных действий (например, подкупа или шантажа ответственных лиц). Таким образом, ответственные лица могут быть одним из источников утечек конфиденциальной информации. Это может привести к неблагоприятным последствиям как для отдельных лиц, чьи данные были украдены, так и для всего государства в целом – если утечка окажется масштабной.

Также стоит вопрос о том, как мошенники могут использовать биометрические данные человека. В настоящее время развивается технология дипфейков. Дипфейк – это видео, которое составлено искусственным интеллектом из нескольких фотографий человека, или аудиозапись, в которой синтезирован голос определенного человека. Чем больше исходных данных загружено в систему, тем более реалистичная запись получится в результате. Самые качественные дипфейки можно с трудом отличить от настоящих видео, снятых с реальными людьми [10]. Это может привести к распространению ошибок типа I в системах биометрического распознавания [11]. Такие ошибки называются «Ложное сходство». Ошибка типа I заключается в том, что система аутентификации принимает решение, что данные биометрические параметры принадлежат определенной личности, хотя это не так. Если мошенникам удастся создать дипфейк на основе открытых данных о человеке – его внешности и записях голоса, они смогут проходить удаленную аутентификацию за него, тем самым совершая действия от его лица. В таком случае биометрическая аутентификация с использованием лица и голоса станет менее надежной. Разработчикам биометрических систем аутентификации необходимо предусмотреть меры противодействия злоумышленникам, которые будут использовать дипфейки.

Эту проблему делает более острой перспектива создания биороботов. Если человечеству удастся создавать биороботов, наделенных способностями и внешностью настоящих людей, а также использующих искусственный интеллект, это даст возможность создавать копии людей. Если придать биороботу внешность определенного человека и наделить его голосом этого человека, он сможет проходить биометрическую аутентификацию вместо него. Это значит, что, по сути, человек и его копия, биоробот, смогут на равных правах участвовать во всех отношениях, требующих удостоверения личности.

При этом на данный момент неизвестно, возможен ли такой сценарий в принципе. Эксперименты по клонированию людей находятся под запретом. Но неизвестно, какой юридический статус получит создание биороботов, похожих на настоящих людей.

В случае, если биометрия станет обязательной, наравне с существующими документами, могут появиться те, кто будет против – люди, которые откажутся от сдачи и использования биометрических данных. Таких придется заставлять сдавать биометрические данные принудительно, или делать это без их ведома и согласия – например, фотографировать их при входе в транспорт или государственные учреждения, а записи голоса получать из разговоров по телефону. Альтернативный вариант – делать жизнь в обществе для таких людей невозможной, запрещать им оплачивать товары и услуги, пользоваться банками и транспортом, посещать больницы и государственные органы.

Подобная ситуация наблюдается сейчас с теми, кто по каким-либо причинам отказывается от вакцинации от Covid-19. Государства мира обязуют рестораны, музеи, театры, торговые центры, транспорт и другие общественные заведения проверять наличие сертификатов о прививке. В случае, если у посетителя такого сертификата нет, он не может воспользоваться необходимыми услугами: не попадет в ресторан, не сможет проехать на транспорте и т. п.

Из-за этого встает более глобальный вопрос за рамками информационной безопасности, вопрос скорее этический. Это вопрос о допустимости сегрегации, разделения людей на группы и придание этим группам разных прав. Если Конституция провозглашает всеобщее равенство перед законом, встает вопрос о допустимости создания условий, в которых у одних людей прав меньше, чем у других. В таких условиях граждане не будут допущены к получению определенных услуг по причине того, что они не выполнили требования, вмененные им в обязанность.

Кроме того, в контексте использования биометрии и сопряженного с ней обобществления персональных данных человека также встает вопрос о границе между частным и общественным. Непонятно, где именно находится эта граница. Неясно, как разделить пользу для государства и общества и интересы отдельных людей. Кажется, что каждый гражданин должен сам решать, до какой степени доверять государству и как много сообщать о себе. Вопрос в том, позволит ли это само государство.

Подключение большинства граждан к единой системе, которая содержит их биометрию, создаст возможность по отслеживанию действий, перемещений и социальных связей для государства и иных заинтересованных сторон. Если лицо человека есть в системе, государство может узнать его не только при обращении в государственные органы, но также на камерах для биометрической оплаты в транспорте и магазинах. Государство сможет отслеживать перемещение человека по городским камерам и его

покупкам, которые совершаются лицом. Государство будет знать обо всех сделках, которые совершает человек. И вместе с государством доступ ко всей этой информации могут получить злоумышленники, способные использовать ее в собственных корыстных целях. Например, они могут проходить аутентификацию под видом человека, чтобы анонимно совершать определенные действия от его лица. Или они могут продавать полученные данные другим заинтересованным лицам. Это не только повышает требования к обеспечению безопасности данных, но и может уменьшить доверие граждан своему государству.

Таким образом, широкое и повсеместное применение биометрических данных для аутентификации граждан имеет ряд рисков, проблем и вопросов. Тем не менее в будущем применение этой технологии может стать нормой и обыденной практикой. Для этого должен быть принят ряд мер, которые сделают технологию более легитимной и безопасной. В число таких мер входят:

- совершенствование законодательства в области сбора, обработки, хранения и применения биометрических данных граждан. Создание законодательной базы, которая будет эффективно регулировать все отношения в этой сфере;
- разработка и совершенствование способов защиты информации от утечек и взломов систем защиты информации [12];
- разработка методов противодействия фальсификации биометрических данных;
- предупреждение и оперативное противодействие утечкам данных. Разработка методов борьбы с противоправным использованием биометрических данных третьими лицами;
- разработка и внедрение системы хранения биометрических данных, которая позволит хранить их в обезличенном виде. Таким образом, чтобы администраторы системы и злоумышленники не могли получить доступ к данным конкретного человека;
- выбор или разработка подходящей архитектуры базы данных, которая будет выполнять две основные задачи: содержать большое количество записей с данными о всех зарегистрированных пользователях и обеспечивать быстрый доступ к нужным данным;
- выбор способа оценки точности и достоверности биометрической аутентификации: необходимо разработать систему показателей для оценки качества аутентификации и регулярно контролировать качество системы [13];
- выбор новых биометрических характеристик, более удобных в использовании и более сложных для фальсификации.

Хотя использование биометрической аутентификации и приносит определенную пользу как отдельным людям, так и бизнесу и государству, она не может непродуманно внедряться во все сферы жизнедеятельности общества. Специалисты в области информационных технологий, информационной безопасности, права, политики, нравственности и этики должны обсуждать перспективы применения биометрии и совместно с государством и обществом разрабатывать подходы к использованию этой технологии. Важно найти баланс между инновациями и безопасностью.

СПИСОК ЛИТЕРАТУРЫ

1. Биометрия в банках: что это, зачем и к чему приведет [Электронный ресурс]. — Режим доступа: trends.rbc.ru/trends/industry/5fd3ac6a9a79475333bfcb4f#card_5fd3ac6a9a79475333bfcb4f_2

2. Сегодня на всех станциях мосметро запустилась система оплаты проезда по биометрии [Электронный ресурс]. — Режим доступа: mosmetro.ru/news/detail/?news=802

3. Пропускную систему по лицам начали внедрять в школы Кузбасса [Электронный ресурс]. — Режим доступа: mk-kuzbass.ru/social/2021/11/16/propusknuyu-sistemu-po-licam-nachali-vnedryat-v-shkoly-kuzbassa.html?utm_source=yxnews&utm_medium=desktop

4. МТС внедрила биометрический контроль на складе ростовской компании RUNA TEX [Электронный ресурс]. — Режим доступа: expertsouth.ru/company_news/mts-vnedrila-biometricheskiy-kontrol-na-sklade-rostovskoy-kompanii-runa-tex-/?utm_source=yxnews&utm_medium=desktop

5. Единая биометрическая система [Электронный ресурс]. — Режим доступа: digital.gov.ru/ru/activity/directions/802/

6. О Единой биометрической системе [Электронный ресурс]. — Режим доступа: bio.rt.ru/about/

7. Россияне смогут оформить eSIM с помощью биометрии [Электронный ресурс]. — Режим доступа: vedomosti.ru/technology/articles/2021/06/02/872365-rossiyane-smogut-oformit-esim

8. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Статья 11. Биометрические персональные данные [Электронный ресурс]. — Режим доступа: consultant.ru/document/cons_doc_LAW_61801/7336c78762a98b5f4f698b8c3800dca1111acc16/

9. Ник Бостром. Искусственный интеллект / Ник Бостром – М.: Манн, Иванов и Фербер, 2016. – 496 с.

10. Дипфейк: что вы должны знать [Электронный ресурс]. — Режим доступа:forbes.com/sites/tomtaulli/2019/06/15/deepfake-what-you-need-to-know/?sh=38b3fb5c704d

11. Р. М. Болл. Руководство по Биометрии / Р.М. Болл, Дж.Х. Коннел, Ш. Панканти, Н.К. Ратха, Э.У. Сеньор – М.: Техносфера, 2007. – 368 с.

12. ГОСТ Р 54412 – 2011 «Информационные технологии – обучающая программа по биометрии».

13. А.М. Прудник. Биометрические методы защиты информации: учебно-методическое пособие / А.М. Прудник, Г.А. Власова, Я.В. Рощупкин. – Минск: БГУИР, 2014. – 123 с.

Щербина П.А.
ЮРГПУ (НПИ) им. М.И.Платова, студент
sherbina_pa@npi-tu.ru
Баранов В.В
ЮРГПУ (НПИ) им. М.И.Платова, заведующий кафедрой, к.в.н., доцент
baranov.vv.2015@yandex.ru
Корчагина А. П.
ЮРГПУ (НПИ) им. М.И.Платова, студент
Email: Korchagina.Annaa@yandex.ru
Игнатьев Д.Р.
ЮРГПУ (НПИ) им. М.И.Платова, студент

ПУТИ РЕШЕНИЯ ЗАДАЧ РАЗВЕРТЫВАНИЯ СИСТЕМ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Безопасность информации является крайне важным аспектом функционирования как государственных, так и коммерческих организаций. Ее защита становится неотъемлемой частью функционирования информационных систем, так как в случае несанкционированного доступа и (или) утечки информации по техническим каналам может быть нанесен ущерб конфиденциальности, целостности и доступности.

Для обеспечения качественного выполнения этой задачи система защиты информации должна быть непрерывной и комплексной. Это обстоятельство требует включения различных средств и комплексов, которые, действуя в совокупности, смогут осуществить наиболее полную защиту.

Следует отметить, что каждый компонент комплексной системы защиты информации выполняет строго определенные функции, в то время как специалист по безопасности должен оперативно и в полном объеме получать сведения об их состоянии, анализировать их и принимать своевременные и оптимальные решения по поддержании их в требуемом состоянии.

Иными словами, для обеспечения комплексной защиты необходимы не только разнотипные средства, позволяющие осуществить организационные, технические и иные меры защиты, но также и система, способная их интегрировать и обеспечить мониторинг событий информационной безопасности для поддержки принятия управленческих решений.

Впервые понятие «управление событиями информационной безопасности (SIEM, Security information and event management)» было введено в 2005 году Марком Николеттом и Амритом Вильямсом из компании Gartner [1]. Последующие исследования привели к разработке и активному использованию систем управления событиями информационной безопасности. Это позволило обеспечить анализ событий безопасности в режиме реального времени.

Системы безопасности информации и управления событиями сегодня стали важным компонентом всех корпоративных сетей. SIEM-системы способны в режиме реального времени вести постоянный мониторинг сети для обнаружения и предупреждения событий информационной безопасности. Основные роли SIEM-решения

должны выполнять отслеживание данные журнала, сбор и хранение их, анализ данных журнала, фильтрацию предупреждений и построение правил корреляции.

Совершенствование систем управления событиями информационной безопасности требует решения следующих задач:

1. Объединение и хранение журналов событий от различных источников [4]. Например, сетевых устройств, приложений, журналов ОС, средств защиты. Это позволяет специалистам в области информационной безопасности оперативно просматривать все события и отчеты по ним. Тем самым минимизируется время поиска необходимой информации и ускоряется процесс принятия решения.

2. Предоставление инструментов анализа событий и разбора инцидентов. Как правило, некоторые классы систем управления событиями информационной безопасности унифицируют события и делают их более информативными и удобными для восприятия. Интерфейс системы визуализирует важные информационные события.

3. Корреляция событий и их обработка по установленным правилам. Одно событие не дает полной информации об инциденте, но даже в таком случае в SIEM-системе представлены правила обработки, которые содержат набор условий, способы обработки поступающей информации и сообщения о детализации инцидента.

4. Автоматическое оповещение и возможность осуществлять управление инцидентами подразумевает под собой наличие своевременного оповещения о произошедшем событии.

Основными источниками исходных данных для системы управления событиями информационной безопасности являются записи журналов событий безопасности, также называемые логами [5]. Они отражают действия пользователей и программ, которые могут оказать влияние на безопасность. Из общего множества событий находятся и выделяются только такие, которые свидетельствуют об атаках или иных деструктивных действиях.

В процессе защиты информации SIEM-системы является универсальными и востребованными объектами, но для того, чтобы возложенные на них задачи успешно решались, необходимы достоверные источники и соответствующие правила корреляции событий. В этом случае любое событие будет адекватно проанализировано и идентифицировано.

Как и любая система защиты информации, система управления событиями информационной безопасности имеет специфические достоинства и недостатки.

Среди очевидных плюсов эксплуатации SIEM-системы следует назвать следующие: выявление сетевых атак, вирусных заражений, попытки несанкционированного доступа к конфиденциальной информации, ошибок, сбоев и т.д.; активное развитие и разнообразие продукта на рынке.

Любое приложение, сервер или база данных, ведут один или несколько журналов событий [3]. Средства и системы используют различные правила ведения логов, исходя из чего, возникает проблема сопряжения системы управления событиями информационной безопасности с разнородными средствами. Иными словами, не все средства и системы могут подключаться к SIEM-системам автоматически. Для некоторых из них, при условии того, что они несут важный информационный сигнал о состоянии безопасности системы, необходимо создание специализированного ПО.

В настоящее время данная проблема является крайне актуальной, так как применение информационных систем в жизнедеятельности компаний активно растет, тем самым увеличивается количество возможных уязвимостей сети, через которые могут быть совершены атаки на информационные ресурсы.

Ее решением может стать создание ПО, направленного на преобразование информации, содержащейся в журналах событий в вид, доступный для анализа системой управления событиями информационной безопасности. Для этого необходимо, чтобы программное обеспечение выполняло следующие функции:

- определяло, является ли тип анализируемого лога текстом;
- преобразовывало данные в формат syslog;
- разделяло лог на базовые элементы;
- экспортировало данные в SIEM-систему.

Работу алгоритма можно представить в виде следующей блок-схемы (Рис. 1). На начальном этапе необходимо выбрать файл, который будет преобразован в формат syslog. Если файл является текстовым, то необходимо осуществить разделение данных и преобразовать его в требуемый формат. Если файл не является текстовым, то его необходимо сначала преобразовать. На следующем этапе выявляются элементы набора и затем выбирается текущий лог, выполняется проверка возможности его разделения на базовые элементы.

Если лог не может быть разделён на базовые элементы, то выполняется полная обработка. Если может, то сначала выполняется его разделение, а затем – обработка частей. Когда все фрагменты обработаны, производится экспорт данных в систему управления событиями информационной безопасности.

Для быстрого поиска необходимой информации в текстовом файле можно применить распределенные системы индексирования, например, такие как **ElasticSearch.**

Для анализа информации можно применить **Apache HBase,** обеспечивающий упорядочивание и агрегацию (суммирование) больших массивов данных. Стоит отметить, что при увеличении объемов и количества логов такие системы перестают справляться с задачей быстрой агрегации. В этих случаях наилучшим решением будет применение систем, использующих параллельную обработку данных, например, таких как **Apache Hadoop**. При этом существенным недостатком последнего является то, что он не обеспечивает доступ к чтению и записи в режиме реального времени.

Результатом подключения разнотипных средств и систем к системе управления событиями информационной безопасности станет не только увеличение выявляемости событий информационной безопасности, но и уменьшение времени, необходимого на соответствующее реагирование, улучшение качества расследований по произошедшим событиям и возможность их анализа как в режиме реального времени, так и в выбранном временном промежутке.

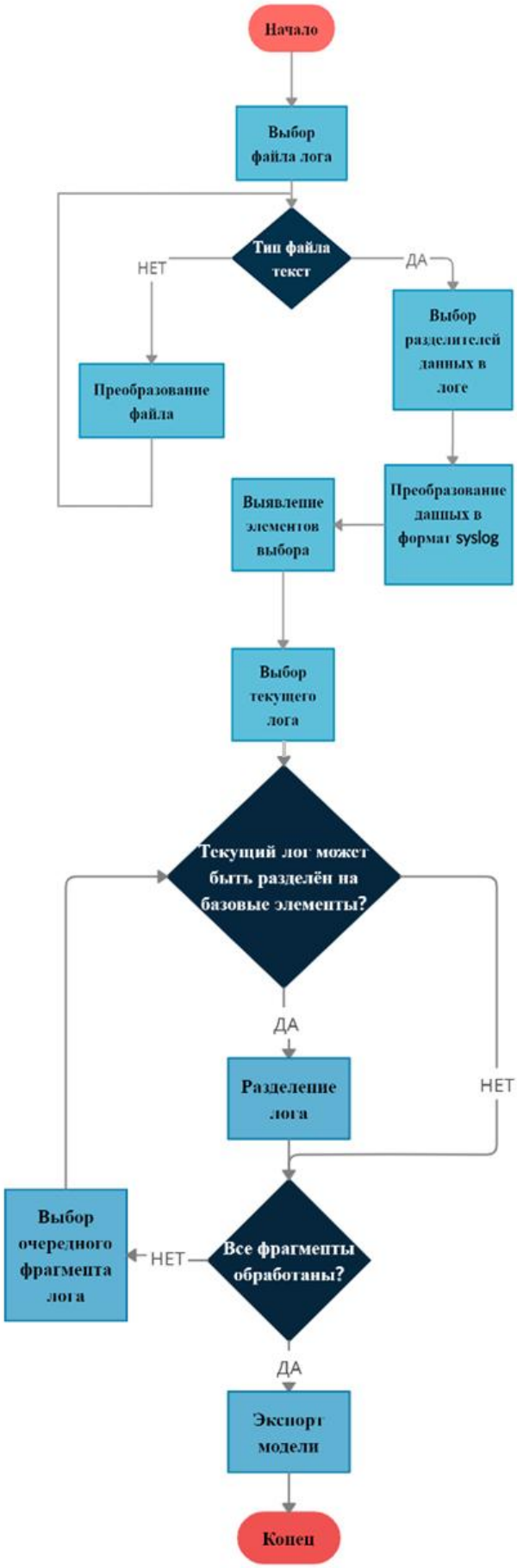


Рис. 1. Алгоритм работы программы сопряжения лога

СПИСОК ЛИТЕРАТУРЫ

1. Грибунин В.Г. Комплексная система защита информации на предприятии : учеб. Пособие для студ. Высш. Учеб. Заведений / В.Г. Грибунин, В.В. Чудовский. - М. : Издательский центр «Академия», 2009. - 416 с. ISBN 978-5-7695-5448-3.

2. Гришина Н. В., Комплексная система защиты информации на предприятии, Издательство: Форум, 2010 г., 240 стр.

3. Сердюк В. А., Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий, Издательство: Высшая Школа Экономики (Государственный Университет), 2011 г., 576 стр.

4. Мелехин И. Управление инцидентами безопасности. / Сетевые решения. М.: 2006. - №12. [Электронный ресурс]. - Режим доступа: http://www.nestor.minsk.by/sr/2006/12/sr61209.html

5. Шаньгин В. Ф., Комплексная защита информации в корпоративных системах, Издательство: Форум, Инфра-М, 2010 г., 592 стр.

Головлев М.О.
ЮУрГУ, студент,
golowlev.maksim@yandex.ru
Рагозин А.Н.
ЮУрГУ, к.т.н., доцент,
ragozinan@susu.ru

ИДЕНТИФИКАЦИЯ ВИДОВ МОДУЛЯЦИИ СИГНАЛОВ В КАНАЛАХ СВЯЗИ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ С ИСПОЛЬЗОВАНИЕМ САМООРГАНИЗУЮЩИХСЯ ИССКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

При взаимодействии с большими объемами массивов данных возникают задачи, связанные с исследованием структуры данных, объединением их в группы (кластеры), распределением по классам. Такие задачи могут быть успешно решены с применением самоорганизующихся искусственных нейронных сетей (ИНС), впервые описанных финским ученым Кохоненом [1]. Важным приложением самоорганизующихся ИНС в области инженерно-технической защиты информации является идентификация видов модуляции сигналов в каналах связи, например, для решения задач радиоразведки и реализации систем перехвата данных, передаваемых по радиоканалам систем телекоммуникаций.

Самоорганизующиеся ИНС (сети Кохонена) — специальный класс ИНС, основанный на обучении без учителя (то есть, результат обучения зависит только от структуры входных данных). Нейроны данного класса сетей обучаются выявлению групп (кластеров) векторов входа, обладающих некоторыми общими свойствами [2–3]. При этом, разбиение объектов по кластерам осуществляется при одновременном формировании самих кластеров.

Дополнительно, самоорганизующиеся ИНС разделяются на два подкласса: сети с неупорядоченными нейронами (слои Кохонена) и сети с упорядоченными нейронами (карты Кохонена).

Общая структура слоя Кохонена [4] характеризуется наличием совокупности нейронов, являющихся адаптивными линейными взвешенными сумматорами, и конкурирующей функции активации. Каждый нейрон такого слоя соединен со всеми компонентами n-мерного входного вектора. С выхода нейронов (адаптивных сумматоров) сигнал поступает на активационную функцию, работающую по принципу WTA (Winner Takes All — победитель получает все). Задача активационной функция состоит в нахождении номера нейрона с максимальным значением выхода, что задает ту группу (кластер), к которой наиболее близок поступивший входной вектор.

Соответственно, процесс обучения слоя Кохонена [5–6] можно охарактеризовать как применение специальных обучающих алгоритмов для подбора значений весов нейронов (адаптивных сумматоров), минимизирующих ошибки от замены близких в смысле используемой метрики входных векторов вектором весов. В наиболее простом случае в ходе обучения слоя Кохонена циклически происходит подача исходных данных (случайного вектора из всего объема векторов, предусмотренных для обучения) на входы, определяется нейрон-победитель и выполняется корректировка текущих весов «выигравшего» нейрона по правилу Кохонена. По достижению максимального количества

циклов обучения ИНС готова к работе для последующей кластеризации новых входных данных (векторов).

Модуляцией называется процесс управления одним или несколькими параметрами колебаний высокой частоты в соответствии с законом передаваемого сообщения [7–8].

В результате модуляции спектр информационного сигнала переносится из области низких частот на частоту несущего колебания в область высоких частот [9].

В зависимости от того, какой параметр несущего колебания изменяется при модуляции, выделяют амплитудную, частотную и фазовую модуляции.

Амплитудная модуляция (АМ) — вид модуляции, при которой по закону модулирующего сигнала изменяется амплитуда несущего колебания (1):

$$\begin{aligned} u_{AM}(t) &= U_0\left[1+k_{AM}E_m\cos\left(\Omega_m t+\theta_m\right)\right]\cos(\omega_0 t+\varphi_0) = \\ &= U_0\left[1+M\cos\left(\Omega_m t+\theta_m\right)\right]\cos(\omega_0 t+\varphi_0) \end{aligned}, \quad (1)$$

где E_m, U_0 – амплитуды модулирующего и несущего колебаний, В;

k_{AM} – коэффициент пропорциональности;

M – коэффициент (глубина) амплитудной модуляции;

Ω_m, ω_0 – частоты модулирующего и несущего колебаний, рад/с;

θ_m, φ_0 – начальные фазы модулирующего и несущего колебаний, рад.

При частотной модуляции (ЧМ), по закону модулирующего сигнала изменяется мгновенная частота несущего колебания (2):

$$\begin{aligned} u_{ЧМ}(t) &= U_0\cos(\omega_0 t+k_{ЧМ}E_m\int_{-\infty}^{t}\cos\left(\Omega_m t+\theta_m\right)dt+\varphi_0) = \\ &= U_0\cos\left(\omega_0 t+m_{ЧМ}\sin\left(\Omega_m t+\theta_m\right)+\varphi_0\right) \end{aligned}, \quad (2)$$

где E_m, U_0 – амплитуды модулирующего и несущего колебаний, В;

$k_{ЧМ}$ – коэффициент пропорциональности между частотой и напряжением;

$m_{ЧМ}$ – индекс частотной модуляции;

Ω_m, ω_0 – частоты модулирующего и несущего колебаний, рад/с;

θ_m, φ_0 – начальные фазы модулирующего и несущего колебаний, рад.

Фазовая модуляция — вид модуляции, при которой по закону модулирующего сигнала изменяется полная фаза несущего колебания (3):

$$\begin{aligned} u_{ФМ}(t) &= U_0\cos\left(\omega_0 t+k_{ФМ}E_m\cos\left(\Omega_m t+\theta_m\right)+\varphi_0\right) = \\ &= U_0\cos\left(\omega_0 t+m_{ФМ}\cos\left(\Omega_m t+\theta_m\right)+\varphi_0\right) \end{aligned}, \quad (3)$$

где E_m, U_0 – амплитуды модулирующего и несущего колебаний, В;

$k_{ФМ}$ – коэффициент пропорциональности между фазой и напряжением;

$m_{ФМ}$ – индекс фазовой модуляции;

Ω_m, ω_0 – частоты модулирующего и несущего колебаний, рад/с;

θ_m, φ_0 – начальные фазы модулирующего и несущего колебаний, рад.

Ставится задача обучения самоорганизующейся ИНС для идентификации типа модуляции модулированного сигнала, передаваемому по радиоканалу системы связи.

Для реализации поставленной задачи в процессе моделирования используется подсистема приложения MATLAB для тестирования ИНС Neural Network Toolbox (NNT) [10–11].

Рассмотрим сигнал с тональной модуляцией: гармонический несущий сигнал с частотой f_0 = 10 кГц, амплитудой U_0 = 1 В и нулевой начальной фазой и гармонический модулирующий сигнал с частотой f_m = 1 кГц, амплитудой E_m = 1 В и нулевой начальной фазой. Параметры модуляции выбраны следующими: M = 0,5, $m_{ЧМ} = m_{ФМ}$ = 5. Стоит отметить, что в действительности может использоваться любой набор базовых сигналов с произвольными параметрами модуляции.

Используется однослойная самоорганизующаяся ИНС (слой Кохонена). Для обучения ИНС формируется массив из 150 сигналов, в массиве сигналов равномерно распределены идентифицируемые виды модуляции. При формировании каждого сигнала из массива сигналов производится отклонение частот несущего и модулирующего гармонических сигналов в пределах 5% от их начальных значений, также реализуется зашумление сигналов. В этом случае, выборка сигналов для обучения становится максимально приближенной к реальным условиям работы системы, что обеспечивает корректность работы ИНС при идентификации вида модуляции сигналов. Для обучения ИНС устанавливается параметр – 3000 циклов. Размерность каждого сигнала в массиве – 1001 отсчет. Примеры сигналов, содержащихся в выборке для обучения ИНС, сопоставленные с модулирующим сигналом (рис. 1):

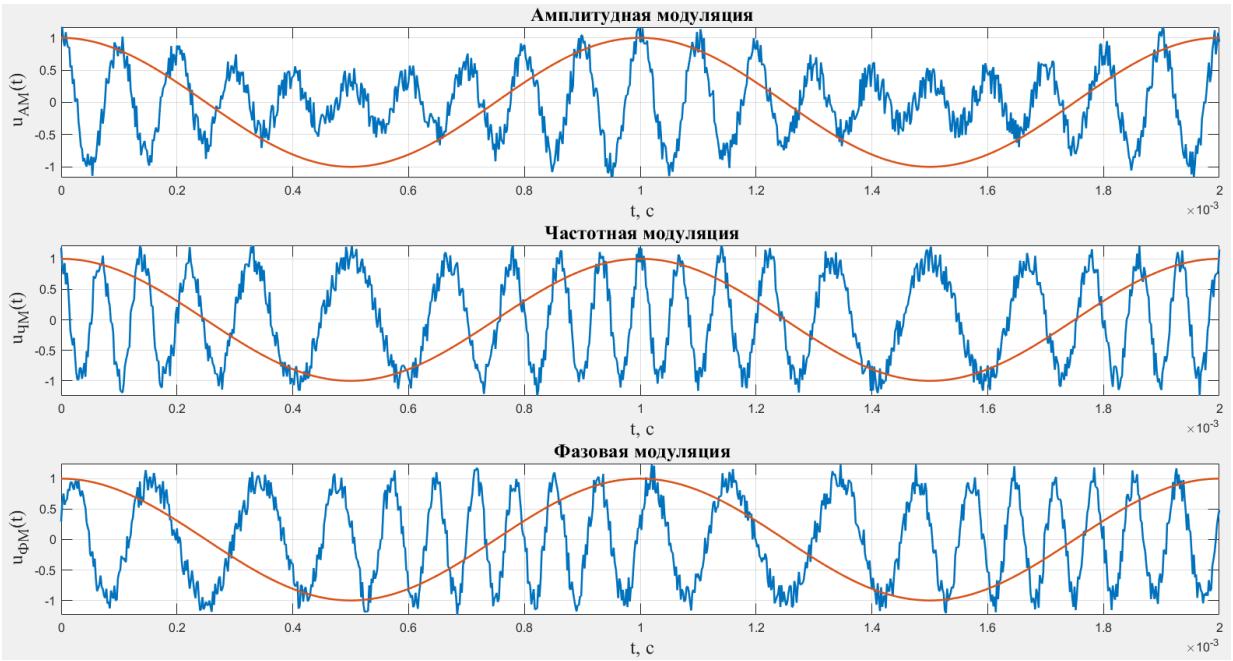


Рис. 1. Сигналы для обучения ИНС

По окончании обучения самоорганизующаяся ИНС формирует вокруг каждого нейрона в слое свой кластер (порядковый номер нейрона соответствует порядковому

номеру кластера), ответственный за идентификацию определенного вида модуляции. При этом весовые коэффициенты каждого из обученных нейронов сформированы следующим образом (рис. 2):

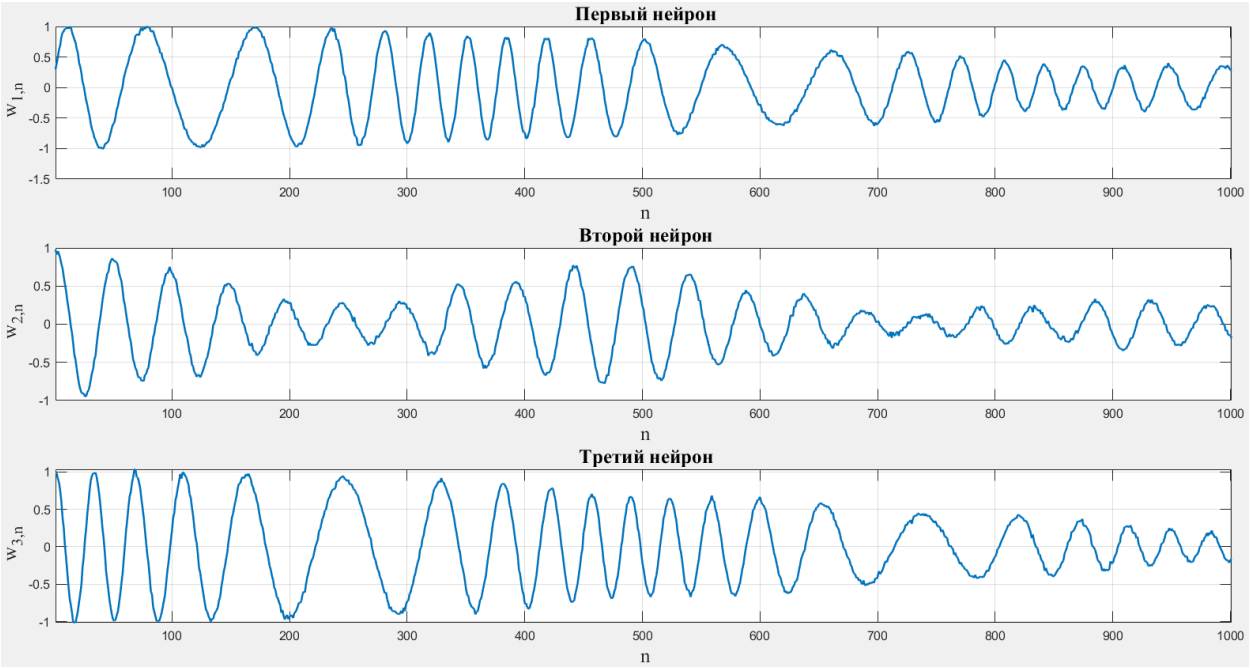


Рис. 2. Весовые коэффициенты обученных нейронов слоя Кохонена

Из рис. 2 при сопоставлении с рис. 1 видно, что первый нейрон в слое Кохонена идентифицирует фазовую модуляцию (то есть, сигналы с данным видом модуляции будут отнесены к первому кластеру), второй нейрон распознает амплитудную модуляцию (то есть, сигналы с данным видом модуляции будут отнесены ко второму кластеру), а третий нейрон определяет частотную модуляцию (то есть, сигналы с данным видом модуляции будут отнесены к третьему кластеру).

Первоначальный массив модулированных сигналов (векторов) для обучения ИНС отображен на рис. 3.

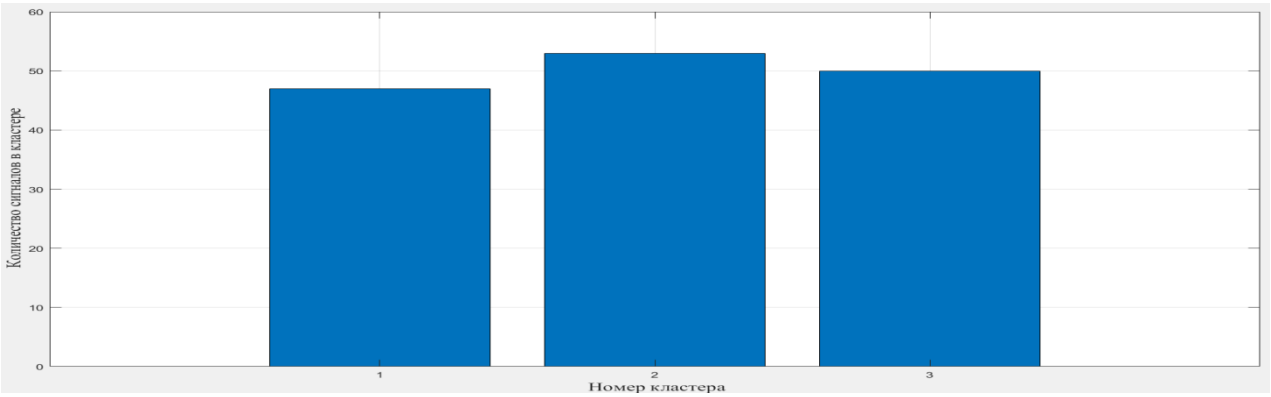


Рис. 3. Распределения модулированных сигналов обучения ИНС по кластерам

Таким образом, в каждый кластер помещено практически одинаковое число сигналов (векторов) из выборки. Это значит, нейронная сеть работает корректно и подготовлена к кластеризации новых входных векторов.

Произведем тестирование работы ИНС для следующих условных входных сигналов:

$$u_{AM}(t) = \left[1 + 0{,}55\cos\left(2\pi \cdot 1{,}1 \cdot 10^3 t\right)\right]\cos(10{,}4 \cdot 10^3 t);$$

$$u_{ЧМ}(t) = \cos\left(10{,}1 \cdot 10^3 t + 4{,}5\sin\left(2\pi \cdot 1{,}05 \cdot 10^3 t\right)\right);$$

$$u_{ФМ}(t) = \cos\left(9{,}8 \cdot 10^3 t + 5{,}2\cos\left(2\pi \cdot 0{,}95 \cdot 10^3 t\right)\right).$$

Каждый из этих сигналов реализует свой вид модуляции.

Сигнал с однотональной амплитудной модуляцией, во временной области имеющий вид, показанный на рис. 4 (с учетом нормировки по амплитуде), относится обученной нейронной сетью к кластеру № 2:

A = vec2ind(sim(net,p))

A = 2.

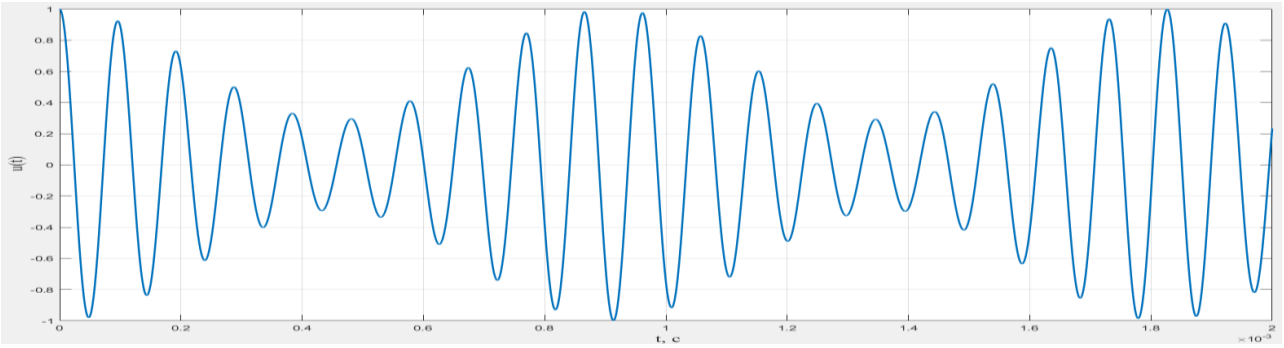


Рис. 4. Тестовый входной сигнал с однотональной амплитудной модуляцией

Сигнал с однотональной частотной модуляцией, во временной области имеющий вид, представленный на рис. 5, относится обученной нейронной сеть к кластеру № 3:

A = vec2ind(sim(net,p))

A = 3.

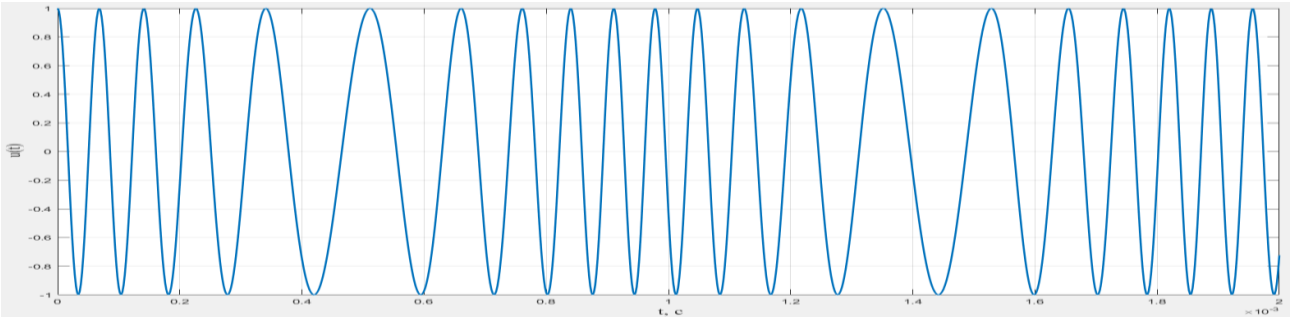


Рис. 5. Тестовый входной сигнал с однотональной частотной модуляцией

Сигнал с однотональной фазовой модуляцией, во временной области имеющий вид, показанный на рис. 6, относится обученной нейронной сеть к кластеру № 1:

A = vec2ind(sim(net,p))

A = 1.

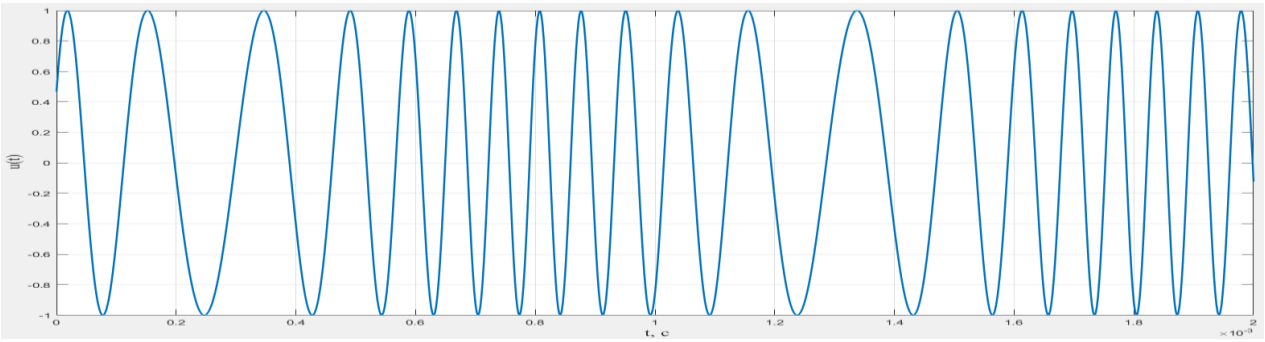


Рис. 6. Тестовый входной сигнал с однотональной фазовой модуляцией

В проведённом исследовании показано, что с использованием самоорганизующихся ИНС возможна успешная идентификация типов модуляции сигналов, передаваемых по каналам связи систем телекоммуникаций, что важно при решении задач инженерно-технической защиты информации, перехвата сигналов и радиоразведки.

СПИСОК ЛИТЕРАТУРЫ

1. Кохонен, Т. Самоорганизующиеся карты / Т. Кохонен; пер. В.Н. Агеева. — М.: БИНОМ. Лаборатория знаний, 2008. — 655 с.
2. Осовский, С. Нейронные сети для обработки информации / С. Осовский; пер. И.Д. Рудинского. — М.: Финансы и статистика, 2002. — 344 с.
3. Хайкин, С. Нейронные сети: полный курс / С. Хайкин; пер. Н.Н. Куссуль, А.Ю. Шелестова. — М.: Вильямс, 2006. — 1104 с.
4. Бодянский, Е.В. Искусственные нейронные сети: архитектуры, обучение, применения / Е.В. Бодянский, О.Г. Руденко. — Харьков: ТЕЛЕТЕХ, 2004. — 369 с.
5. Круглов, В.В. Искусственные нейронные сети. Теория и практика / В.В. Круглов, В.В. Борисов. — М.: Горячая линия – Телеком, 2002. — 382 с.
6. Каллан, Р. Основные концепции нейронных сетей / Р. Каллан; пер. А.Г. Сивака. — М.: Вильямс, 2001. — 287 с.
7. Баскаков, С.И. Радиотехнические цепи и сигналы / С.И. Баскаков. — М.: Высшая школа, 2005. — 462 с.
8. Нефедов, В.И. Основы радиоэлектроники и связи / В.И. Нефедов, А.С. Сигов; под ред. В.И. Нефедова. — М.: Высшая школа, 2009. — 735 с.
9. Гоноровский, И.С. Радиотехнические цепи и сигналы / И.С. Гоноровский, М.П. Демин. — М.: Радио и связь, 1994. — 512 с.
10. Медведев, В.С. Нейронные сети. MATLAB 6 / В.С. Медведев, В.Г. Потемкин; под ред. В.Г. Потемкина. — М.: ДИАЛОГ-МИФИ, 2002. — 496 с.
11. Николаева, С.Г. Нейронные сети. Реализация в Matlab: учеб. пособие / С.Г. Николаева. — Казань: Казан. гос. энерг. ун-т, 2015. — 92 с.

Дахнович А.Д.
СПбПУ, старший преподаватель,
add@ibks.spbstu.ru

ПЛАТФОРМА ЗАЩИЩЕННОГО ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Промышленный Интернет Вещей (ИВ) – это расширение применения технологий Интернета Вещей с уклоном в промышленные процессы. Концепция ИВ сама по себе не нова и давно применяется для автоматизации бытовых задач. Основной спецификой ИВ является то, информационные процессы влияют на физическое состояние системы. Таким образом, появляется задача обеспечения безопасности киберфизических систем (КФС). Однако применение ИВ на таких объектах, как критических информационных инфраструктура (КИИ), с точки зрения обеспечения кибербезопасности приобретает новый характер с точки зрения критичности, так как компрометация одного из компонент может привести к катастрофическим последствиям.

Цифровое производство (ЦП) – это основной «потребитель» технологий промышленного ИВ, так как промышленность больше всего заинтересована в минимизации затрат на производство. Термин «Цифровое производство» (ЦП) пока не имеет устоявшегося определения, но в большинстве случаев означает применение ИТ-технологий в производстве [4].

Новые заводы появились благодаря изменению цепи постав: цифровые сети поставок. Раньше все производство было линейно: проектирование – планирование – покупка ресурсов – производство – доставка – поддержка. Теперь все общаются друг с другом. Все ради уменьшения задержек между спросом и предложением (Рис. 1).

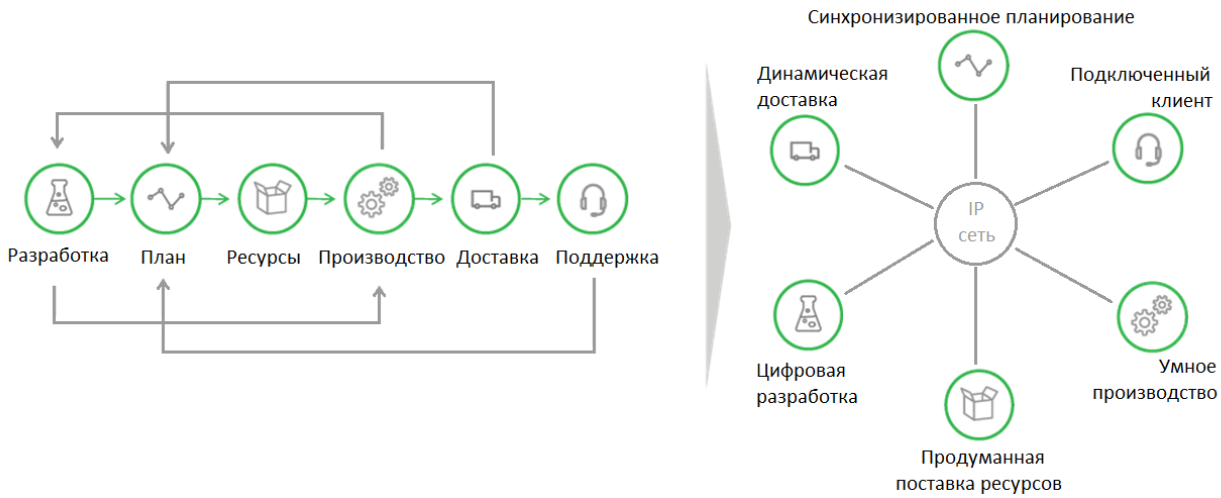


Рис. 1. Схематичная трансформация в сеть цифрового производства

МОДЕЛЬ УГРОЗ

На первом этапе разработки модели угроз необходимо составить список активов платформы промышленного ИВ, которые могут быть подвержены угрозам и требуют защиты.

Основными сегментами платформы промышленного ИВ являются:

1. Сегмент конечных устройств ИВ: датчики, исполнительные механизмы, сетевые шлюзы (ранее называемые программируемыми логическими контроллерами,

ПЛК). В соответствии с номенклатурой консорциума IIC назовем данный сегмент Edge Tier.

2. Сегмент сетевых каналов связи.

3. Сегмент управления промышленным ИВ: серверы обработки данных; серверы хранилищ данных; внешние сервисы и программные интерфейсы; серверы разработчиков программного обеспечения. В соответствии с номенклатурой консорциума IIC назовем данный сегмент Platform Tier.

Данные сегменты представляют из себя единую платформу промышленного ИВ (Рис. 2).

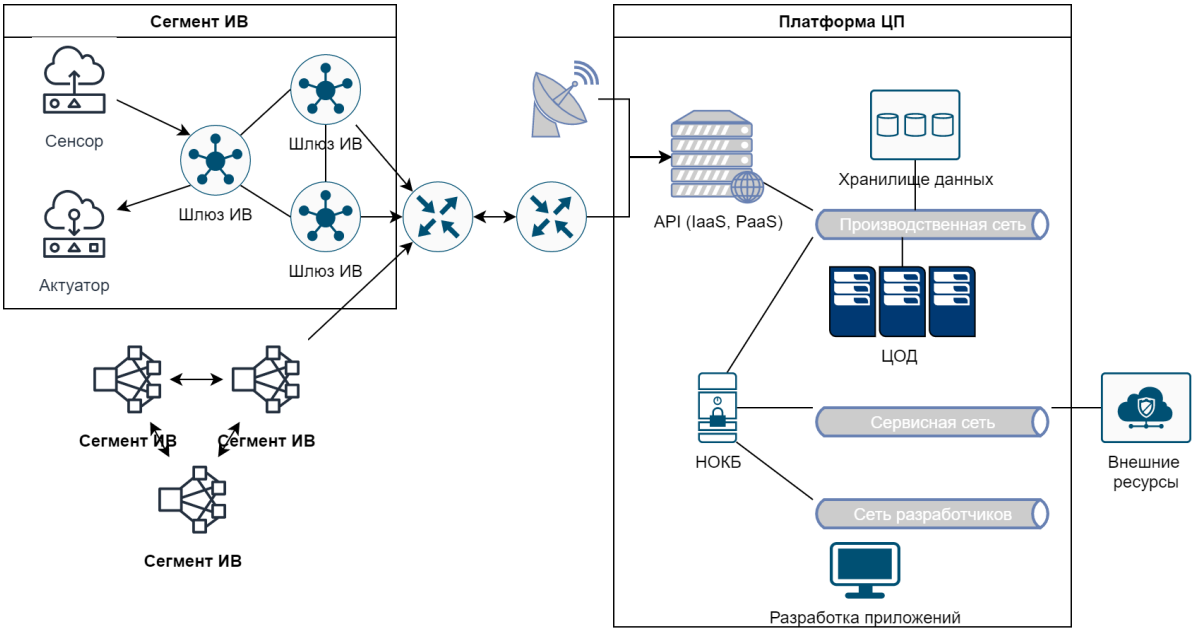


Рис. 2. Типовая архитектура платформы промышленного ИВ

В таблице 1 представлена соответствующий перечень угроз.

Удобно разбить угрозы на следующие классы:

1. Компрометация системы – угрозы 1-6
2. Перехват и прослушка – угрозы 7-9
3. Отказ работы – угрозы 10-13
4. Физическое воздействие – угроза 14.

Модель угроз информационной безопасности представлена на рис. 3.

Оперативный. Выявление кибератак и обеспечение устойчивости к киберугрозам.

Тактический. Регулярное экспериментальное тестирование киберзащищенности, предназначенное для оценки и анализа текущего состояния кибербезопасности объектов Цифрового Производства и выработки рекомендаций по усилению киберзащиты на тактическом уровне

Стратегический. Имитационное моделирование, позволяющее проигрывать сценарии кибератак и стратегии защиты от них для выбора наиболее эффективной

Табл. 1. Актуальные угрозы кибербезопасности промышленного Интернета Вещей

ID угрозы	Наименование угрозы	Описание угрозы
У-1	Вредоносное ПО	ПО, спроектированное с целью получения несанкционированного доступа к системе, причинения ущерба отдельному устройству, нарушения технологического процесса или кражи информации.
У-2	Уязвимости в ПО	Программные компоненты, работающие в производственых системах, имеют собственные уязвимости и/или неправильные конфигурации, ведущие к несанкционированному доступу.
У-3	Целенаправленные атаки	Многоступенчатая атака с целью получения доступа к конфиденциальной информации, управлению устройствами и (или) выводу их из строя. Атака может быть краткосрочной или долгосрочной
У-4	Внедрение поддельных устройств	Внедрение на предприятие устройств, визуально и (или) технически повторяющее оригинал, но при этом обладающее программно-аппаратными закладками, позволяющими злоумышленнику осуществлять воздействие на объекты системы предприятия, что зачастую используется при проведении атак
У-5	Отказ в обслуживании (DoS/DDoS)	Атака на компоненты, устройства и каналы связи с целью вывода их из строя.
У-6	Модификация информации	Модификация информации, обрабатываемой компонентами системы, с целью влияния на производственные процессы.
У-7	Разведка сети предприятия	Пассивный сбор информации, характеризующей информационную сеть предприятия, выявление ее проргаммных и аппаратных компонентов
У-8	Перехват данных	Скрытый перехват и модификация данных, передаваемых по внешним и внутренним каналам связи, вызывающий утечку конфиденциальной информации.
У-9	Повтор или задержка передаваемых по сети сообщений	Повторная отправка данных между компонентами с целью влияния на производственные процессы или выводу компонентов из строя.
У-10	Отказ работы сети	Различные прерывания передачи данных, зависящие от среды (проводная, беспроводная) и технологий передачи данных.
У-11	Отказ устройств	Работа устройств неожиданно завершается в результате проявления непредвиденной ошибки в аппаратных компонентах или перебоях электросети
У-12	Отказ систем	Работа программных компонентов неожиданно завершается по причине ошибки на уровне сервисов и приложений.
У-13	Отказ сторонних систем	Сторонние сервисы, участвующие в процессе производства, становятся недоступны на неопределенное время.
У-14	Физическое воздействие	Вывод из строя или подмена устройств, отвечающих за контроль физических процессов.

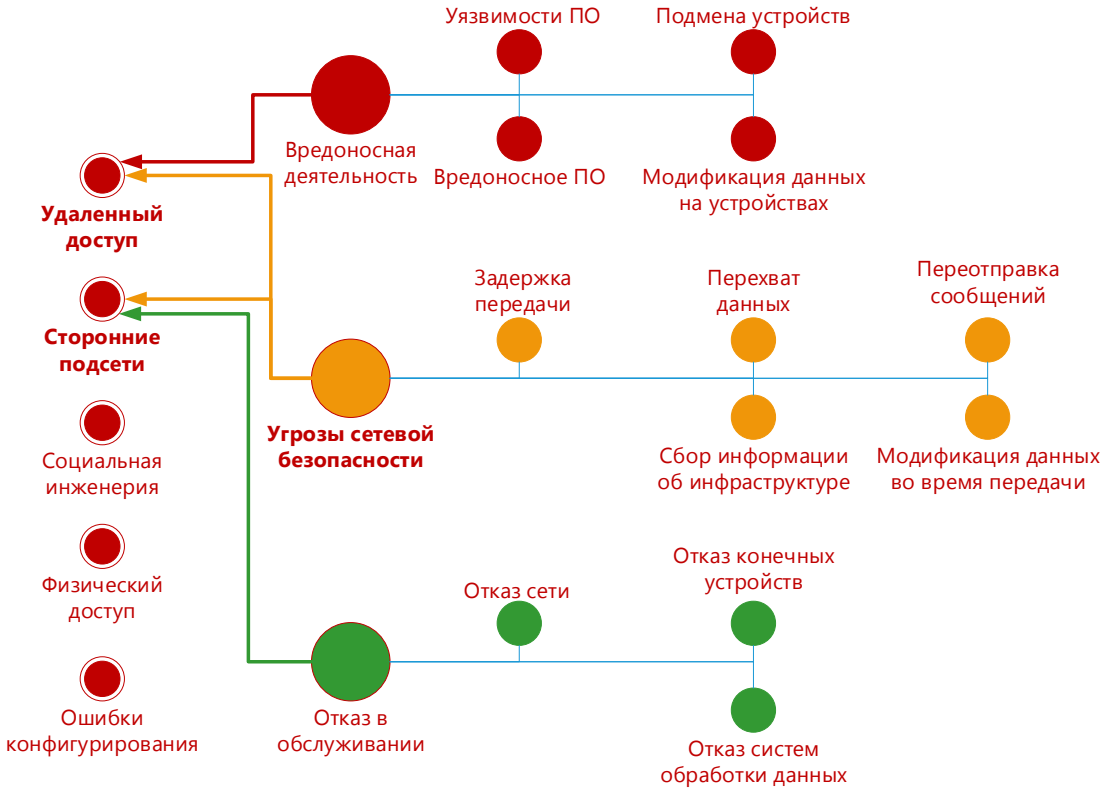


Рис. 3. Категории киберугроз промышленного Интернета Вещей

Для реализации киберзащиты на всех трех перечисленных уровнях жизненный цикл процесса обеспечения кибербезопасности Цифрового Производства включает пять основных этапов, которые выполняются циклически (рис. 4**Ошибка! Источник ссылки не найден.**).

Рис. 4. Жизненный цикл обеспечения кибербезопасности

Выполнение цикла обеспечения кибербезопасности обеспечивается работой трех подсистем, работающих параллельно и направленных в конечном итоге на выработку рекомендаций по усилению защиты для противодействия угрозам кибербезопасности.

Для обеспечения кибербезопасности промышленного ИВ предлагается следующая стратегия применения данных систем защиты (рис. 5):

1. Применение статических средств защиты для обеспечения кибербезопасности промышленного ИВ от конечного набора угроз.
2. Построение отказоустойчивой и защищенной архитектуры промышленного ИВ.
3. Применение активных, адаптивных и динамических средств защиты для внесения изменений в статические средства защиты и архитектуру, а также анализа перспективных угроз.

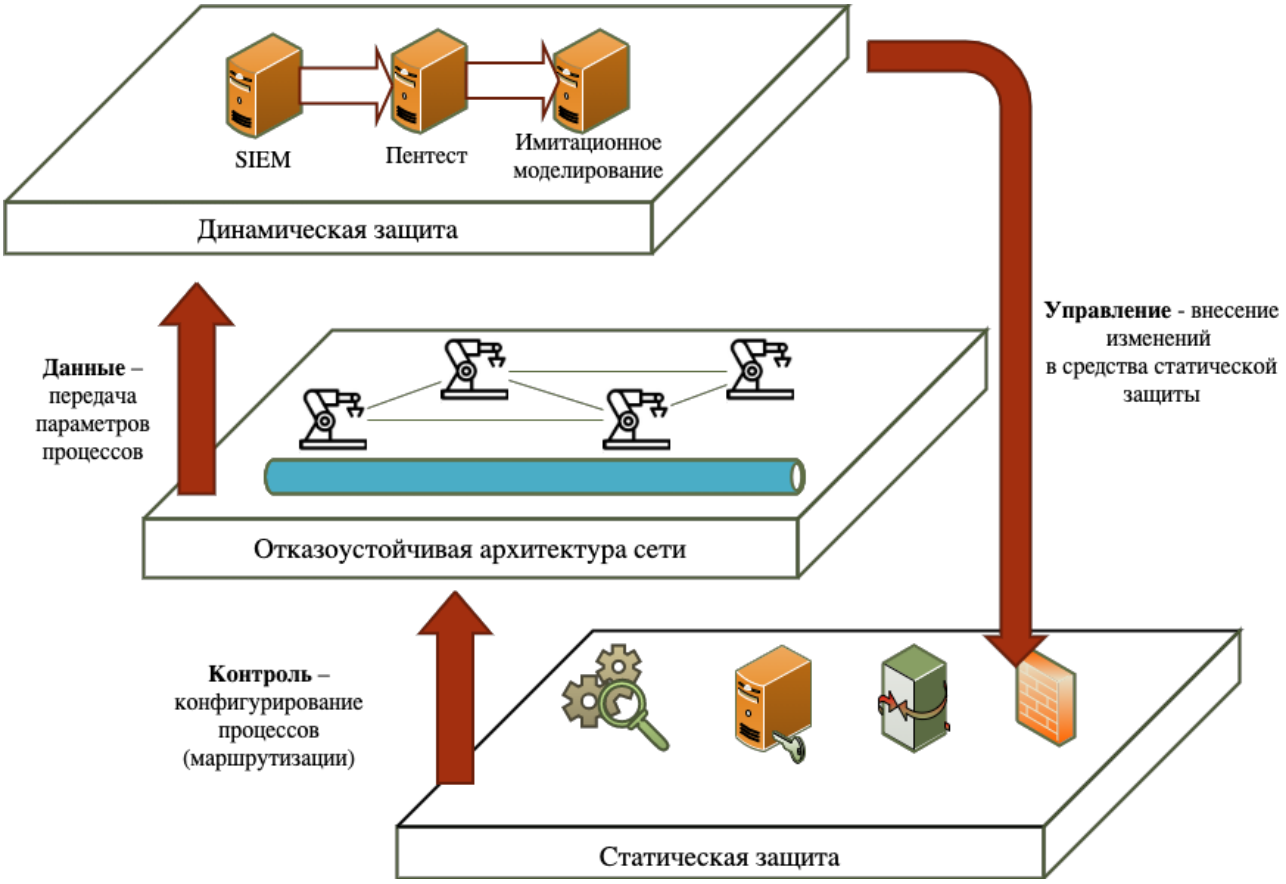


Рис. 5. Архитектура платформы защищенного промышленного Интернета Вещей

Подсистема выявления кибератак и обеспечения устойчивости состоит из трех отдельных комплексов:

система обработки и преобразования данных;

система обнаружения аномалий;

система оценки киберустойчивости.

Сегмент ИВ состоит из различных датчиков и исполнительных механизмов, которые используются для автоматизации производственного процесса с помощью контрольных команд от платформы ЦП. Данные устройства в ЦП образуют сегменты промышленного ИВ или IIoT, где устройства взаимодействуют друг с другом при помощи протоколов уровня TCP/IP. Для обеспечения устойчивой архитектуры сегмента ИВ

предлается применить механизм чесночной маршрутизации. Данный подход удовлетворяет требования как ИБ, так и ФБ.

Свое основное применение принципы чесночной маршрутизации получили в построении сети I2P. Данная сеть является оверлейной, то есть работает поверх сети Интернет, и изначально создавалась для обеспечения анонимности как клиентов, так и серверов. Для обеспечения безопасности в данной сети применяются следующие меры:

1. Применение криптографии с открытым ключом для шифрования данных и подписи информации об узле (у каждого участника создаются две пары открытых и закрытых ключей).
2. Применение многослойного лукового шифрования при построении исходящих и входящих тоннелей I2P, в котором каждый узел в цепи передачи расшифровывает только свой «слой».
3. Использование различных каналов для входящих и исходящих туннелей при уведомлении о статусе успешной или неуспешной доставки сообщения. Данные туннели имеют ограниченный срок жизни.
4. Упаковка множества сообщений («чесночин») в одно-единственное «чесночное» сообщение, передаваемое по туннелям между узлами.

Для обеспечения безопасного взаимодействия сегментов сети цифрового производства предприятия важны принципы чесночной маршрутизации, перечисленные в таблице 2 и задачи безопасности, которые они позволяют решить.

Табл. 2. Применение принципов чесночной маршрутизации для решения задач безопасности цифрового производства

Механизм защиты	Решаемая задача безопасности
Сквозное шифрование данных между конечными узлами взаимодействия	Обеспечение конфиденциальности передаваемых по недоверенной сети данных
Аутентификация узлов взаимодействия	Обеспечение защиты от атак типа «человек по середине» и подделки узлов
Подпись передаваемых данных	Проверка целостности данных
Наличие нескольких маршрутов, ведущих к узлам передачи данных, в том числе для получения входящих и передачи исходящих сообщений	Защита от перехвата и обеспечение доступности узлов
Упаковка нескольких сообщений-чесночин в одно	Защита от анализа внутренних процессов, протекающих в сети цифрового производства

Визуально устранение угроз представлено на рисунке 6.

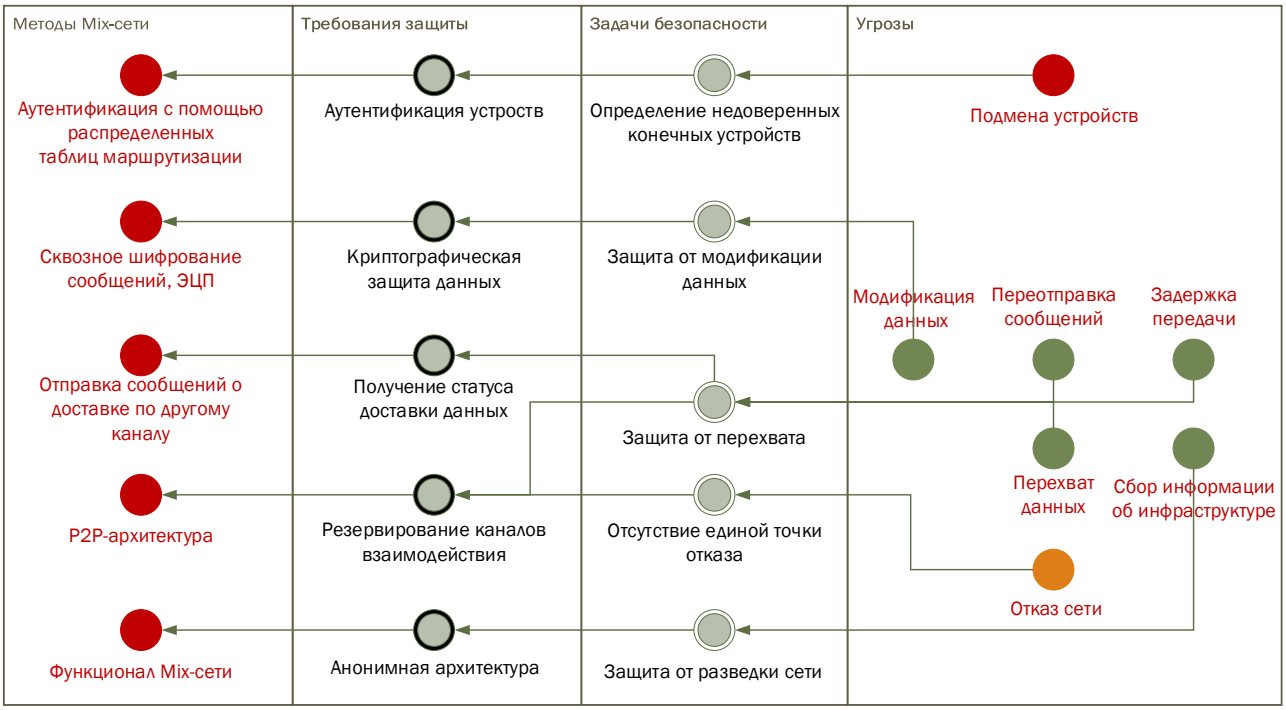


Рис. 6. Устранение угроз динамической многопутевой маршрутизацией

На примере рисунка 7 вероятность доставки пакета от узла *X* к узлу *Y* при отправке только по одному маршруту составляет 0.5, так как ровно половина узлов в маршрутах скомпрометирована. Однако при отправке пакета по ≥ 3 маршрутам увеличивает вероятность доставки до 1, так как хотя бы один из них будет проходить не через скомпрометированные узлы.

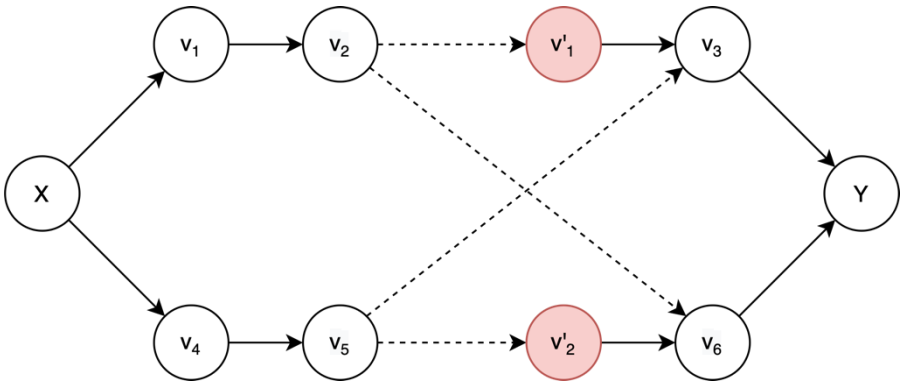


Рис. 7. Пример подграфа системы с двумя скомпрометированными узлами

Для всего маршрута s_k вероятность прохождения пакета по пути из нескомпрометированных узлов:

$$p_{s_k} = \frac{1}{N_k} \times \sum_{i=0}^{N_k} p_{s_{ki}},$$

где N_k – число узлов в маршруте k. В данном случае мы делаем допущение, что вероятность отправки пакета в скомпрометированный узел на каждом из узлов $v_{s_{ki}}$ – равновероятные события. На рисунке 8 представлен пример маршрута.

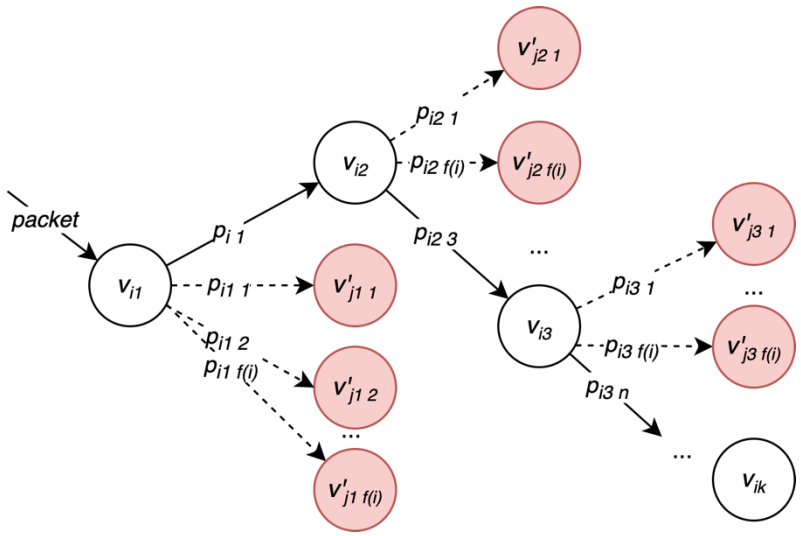


Рис. 8. Маршрут пакета через нескомпрометированные узлы

Следовательно, для пути S, состоящего из K маршрутов s_k, является отношением:

$$p_S = \frac{1}{K} \times \sum_{i=0}^{K} p_{s_k}$$

Энтропия пути S, в котором мы пытаемся вырать устойчивый маршрут s_k, при этом будет высчитываться по формуле:

$$H(S) = -\sum_{i=0}^{K}\left(p_{s_i} log_2 p_{s_i}\right)$$

Чтобы пакет имел возможность дойти по пути S от узла X к узлу Y, необходимо резервирование маршрутов. Для этого маршруты должны выбираться так, чтобы с большей долей вероятности компрометация первого маршрута не привела к компрометации второго и более маршрутов. Обозначим энтропию выбора двух маршрутов как $H(SS')$.

Сформулируем это требование в виде теоремы.

Теорема 1. Энтропия пути S схемы вероятности выбора устойчивых маршрутов s_kи $s_{k'}$ из конечного числа K маршрутов должна удовлетворять требованию: энтропия $H(S')$ выбора $s_{k'}$ при имеющейся энтропии $H(S)$ выбора маршрута s_k являются взаимно независимыми, то есть $H(S) + H_S(S') = H(S) + H(S')$.

Доказательство. Пусть маршрут s_i содержит n узлов: $v_{i,[1..n]} \in s_i$. Маршрут s_j содержит m узлов: $v_{j,[1..n]} \in s_j$.

Компрометация маршрута означает, что злоумышленник получил контроль либо над узлом v. Если $v \in s_i$ и $v \in s_j$, это означает, что компрометация маршрутов s_i и s_j являются совместимыми событиями A и B соответственно. Т.е. компрометация маршрута s_i приведет к компрометации маршрута s_j. Тогда $H(SS') = H(S) + H_S(S')$. Если это справедливо для $\forall v \in s_k, k = \{i, j\}$, то $H(SS') = H(S')$. Таким образом, ни один из путей не может быть устойчивым.

Сулавко А.Е.
ОмГТУ, доцент, к.т.н.,
sulavich@mail.ru

ГИБРИДНЫЕ МЕТОДЫ И АЛГОРИТМЫ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧАХ РАСПОЗНАВАНИЯ БИОМЕТРИЧЕСКИХ ОБРАЗОВ С ОБЕСПЕЧЕНИЕМ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ЭТАЛОНОВ ОТ КОМПРОМЕТАЦИИ[1]

Любое несанкционированное вмешательство в работу искусственного интеллекта (ИИ) может повлечь за собой последствия – материальный ущерб, нарушение информационной безопасности, угрозу жизни, здоровья граждан, технологический сбой или катастрофу и т.д. Все зависит от назначения конкретной реализации ИИ и возможностей, которыми данный экземпляр обладает. Поэтому в ответственных приложениях ИИ должен обладать поддержкой защищенного режима исполнения. Под «защищенным исполнением» понимается невозможность анализа логики работы ИИ, управления ИИ и извлечения знаний из памяти ИИ (например, персональных данных) любым неавторизованным лицом.

К ответственным приложениям ИИ относятся системы биометрической аутентификации по изображению отпечатка пальца, радужки, рукописного образа, голосу и другим параметрам. Биометрические образы являются персональными данными, которые нуждаются в надежной защите от компрометации. Защищенное исполнение процедуры биометрической аутентификации можно реализовать на базе гомоморфного шифрования либо специальных методов, позволяющих связать биометрический образ человека с его паролем или личным криптографическим ключом. Эти методы можно разделить на две основные категории:

- fuzzy extractors (fuzzy commitment, fuzzy vault, fuzzy embedder), основанные на применении кодов, исправляющих ошибки;

- нейросетевые преобразователи биометрия-код (НПБК), основанные на применении искусственных нейронных сетей (ИНС).

Каждая группа методов обладает принципиальными недостатками.

Другой важнейшей проблемой искусственного интеллекта, особенно актуальной для биометрических систем является обеспечение возможности быстрого и устойчивого обучения на малом числе примеров, способности ИИ обрабатывать большие объемы данных, а также формировать достоверные решения и делать высокоточные предсказания, даже если обучающая выборка ограничена в объеме и не в полной мере репрезентативна.

Алгоритмы обучения глубоких нейронных сетей сложно полностью автоматизировать, так как в той или иной степени они подвержены проблемам переобучения. Чем меньше объем обучающей выборки, тем больше склонность к переобучению. Поэтому обучение глубоких нейронных сетей ведется под контролем человека. Инженер-исследователь вынужден подбирать слишком много параметров, влияющих на структуру нейронной сети и алгоритм обучения, что создает большие трудозатраты. В ответственных приложениях (производство, медицина, информационная

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ), проект № 6.

безопасность) обучение (дообучение) нейросетевого искусственного интеллекта должно выполняться в автоматическом режиме, без контроля со стороны человека.

Настройка биометрической системы должна выполняться быстро (нельзя требовать от пользователя повторять ввод биометрических данных множество раз, иначе система не будет востребована на практике). Данный пример характерен тем, что проблема нехватки выборки в будущем никуда не исчезнет, независимо от того, какие объемы биометрических данных накоплены исследователями по всему миру. В реальной практике система все равно будет обучаться на малом числе примеров.

Биометрические системы, построенные на базе динамических образов (голос, рукописный и клавиатурный почерк), имеют склонность к снижению точности со временем, так как динамический образ может меняться с течением жизни и в зависимости от психофизиологического состояния человека. Этот процесс является частным случаем более общей проблемы концептуального дрейфа (смещения) моделей искусственного интеллекта.

Настоящая работа посвящена решению следующих фундаментальных проблем, которые создают значительные риски с точки зрения безопасности ИИ, конфиденциальности знаний и данных ИИ, надежности и робастности работы ИИ, снижающие доверие к системам ИИ:

- робастное автоматическое машинное обучение нейросетевых моделей искусственного интеллекта на малых выборках;
- защита ИИ от состязательных атак, зондирования моделей, извлечения знаний и других угроз информационной безопасности;
- онлайн-обучение гибких нейросетевых моделей ИИ (моделей на базе гибридных методов машинного обучения, способных к развитию в процессе функционирования) для предупреждения дрейфа концепций.

В качестве приложения искусственного интеллекта рассматриваются системы высоконадежной аутентификации субъектов на основе тайных биометрических образов (строение ушного канала, рукописный и голосовой пароли) и динамических биометрических образов (голос, клавиатурный почерк), изменяющихся с течением времени и в зависимости от психофизиологического состояния. Данный класс биометрических систем защиты в наибольшей степени подвержен обозначенным проблемам.

Работа поддержана грантом Минобрнауки России (грант ИБ №6).

Цель исследования: разработать технологию построения высоконадежных систем биометрической аутентификации с обеспечением защиты биометрических эталонов от компрометации на основе гибридных методов машинного обучения.

Для достижения поставленной цели были решены следующие основные **задачи по разработке**:

1. Концепции доверенного машинного обучения для построения нейросетевых моделей ИИ, изначально устойчивых к деструктивным воздействиям и способных к обучению на малых выборках.
2. Нейросетевых моделей ИИ, потенциально устойчивых к деструктивным воздействиям и концептуальному дрейфу, способных к робастному автоматическому обучению на малых выборках данных и саморазвитию.

3. Гибких нейросетевых моделей ИИ и алгоритмов их онлайн-обучения в процессе функционирования, позволяющих предупредить или снизить влияние концептуального дрейфа.
4. Методов и алгоритмов многофакторной аутентификации и генерации электронной подписи на основе тайных биометрических образов с обеспечением защиты биометрических данных от компрометации.
5. Технологии высоконадежной биометрической аутентификации, устойчивой к компьютерным атакам, извлечению знаний и концептуальному дрейфу моделей, а также программного комплекса на базе предложенных концепции, моделей, методов и алгоритмов.

Концепция искривленного пространства признаков и мета-пространство признаков Байеса-Минковского.

В [1] введена мера Байеса-Минковского, позволяющая точнее определять расстояния в искривленном пространстве признаков, что дает снижение количества ошибок классификации образов почти до уровня, соответствующего «плоскому» пространству:

$$y = \sqrt[p]{\sum_{j=1}^{n} \left| \frac{(m_j - a_j)}{\sigma_j} \right|^p},$$

где a_j – значение j-го признака из вектора $\bar{a}$, представляющего собой распознаваемый образ; n – количество признаков; m_j и σ_j – математическое ожидание и среднеквадратичное отклонение значений j-го признака для класса "Свой", с которым сравнивается образ $\bar{a}$ (класс "Свой" представляет биометрические образы одного из легитимных пользователей); p – степенной коэффициент, определяющий уровень «искривления» пространства. Рис. 1 иллюстрирует, как может выглядеть окружность в двумерном пространстве Минковского. В отличие от примера на рис. 1 пространство признаков многомерно (каждый признак «создает» одно измерение). Однако для наблюдателя, находящегося в евклидовом пространстве, все многомерные сферы, построенные при $p \neq 2$, будут иметь аналогичные с рис. 1 деформации.

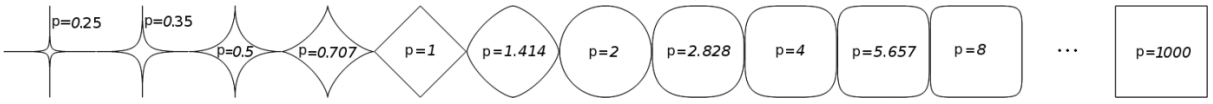


Рис. 1. Окружность на плоскости при различных значениях степенного коэффициента p

Искривление пространства признаков возникает из-за наличия корреляционных связей между измерениями (рис. 2). Как правило, пространство признаков не является ни плоским, ни в равной степени искривленным. Уровень искривления меняется относительно наблюдателя. Все классы образов имеют отличающиеся матрицы коэффициентов корреляции между признаками (биометрический образ каждого человека имеет уникальную корреляционную матрицу). Поэтому относительно различных классов образов пространство признаков искривлено по-разному.

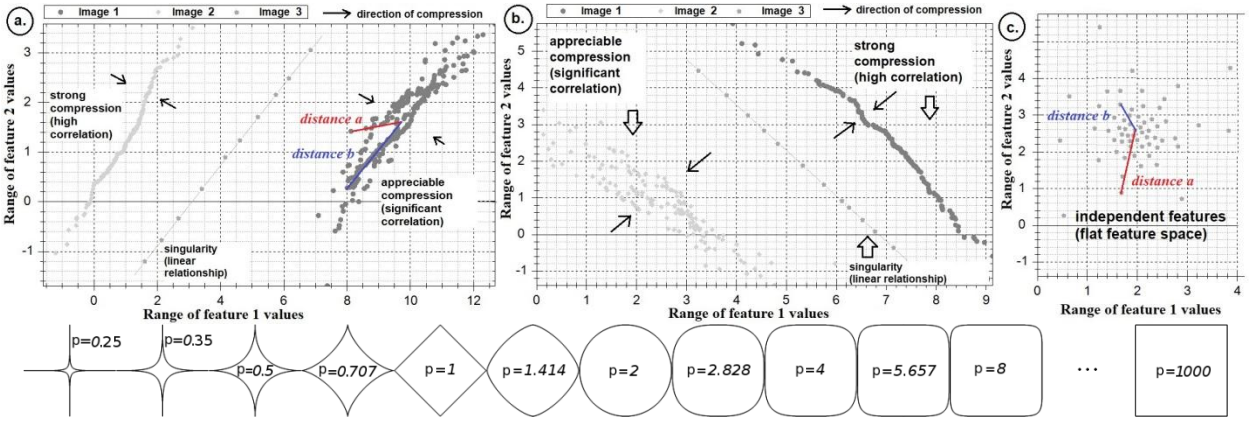


Рис. 2. Направление сжатия пространства двух признаков: a. при положительной корреляции (расстояние «a» на самом деле больше, чем расстояние «b», так как пространство признаков не является «плоским», а искривлено из-за корреляции), b. при отрицательной корреляции, c. при независимости признаков (расстояние «a» больше, чем «b»)

Чтобы извлечь информацию об искривлении пространства признаков введем семейство мер близости Байеса-Минковского (например, (1)), которая оперирует разностями между признаками и таким образом осуществляет анализ данных, которые заключены в мета-пространстве, т.е. между измерениями исходного пространства признаков. Эти метрики принимают тем меньшие значения, чем выше корреляция между признаками.

$$y_t = \sqrt[p]{\sum_{j=1}^{n} \left| \left| \frac{\mu_t - a_t}{\delta_t} \right|^p - \left| \frac{\mu_j - a_j}{\delta_j} \right|^p \right|}, j \neq t, \qquad (1)$$

где μ_j и δ_j – это нормирующие коэффициенты, вычисляемые как математическое ожидание и среднеквадратичное отклонение значений признака для класса «Чужие». Размерность мета-пространства Байеса-Минковского составляет: $n' = 0{,}5(n(n\text{-}1)) = 0{,}5n^2 - 0{,}5n$.

Под мета-признаками подразумеваются разности вида:

$$a'_{j^*} = a'_{t,j} = f(a_t, a_j) = \left| \left| \frac{\mu_t - a_t}{\delta_t} \right|^p - \left| \frac{\mu_j - a_j}{\delta_j} \right|^p \right|, j > t, j^* = \sum_{t^*=1}^{t-1} (n - t^*) + j - t,$$

которые фактически являются грубыми (точечными) оценками корреляционной зависимости между двумя исходными признаками под номерами j и t (чем меньше по модулю a', тем выше внутриклассовая корреляция между соответствующими признаками). Под точечной оценкой понимается оценка, сделанная всего по одному примеру тестовой выборки, но при наличии некоторых априорных знаний (m_j σ_j, δ_j, μ_j), полученных в процессе обучения на выборке небольшого объема. Считается, что «наивная» схема классификации Байеса является полностью корректной, когда признаки независимы, т.е. пространство признаков не имеет кривизны. Мера Минковского измеряет расстояние в искривленном пространстве. Новые метрики преобразуют пространство

коррелированных признаков в мета-пространство более информативных независимых признаков, поэтому они названы метриками Байеса-Минковского. Проведен вычислительный эксперимент по распознаванию образов в пространстве абстрактных (имитированных) признаков, результаты которого показали:

- мета-пространство признаков Байеса-Минковского может содержать в разы больше информации о классах образов, чем исходное пространство, чем выше уровень корреляции, тем информативнее мета-признаки;
- «переход» в мета-пространство признаков не ведет к проявлению проблемы «проклятья размерности».

На первый взгляд это противоречит классической теории математической статистики, которая утверждает: корреляция между признаками указывает на то, что часть информации в признаках повторяется. Но учитывая полученные результаты, данное утверждение стоит уточнить: пространство признаков искривляется из-за корреляционных связей, причем относительно каждого класса образов и каждого измерения характер искривления различен, что влечет за собой уменьшение количества информации об отличии классов, наблюдаемой в пространстве признаков, и появление новой информации в мета-пространстве Байеса-Минковского, но в большем объеме. Полученные результаты свидетельствуют о перспективности использования мета-пространств признаков Байеса-Минковского, по крайней мере, в задачах классификации образов.

Модели корреляционных нейронов и НПБК на их основе.

Предложена модель корреляционного нейрона, который должен разделять входные данные по уровню коррелированности. Для этого нейрон соединяется с мета-признаками, которые были порождены парами признаков с близким уровнем взаимной корреляции. Простейший корреляционный нейрон Байеса-Минковского может быть основан на метрике взвешенного среднеквадратичного отклонения значений мета-признаков. Эта метрика хорошо выделяет как положительно, так и отрицательно коррелированные данные на фоне данных с любой взаимной корреляцией.

В качестве функции активации предлагается использовать многоуровневую пороговую функцию квантования. Каждый нейрон имеет не менее 4 возможных двухбитных состояния выхода. О том, какое именно состояние активации соответствует гипотезе «Свой», известно только на этапе обучения, злоумышленник не обладает этой информацией, так как она не сохраняется после настройки нейрона. Идеальное решение задачи обучения нейрона состоит в том, чтобы при поступлении образа «Свой» на выходе нейрона почти всегда возникало определенное состояние, а в других случаях состояния $\{0, 1, 2, 3\}$ на выходе нейрона стали равновероятны: $P(0) \approx P(1) \approx P(2) \approx P(3) \approx 0.25$, где $P(\phi(y))$ – это относительная частота появления $\phi(y)$ при поступлении на вход образа «Чужой». К значению функции активации применяется одна из таблиц перевода состояний $\{0, 1, 2, 3\}$ в двухбитный код, таблица выбирается случайно на этапе обучения. Таким образом, для обучения нейрона Байеса-Минковского достаточно определить связанные мета-признаки, вычислить пороги квантования по специальным формулам, предложенным автором, и задать хеш-таблицу. Возможны иные более сложные конструкции корреляционных нейронов с множеством вентилей, пропускающих данные с разной коррелированностью (например, вентили отрицательной и положительной корреляции).

Предлагаемая модель НПБК представляет собой однослойную сеть корреляционных нейронов, которую можно комплексировать с глубокой нейронной сетью, извлекающей признаки (рис. 3). Нормирующие коэффициенты для перехода в мета-пространство Байеса-Минковского должны быть вычислены на основании выборки «Чужие» до построения и обучения НПБК. Количество входов η для всех корреляционных нейронов должно быть равным. При синтезе НПБК для конкретного пользователя необходимо убедиться, что имеется достаточное количество пар признаков с уровнями взаимной корреляции $C_{j,t}$<-0,5 и $C_{j,t}$>0,5. Для этого необходимо рассчитать корреляционную матрицу по данным обучающей выборки «Свой». Любая пара коррелированных признаков потенциально порождает один мета-признак. Каждый нейрон должен обрабатывать уникальную комбинацию мета-признаков и генерировать на выходе 2 бита. Нужное количество нейронов определяется, исходя из требуемой длины ключа. Предложен алгоритм синтеза и автоматического обучения НПБК на базе корреляционных нейронов. После обучения состояния «0» и «1» в каждом разряде бинарного кода, возникающего на выходе НПБК при поступлении на его входы образов «Чужих», становятся почти равновероятными.

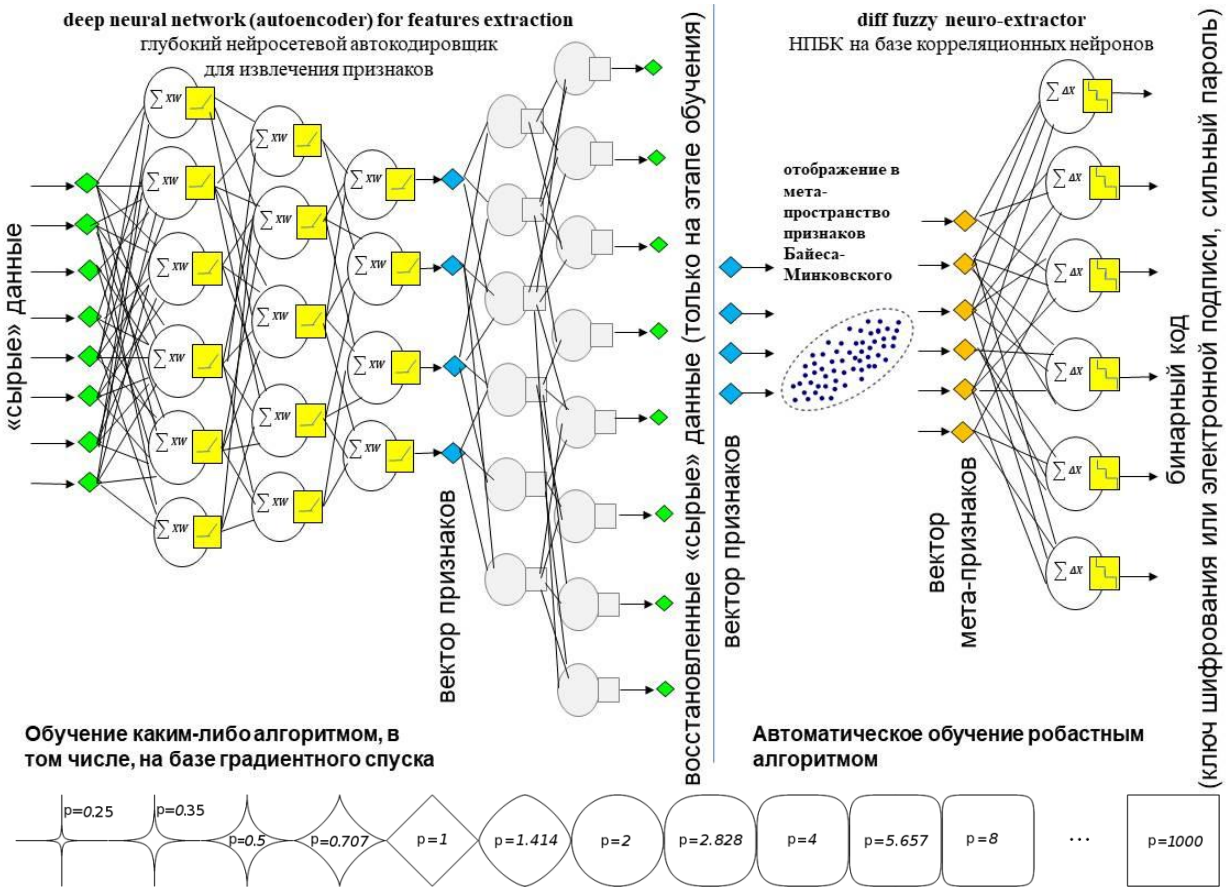


Рис. 3. Структурная схема связывания ключа и биометрического образа

Отметим следующие преимущества предложенной модели:

- корреляционные нейроны не подвержены несбалансированности обучения;
- процесс настройки корреляционной сети является робастным и переобучения не возникает;

– длина связанного ключа гораздо выше, чем для нечеткого экстрактора или классического НПБК, обучаемого по ГОСТ Р 52633;
– предложенная модель должна иметь гораздо более высокий уровень устойчивости к состязательным атакам [2, 3], чем классическая глубокая сеть с функцией активации Softmax на выходе, по крайней мере, в плане влияния на показатель FAR.

Предложенную модель НПБК можно использовать как основу для создания систем высоконадежной биометрической аутентификации, средств электронной подписи с биометрической активацией и систем ИИ, исполняемых в защищенном режиме для объектов критической информационной инфраструктуры.

На данный момент в Омском государственном техническом университете под руководством Сулавко А.Е. ведется разработка **национального стандарта** «Искусственный интеллект. Нейросетевые алгоритмы в защищённом исполнении. Автоматическое обучение нейросетевых моделей на малых выборках в задачах классификации», базирующегося на моделях корреляционных нейронов и алгоритмах их автоматического обучения.

Гибкая модель гибридной нейронной сети и алгоритмы ее обучения с учителем и онлайн-обучения с подкреплением.

После обучения сети корреляционных нейронов по предложенному алгоритму для создания НПБК, она теряет способность к онлайн-обучению (дообучению в процессе функционирования). Чтобы обеспечить обновление биометрического эталона в процессе функционирования системы и предупредить концептуальный дрейф модели требуется разработать более гибкую нейросетевую модель. Для этого решено использовать принципы построения и обучения искусственных иммунных систем (ИИС).

Иммунная система содержит множество клеток (макрофаги, дендритные клетки, лимфоциты), которые обладают способностью обнаруживать и удалять чужеродные организмы (антигены). Назовем все такие клетки детекторами. Каждый детектор следует рассматривать как бинарный классификатор, состоящий из нескольких функций, последовательно применяющихся к образу. В общем виде получение реакции i-го детектора на входной образ $\bar{a}$ можно описать формулой (1):

$$u_i = \phi_\chi\left(y' = \varphi\left(y = f_x(\bar{\alpha} = R(\bar{a}, \Psi_i), \breve{g}, \Theta_i), T_i\right)\right),$$

$\bar{\alpha} = R(\bar{a}, \Psi_i)$ – функция-рецептор, предоставляющая интерфейс взаимодействия для детектора и антигена. Данная функция извлекает η из n признаков, содержащихся в $\bar{a}$, Ψ_i – множество номеров признаков из $\bar{a}$, которые должен анализировать i-й детектор; $y = f_x(\bar{\alpha}, \breve{g}, \Theta_i)$ – функция-ядро детектора, параметрический функционал, который вычисляет близость вектора $\bar{\alpha}$ к эталону класса образов «Свой»; x – тип функционала; $\breve{g}$ – вектор параметров функционала, которые влияют на характер вычислений; $\Theta_i=\{\mu_1,\mu_2,\ldots,\mu_\eta,\sigma_1,\sigma_2,\ldots,\sigma_\eta\}$, μ_j и σ_j – статистические оценки параметров распределения значений j-го признака из вектора $\bar{\alpha}$. $y' = \varphi(y, T_i)$ – функция нормирования откликов y относительно порога T_i, который вычисляется в процессе настройки i-го детектора; $u_i = \phi_\chi(y'_i)$ – функция активации, дополнительный нелинейный элемент детектора, который определяет особенности реагирования на антиген. Функция активации также необходима, чтобы привести отклик детектора к области значений [0;1].

В настоящей работе для построения ядер детекторов применялись меры близости Минковского и Байеса-Минковского, а в качестве функций активации – сигмоиды (арктангенс, гиперболический тангенс и др.).

Предлагается разделить детекторы на две группы: врожденный и приобретенный иммунитет, и рассматривать их как *два комитета (ансамбля)* слабых классификаторов, обучаемых при помощи разных алгоритмов. Каждый детектор является своего рода оболочкой над нейроном. Вместе детекторы представляют собой гибридную нейронную сеть.

Врожденный иммунитет (ВИ) передается посредством генов, органы иммунной системы формируются еще при эмбриональном развитии. ВИ формируется в процессе итерационного обучения с использованием *тренировочной* и *валидационной* выборок. Обе выборки являются *непересекающимися* подмножествами *обучающей* выборки. *Приобретённый иммунитет (ПИ)* развивается с течением жизни и определяет способность организма обезвреживать специфические антигены, которые попадали в организм ранее. В предложенной модели тимус осуществляет настройку и отбор иммунокомпетентных детекторов, используя валидационную выборку. Адаптивный иммунный ответ приводит к появлению иммунологических клеток памяти, которые долгое время пребывают в «спящем состоянии» до повторной встречи с тем же антигеном. В разработанной модели приобретенный иммунитет формируется в процессе функционирования сети. Если решение об отнесении образа к категории «Свой» или «Чужой» является неоднозначным, могут генерироваться новые иммунокомпетентные детекторы. Имеются следующие *гиперпараметры*, которые влияют на эффективность комитета детекторов: количество детекторов, матрица коэффициентов корреляции между решениями всех возможных пар детекторов, сила детекторов (их способность давать как можно более высокие показатели разницы уровней реакции на образы «Свой» и «Чужой»).

Предложен итерационный алгоритм обучения с учителем для формирования ВИ, а также алгоритм онлайн-обучения для формирования ПИ в процессе функционирования. При разработке алгоритма применялись следующие идеи и методы: бэггинг, подпространства признаков, неявный бустинг (образы обучающей выборки, которые хуже всего распознаются в процессе обучения скрещиваются по ГОСТ Р 52633.2 и добавляются в обучающую выборку, на следующей итерации алгоритм учится распознавать их). Описанная модель, алгоритмы ее обучения и результаты их экспериментальной проверки подробно изложены в работе [4].

Технология, методы и алгоритмы высоконадежной многофакторной биометрической аутентификации.

В настоящей работе в целях биометрической аутентификации использовались следующие виды образов: рукописный пароль, голосовой пароль, клавиатурный почерк и особенности внутреннего строения слухового канала и наружного уха. Последний тип образов был предложен в рамках настоящей работы.

Строение человеческого уха закладывается в детстве (до 8 лет), во взрослом возрасте значительных изменений в пропорциях ушных раковины и канала не происходит [5]. Длина, толщина и форма ушного канала различаются у людей. Ушная раковина и слуховой канал являются резонансными системами. Чтобы получить информацию о

внутреннем строении наружного уха, можно воздействовать на ушной канал акустическими волнами, которые будут искажаться, отражаясь от стенок канала. Отраженный сигнал будет иметь отличия от исходного, обусловленные индивидуальными особенностями ушных раковины и канала человека. Параметры эхо-сигнала или его передаточной функции могут содержать информацию о геометрии слухового канала и ушной раковины, поэтому их можно воспринимать как вектор биометрических параметров (*признаков*), характеризующих особенности строения наружного уха индивидуума. Разработано устройство для регистрации биометрических характеристик уха, которое состоит из двух электретных микрофонов, звукоизолирующего корпуса (в виде наушников), экранированного медного провода, двух динамиков и звуковой карты фирмы. Собрана база акустических образов уха с привлечением 75 испытуемых, которую можно скачать в обезличенном виде на сайте проекта [6]. Подробнее результаты исследования описаны в работах [7, 8].

Разработанные методы и технология основаны на предложенных моделях корреляционных нейронов, НПБК, гибридных сетей и алгоритмах обучения. Аналитико-синтетическое исследование документального потока показало, что полученные результаты соответствуют мировому уровню по точности классификации или превосходят его по уровню защищенности биометрических образов от компрометации.

ModelOps платформа для разработки и внедрения доверенного ИИ.

На базе предложенных концепции, моделей и алгоритмов разрабатывается серия программных продуктов AIConstructor (AIC) [9]. На данный момент разработан программный комплекс для проведения научных исследований по машинному обучению AIC desktop. Он ориентирован на задачи информационной безопасности, анализ биомедицинских данных, классификацию образов может быть использован в образовательных целях, а также для работы над малыми и средними научными проектами (диссертациями, отчетами и т.д.). AIC desktop является прототипом программной платформы AIC ModelOps Platform, которая пока находится в разработке. AIC ModelOps Platform – это корпоративная среда управления жизненным циклом искусственного интеллекта и моделей принятия решений, которая может быть использована для автоматизации, отслеживания и контроля рабочих процессов на всех этапах построения модели: от исследования до внедрения в бизнес среду. Это полнофункциональный продукт для обеспечения надежности, прозрачности и безопасности процессов разработки и внедрения искусственного интеллекта. Предлагаемый продукт позволит:

- Ускорить процесс цифровой трансформации за счет быстрого развертывания модели в бизнес-среде и непрерывного мониторинга с обеспечением объяснимости и прозрачности функционирования ИИ
- Объединить группы специалистов по анализу данных с помощью удобной среды для командной работы и управления экспериментами;
- Ускорить процесс исследований и разработки ИИ;
- Обеспечить гибкость разработки и поддержки ИИ благодаря интеграции продукта с множеством фреймворков и инструментов машинного обучения;
- Обеспечить устойчивость к состязательным атакам и зондированию моделей на уровне построения архитектуры ИИ;

– Снизить риски от внедрения ИИ, связанных с неверным функционированием, безопасностью, дрейфом модели и объяснимостью результатов работы ИИ.

В заключение работы сформулируем основные результаты:

1. Предложена концепция искривленного пространства признаков. Общее количество информации о различии распознаваемых образов зависит не только от взаимного расположения собственных областей классов образов, но и от характера искривления пространства признаков. На искривление пространства признаков влияют корреляционные связи между признаками. Предложено отображение для перехода из исходного (искривленного) пространства признаков в плоское (спрямляющее) мета-пространство признаков Байеса-Минковского более высокой размерности, в котором знания ИИ не компрометируются после обучения. Новая концепция указывает на то, что корреляция между признаками не уменьшает количество информации в образе, а наоборот, повышает информативность образа. Использование корреляционных связей в качестве признаков позволяет существенно сократить объем обучающей выборки.
2. Разработаны новые модели нейронов и гибридных нейронных сетей. Впервые предложена модель корреляционных нейронов, анализирующих корреляционные связи между признаками вместо значений признаков в задачах классификации образов. Корреляционные нейроны не подвержены проблеме несбалансированности обучения. Процесс синтеза и обучения сетей корреляционных нейронов полностью автоматический и сохраняет робастность даже на малых обучающих выборках. Предложена модель НПБК на базе корреляционных нейронов, которая не компрометирует биометрический эталон пользователя даже без применения средств шифрования знаний ИИ (нейросетевых контейнеров). Предложенная модель НПБК потенциально устойчива к состязательным атакам и извлечению знаний путем зондирования модели.
3. Разработана гибкая модель гибридной нейронной сети, состоящей из корреляционных, квадратичных, классических и других видов нейронов, обладающая свойством двойной пластичности, позволяющим менять как параметры, так и структуру гибридной сети в процессе функционирования. Разработаны алгоритмы обучения гибридной сети с учителем и онлайн-обучения с подкреплением, позволяющие предупредить концептуальный дрейф модели.
4. Разработаны методы и алгоритмы высоконадежной аутентификации (многофакторной и однофакторной) в защищенном режиме и генерации электронной подписи на основе образов слухового канала, а также рукописного и голосового паролей с обеспечением защиты биометрических данных от компрометации при хранении и передаче по каналам связи.

Разработаны технология высоконадежной многофакторной биометрической аутентификации, а также прототип программной платформы для цифровой трансформации предприятий, которая позволяет создавать и внедрять в бизнес-процессы организаций доверенный ИИ, устойчивый к компьютерным атакам и концептуальному дрейфу моделей.

СПИСОК ЛИТЕРАТУРЫ

1. Sulavko, A. E. Bayes-Minkowski measure and building on its basis immune machine learning algorithms for biometric facial identification / A. E. Sulavko. – DOI:10.1088/1742-6596/1546/1/012103 // Journal of Physics: Conference Series. – 2020. – Vol. 1546. – P. 012103
2. M. A. Alcorn et al., "Strike (With) a Pose: Neural Networks Are Easily Fooled by Strange Poses of Familiar Objects," 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 4840-4849, doi: 10.1109/CVPR.2019.00498.
3. Hafemann L.G., Sabourin R., Oliveira L.S. Characterizing and evaluating adversarial examples for Offline Handwritten Signature Verification // IEEE Transactions on Information Forensics and Security, 2019.
4. Сулавко, А.Е. Абстрактная модель искусственной иммунной сети на основе комитета классификаторов и ее использование для распознавания образов клавиатурного почерка // Компьютерная оптика. – 2020. – Т. 44, № 5. – С. 830-842. – DOI: 10.18287/2412-6179-CO-717.
5. Rudolf Probst, Gerhard Grevers, Heinrich Iro. Basic Otorhinolaryngology: A Step-by-Step Learning Guide Paperback. – TPS. - 2nd edition. – 2017. – 430 p.
6. http://aiconstructor.ru/page14247028.html
7. Sulavko, A. E., Samotuga A.E., Kuprik I.A. Personal Identification Based on Acoustic Characteristics of the Outer Ear Using Cepstral Analysis, Bayesian Classifier and Artificial Neural Networks // IET Biometrics. - 2021. - Volume10, Issue6. - Pages 692-705
8. Sulavko, A.E., Lozhnikov, P.S., Kuprik, I.A. et al. Personal Identification Based on the Individual Sonographic Properties of the Auricle Using Cepstral Analysis and Bayes Formula. Cybern Syst Anal 57, 455–462 (2021).
9. http://aiconstructor.ru/

НАУЧНАЯ СЕКЦИЯ
«БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИЙ»

Место проведения:
г. Москва, ул. Авиамоторная, д. 8а, стр. 12 (библиотечный корпус), 2-й этаж, каб. 201

Подсекция № 2

«Аппаратно-программные средства защиты телекоммуникаций»

Руководитель: **Крылов Григорий Олегович,**
Московский технический университет связи и информатики,
профессор кафедры «Безопасность телекоммуникаций»,
Финансовый университет при Правительстве РФ, профессор;
Национальный исследовательский ядерный университет «МИФИ»,
профессор, доктор физико-математических наук, профессор

Секретарь: **Закомолдин Семён Дмитриевич,**
Московский технический университет связи и информатики,
студент кафедры «Безопасность телекоммуникаций»

Макарова О.С.
УрФУ младший научный сотрудник
o.s.makarova@urfu.ru

ИСПОЛЬЗОВАНИЕ ТЕОРИИ ДУФФУЗИИ ИННОВАЦИЙ ДЛЯ МАТЕМАТИЧЕСКОГО ОПИСАНИЯ ДИНАМИКИ РЕАЛИЗАЦИИ КОМПЬЮТЕРНОЙ АТАКИ

Математическая модель, описывающая динамику возможности реализации компьютерной атаки во времени

Для разработки математической модели, описывающей динамику возможности реализации компьютерной атаки (КА) во времени, проведем анализ особенностей КА с точки зрения нарушителя (этапы и методы реализации КА) и факторов, определяющих динамику изменения возможности реализации КА.

При этом учтем, что компьютерные преступления, в отличие от правонарушений, являющихся предметом, изучаемым криминологией, требуют от нарушителя наличия специальных знаний, умений и навыков, а также возможности практически совершить КА. Рассмотрим подробнее умения и навыки нарушителя. Знания о методах КА нарушитель может приобрести в сети DarkNet – области интернета, в которые не может попасть обычный пользователь через поисковики Google или Yandex. Анализ форумов в DarkNet позволяет собрать информацию о стратегиях, тактиках и методах, которые используют и/или разрабатывают нарушители для реализации КА. Различные решения по сбору информации с форумов DarkNet рассматриваются в [1-5].

Таким образом, на подготовительном этапе проведения КА нарушитель стремится получить сведения о новых для него технологиях проведения КА, которые, следуя [6], является синонимом понятия «инновация» (инновация – технологическая идея, метод или объект, являющийся новым для члена социальной системы). В этой связи, можно предположить, что динамика КА может быть построена на основе положений и математических моделей Теории диффузии инноваций ТДИ (здесь диффузия инноваций – это процесс, с помощью которого инновации распространяются по каналам передачи с течением времени среди членов социальной системы), развитой в Э. Роджерсом [6], Ф. Бассом [7], Э. Мэнсфилдом [8] и Т. Хагерстранда [9].

Напомним, что накопленные суммы приобретенных инноваций от времени описываются зависимостью $Y(t)$ вида:

$$Y(t) = \frac{1}{1+\alpha e^{-\beta t}}, \quad (1)$$

где α, β – параметры модели, называемых *s*-образными кривыми Перла-Рида.

Согласно исследованиям, проведенным [9] инновация может также развиваться по каскадной модели, описываемой следующе формулой:

$$Y(t)=\begin{cases}\dfrac{1}{1+\alpha_1 e^{-\beta_1(t-t_0)}},\ \text{если } t_0\le t\le t_1,\\ \dfrac{1}{1+\alpha_1 e^{-\beta_1(t_1-t_0)}}+\dfrac{1}{1+\alpha_2 e^{-\beta_2(t-t_1)}},\ \text{если } t_1<t\le t_2,\\ \text{L}\\ \dfrac{1}{1+\alpha_1 e^{-\beta_1(t_1-t_0)}}+\dfrac{1}{1+\alpha_2 e^{-\beta_2(t_2-t_1)}}+\text{L}\ +\dfrac{1}{1+\alpha_n e^{-\beta_n(t-t_{n-1})}},\ \text{если } t_{n-1}<t\le t_n,\end{cases} \quad (2)$$

где

$[t_0,t_1]$ – длительность первого этапа развития инновации;

$]t_1,t_2]$ – длительность второго этапа развития инновации;

…

$]t_{n-1},t_n]$ – длительность *n*-го этапа внедрения инновации.

Корректность такого упрощения для новых прогрессивных технологий, к которым относятся информационные технологии и информационная безопасность технологии, была подтверждена Э. Мэнсфилдом [8].

Одним из способов подтверждения адекватности описанной математической модели, описывающей динамику развития КА является анализ общедоступных доступных данных о динамике КА, например, реализованной с помощью вредоносного программного обеспечения (ВПО) WannaCry.

Подтверждение адекватности математической модели динамики распространение компьютерной атака на примере компьютерной атаки, реализованной с помощью вредоносного программного обеспечения WannaCry

Приведем аналогию «социальной системы» как совокупности «узлов» организации, на которые воздействует нарушитель для распространения КА. Таким образом, динамика изменения вероятности КА эквивалентна динамике увеличения количества «зараженных» узлов, характеризующейся отношением числа узлов, зараженных в результате успешно реализованной КА, к общему количеству узлов, которое далее будем называть относительным числом атакованных узлов компьютерной сети (КС) в момент времени t.

Для анализа динамики распостранения КА, характеризующейся зависимостью относительного числа атакованных узлов КС от времени были использованы соответствующие данные, зарегистрированные во время проведения КА с помощью ВПО WannaCry, которые размещены на сайте MalwareTech [10]. Исходная информация представляет собой отсчеты числа атакованных узлов за выбранный период времени (1 минуту, 5 минут, 30 минут, 1 час, 24 часа) от времени, представленные в виде графика.

Однако возможности выгрузить первичную информацию в виде файла разработчик сайта не предоставил. В результате пришлось извлекать ее вручную, последовательно просматривая каждую точку зависимости числа вновь атакованных в течение 24 часов узлов от времени. Из полученной первичной информации видно, что 02.06.2017

информация о числе вновь зараженных узлов не выкладывалась на сайте, а с 03.06.2017 изменилось время публикации данных с 24:00 часов на 04:00.

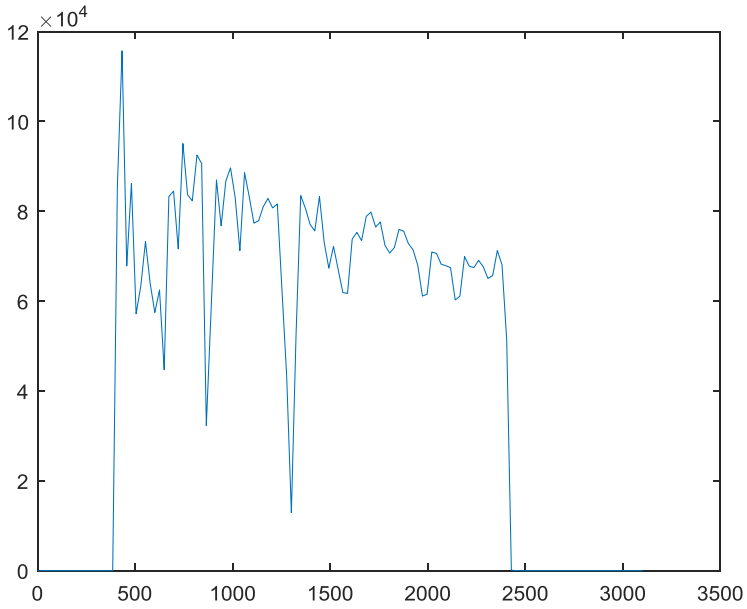


Рис. 1. Зависимость числа вновь зараженных узлов КА ВПО WannaCry в период с 26.04.2017 по 31.08.2017

Для нахожденния аппрокисмации зависимости числа вновь зараженных узлов компьютерной сети от времени требуется преобразовать значения абсцисс отсчетов, задаваемых в формате дата/время, анализируемой зависимости в порядковую временную шкалу. Для выполения данной процедуры, как очевидно, необходимо выбрать единицу измерения времени (принимая во внимание отмеченные выше особенности первичных данных была выбрана единица измеренния 1 час) и далееи далее указать значение моментов времени между последовательными измерениями: первый отсчет – 0, второй отсчет 24 часа и т.д., в связи с отсутствием данных на 02.06.2017 момент времени между пердшествующим ему и данным отсчетом выбирался равным 52 часа. Тогда накопленная сумма значений временных интервалов между отсчетами анализируемой зависимости есть искомая временная сетка, значения узлов которой измеряются в часах. Для того, чтобы в анализируемой зависчимости присутсвовала информация, соответствующая периоду до начала КА и после ее окончания, данные дополнялись справа и слева 17-ю нулевыми отсчетами. Полученная в результате проведенных преобразований зависимость представлена на рисунке 1.

Далее для нахождения зависимости общего количества зараженных узлов в течение 24 часов от времени, вычислялись первые накопленные суммы зависимости, представленной на рисунке 2. Зависимость общего количества зараженных узлов в течение 24 часов ВПО WannaCry от времени, нормированная на максимальное число зараженных узлов, представлена на рисунке 2.

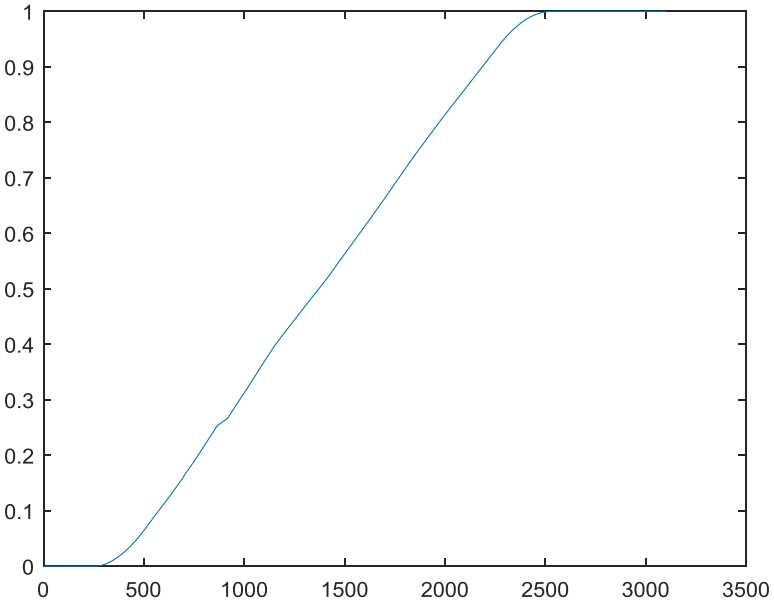


Рис. 2. Зависимость числа вновь зараженных узлов КА ВПО WannaCry в период с 26.04.2017 по 31.08.2017

Визуальный анализ зависимости, представленной на рисунке 3 позволяет предположить, что данную зависимость можно аппроксиммировать s-образной кривой Перла-Рида (1). Результаты, подтверждающие данную гипотезу представлены в следующем разделе.

Математическое обоснование выбора апроксимирующей функции методом наименьших квадратов

Рассмотрим результаты аппроксимации зависимости, представленной на рисунке 2, в соответствие с методом наименьших квадратов с помощью линейной и квадратической функций, а также s-образной кривой Перла-Рида (1). Значения коэффициентов линейной и квадратической аппроксимирующих функций, а также s-образной кривой Перла-Рида (1), находились, соответственно, из условий:

$$\arg\min_{\alpha_1,\alpha_2}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1 t_i+\alpha_2\right)\right)\right)^2, \tag{3}$$

$$\arg\min_{\alpha_1,\alpha_2,\alpha_3}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1 t_i^2+\alpha_2 t_i+\alpha_3\right)\right)\right)^2, \tag{4}$$

$$\arg\min_{\alpha_1,\alpha_2,\alpha_3,\alpha_4}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1+\frac{\alpha_2}{1+\alpha_3\exp\left(-\left(\alpha_4\left(t_i-t_1\right)\right)\right)}\right)\right)\right)^2, \tag{5}$$

N – число отсчетов аппроксимируемой зависимости. Для нахождения решения задач (3), (4) использовалась функция пакета MATLAD regress.m, задачи (5) – функция fminsearch.m.

Значения коэффициентов аппроксиммирующих функций, а также остатки данных моделей представлены в таблице 1. Графики аппроксимируемой зависимости и аппроксимирующие функции представлены на рисунке 3.

Табл. 1. Значения коэффициентов аппроксимирующих функций

Тип функции	α_1	α_2	α_3	α_4	Дисперсия остатков модели
Линейная	0,00041	–0.073	–	–	0.065
Квадратическая	$-5\cdot10^{-8}$	0,00056	–0.15	–	0.053
s-образная	–0.11025	1.18080	0.00197	13.7642	0.021

Из таблицы 1, что минимальное значение среднеквадратического отклонения остатков аппроксимации оказывается у s-образной кривой Перла-Рида, что подтверждает провомерность ее использования в дальнейшихх исследованиях математической модели.

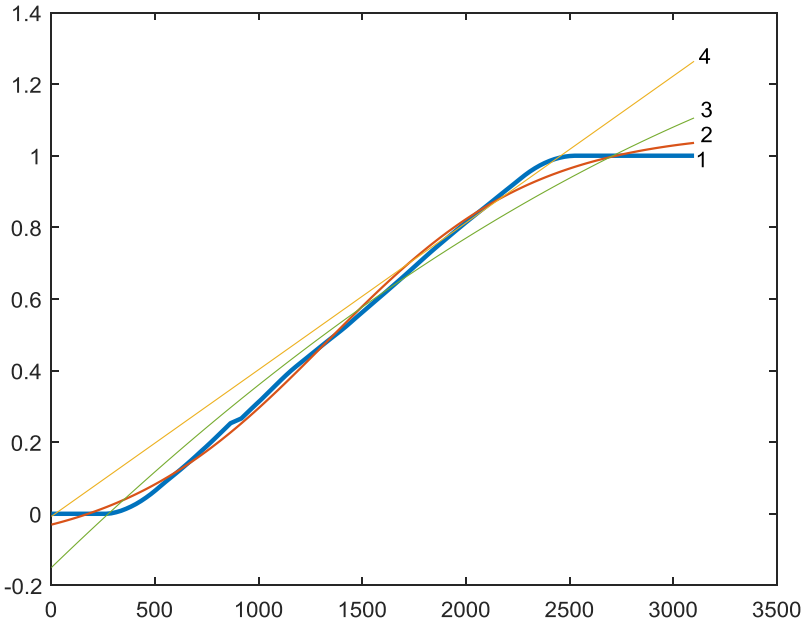


Рис. 3. Аппроксимации зависимости общего числа зараженных узорв КС, зараженных ВПО WannaCry, от времени: 1 - аппроксимируемая зависимость; 2 - s-образная кривая Перла-Рида; 3 - квадратическая функция 4 - линейная функция

Выводы

Обоснованы базовые принципы и подходы, на которых построены с точки зрения нарушителя математическая модель, описывающей динамику изменения вектора КА во времени.

Оценка результатов практической апробации подтвердила, что вид функции изменения вектора КА соответсвует предложенной математической модели. Вектор КА определяется характеристиками самой КА, в частности, экономичностью и рентабельностью реализации метода КА, наличием рекламы в DarkNet и данными межличностного взаимодействия нарушителей и апробации (совместимости с

инфраструктурой атакуемых организаций, простотой реализации, наличием средств ЗИ и методов обнаружения КА).

Перспективы дальнейшей разработки темы исследования заключаются в:

1. Определении значений параметров функции вероятности возможности реализации КА во времени.
2. Автоматизации сбора и анализа информации из общедоступных источников информации о КА для прогнозирования векторов КА во времени с точки зрения нарушителя.

СПИСОК ЛИТЕРАТУРЫ

11. Чои С. A Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments = Исследование по анализу информации о поведении вредоносного кода для прогнозирования угроз безопасности в новых средах / С. Чои, Т. Ли, Д. Квак // KSII Transactions on Internet and Information Systems. – 2019. – № 13 (3). – С. 1611–1625.
12. Фенг Б. Stopping the Cyberattack in the Early Stage: Assessing the Security Risks of Social Network Users = Остановка кибератаки на ранней стадии : Оценка рисков безопасности пользователей социальных сетей / Б. Фенг, Ц. Ли, Ю. Цзи [и др.] // Hindawi magazine. – 2019.
13. Налини М. Digital risk management for data attacks against state evaluation = Цифровое управление рисками для атак на данные против оценки состояния / М. Налини, А. Чакрам // International Journal of Innovative Technology and Exploring Engineering (IJITEE). – 2020. – № 88.
14. Деб А. Predicting Cyber Events by Leveraging Hacker Sentiment = Прогнозирование кибер-событий с помощью настроений хакеров / А. Деб, К. Лерман, Э. Феррара // Information. – 2018. – № 9 (11). – С. 18.
15. Зенебе А. Cyber Threat Discovery from Dark Web = Обнаружение киберугроз из Даркнета / А. Зенебе, М. Шумба, А. Карилло, С. Куэнка // EPiC SeriesinComputing. – 2019. – № 64. – С. 174–183.
16. Рогерс Э. Diffusion of Innovations = Распространение инноваций / Э. Рогерс, А. Сингал, М. М. Квинлан // New York: Free Press. – 2002.
17. Бас Ф. A new product growth model for consumer durables = Новая модель роста потребительских товаров длительного пользования / Ф. Бас // INFORMS. – 1969. – № 15 (5). – С. 215–227.
18. Мансфилд Э. Technical Change and the Rate of Imitation = Технические изменения и скорость имитации / Э. Мансфилд // The Econometric Society. – 1961. – № 29 (4).
19. Хагерстранд Т. Innovation diffusion as a spatial process= Дифуззия инновации как пространственный процесс / Т. Хагерстранд // Chicago, University of Chicago Press. – 1967.
20. Карта распространения сетевого червя WannaCry. – Изображение (картографическое; неподвижное; двухмерное) : электронное // Intel : [сайт]. – URL : http://web.archive.org/web/20170519161205/https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all (дата обращения: 08.07.2021).

Иваников А.А.
СКФУ, магистрант,
e-mail: armgedon@mail.ru

МЕТОДЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОРПОРАТИВНУЮ СИСТЕМУ ПРЕДПРИЯТИЯ: СРАВНЕНИЕ И АНАЛИЗ

Аннотация

В данной статье рассматриваются системы обнаружения и предотвращения вторжений, а также приводится краткое описание структуры и принципов их работы. Отдельно в статье уделено внимание сравнению и анализу методов обнаружения вторжений в корпоративную систему предприятия, выявлен наиболее предпочтительный.

Ключевые слова: обнаружение вторжений, предотвращение вторжений, корпоративная система.

По данным исследования Data Breach Investigation report, проведенном компанией Verizon в текущем году, более 90% всех атак, направленных на корпоративные информационные ресурсы, проводятся сторонними структурами-злоумышленниками, не имеющими никаких преимуществ в информационной сети жертв.

Еще одной из ключевых угроз безопасности критически важных информационных систем являются сотрудники предприятия, которые, даже не подозревая этого, в процессе своей работы в глобальной сети подвергают свое рабочее место риску стать частью информационного ресурса взломщика. Хакерская атака на компьютер сотрудников корпоративной сети является крайне опасной, так как мгновенно открывает неограниченный доступ к критически важным информационным ресурсам компании.

Корпоративные системы предприятий нуждаются в постоянном совершенствовании технологий безопасности в связи с тем, что постоянно растёт количество атак, а также ежегодно появляются новые, более совершенные методы сетевых вторжений.

Одним из исследований, ежегодно проводимых для мониторинга положения дел в области безопасности корпоративных систем является исследование компании Kaspersky. По данным последнего исследования за 2020 год, общее количество атак на сетевые корпоративные ресурсы показало четырёх кратный рост по сравнению с аналогичным периодом прошлого года: с 550 млн до 1,9 млрд. С целью мониторинга, анализа и выявления различных типов атак на корпоративные ресурсы предприятиями используются специализированные программно-аппаратные комплексы обнаружения и предотвращения вторжений (сокр. – СОВ/СОА).

Сегодня СОВ/СОА (англ. - IDS/IPS, Intrusion detection system / Intrusion prevention system,) — неотъемлемый компонент защиты критически важных информационных ресурсов от сетевых атак. Главное назначение этих систем — обнаружение попыток несанкционированного доступа к данным в корпоративной сети и защита от этих атак путем выполнения комплекса мер противодействия: изменение правил брандмауэра и сетевых политик, разрыв сетевого соединения, информирование специалистов по информационной безопасности о факте атаки.

К ключевым возможностям таких систем можно отнести:

– мониторинг сети в режиме реального времени для выявления сетевых атак;
– поиск и выявление различных вирусных программ;
– применение разнообразных методов выявления вредоносной активности;
– своевременное оповещение специалистов по информационной безопасности о случившихся атаках.

Структуру систем обнаружения и предотвращения вторжений можно представить в виде трёх уровней.

1. Сенсоры обнаружения и предотвращения атак.
2. Подсистемы централизованного управления.
3. Автоматизированное рабочее место (АРМ) специалиста информационной безопасности.

Первый уровень представляет собой устройство контроля трафика, подключаемые в наиболее важных точках сетевой инфраструктуры.

Второй – осуществляет контроль и управление событиями в информационной системе предприятия посредством различных консолей.

Последний уровень осуществляет непосредственное управление всеми индикаторами обнаружения и предотвращения вторжений в информационные ресурсы предприятия.

Типовая схема системы предотвращения и обнаружения вторжений представлена ниже на рисунке 1.

Рис. 1. Схема IPS IDS системы предотвращения и обнаружения вторжений

Среди задач, которые должна решать система можно выделить четыре основные.

Постоянный мониторинг и оперативная реакция на внешнее и внутреннее сетевое воздействие со стороны злоумышленников в режиме реального времени.

Анализ и консолидация статистики вредоносной сетевой активности в критически-важных информационных ресурсах предприятия с последующей ее визуализацией в виде общего состояния информационной безопасности в корпоративной системе.

Отслеживание работы сотрудников в сети «Интернет» и предотвращение

возможных угроз на границе внутренней и внешней сетей.

Обеспечение соответствия информационной безопасности на предприятии различным требованиям нормативных правовых актов как российских, так и международных.

Ключевыми методами обнаружения атак, используемыми в СОВ/СОА, можно назвать следующие: метод сигнатурного анализа, метод, основанный на анализе статистических данных, метод контроля целостности системы, методы основанные на использовании нейросетевого и иммунного анализа, метод, основанный на мониторинге общего состояния системы, метод генерации сценариев атак с использованием графов, экспертные системы, методы, основанные на использовании спецификаций защищаемой системы, метод анализа кластеров системы, метод с использованием поведенческих биометрических характеристик.

Метод сигнатурного анализа в ходе своей работы осуществляет сопоставление базы данных, в которую занесены заранее предопределенные значения о состоянии системы и действия, которые можно над ней осуществлять с их текущими характеристиками. К основному плюсу данного метода, позволяющему одновременно уменьшить вероятность ложноположительного срабатывания и увеличить его скорость, можно отнести, то, что поиск осуществляется только по полному соответствию признаков известных атак.

Метод анализа статистических данных в ходе своей работы собирает данные различных параметров защищаемой им системы, которые принимаются за так называемое «нормальное» поведение системы и затем на основе этих данных формируются статистические профили используемые для обнаружения атаки. При использовании данного метода обнаружение атаки на информационную систему происходит посредством отклонения параметров этой системы от допустимых значений.

Метод, основанный на использовании анализа общего состояния системы, можно интерпретировать в виде ориентированного графа, где его вершинами являются функциональные характеристики системы, выявленные в ходе её нормальной эксплуатации.

В ходе использования этого метода осуществляется поиск недопустимых путей в построенном ориентированном графе, если таковой путь был обнаружен, это может являться сигналом о вторжении в данную, защищаемую систему.

Метод генерации сценариев атак с использованием графов, хотя и содержит в своей основе построение графов, но в отличие от рассмотренного ранее метода, включает все возможные пути атаки. Помогает ему в этом так называемое свойство корректности системы, именно оно позволяет данному методу трактовать те или иные события в системе как нормальное поведение или же отклонение от него, что в свою очередь может свидетельствовать о потенциальной атаке на защищаемую систему. К основному достоинству данного метода можно отнести формирование в ходе эксплуатации наиболее полной базы отклонений в поведении защищаемой системы, что в свою очередь увеличивает количество обнаружений возможных атак.

Метод обнаружения атаки в основе которого лежит применение экспертных систем в ходе его использования представляет защищаемую им систему в виде различных фактов и требований для её нормального функционирования. Вывод о начале атаки на корпоративные информационные ресурсы предприятия экспертные системы делают на

основании этих фактов и требований, которые они получают в начале работы.

Методы, основанные на спецификациях – это описание совокупности ограничительных мер, призванных предотвратить недопустимое поведение объектов в корпоративной системе предприятия. К этой совокупности могут относится различные ограничения, например, список недопустимых действий и их комбинаций, ограничения на время действия, запрет на использование ресурсов.

Метод иммунных сетей заключается в имитации механизма негативной селекции, основанного на сравнении эталонного профиля с раннее неизвестными автоматически генерируемыми сигнатурами. Если же говорить о методе, основанном на использовании нейронных сетей, то он рассматривает не только защищаемую информационную систему, но и воздействующие на нее действующие объекты. Метод обнаружения вторжений с применением нейросетевого анализа основан на способности системы к самообучению. Все атаки делятся на классы, примеры которых используются для обучения нейронной сети, что позволяет выявлять принадлежность текущей атаки к одному из этих классов.

Что касается кластерного анализа, то в его основе лежит использование кластеров. Кластеры – это совокупность векторов-свойств защищаемой системы, которые делятся на допустимые и не допустимые. Существует множество методов кластерного анализа и в каждом из них используются различные метрики, которые позволяют сделать вывод о допустимости того или иного кластера.

Ниже в таблице 1 представлено общее сравнение методик обнаружения атак по совокупности характеристик.

Табл. 1. Сравнение методик обнаружения атак

Методы	Уровень наблюдения за системой	Верифицируемость	Адаптивность	Устойчивость	Вычислительная сложность
Анализ сигнатур	Host; Network; Application	+	-	глобальная	O(logn)
Статистический анализ	Host; Network	-	+	локальная	O(n)
Контроль целостности	Host	+	-	глобальная	O(n)
Анализ систем состояний	Host; Network; Application	+	-	локальная	O(n)
Графы сценариев атак	Host; Network; Application	+	+	локальная	NP
Экспертные системы	Host; Network;	+	+	глобальная	NP
Методы, основанные на спецификациях	Network;	+	-	локальная	O(logn)
Нейронные сети	Host; Network; Application	+	+	локальная	O(n)
Иммунные сети	Host; Network;	-	+	локальная	O(n)
Кластерный анализ	Host; Network; Application	-	+	локальная	O(n)
Поведенческая биометрия	Host;	-	+	локальная	O(n)

Из перечисленных выше, наиболее эффективными на сегодняшний день, в связи с постоянным ростом как общего количества атак, так и разнообразия их типов являются адаптивные методы.

На основании анализа, приведенного в таблице 1, можно сделать вывод, что к методам адаптивного типа можно отнести метод, основанный на анализе статистических данных, метод генерации сценариев атак с использованием графов, метод с использованием экспертных систем, методы, основанные на использовании нейросетевого и иммунного анализа, метод с использованием поведенческих биометрических характеристик.

Если рассматривать использование перечисленных методов на практике, то методы, базирующиеся на поведенческой биометрии и иммунных сетях не целесообразны к использованию в связи со сложностью их реализации. Также не целесообразны к использованию из адаптивных методов близкие друг к другу методы кластерного и статистического анализа в связи с большим риском ошибочного срабатывания. Также существенным недостатком перечисленных выше методов, который может привести к неправильной работе системы обнаружения вторжения, является отсутствие возможности изменить параметры объекта на этапе функционирования методов.

Таким образом, сравнительный анализ, проведенный в ходе работы, позволяет заключить, что методы, в основе функционирования которых лежат нейронные сети, являются наиболее предпочтительными с точки зрения обеспечения наибольшей безопасности корпоративных систем предприятия. Данные методы обладают целым рядом преимуществ, среди которых высокая способность к адаптации, малая вычислительная сложность, невысокая вероятность ложного срабатывания, что в совокупности дает возможность выявлять различные типы атак, как известные на данный момент, так и потенциально возможные, а также позволяет обеспечить наиболее надежное функционирование систем обнаружения и предотвращения вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. Кириленко В.П. Международное право и информационная безопасность государства. СПб.: СПбГИКиТ, 2016. 396с
2. Брюховецкий А.А., Сосоновский Ю.В., Милюков В.В. Фундаментальное исследование в области методов построения систем обнаружения и предотвращения сетевых вторжений. Вестник СЕВНТУ. 2017. №154. с. 60-63
3. Царегородцев, Тараскин: Методы и средства защиты информации в государственном управлении. Учебное пособие. Проспект, 2017. 208 с.
4. Соловьева И.В., Мандрица И.В., Петренко В.И., Копытов В.В., Жук А.П., Мандрица О.В., Рачков В.Е., Антонов В.В., Минкина Т.В. Методика технико-экономического обоснования проектных решений по информационной безопасности // Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (ИНФОБЕЗОПАСНОСТЬ -2019). / доклады XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции. Отв. редактор: В.И. Петренко. 2019. С. 183-193.
5. Naumenko V.V., Petrova T.M., Rachkov V.E., Minkina T.V. Analysis of modern decisions in the field of safety event management // Приоритеты и тенденции управления бизнес-процессами в структуре информационных систем: Сборник материалов Международной научно-практической конференции / СтГАУ. - Ставрополь: Агрус Ставропольского гос. аграрного университета, 2019. -С. 51-55.
6. Гусева Т.М., Партоян Р.Р., Ручий Н.С., Черкашин Е.В., Адамчук А.С. Анализ рисков информационной безопасности предприятия с использованием методики BSI Standart100-3 // Студенческая наука для развития информационного общества. /Сборник материалов X Всероссийской научно-технической конференции с международным участием. 2019. С. 68-75.

7. Иванников А.А. DLP-система и ее роль в предотвращении утечки конфиденциальной информации // В сб: Инновационные процессы в сфере информационных технологий и современного образования в регионах России / Сборник научных статей по материалам Всероссийской научно-практической конференции. Российский технологический университет МИРЭА, Московский финансово-юридический университет и др. 2020. С. 162-165.
8. Иванников А.А., Аткина Ю.В., Орёл Д.В., Минкина Т.В. Эффективность использования DLP-систем в предотвращении утечек конфиденциальной информации //В сб: «Теория и практика применения новых информационных технологий» / Сборник трудов II Всероссийской научно-практической конференции кафедры электротехники, автоматики и метрологии электроэнергетического факультета. 2021. С. 49-52.
9. Зарубин А. В., Харитонов С. В., Денисов Д. В., Смирнов М. Б. Основные драйверы и тенденции развития dlp-систем в российской федерации. Синергия, 2020. С. 75-90.
10. Мазитов Р.Р. Информационная безопасность Российской Федерации на современном этапе // Российская юстиция. 2017. No 11. С. 4-7.

Дорохов С.В.
РТУ МИРЭА, доцент, к.т.н., с.н.с.,
dorohov_s@mirea.ru
Михайлов В.Э.
МТУСИ, ассистент,
РТУ МИРЭА, ассистент,
v.e.mihaylov@mtuci.ru

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ SSRF ПРИ ЭКСПЛУАТАЦИИ WEB-ПРИЛОЖЕНИЙ

SSRF (Server-Side Request Forgery) – уязвимость WEB-приложений, позволяющая атакующему «спровоцировать» серверное программное обеспечение (ПО) на отправку HTTP-запросов на произвольный адрес [1], [2].

В независимом рейтинге OWASP Top 10 за 2021 год уязвимость SSRF занимает 10 место [3].

Во время типовой SSRF-атаки злоумышленник имеет возможность создавать подключения к внутренним сервисам инфраструктуры сети организации через атакуемый сервер. Также возможны варианты, при которых злоумышленник может подключаться к внешним ресурсам, что создает потенциальную возможность утечки конфиденциальных данных, таких как учетные данные авторизации. Уязвимость SSRF может быть использована при совершении DoS-атаки для сокрытия реального источника нападения [4].

Результатом успешной SSRF-атаки может являться получение несанкционированного доступа к данным в организации, уязвимому ПО либо другим серверам, с которыми данное ПО обменивается информацией. В некоторых случаях уязвимость SSRF позволяет атакующему выполнять произвольные команды на сервере.

Типовые SSRF-атаки

При проведении атаки SSRF часто используются доверенные соединения для эскалации атаки со стороны уязвимого WEB-приложения и выполнения несанкционированных действий. Такие доверенные соединения могут существовать по отношению к самому серверу или к другим внутренним системам в организации.

1) SSRF-атаки на сервер приложения

При выполнении атаки SSRF злоумышленник «заставляет» WEB-приложение совершать HTTP-запрос на сервер, на котором находится данное приложение, через loopback-интерфейс. При этом обычно используется IP-адрес *127.0.0.1* либо имя хоста *localhost*.

В качестве примера, приведенного в [5], рассмотрим WEB-приложение интернет-магазина, которое позволяет покупателю узнавать наличие товара на определенном складе. Для того чтобы предоставить информацию о наличии, приложение должно направлять различные REST API-запросы в зависимости от товара и склада, указанных в запросе. Данная функция реализуется путем передачи URL-адреса соответствующей конечной точке API на сервере через внешний HTTP-запрос. Таким образом, когда покупатель запрашивает факт наличия товара, веб-браузер делает запрос:

POST /prod/isInStock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
var=http://www.myownshop.org:8888/prod/isInStock/%3FprodID%3D78%26storeID%3D20

Такая процедура позволяет серверу совершать запрос на указанный URL-адрес, получать информацию о наличии товара на складе и направлять данные покупателю. В этой ситуации атакующий может модифицировать запрос через подстановку локального URL-адреса с целью несанкционированного получения информации. Например:

POST /prod/isInStock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
var=http://localhost/admin

В ответе от сервера будет находиться содержимое URL-адреса *http://localhost/admin*, которое направляется обратно пользователю.

Обычно административный функционал WEB-сайта доступен только определенным авторизованным пользователям. Использование уязвимости SSRF дает возможность злоумышленнику получить несанкционированный доступ к данным по адресу *http://localhost/admin* в обход локальной системы контроля доступа.

Соблюдение некоторых правил и рекомендаций поможет снизить риски от атак SSRF:

1. Проверка контроля доступа должна быть организована таким образом, чтобы проверять запросы от WEB-приложения к серверу.
2. В целях восстановления при внештатных ситуациях WEB-приложение должно обеспечивать административный доступ без процедуры авторизации любому локальному пользователю. Это позволит администратору системы получить доступ к информации при возникновении внештатных ситуаций.
3. Панель администратора должна располагаться по адресу с номером порта, отличным от используемого номера порта основного веб-сайта, чтобы не быть напрямую доступной для пользователей.

2) SSRF-атаки на другие серверные системы

Другой тип доверенных соединений, который часто возникает при подделке запросов на стороне сервера, имеет место быть при взаимодействии сервера приложений с другими внутренними системами, недоступными для пользователей напрямую. Поскольку серверные системы обычно защищены топологией сети, они часто имеют более слабый уровень безопасности. Во многих случаях внутренние серверные системы содержат конфиденциальные функции, доступ к которым может получить любой пользователь, взаимодействующий с данными системами.

В предыдущем примере предполагалось, что административный интерфейс доступен по внутреннему URL-адресу *http://172.16.0.1/admin*. Атакующий может проэксплуатировать SSRF-уязвимость в целях получения доступа к панели администратора через сформированный специальным образом HTTP-запрос:

POST /prod/isInStock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 94

var=http://172.16.0.1/admin

Способы обхода средств защиты от SSRF-уязвимостей

Нередко можно увидеть приложения, в которых используются потенциально опасные с точки зрения SSRF запросы совместно со встроенной защитой, направленной на предотвращение злонамеренного использования. Существуют способы обхода таких средств защиты.

1) SSRF с применением фильтров ввода на основе «черных» списков

Некоторые приложения блокируют ввод данных, содержащих в себе имена хостов *127.0.0.1* и *localhost* или конфиденциальные URL-адреса, например, /admin. Для таких ситуаций существуют различные техники обхода встроенной защиты:

1. Использование альтернативных представлений IP-адреса *127.0.0.1*.
2. Регистрация собственного доменного имени, которое бы указывало на *127.0.0.1*.
3. Обфускация заблокированного содержимого HTTP-запросов при помощи кодировок [6] или смены регистра вводимых символов.

2) SSRF с применением фильтров ввода на основе «белых» списков

В некоторых приложениях разрешается только ввод данных, которые соответствуют, начинаются или содержат разрешенные значения из «белого» списка [7].

Спецификация URL-адреса содержит ряд функций, которые могут быть упущены при реализации специального синтаксического анализа и проверки URL-адресов. К таким функциям относятся:

1. Возможность добавления учетных данных к URL перед именем хоста с использованием символа @.
2. Возможность использования символа # для обозначения фрагмента URL.
3. Возможность использования иерархии имен DNS для добавления требуемых данных в полностью определенное имя DNS, находящееся под контролем злоумышленника.
4. Возможность одновременного использования рассмотренных выше функций.

3) Обход SSRF-фильтров через открытое перенаправление

Иногда имеется возможность обойти защиту путем эксплуатации уязвимостей, связанных с открытым перенаправлением.

В предыдущем примере SSRF-уязвимости предполагалось, что отправленный пользователем запрос был тщательно проверен средствами защиты на предмет возможной SSRF-атаки. Однако приложения все также остаются подвержены другому типу уязвимостей – открытому перенаправлению. С применением API, используемого для создания внутренних HTTP-запросов, поддерживающих перенаправления, существует возможность формирования URL-адреса, который будет одновременно удовлетворять правилам фильтрации и содержать в себе перенаправление на внутренние ресурсы.

Например, предполагается, что приложение содержит в себе уязвимость, связанную с открытым перенаправлением, когда сформированный URL:
/prod/?curProdID=2&path=http://evildomain.org
осуществляет перенаправление на:

http://evildomain.org

В таком случае возможно использовать данную уязвимость для обхода URL-фильтра и проведения SSRF-атаки следующим образом:

POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
var=http://myownshop.org/prod/?curProdID=2&path=http://172.16.0.1/admin

Этот SSRF-эксплойт «работает» потому, что приложение, во-первых, проверяет, содержит ли значение переменной *var* разрешенное доменное имя. Во-вторых, приложение отправляет запрос на указанный адрес, в результате чего происходит открытое перенаправление на внутренний URL-адрес, указанный злоумышленником.

«Слепые» SSRF-уязвимости

«Слепые» уязвимости SSRF возникают, когда существует возможность «заставить» приложение отправить внутренний HTTP-запрос на указанный злоумышленником URL-адрес, при этом ответ от такого запроса не отображается в ответе приложения. Пример эксплуатации приведен в [8].

Поиск скрытого вектора проведения SSRF-атаки

Многие уязвимости, связанные с подделкой запросов на стороне сервера, относительно легко обнаружить, поскольку обычный трафик приложения включает в себя параметры запроса, содержащие полные URL-адреса.

1) Неполные URL-адреса в запросах

Иногда приложение помещает в параметры запроса только имя хоста или часть пути URL. Отправленное значение затем добавляется к полному запрашиваемому URL-адресу на стороне сервера. В случае если значение легко распознается в качестве имени хоста или пути URL, прослеживается потенциальный вектор развития атаки.

2) URL-адреса в форматах данных

Некоторые приложения передают данные в форматах, спецификация которых позволяет включать URL-адреса, которые могут быть запрошены анализатором данных. Когда приложение принимает данные в формате XML, оно может быть уязвимо к внедрению XXE-кода и, в свою очередь, уязвимо для SSRF-атаки через XXE. Данный вектор атаки описан в [9].

3) SSRF через заголовок “Referer”

Некоторые приложения используют специальное ПО для отслеживания посетителей [10], которое регистрирует заголовки “Referer” в запросах. Зачастую такое ПО «посещает» любой сторонний URL-адрес из заголовка “Referer” – обычно это делается для анализа содержимого сайтов по ссылкам. В результате открывается вектор атаки через SSRF-уязвимость.

Выводы

Вопросы обеспечения безопасности в современных WEB-технологиях являются актуальными на сегодняшний день. Рассмотренные в статье векторы проведения SSRF-атаки представляют высокую степень опасности для пользователей WEB-приложений. Поэтому администраторам веб-ресурсов необходимо выстроить надежную систему защиты от атак SSRF.

СПИСОК ЛИТЕРАТУРЫ

1. Веб-безопасность/Атаки SSRF [wiki.cyberschool.msu.ru] – URL: https://wiki.cyberschool.msu.ru/wiki/Веб-безопасность/Атаки_SSRF (дата обращения 18.11.2021). – Текст: электронный.
2. SSRF Bible. Cheatsheet [cheatsheetseries.owasp.org] – URL: https://cheatsheetseries.owasp.org/assets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet_SSRF_Bible.pdf (дата обращения 18.11.2021). – Текст: электронный.
3. OWASP Top 10:2021 [www.owasp.org] – URL: https://owasp.org/Top10/ (дата обращения 18.11.2021). – Текст: электронный.
4. Подделка запросов со стороны сервера (SSRF) [encyclopedia.kaspersky.ru] – URL: https://encyclopedia.kaspersky.ru/glossary/server-side-request-forgery-ssrf/ (дата обращения 18.11.2021). – Текст: электронный.
5. What is SSRF (Server-side request forgery) [www.portswigger.net] – URL: https://portswigger.net/web-security/ssrf (дата обращения 18.11.2021). – Текст: электронный.
6. Server Side Request Forgery [www.github.com] – URL: https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Request%20Forgery (дата обращения 18.11.2021). – Текст: электронный.
7. Server-Side Request Forgery (SSRF) and PortSwigger Academy Lab Examples [www.infinitelogins.com] – URL: https://infinitelogins.com/2021/01/09/server-side-request-forgery-ssrf-portswigger-academy-lab-examples/amp/ (дата обращения 18.11.2021). – Текст: электронный.
8. Подделка серверных запросов, эксплуатация Blind SSRF [www.habr.com] – URL: https://habr.com/ru/post/485888/ (дата обращения 18.11.2021). – Текст: электронный.
9. XML external entity attack SSRF With XXE [www.securiumsolutions.com] – URL: https://securiumsolutions.com/blog/xml-external-entity-attack-ssrf-with-xxe/ (дата обращения 18.11.2021). – Текст: электронный.
10. SSRF (Server Side Request Forgery) [book.hacktricks.xyz] – URL: https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery (дата обращения 18.11.2021). – Текст: электронный.

Губенков А.А.
СГТУ, доцент, к.ф.-м.н., доцент
gubenkovaa@sstu.ru
Буреев К.А.
СГТУ, студент
kir_bureev@mail.ru
Жильцов М.К.
СГТУ, студент
zhilcov.maksim@mail.ru

РАЗРАБОТКА НАБОРА СИГНАТУР ДЛЯ ОБНАРУЖЕНИЯ АТАК ТИПА LLMNR POISONING

Сигнатура атаки – это образец данных, используемый для идентификации сетевой атаки, эксплуатирующей уязвимость операционной системы или приложения [1]. Такие сигнатуры применяются системой обнаружения вторжений (СОВ) или межсетевым экраном для обнаружения вредоносного трафика. Разработанные сигнатуры позволяют системным администраторам и специалистам по информационной безопасности вовремя обнаруживать факт проведения атаки, записывать информацию о времени проведении атаки и об IP-адресе источника атаки, что облегчает расследование инцидентов информационной безопасности [2, 3].

Разработка сигнатур вредоносной активности проводится специалистами путем анализа поведения вредоносных программ и генерируемого ими сетевого трафика [4]. Программы, удаленно эксплуатирующие уязвимости, генерируют сетевой трафик, особенности которого могут быть соотнесены с конкретной атакой и являться индикатором компрометации системы, то есть информацией, свидетельствующей о проводимой атаке. Следовательно, характерные особенности генерируемого при проведении атаки сетевого трафика могут быть использованы при разработке правил для системы обнаружения вторжений [5]. Для перехвата и анализа трафика в локальной сети может быть использована программа Wireshark [6].

Разработка сигнатур атак проводится для сетевой системы обнаружения вторжений «Snort», т.к. эти правила могут использоваться и в ряде других СОВ, например «Suricata» или «Континент» [7]. В процессе разработки правил для СОВ Snort была использована локальная сеть, состоящая из виртуальных машин:

- Windows Server 2019 (LAB-DC),
- Windows 10 (USER-PC),
- Windows 10 (EMPLOYEE-PC).

В сети был настроен домен Active Directory с использованием сервера DNS и сервера LDAP.

В качестве компьютера атакующего внутри локальной сети выступала виртуальная машина Kali Linux 2021.2. Для тестирования создаваемых правил была установлена СОВ Snort версии 2.9.15.1 на машине Kali Linux с целью перехвата всего трафика, генерируемого системой атакующего.

Создаваемые правила размещались в файле local.rules, включенного с помощью директивы include в файл настроек snort.conf. Идентификатор SID пользовательских правил должен быть равен 1000000 или выше.

Тестовый запуск СОВ для проверки работоспособности правил осуществлялся посредством выполнения следующей команды:

sudo snort -c /etc/snort/snort.conf -A console -k none

Опция «-k none» использовалась для решения проблемы с отсутствием оповещений об исходящем вредоносном трафике.

Когда процесс инициирует сетевое подключение к компьютеру по имени хоста, операционная система пытается найти IP-адрес, соответствующий указанному имени, в локальном кэше и на DNS-сервере. Если сервером DNS запрошенное имя не было разрешено, то система Windows использует протокол LLMNR (Link-Local Multicast Name Resolution), предназначенный для обнаружения компьютеров в локальной одноранговой сети [8]. Протокол LLMNR пришел на смену устаревшему протоколу NetBIOS Name Service.

Протокол LLMNR обладает серьезным недостатком: любой компьютер в локальной сети может ответить на запрос, и в таком случае будет произведена попытка аутентификации на ответившем хосте, в ходе которой будут сразу отправлены имя учетной записи и NTLMv2-хэш пароля пользователя. Злоумышленник может попытаться восстановить пароль из хэша методом перебора с помощью таких программ, как Hashcat или John the Ripper, или использовать хэш для аутентификации на другом сервере с помощью техники Pass-The-Hash [3].

Атака LLMNR Poisoning заключается в отправке поддельных ответов на многоадресные запросы разрешения имени. Данная атака является очень распространенной и опасной, поскольку использует конфигурацию компьютеров по умолчанию [9]. Для предотвращения атаки и ее обнаружения, необходимо просматривать трафик в сети на наличие многоадресных запросов LLMNR, а также ответов на них. Оповещение об обнаружении многоадресного трафика LLMNR будет сообщать о наличии потенциально опасного трафика.

Как видно из записанного трафика, запросы LLMNR отправляются по протоколу UDP на порт 5355 на адреса 224.0.0.252 и FF02::1:3 (Рис. 1).

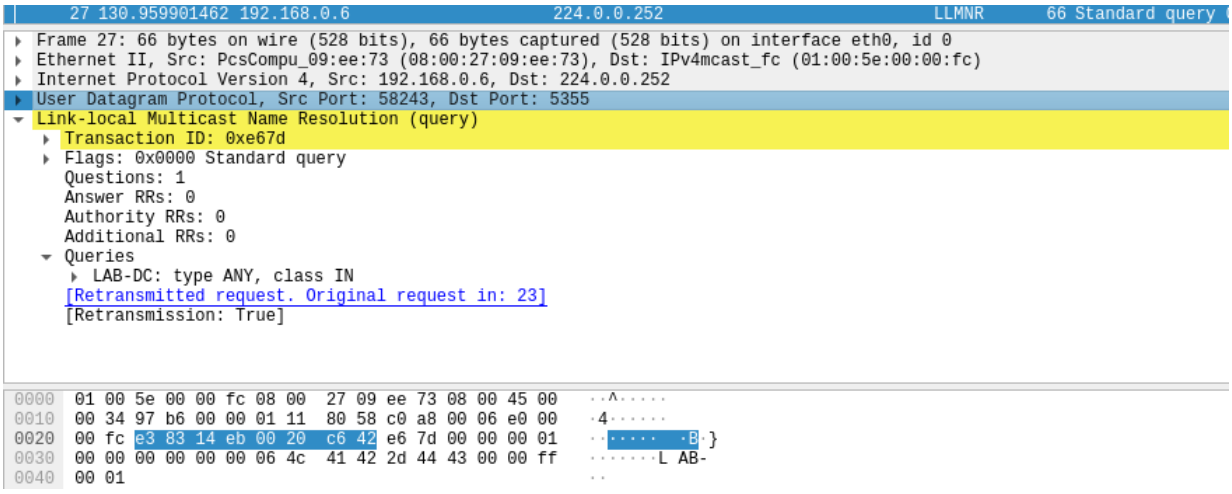


Рис. 1 Многоадресный запрос LLMNR

Ответы LLMNR отправляются в дейтаграммах с порта 5355, в заголовке установлен флаг Response (Рис. 2).

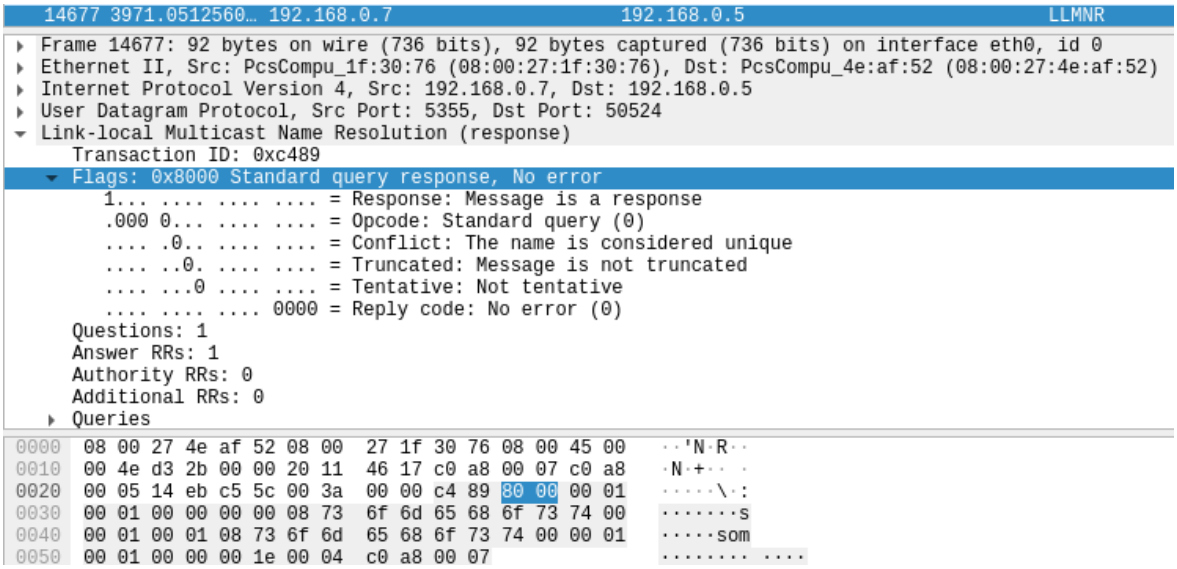


Рис. 2 Флаг Response в сообщении LLMNR

Следующий набор правил может быть применен для обнаружения нежелательного LLMNR трафика:

alert udp any any -> 224.0.0.252 5355 (msg:"Potentially risky LLMNR multicast traffic"; detection_filter: track by_dst, count 4, seconds 30; classtype:bad-unknown; sid:1000000;)

alert udp ::/0 any -> FF02::1:3 5355 (msg:"Potentially risky IPv6 LLMNR multicast traffic"; detection_filter: track by_dst, count 4, seconds 30; classtype:bad-unknown; sid:1000001;)

alert udp any 137 -> $BROADCAST_IP 137 (msg:"Potentially risky NetBIOS traffic"; detection_filter: track by_dst, count 2, seconds 30; classtype:bad-unknown; sid:1000002;)

alert udp any 137 -> 169.254.255.255 137 (msg:"Suspicious NetBIOS query within link-local range 169.254.0.0/16"; detection_filter: track by_dst, count 2, seconds 30; classtype:bad-unknown; sid:1000003;)

В целях уменьшения количества оповещений в правила добавлено поле detection_filter, позволяющее отправлять оповещение об обнаружении нежелательного трафика только после достижения определенного количества (count) перехваченных пакетов, на которых сработало правило, за определенное время (seconds), считая (track) по отправителю (by_src) или по адресату (by_dst). Количество сообщений и время следует устанавливать для конкретной сети исходя из количества компьютеров и обычного объема трафика в ней.

Дополнительно разработан набор сигнатур для обнаружения атаки LLMNR Poisoning по множественным ответам на запросы LLMNR за относительно короткое время. Количество ответов и время протестированы на примере атаки на один компьютер с помощью утилиты Responder. Тестовая атака была произведена вследствие инициированного системой жертвы подключения к несуществующему сетевому ресурсу, которая вызвала попытку разрешения неизвестного имени при помощи запросов LLMNR и NBT-NS. Значения count и seconds в данном наборе рекомендуется оставить без изменений.

alert udp any 5355 -> any any (msg:"Possible LLMNR Poisoning: More than 4 LLMNR replies in 30 seconds"; byte_test:1,&,0x80,2; detection_filter: track by_src, count 4, seconds 30; classtype:attempted-user; sid:1000004;)

alert udp ::/0 5355 -> any any (msg:"Possible LLMNR Poisoning: More than 4 IPv6 LLMNR replies in 30 seconds"; byte_test:1,&,0x80,2; detection_filter: track by_src, count 4, seconds 30; classtype:attempted-user; sid:1000005;)

Для работы данного набора сигнатур необходимо указание в файле набора правил или файле конфигурации snort.conf переменной $BROADCAST_IP, которая используется в правиле 1000002 и должна содержать широковещательный адрес для сегмента сети, в котором используется правило, к примеру:

ipvar BROADCAST_IP 192.168.0.255

Рекомендуется поместить объявление данной переменной сразу после объявления переменной HOME_NET, чтобы в случае изменения конфигурации сети не возникло проблем с работой правил.

На следующем скриншоте приведен результат обнаружения атаки LLMNR Poisoning (Рис. 3):

```
06/01-03:40:13.841983  [**] [1:1000001:0] Potentially risky IPv6 LLMNR multicast traffic [**] [Classification: Pot
entially Bad Traffic] [Priority: 2] {UDP} fe80::588e:c9c8:7e2c:4058:56551 -> ff02::1:3:5355
06/01-03:40:13.841983  [**] [1:1000000:0] Potentially risky LLMNR multicast traffic [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {UDP} 192.168.0.5:56551 -> 224.0.0.252:5355
06/01-03:40:13.842198  [**] [1:1000001:0] Potentially risky IPv6 LLMNR multicast traffic [**] [Classification: Pot
entially Bad Traffic] [Priority: 2] {UDP} fe80::588e:c9c8:7e2c:4058:63004 -> ff02::1:3:5355
06/01-03:40:13.842198  [**] [1:1000000:0] Potentially risky LLMNR multicast traffic [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {UDP} 192.168.0.5:63004 -> 224.0.0.252:5355
06/01-03:40:14.278402  [**] [1:1000001:0] Potentially risky IPv6 LLMNR multicast traffic [**] [Classification: Pot
entially Bad Traffic] [Priority: 2] {UDP} fe80::588e:c9c8:7e2c:4058:63004 -> ff02::1:3:5355
06/01-03:40:14.279020  [**] [1:1000000:0] Potentially risky LLMNR multicast traffic [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {UDP} 192.168.0.5:63004 -> 224.0.0.252:5355
06/01-03:40:14.774740  [**] [1:1000001:0] Potentially risky IPv6 LLMNR multicast traffic [**] [Classification: Pot
entially Bad Traffic] [Priority: 2] {UDP} fe80::588e:c9c8:7e2c:4058:63111 -> ff02::1:3:5355
06/01-03:40:14.774740  [**] [1:1000000:0] Potentially risky LLMNR multicast traffic [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {UDP} 192.168.0.5:63111 -> 224.0.0.252:5355
06/01-03:40:14.775031  [**] [1:1000001:0] Potentially risky IPv6 LLMNR multicast traffic [**] [Classification: Pot
entially Bad Traffic] [Priority: 2] {UDP} fe80::588e:c9c8:7e2c:4058:57320 -> ff02::1:3:5355
06/01-03:40:14.775031  [**] [1:1000000:0] Potentially risky LLMNR multicast traffic [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {UDP} 192.168.0.5:57320 -> 224.0.0.252:5355
06/01-03:40:14.775285  [**] [1:1000004:0] Possible LLMNR Poisoning: More than 4 LLMNR replies in 30 seconds [**] [
Classification: Attempted User Privilege Gain] [Priority: 1] {UDP} 192.168.0.7:5355 -> 192.168.0.5:63111
06/01-03:40:15.186030  [**] [1:1000001:0] Potentially risky IPv6 LLMNR multicast traffic [**] [Classification: Pot
entially Bad Traffic] [Priority: 2] {UDP} fe80::588e:c9c8:7e2c:4058:57320 -> ff02::1:3:5355
```

Рис. 3. Успешное обнаружение атаки LLMNR Poisoning

При появлении оповещений о нежелательном широковещательном трафике необходимо обратить внимание на то, что не на всех компьютерах в сети отключено использование протокола LLMNR, и предпринять соответствующие меры. Оповещения о множественных ответах на запросы разрешения имени могут свидетельствовать об успешно проводимой атаке LLMNR Poisoning и требуют немедленного реагирования.

Рекомендуется полностью отключать протокол LLMNR в локальной сети. Это можно сделать с помощью групповых политик на контроллере домена, создав новую политику, применяющуюся ко всем компьютерам и серверам в сети, и установив в ней значение «Enabled» для политики «Turn off multicast name resolution» в разделе Computer Configuration – Policies – Administrative Templates – Network – DNS Client.

Отключить LLMNR можно также локально на каждом компьютере, установив в редакторе локальной групповой политики значение «Включена» для «Отключить

многоадресное разрешение имен» в разделе Конфигурация компьютера – Административные шаблоны – Сеть – DNS клиент [8].

Таким образом, применение сигнатур для обнаружения сетевых атак является одной из возможных мер безопасности сети для своевременного реагирования на инциденты информационной безопасности [10]. Разработанные сигнатуры могут применяться в различных системах обнаружения вторжений для оперативного обнаружения и предотвращения сетевых атак типа LLMNR Poisoning.

СПИСОК ЛИТЕРАТУРЫ

1. Сигнатура атаки. Энциклопедия «Касперского» [Электронный ресурс]. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/attack-signature/ (дата обращения 31.10.2021)
2. Шелухин О.И. Системы обнаружения вторжений в компьютерные сети: учебное пособие / О.И. Шелухин, А.Н. Руднев, А.В. Савелов. – Москва: Московский технический университет связи и информатики, 2013. – 88 с.
3. Диогенес Ю. Кибербезопасность: стратегия атак и обороны / Ю.Диогенес, Э.Озкай. – Москва: ДМК Пресс, 2020. – 326 с.
4. Коллинз М. Защита сетей. Подход на основе анализа данных / М. Коллинз. – Москва: ДМК Пресс, 2020. – 308 с.
5. Буреев К.А. Разработка набора сигнатур для обнаружения атак на Active Directory / К.А. Буреев, А.А. Губенков // Проблемы управления в социально-экономических и технических системах: Материалы XVII Международной науч. конф. – Саратов: ИЦ «Наука», 2021. – С. 450-453.
6. Монаппа К.А. Анализ вредоносных программ / К.А. Монаппа. – Москва: ДМК Пресс, 2019. – 452 с.
7. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
8. Левицкий Н.Д. Справочник системного администратора. Полное руководство по управлению Windows-сетью / Н.Д. Левицкий. – М.:Наука и Техника, 2020. – 466 с.
9. Атаки на домен. Блог компании Инфосистемы Джет [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/jetinfosystems/blog/449278/ (дата обращения 31.10.2021)
10. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А.А. Губенков. – Саратов: СГТУ, 2009. – 88 с.

Пестов И. Е.,
СПбГУТ, старший преподаватель,
Федоров П. О.,
СПбГУТ, студент,
Алехин Р.В.,
СПбГУТ, студент,
Руденко С.А.,
СПбГУТ, студент,

ИССЛЕДОВАНИЕ ВОЗДЕЙСТВИЯ DDoS-АТАКИ НА ВИРТУАЛЬНУЮ МАШИНУ ПРИ НАЛИЧИИ И ОТСУТСТВИИ ТЕХНОЛОГИИ FIREWALL

Вступление

Для начала, рассмотрим определение DoS-атаки и её разновидности в виде DDoS-атаки. DoS-атакой называется атака, направленная на программно-аппаратный комплекс интеллектуальной системы с целью доведения последней до состояния неработоспособности. DoS-атаки различаются по принципу воздействия на цель. Одновременная атака с большого числа компьютеров свидетельствует о DDoS-атаке – распределенной атаке типа «отказ в обслуживании». Такую атаку так же называют распределенной. В результате DDoS-атаки на сетевой ресурс, подверженный нападению, поступает огромное количество запросов, которое система неспособна обработать, таким образом возникает нагрузка на различные компоненты хоста, в число которых входят RAM, CPU, сеть и память. В процессе нападения в определённый момент нагрузка достигает критического состояния, и интеллектуальная система доходит до частичного или полного отказа в доступе к ресурсам необходимым для рабочего процесса. Такие атаки, например, применяются, если необходимо вызвать отказ в обслуживании хорошо защищенной компании или правительственной организации.

Для полного восприятия эксперимента, на основе которого базируется данная публикация, немного вдадимся в подробности технологии межсетевого экранирования, так же известного, как Firewall или брандмауэр. Firewall – программно-аппаратный комплекс, который представляет собой своеобразный фильтр, регулирующий трафик, который поступает из внешней сети или, как ее принято называть, глобальной сети – Интернет, во внутреннюю, представляющую собой как сеть какой либо организации, так и домашнюю сеть. Одним из самых простых примеров сети может являться даже обычный, подключённый к сети Интернет, компьютер. Аналог такой сети и был взят за основу в эксперименте, описанном в данной статье. В общем виде брандмауэр позволяет производить разграничение входящего трафика по двум основным типам. Первым способом фильтрации трафика является фильтрация типа «разрешено всё, что не запрещено», при котором блокируется только тот трафик, который был запрещён администратором. Во втором способе фильтрации трафика будет проходить только тот трафик, который разрешён, что делает этот способ фильтрации более защищённым, этот способ имеет название «запрещено всё, что не разрешено».

Ход эксперимента

Перейдём к описанию экспериментального стенда, представленного на схеме 1.

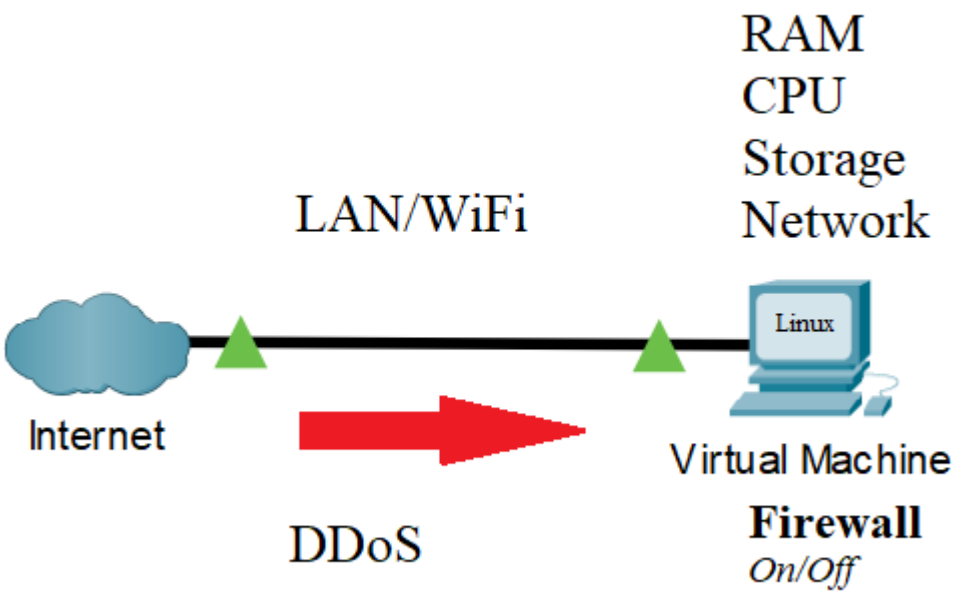


Рис. 4. Экспериментальный стенд

В качестве сети используется виртуальная машина в виде персонального компьютера, который может быть подключён к глобальной сети – Интернет, как LAN-кабелем, так и посредством беспроводного подключения. В рамках данной схемы у пользователя, который подвержен DDoS-атаке со стороны внешней сети – Internet, имеется межсетевое экранирование. Также у виртуальной машины, работающая на базе ОС семейства Linux, есть доступ к мониторингу нагрузки следующих своих составляющих: RAM, CPU, памяти и сети – что представлено на схеме.

В рамках эксперимента, на протяжении трёх часов виртуальная машина была подвергнута DDoS-атаке, с интервалом в каждые 10 минут происходила регистрация показателей нагрузки на составляющих устройства, подверженного атаке. Эксперимент проводился в 2 этапа при разных условиях – наличие и отсутствие брандмауэра.

На первом этапе исследования межсетевой экран был отключен. Результаты нагрузки компоненты виртуальной машины приведены на графиках.

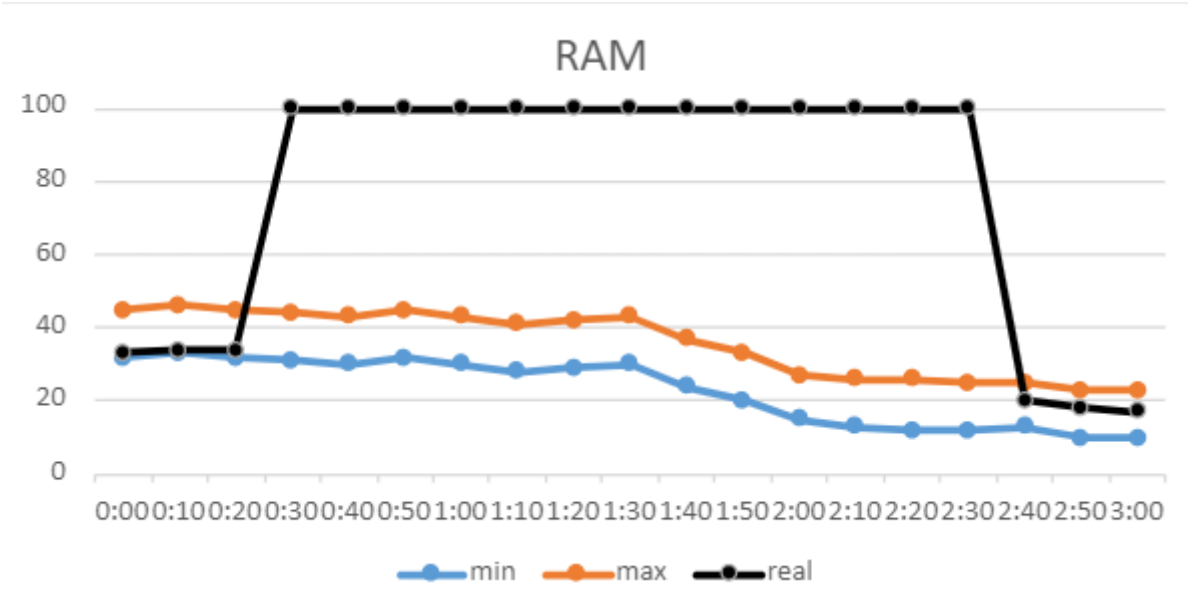


Рис. 2. Нагрузка на RAM

Реальная нагрузка на RAM (на графике изображена кривой «real») превышает допустимое значение (на графике изображена кривой «max»), что свидетельствует о чрезмерной нагрузке, замедляющей процесс взаимодействия компонентов системного ресурса, что соответствует уменьшению производительности машины.

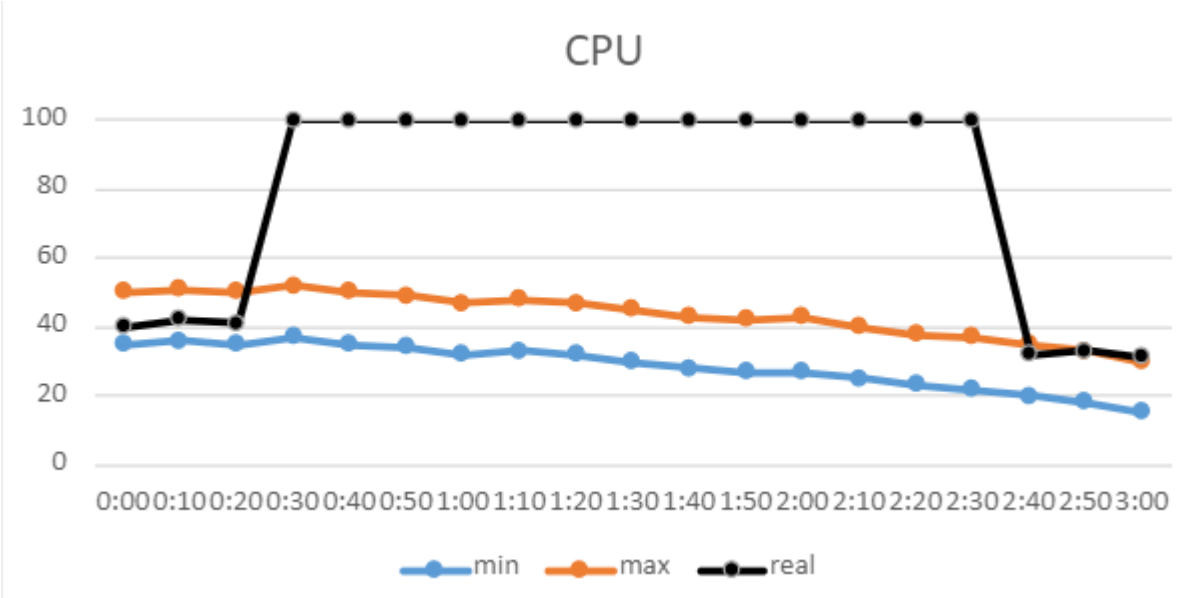


Рис.3. Нагрузка на CPU

Реальная нагрузка на CPU (на графике изображена кривой «real») превышает допустимое значение (на графике изображена кривой «max»), что демонстрирует загруженность CPU, который из-за этого не в состоянии в полной мере выполнять свои функции, а именно: ввод и вывод данных, обработка данных, адресация памяти и др.

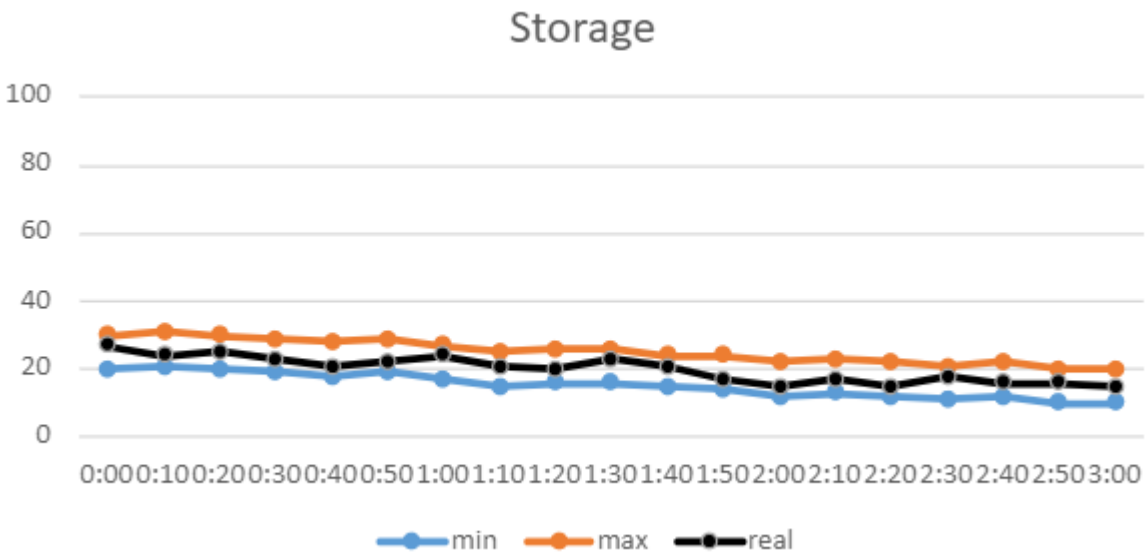


Рис.4. Нагрузка на память

График нагрузки на память демонстрирует, что память остаётся работоспособной в момент DDoS-атаки.

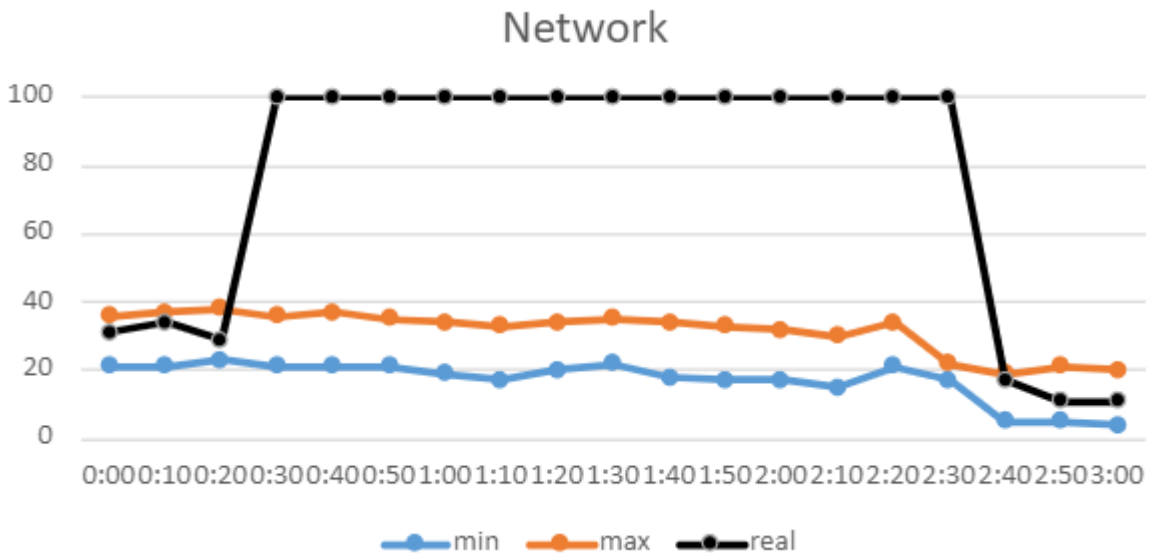


Рис.5. Нагрузка на сеть

Реальная нагрузка на сеть (на графике изображена кривой «real») превышает допустимое значение (на графике изображена кривой «max»), что препятствует нормальному взаимодействию пользователя с глобальной сетью – Интернет.

На втором этапе эксперимента межсетевой экран был выключен. Результаты нагрузки на компоненты машины представлены на графиках.

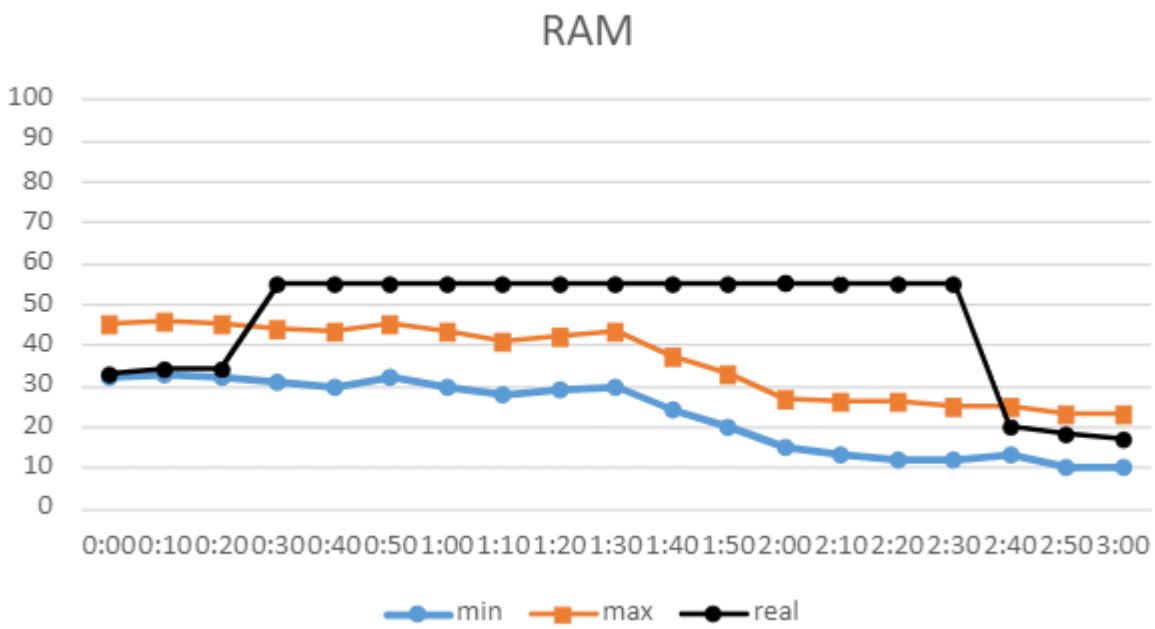


Рис.6. Нагрузка на RAM

Реальная нагрузка на RAM (на графике изображена кривой «real») незначительно превышает допустимое значение (на графике изображена кривой «max»), в сравнении с первым этапом нагрузка снижена.

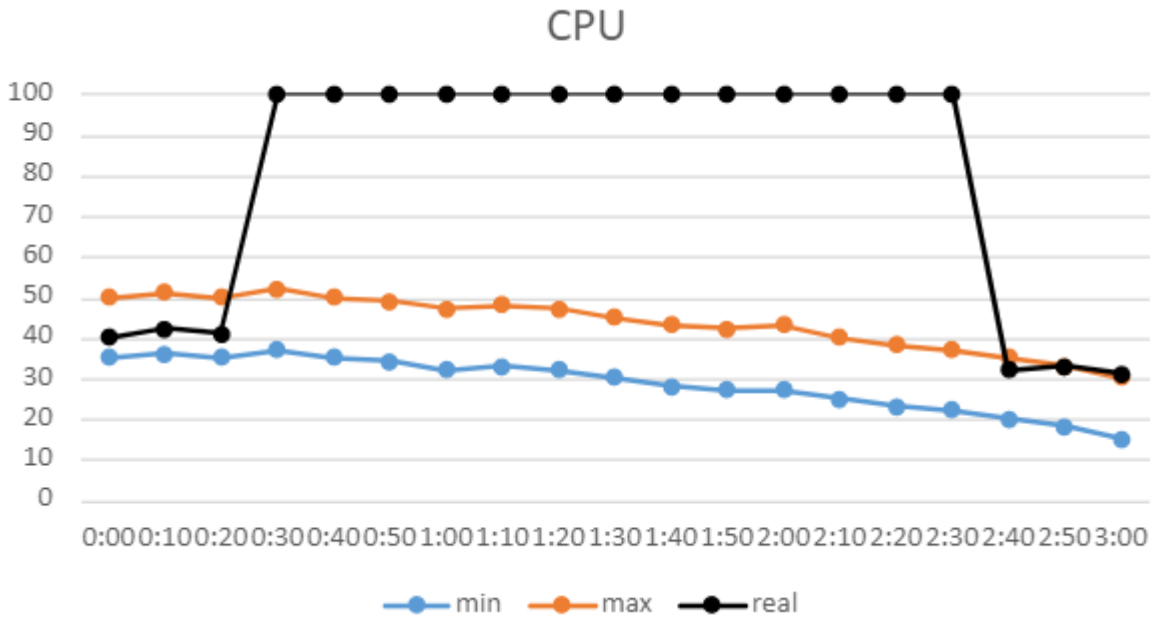


Рис.7. Нагрузка на CPU

Реальная нагрузка на CPU (на графике изображена кривой «real») превышает допустимое значение (на графике изображена кривой «max»), что соответствует значению на первом этапе исследования.

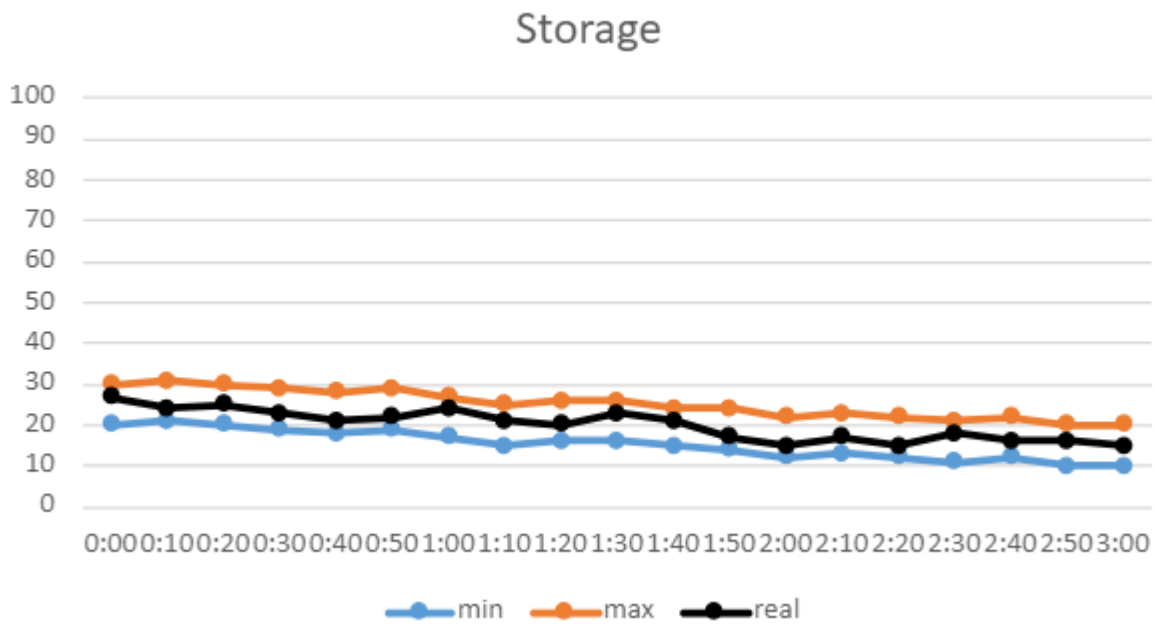


Рис.8. Нагрузка на память

Память также остаётся работоспособной в момент DDoS-атаки, при отключенном межсетевом экране.

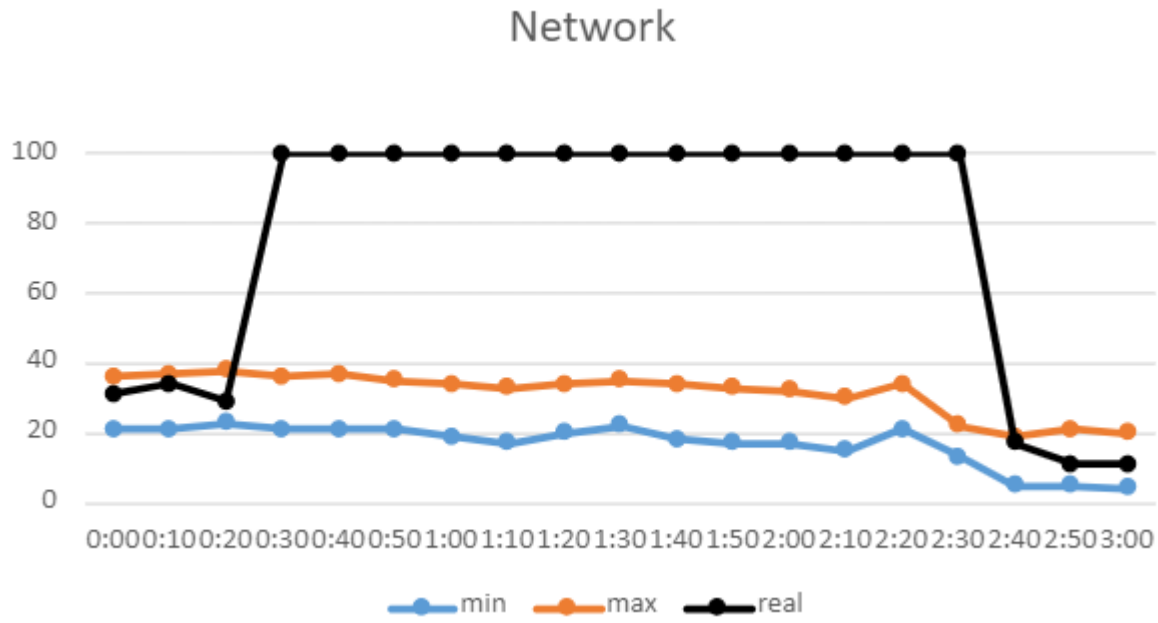


Рис.9. Нагрузка на сеть

Реальная нагрузка на сеть (на графике изображена кривой «real») превышает допустимое значение (на графике изображена кривой «max»), так же как и на первом этапе эксперимента.

Вывод:

Сопоставив и проанализировав графики в первом и втором этапе исследования, можно прийти к заключению о том, что выключение межсетевого экрана при DDoS-атаке влияет только на функционирование RAM, а остальные компоненты, находящиеся под мониторингом в ходе эксперимента, изменений не показали. Целесообразнее отключать

Firewall при данном типе атаке, так как при его отключении снижается нагрузка на RAM виртуальной машины.

СПИСОК ЛИТЕРАТУРЫ

1. ПРЕДУПРЕЖДЕНИЕ DOS-АТАК ПУТЕМ ПРОГНОЗИРОВАНИЯ ЗНАЧЕНИЙ КОРРЕЛЯЦИОННЫХ ПАРАМЕТРОВ СЕТЕВОГО ТРАФИКА *Лаврова Д.С., Попова Е.А., Штыркина А.А., Штеренберг С.И.*
2. ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ *Ушаков И.А., Красов А.В., Савинов Н.В. Учебник для студентов учреждений высшего профессионального образования / Москва, 2019.*
3. ЗАЩИТА ДЛЯ РАСПРЕДЕЛЕННЫХ ОТКАЗОВ В ОБСЛУЖИВАНИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ Гельфанд А.М., Косов Н.А., Красов А.В., Орлов Г.А. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи : в 4 т.. 2019. С. 329-334.
4. КОНТРОЛЬ, ИЗМЕРЕНИЕ И ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ ТРАФИКОМ *Алейников А.А., Билятдинов К.З., Красов А.В., Левин М.В. монография / Санкт-Петербург, 2016. Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 70–77.*
5. РАЗРАБОТКА МЕТОДОВ ПРОВЕРКИ СООТВЕТСТВИЯ СЕРВЕРОВ ВИРТУАЛИЗАЦИИ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ СОГЛАСНО СТАНДАРТУ ГОСТ Р 56938-2016 *Багомедова А.Р., Ушаков И.А., Цветков А.Ю. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 58–63.*
6. АНАЛИЗ БЕЗОПАСНОСТИ WI-FI СЕТЕЙ *Волкогонов В.Н., Казанцев А.А., Катасонов А.И., Орлов Г.А. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т. 2019. С. 270–275.*
7. ТЕХНИЧЕСКИЕ АСПЕКТЫ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ *Алейников А.А., Билятдинов К.З., Красов А.В., Кривчун Е.А., Крысанов А.В. Монография / Санкт-Петербург, 2016.*
8. ИССЛЕДОВАНИЕ СУЩЕСТВУЮЩИХ МЕХАНИЗМОВ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА LINUX *Цветков А.Ю. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 657–662.*
9. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ *Красов А.В., Левин М.В., Фостач Е.С. В книге: Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 520–522.*
10. МЕТОДИКА ВИЗУАЛИЗАЦИИ БОЛЬШИХ ДАННЫХ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ФОРМИРОВАНИЯ ОТЧЕТОВ УЯЗВИМОСТЕЙ *Красов А.В., Штеренберг С.И., Голузина Д.Р. Электросвязь. 2019. № 11. С. 39–47.*

Лукин В.С.
ПГУ, ассистент,
vitaly-lukin@mail.ru
Иванов А.И.
АО «ПНИЭИ», научный консультант,
bio.ivan.penza@mail.ru

ФОРМИРОВАНИЕ КОДА АУТЕНТИФИКАЦИИ ИЗ БИОМЕТРИЧЕСКИХ ДАННЫХ НА ОСНОВЕ АВТОМАТИЧЕСКОГО ОБУЧЕНИЯ НОВОГО КЛАССА ИСКУССТВЕННЫХ НЕЙРОНОВ СРЕДНЕГО ГАРМОНИЧЕСКОГО

Ключевые слова: информационная безопасность, уровень защищенности, аутентификация, нейросети, биометрия, пространство среднего гармонического, доверенная вычислительная среда, нейросетевой преобразователь биометрия-код.

В настоящее время биометрические системы аутентификации пользователей набирают всё большую популярность в сфере информационной безопасности из-за удобства пользования и возможности кодирования собственных биометрических признаков. В качестве мер по обеспечению защищенности данных мобильного пользователя применяется доверенная вычислительная среда (SD- и microSD-карты, SIM-карты) [1]. Совместное использование криптографии и биометрии существенно повышают уровень защищенности доверенной среды. Нейронные сети строятся по отечественному стандарту ГОСТ Р 52633.5 [2], который имеет существенный недостаток в виде хранения биометрического контейнера с таблицей весовых коэффициентов. Доказано, что в случае взлома контейнера, имея данные с таблицы весовых коэффициентов, можно подобрать код доступа. Кроме того, нейронные сети, построенные только на линейных нейронах, имеют симметрию. Известны атаки, позволяющие извлекать знания из нейронной сети, пользуясь этой симметрией.

Целью научной работы является защита цифрового биометрического образа личности через использование нового класса сетей нейронов среднего гармонического. Следует отметить, что в настоящее время существует достаточно много различных видов нейронов [3]. В ближайшем будущем ожидается создание групп из 9 и более статистических критериев, обладающих низкой корреляционной сцепленностью и приемлемой мощностью для многокритериальной оценки достоверности гипотезы нормального распределения данных малых выборок [4]. Основным отличием линейных нейронов от нейронов среднего гармонического является то, что многократно снижается число запоминаемых параметров [5]. Алгоритм, построенный вокруг гармонических нейронов, предусматривает хранение лишь одного порогового значения для прохождения этапа идентификации/аутентификации. По одному лишь значению злоумышленник не сможет взломать биометрический код-доступа пользователя. Реализация данного алгоритма позволит решить вопрос безопасности биометрических данных и отказать от хранения контейнера с таблицей весовых коэффициентов.

Одним из классов перспективных нейронов являются искусственные нейроны среднего гармонического. Искусственный нейрон, воспроизводящий работу этого нового критерия, описывается системой функциональных преобразований (1.1) [6, 7]. В этих преобразованиях не используются значения математических ожиданий $E(x_i)$ и

стандартных отклонений $\sigma(x_i)$. Как следствие данные таблиц, обученных искусственных нейронов среднего гармонического, не требуют их защиты классическим шифрованием.

$$\begin{cases} x \leftarrow sort(x) \\ \tilde{x}_i \leftarrow x_i - x_0 + 1 \\ sga \leftarrow 5 \cdot \sqrt[16]{\prod_{i=1}^{16} \tilde{x}_i} / \sum_{i=1}^{16} \tilde{x}_i \\ z(sga) \leftarrow "0" \ if \ sga \le k \\ z(sga) \leftarrow "1" \ if \ sga > k \end{cases} \quad (1.1)$$

где x_i – данные анализируемой выборки объемом в 16 опытов, z – операция квантования обогащенных накоплением данных, k – пороговое значение.

В рамках работы построена модель нейронной сети с использованием нейронов среднего гармонического. Результаты численного моделирования нейрона среднего гармонического отражает рисунок 1 [8]. На нём показана плотность распределения вероятности выходных состояний нейрона среднего гармонического, обученного распознавать малую выборку из 5 опытов с нормальным распределением и такую же малую выборку с равномерным распределением данных. При этом порог срабатывания выходного квантователя нейрона имеет вероятности ошибок первого и второго рода приблизительно равные значения $P_1 \approx P_2 \approx P_{EE} \approx 0.031$ [9]. Известно, что мощность нейрона среднего гармонического более чем в 2 раза выше мощности нейрона среднего геометрического 0.081/0.031≈2.61.

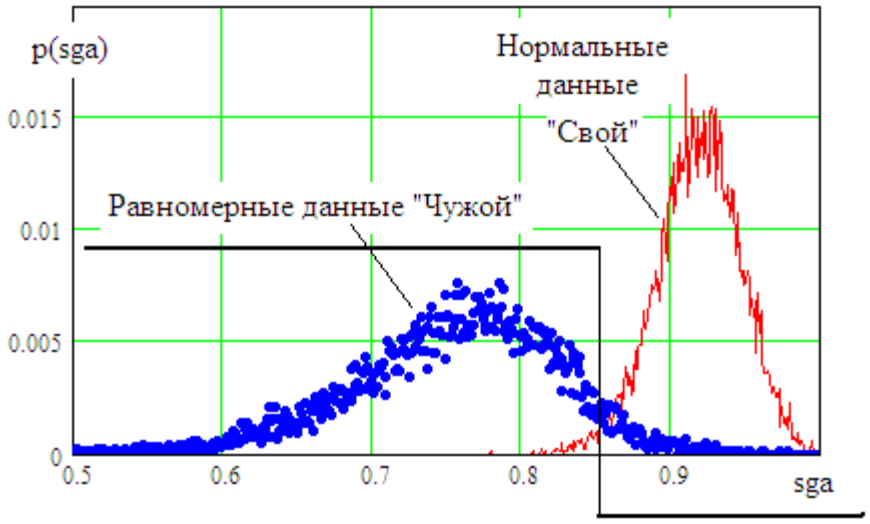


Рис. 1. Плотности распределения вероятности появления различных состояний, нейрона среднего гармонического с 5 входами, обученного различать малые выборки с нормальным и равномерным распределениями

Еще одним важнейшим фактором является то, что выходные состояния двух рассматриваемых нейронов имеют не полную корреляцию приблизительно равную 0.52. Запрет на использование нескольких нейронов, анализирующих одни и те же данные в разных нелинейных многомерных пространствах, может быть снят, если многомерные пространства накопления данных (обогащения данных) взаимно ортогональны. Если же

многомерные пространства нейросетевого полинома ортогональны не полностью, то запрет иметь общие входные связи значительно ослабляется.

Рассмотрен принцип построения таблицы связей для гармонических нейронов. Каждый бит ключа соответствует конкретному нейрону, который в свою очередь соответствует набору биометрических параметров. Рассмотрено построение алгоритма соответствия бита нейрона определенным разрядам (индексам) вектора биометрических параметров. Отличительной особенностью алгоритма является то, что таблица связей нейронов создаётся каждый раз при обучении, а не хранится отдельно зашитой в файле. Длина выходного ключа для сетей данного типа осталась неизменна и равна 265 битам – последовательность «0» и «1». В ходе тестирования выявлено необходимое количество входов для каждого нейрона, равное 16 разрядам. Создание таблицы происходит относительно природы биометрических данных (рисунка вен ладони, лица, почерка, голоса). В качестве входных образов при проведении работы использовались рукописные биометрические параметры (рисунок 2).

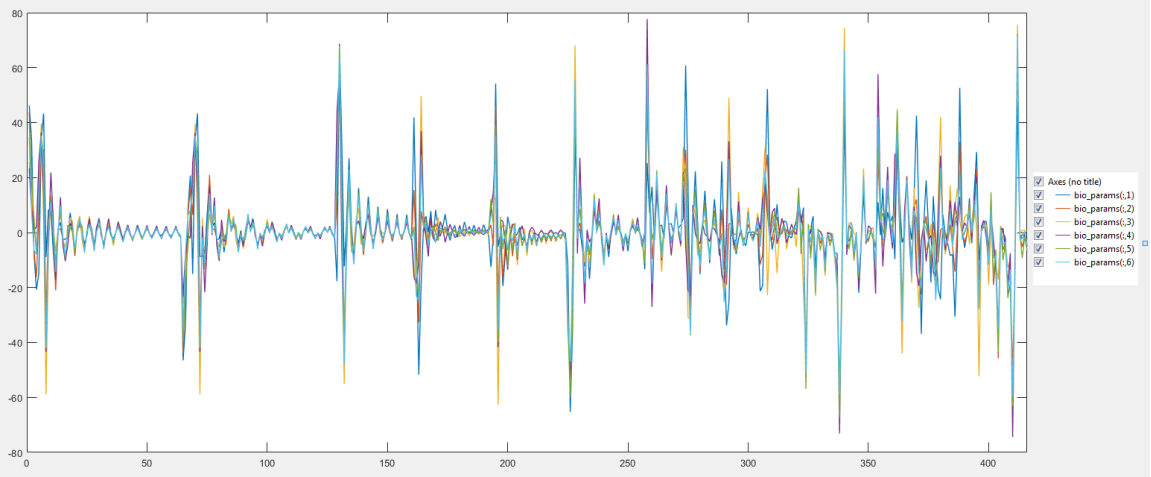


Рис. 2. Векторы биометрических параметров слова-пароля

В первую очередь необходимо построить вектор математического ожидания из обучающей выборки по каждому биометрическому параметру. Данный вектор имеет размер в 416 элементов, соответствующий стандарту снятия биометрических данных рукописного почерка. Далее на его основе строится сортированный вектор математического ожидания.

Для каждой биометрической технологии формируются рамки задания кода-доступа, который соотносится с полученным в ходе обучения вектором сортированного математического ожидания. Последним этапом является подстановка оригинальных индексов из вектора математического ожидания, относительно сортированного, а также получение порогового значения. На этапе идентификации каждый нейрон будет сравниваться с данным числом на предмет соответствия выходного кода. Данная схема обогащает работу нейронной сети и позволяет не хранить таблицу связей внутри биометрического контейнера.

Разработан программный макет нейросетевого преобразователя биометрия-код для аутентификации на основе нового класса сетей нейронов с обогащением данных в пространстве среднего гармонического – программный продукт «Среда моделирования «БиоНейроАвтограф» с нейронами среднего гармонического» (рисунок 3). Имеется свидетельство №2021661505 от 12 июля 2021 г.. о государственной регистрации

программы для ЭВМ (авторы: Лукин В.С., Иванов А.И. и др.). Для реализации программного продукта использован объектно-ориентированный язык C++, среда разработки «Visual Studio 2019».

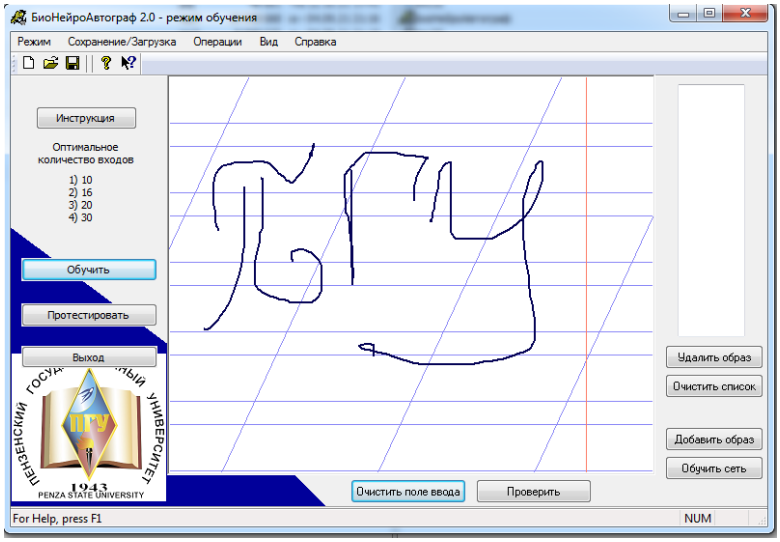


Рис. 3. Окно ввода образов для обучения «Среды моделирования «БиоНейроАвтограф» с нейронами среднего гармонического»

Ввод образов можно осуществлять с использованием компьютерной мыши или графического планшета.

С целью тестирования нейронной сети, построенной по разработанному алгоритму, был проведен ряд лабораторных работ. При проведении сравнительной оценки по качеству распознавания, сделаны следующие выводы:

1) на длинных паролях новая сеть работает приблизительно с тем же качеством, как и линейные сети. В результате оценки вероятности ошибки первого рода имеем практически равные ошибки первого рода. P_1=0.09 – для линейных сетей и P_1=0.095 – для гармонических;

2) на коротких паролях линейные сети работают лучше, несмотря на приемлемый результат, так как ошибка вероятности второго рода до 3 букв выше;

3) в результате тестирования качества на предмет ошибки первого рода, в обоих случаях результаты удовлетворительны требованиям работы нейронной сети для распознавания рукописного почерка;

4) в линейных нейронных сетях ошибки распределены равномерно для каждого разряда, а в гармонических – ошибка возникает в конкретных разрядах;

5) при оценке стойкости к атакам подбора частично и полностью скомпрометированного пароля было сделано 3 проверки:

а) Пользователь намеренно пытался идентифицировать посторонние пароли. Вероятность ошибки второго рода составила 0,0002771;

б) Посторонний пользователь пытался повторить почерк, зная парольное слово. Вероятность ошибки второго рода составила 0,0494;

в) Посторонний пользователь пытался повторить почерк, зная парольное слово и зная шаблон прописи. Вероятность ошибки второго рода составила 0,0494062848;

В случаях «а» и «б» получены отличные результаты, но доказано, что полная компрометация рукописного пароля приводит к практически полной утрате его стойкости к атакам подбора. Стойкость снижается до 10-20 попыткам атаки подбора;

6) математическое ожидание мер Хемминга (количества не совпавших разрядов кодовых откликов преобразователя биометрия-код на изучаемые образы [10]) у сети с линейными нейронами незначительно, но смещено к центру. На отрезке выходного кода от 20 до 40 бит преобладает большое количество попаданий у сети с гармоническими нейронами;

7) тестирование стойкости преобразователя биометрия-код необходимо проводить на реальных биометрических образах, имеющих значительно коррелированные данные, т.к. тестирование на совершенно случайных данных, полученных от программного генератора случайных чисел даёт значительную методическую погрешность, завышающую стойкость к атакам подбора;

8) в исследованных сетях также замечен эффект «дообучения». Среднее число данных для обучения меньше и составляет 5-7 образов, вместо 8-12, как представлено в сетях с линейными нейронами.

Все выводы подтверждены тестированием на больших объемах данных.

Стоит отметить, что нейронные сети, построенные на нейронах среднего гармонического, могут работать на любых биометрических данных, будь то отпечаток пальца, сетчатка глаза, голос, рисунок линий вен ладоней, статический или динамический образ лица и др. При выборе вида биометрических данных для тестирования руководствовались следующими требованиями: тестирование должно быть дешевым (то есть с минимальными финансовыми затратами), а также простым (не нужно долго собирать базу образов, а можно найти готовую в открытом доступе или самостоятельно, но быстро построить базу). Исходя из таких требований, наиболее подходящим оказался рукописный почерк, так как можно быстро и бесплатно создать базу биометрических данных. Тестирование проводилось на базе данных из 1000 образов рукописного почерка. Кроме того, алгоритм, осуществляющий работу созданного для тестирования программного продукта, достаточно прост в написании, а операции, проводимые в ходе выполнения программы, не требует высокой вычислительной мощности компьютера. Рукописный почерк не является самым надежным видом биометрических данных для осуществления биометрической идентификации пользователя, поэтому в перспективе планируется тестирование нейронных сетей, построенных с использованием нейронов среднего гармонического, на голосе и статистическом и динамическом образе лица. Уже ведутся работы по составлению баз данных этих видов биометрических образов, которые будут использоваться при тестировании в будущем.

По итогам проведенной работы выявлен ряд преимуществ использования нейронов среднего гармонического. Во-первых, использование нового класса сетей нейронов среднего гармонического повышает уровень защищенности цифрового биометрического образа личности, так как не хранит в себе таблицы весовых коэффициентов. Во-вторых, совместное использование в нейронной сети гармонических и линейных нейронов позволит исключить потенциальные атаки, построенные на симметрии, что также повысит уровень защищенности данных. В-третьих, совместное использование в нейронной сети гармонических и линейных нейронов позволит увеличить длину кода аутентификации из-

за линейной независимости, что повысит уровень защищенности данных от атак методом подбора.

В перспективе предлагается создание гибридных нейросетей в мобильной доверенной вычислительной среде, которые на половину состоят из линейных нейронов, на половину из гармонических нейронов, соотносящихся между собой в случайном порядке. Это позволит сэкономить память мобильного устройства из-за отсутствия необходимости хранения таблицы весовых коэффициентов для гармонических нейронов (особенно актуально для SIM-карт), а также повысить скорость работы за счет снятия нагрузки со слабых процессоров мобильных устройств (актуально для DS- и microSD-карт).

СПИСОК ЛИТЕРАТУРЫ

1. Безяев, А.В. Биометрико-нейросетевая аутентификация: обнаружение и исправление ошибок в длинных кодах без накладных расходов на избыточность: препринт / А.В. Безяев // Издательство ПГУ – 2020.
2. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа»
3. Князьков, В.С. Бескомпроматное привлечение сторонних ресурсов низкого доверия для выполнения вычислений высокого доверия в SIM- картах и microSD-картах с защитой персональных биометрических данных нейро-гомоморфным шифрованием / В.С. Князьков, А.И. Иванов, А.В. Безяев, В.С. Лукин // Безопасность информационных технологий. – 2021. – Т. 1. – С. 55-62
4. Иванов, А.И. Компактная графическо-иероглифная система отображения схем многообразных нейросетевых вычислений / А.И. Иванов, Е.А. Малыгина, В.С. Лукин // Известия высших учебных заведений. Поволжский регион. Технические науки. — 2020. — №4. — С. 5-18
5. Лукин, В.С. Доверенный искусственный интеллект, построенный с использованием нейронов среднего гармонического / В.С. Лукин, А.И. Иванов // Искусственный интеллект в решении актуальных социальных и экономических проблем XXI века. – 2021. – №1. – С. 441-445
6. Иванов, А.И. Коллекция искусственных нейронов эквивалентных статистическим критериям для их совместного применения при проверке гипотезы нормальности малых выборок биометрических данных / А. И. Иванов, А. Г. Банных, Е. Н. Куприянов, В. С. Лукин, К. А. Перфилов, К. Н. Савинов // Безопасность информационных технологий. – 2019. – С. 156-164
7. Иванов, А.И. Нейросетевое обобщение семейства статистических критериев среднего геометрического и среднего гармонического для прецизионного анализа малых выборок биометрических данных. / А.И. Иванов, К.А. Перфилов, В.С. Лукин // Информационно-управляющие телекоммуникационные системы, средства поражения и их техническое обеспечение. — 2019. — С. 50-63
8. Лукин, В.С. Сравнение мощности обычной и логарифмической форм статистических критериев среднего гармонического при использовании для проверки гипотезы нормального распределения данных малой выборки / В.С. Лукин // Известия высших учебных заведений. Поволжский регион. Технические науки. — 2020. — №4. — С. 19-26

9. Иванов, А. И. Учет влияния корреляционных связей через их усреднение по модулю при нейросетевом обобщении статистических критериев для малых выборок / А. И. Иванов, А. Г. Банных, Ю. И. Серикова // Надежность. – 2020. – № 20 (2). – С. 28-34
10. Андреев, Д.Ю. Сокращение затрат на нечеткую взаимную адресацию биометрических образов через использование взвешенной меры Хэмминга / Д.Ю. Андреев // Безопасность информационных технологий. – 2012. – Т. 8 – С. 32-35

Лисютин П.А.
АО «НИИ Кулон», инженер-конструктор
МТУСИ, аспирант
pavelis@yandex.ru
Малышев Г.А.
МТУСИ, студент
goshamal@yandex.ru

УСТРОЙСТВО КОММУТАЦИИ IMEI И SIM-КАРТ АБОНЕНТСКИХ ТЕРМИНАЛОВ ДЛЯ ИЗМЕРЕНИЯ ВРЕМЕНИ АУТЕНТИФИКАЦИИ В СЕТЯХ СОТОВОЙ СВЯЗИ 2G-4G

Современные абонентские терминалы (смартфоны) поколения 4G конструктивно выполнены в герметичном неразъемном корпусе с лотком для установки и извлечения SIM-карт (далее SIM).

В телефонах предшествующих поколений установка, перестановка (для аппаратов, оснащенных двумя держателями карт), извлечение SIM были возможны лишь после извлечения аккумулятора, то есть отключения питания телефона.

На факультативных занятиях по конструированию электронных устройств со студентами младших курсов МТУСИ на одном мобильном устройстве контакты питания аккумулятора были припаяны к контактам питания телефона с помощью отрезков проводов (Рис.1).

Рис. 5. Смартфон с открытым разъемом для установки SIM

Случайно возник вопрос: «Как поведет себя мобильное устройство при извлечении, установке, перестановке SIM при включенном питании?»

Оказалось, что в отличие от телефонов с лотком для SIM в телефонах поколения 2G и 3G отключение абонента от сотовой сети оператора, происходящее **в режиме телефонного разговора**, осуществляется с задержкой по времени.

Было бы интересно проверить происходит ли подобное при работе SIM с посекундной тарификацией (обзор тарифов операторов связи представлен в [1]), но это иная задача.

На Рис.2 представлен модифицированный абонентский терминал поколения 2G

Рис. 6. Мобильный телефон с открытым слотом для действий с SIM

Результат тестирования представлен в Таблице 1.

Табл. 1. Данные тестирования голосовой связи в Москве в ноябре 2021г.

№п/п	Модель абонентского терминала, год выпуска	Сеть сотовой связи	Операторы связи	Длительность отключения абонента от сети связи, время звонка	Примечание
1	Samsung SGH-D780 2008	2G	Городской стационарный телефон МГТС (исходящий) – Билайн (входящий)	Около трех секунд Выходной, 22 ч. по Московскому времени	После извлечения сим карты спустя три секунды происходит автоматическая программная

					перезагрузка абонентского терминала
2	Alcatel-985D 2012	2G	Городской стационарный телефон МГТС (исходящий) – Билайн (входящий)	До 1 минуты Будни, 22 ч.	Повторная аутентификация абонента без перезагрузки абонентского терминала не возможна
		3G	Теле2(исходящий)– Билайн (входящий)	7 секунд Будни 13 ч.	
			Билайн (входящий) -Теле2(исходящий)	14 секунд Будни 19 ч.	
3	Alcatel-4009D 2015	3G	Теле2(исходящий)– Билайн (входящий)	14 секунд Выходной 21 ч.	Возможна неоднократная повторная аутентификация абонента без перезагрузки абонентской станции
4	Vertex Impress Luck 2018	3G	-	-	
5	Xaomi 5A 2018	4G	Билайн (входящий) -Теле2(исходящий)	Мгновенное отключение в любое время	

В источнике [2] удалось выяснить, что в сети GSM процедуры аутентификации абонента в режиме голосовой связи и в режиме передачи данных во многом схожи и различаются длиной ключей RAND (128 бит для голоса и 32 бита для передачи данных).

В представленной на Рис. 3 архитектуре работы сети GSM аутентификация происходит с обращением к базе HLR (Home Local Reestr – Реестр домашних абонентов).

Как выяснилось, IMSI (идентификатор, записанный в память SIM) передается от абонентского терминала базовой станции единожды. После аутентификация происходит по присваиваемому базовой станцией абонентскому терминалу TMSI (временный мобильный идентификатор абонента).

По информации из статьи [3] для идентификации абонента в системе сотовой связи используется **IMSI**, который записан в SIM и HLR оператора, и **IMEI** мобильного телефона. После идентификации абонента в сети сотовой связи телефон может находиться в режиме IDLE (режим простоя) и DEDICATED (режим активного соединения и обмена данными с базовой станцией). Частота аутентификации абонентского терминала базовой станцией для этих режимов не известна.

При помощи сервиса Яндекс.Интернетометр. [4] анализировалось время прекращения идентификации в режиме приема-передачи данных в сети 4G.

В режиме **передачи данных абонентским терминалом** прекращение приема пакетов данных базовой станцией после извлечения SIM происходил мгновенно.

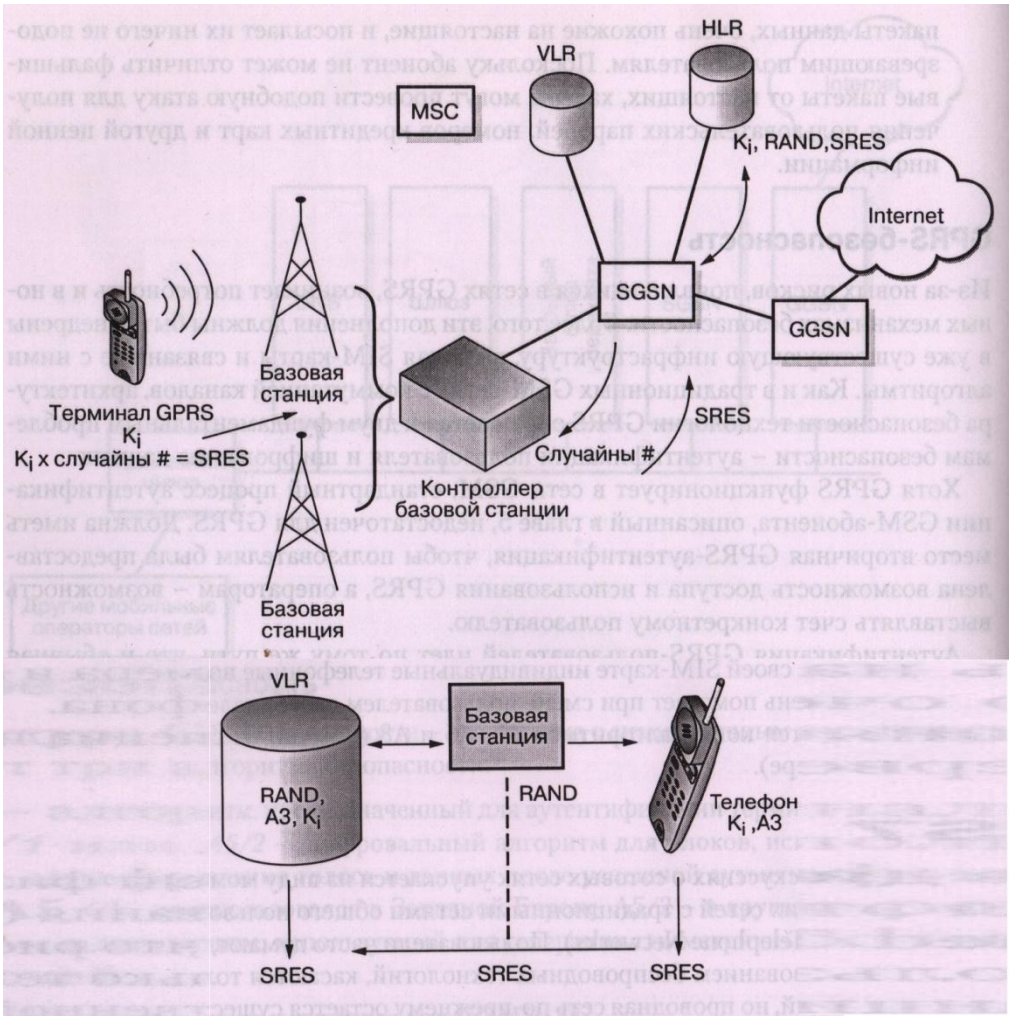


Рис. 7. Аутентификация абонента в сети GSM

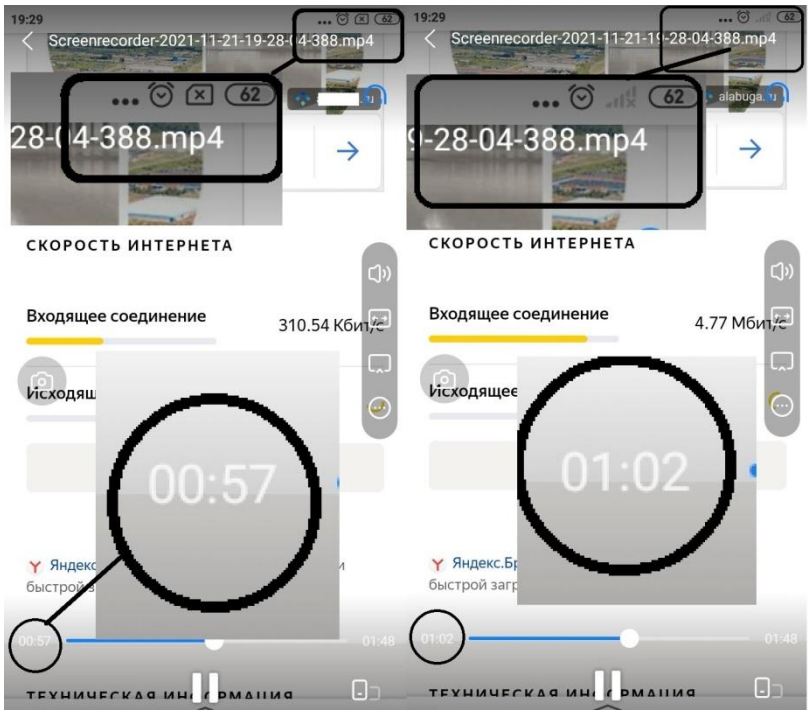


Рис. 8. Использование Яндекс.Интернетометр

В режиме **приема данных** абонентским терминалом прекращение приема пакетов данных после механического извлечения SIM происходил за время от 2 секунд при скорости около 100 Кбит/с и **до 6 секунд**, при скорости передачи данных в несколько Мбит/с.

На Рис. 4 совмещены две фотографии видео с записью работы сервиса «Интернетометр», сделанные в моменты извлечения SIM и отключения абонентского терминала базовой станцией от сети Интернет.

Время авторизации абонента в сети 4G после механической установки SIM около 10 секунд.

Возможно ли действиями с абонентским терминалом как-либо повлиять (продлить) время отправки ему базовой станцией пакетов данных? Например, отключив SIM на пиковой скорости в условиях высокого качества пропускного канала связи с базовой станцией?

Во избежание возможного риска [5]как остановки работы оборудования операторов сотовой сети связи было решено изучить вопрос в два этапа:

- создать **работоспособное** тестовое устройство – коммутатор SIM и IMEI на основе модифицированного мобильного телефона;

- предложить техническим специалистам операторов сотовой связи ознакомится с возможностью проведения опыта – попыткой повторной одновременной идентификации одного номера IMSI в сетях 2G-4G без физического клонирования SIM.

Коммутатор IMEI и SIM абонентских терминалов

В состав коммутатора IMEI и SIM (далее - Коммутатор) на Рис.5 входят:

- монтажная пластина;
- модифицированного мобильного телефона с двумя разъема для установки SIM;
- две SIM (одного или разных операторов);
- два блока из шести двухпозиционных тумблеров МТ1 ОЮ0.360.016ТУ, (первый из которых коммутирует IMEI, второй – переключает SIM) с подключёнными в пары общими контактами;
- корпус прибора, монтажные провода и материалы для паяния.

Рис. 9. В блоке тумблеров «2» (коммутация IMSI) установлена одна SIM

В общем случае SIM состоит из 6 контактов площадью $4 \times 2{,}5 = 10$ мм^2, а площадь каждого из шести контактов держателя SIM – менее 2 мм^2. Напряжение питание SIM составляет 3 вольта. Провода для контактов «передача» и «прием» данных необходимо выполнять в виде витой пары, но с учетом их небольшой длины (0,2 м на представленном рисунке 5) они проведены без свивания.

В сетях 4G и старше используются многоантенные системы передачи информации [6]. Не исключено, что в случае применения в Коммутаторе вместо одного двухсимочного абонентского терминала двух односимочных, - может потребоваться разнесение их в пространстве на некоторое расстояние. Для этого можно использовать кабель из витой пары с сечением жил 0,4мм^2, использовав для контактов питания SIM две жилы с суммарным сечением 0,8 мм^2 (в расчете взято значение 1 мм^2).

Для расчете потерь (на Рис.6) в проводах использовался онлайн калькулятор [7]. С инженерной точки зрения потери примерно в 3% по току для цепей питания вполне допустимы. Частота работы микропроцессора SIM не велика, поэтому помех из-за длинных линий теоретически возникнуть не должно и на расстояние в 25 метров в стороны от Коммутатора.

Для одновременной коммутации блоков из шести тумблеров взят простой кронштейн. Время переключения около одной секунды.

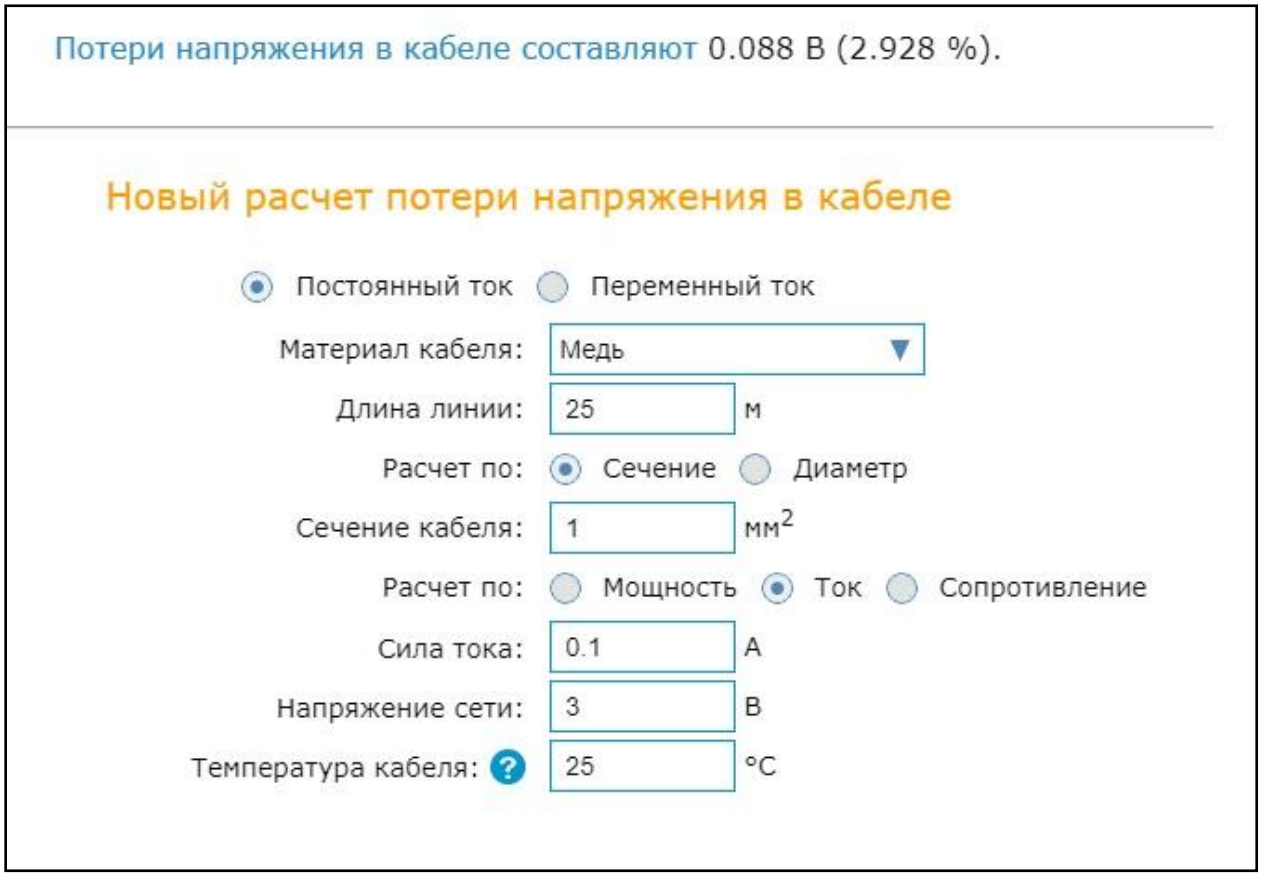


Рис. 10. Расчета потерь в линии.

Расчет абонентов сотовой связи (<u>без учета устройств M2M</u>)
на примере микрорайона Москвы

Попробуем оценить потенциал применения Коммутатора для атаки Denial of Service.

Рассчитаем среднюю загрузку базовой станции абонентами в Москве.

Расчет количества абонентов, охватываемых вышками сотовой связи, представлен в Таблице 2. Использован сервис геолокации вышек сотовой связи [8], выполнена проверка на местности, добавлена вышка, отсутствующая по данным сервиса.

Табл. 2. Расчет количества жителей.

№	Тип здания	Кол-во квартир	Кол-во домов	Кол-во жителей*
1	Пятиэтажное	48	2	288
2	Девятиэтажное	68	6	1224
3	16 эт.	160	1	640
4	17 эт.	200	1	800
5	18 эт.	300	1	1200
6	19 эт.	200	1	800
7	Переменной этажности	350	4	5600
8	20 эт.	228	1	912
9	22 эт.	400	1	1600
10	Офисы, магазины	-	-	250
	Итого:			13314 человек
*При расчете 3-4 человека в квартире				

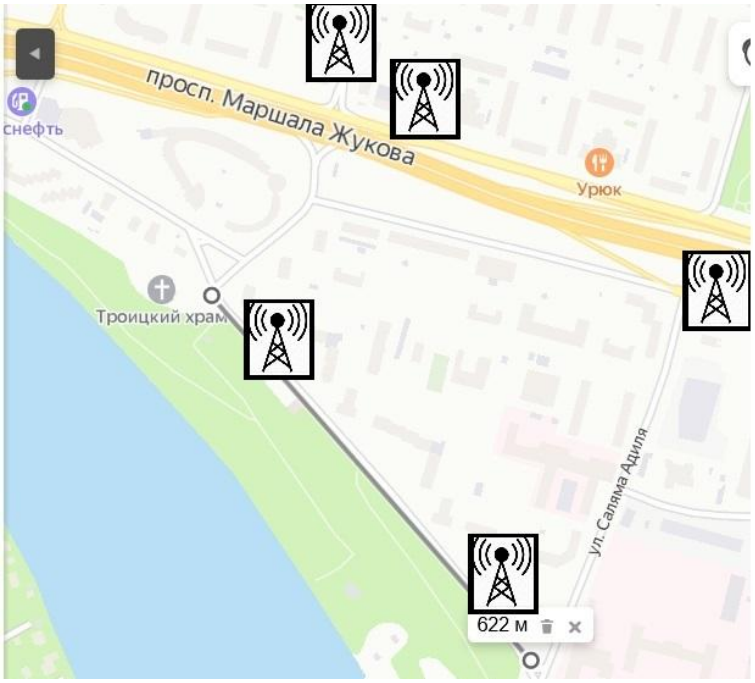


Рис. 11. Карта микрорайона с вышки связи

Площадь жилого участка примерно $0{,}5 \times (0{,}6 \times 0{,}6) + 0{,}32 = 0{,}5$ км2 с учетом прилегающей территории дороги, участка реки, парка. Расчетное значение количества жителей в Таблице 2 в целом соизмеримо со средней плотностью населения 5 тысяч человек на км^2.

Допустим, на одного жителя приходится 1,5 активные подключенные SIM, тогда количество абонентов равно 16 800 человек.

Осведомленность авторов статьи в вопросах аутентификации абонентских терминалов в сетях сотовой связи поколения 4G не позволяют достоверно подтвердить

гипотезу о том, что первичная аутентификация абонентов в сети требует *бОльших* вычислительных мощностей, чем последующая его периодическая аутентификация при приеме и передаче ему данных. Это предположение.

Предположим, что абонент выключает телефон (отключается от абонентской сети) не менее 1 раза в день в основном в рабочее время суток с 8 утра по 24 часа. Из них подавляющее количество раз происходит отключение питания из-за разряженного аккумулятора. Изменение TMSI абонентского терминала, которое в сетях 2G вычисляется с использованием связки IMSI IMEI, происходит не так часто.

Идентификация одного абонента в сети занимает примерно 5-10 секунд.

Коммутатор, способен переподключать SIM между двумя телефонами (IMEI) с минимально необходимым для аутентификации временем - 10 секунд.

За час создается 3600/10=360 подкл./час, или $360 \times 16 = 5760$ подключений в рабочее время суток.

Как видно из Рисунка 8 из-за механического истирание контактов осуществлять физическое перемещение SIM в абонентских терминалах SIM более 200-300 раз невозможно.

Рис. 12 Справа Nano SIM после 50-ти установок в слоты абонентских терминалов

Предположим, что антенна базовой станций в секторе 180 градусов состоит из 90 лучей диаграммы направленности. Наверняка, базовые станции организационно защищены от противоправных действий контролем видеонаблюдения от видеокамер и любая подозрительная активность может вызвать адекватную реакции.

Предположим, мы создали устройство из двух коммутаторов и четырех абонентских терминалах и четырех SIM на длинных 25 метровых проводах.

Предположим, пару человек, использующие Коммутатор, станут немного перемещаться («кружить») вокруг и рядом с вышкой базовой станции, изменяя направление прихода сигналов с запросом аутентификации их абонентскими терминалами к базовой станции. Базовая станции начнет тратить вычислительные мощности на постоянную аутентификацию этих абонентов, хаотично перемещающихся в пространстве со скоростью 50 м/с (180 км/ч) из расчета 2х25 метров в секунду.

Ежесекундно механически переключать IMEI и IMSI (TMSI) в течение 16 часов невозможно из-за человеческого фактора, хотя сам ресурс тумблеров модели МТ1 составляет в переключениях не менее 50 тысяч, при средней наработке на отказ 200 тысяч.

В то же самое время автоматизировать схему коммутации на реле с использованием микроконтроллера (например, Arduino) вполне посильная задача!

Выводы

Предложенный авторами «топорный» способ не претендует на научно-обоснованный метод аудита настроек идентификации базовой станции сети сотовой связи.

В том случае, если заинтересованные сотрудники сотовых сетей связи, сервисные инженеры телекоммуникационного оборудования сочтут возможным проверить озвученную гипотезу, то коллектив авторов статьи будет рад поучаствовать, доработать и предоставить рабочий прототип описанного устройства.

Возможная практическая значимость же разработанного устройства - простое приспособление для тестирования (аудита) фактических настроек базовых станций сервисными инженерами на местности, значительно приближенное к реальной характеристике состояния аутентификации абонентов сотовых сетей связи.

СПИСОК ЛИТЕРАТУРЫ

1. https://ural.topnomer.ru/blog/posekundnaya-tarifikaciya.html
2. Меритт М. Безопасность беспроводных сетей/ Меритт М., Поллино Д. // McGraw-Hill Osborne/ Компния АйТи (ISBN 5-98453-007-4) и ДМК Пресс (ISBN 5-94074-248-4), 2004 г. – 111-114 с.
3. Как работает радиоинтерфейс в GSM-сетях? https://habr.com/ru/post/268127/
4. Онлайн сервис: Яндекс.Интернетометр https://yandex.ru/internet/
5. Переездчиков И. Анализ опасностей промышленных систем человек-машина-среда и основы защиты/ Переездчиков И.В. // учебное пособие/ М.Кнорус ISBN 978-5-406-00245-2, - 2011 - 155 с.
6. Немировский М. Беспроводные технологии от последней мили до последнего дюйма/ Немировский М.С., Шорин О.А.// Учебное пособие М.С.– М.: Эко-рендз, ISBN 978-5-88405-091-4, - 2010 г. - 124-125 с.
7. Онлайн сервис: Калькулятор расчета потери напряжения в кабеле https://www.calc.ru/poteri-napryazheniya-v-kabele-kalkulyator.html
8. Сервис «Карта вышек сотовой связи» http://wifi4g.satx.ru/karta-vyshek-sotovoy-sviazi.php
9. Портал о современных технологиях мобильной и беспроводной связи http://www.1234g.ru.
10. Википедия https://en.wikipedia.org/wiki/Base_transceiver_station

Рыленков Д.А.
РЭУ им. Г.В. Плеханова, студент
davyd.rylenckov@yandex.ru

ПРИМЕНЕНИЕ СТАНДАРТА IEEE 802.1X ДЛЯ УПРАВЛЕНИЯ ДОСТУПОМ В КОРПОРАТИВНЫХ СЕТЯХ

В любой, даже небольшой современной организации на данный момент есть своя локальная сеть, к которой подключены рабочие станции сотрудников, корпоративные серверы и другие устройства. С развитием технологий, эволюцией применяемых информационных систем является актуальным вопрос защиты данных.

Компания Positive Technologies опубликовала отчёт «Актуальные киберугрозы: I квартал 2021 года». В результате исследования стало известно, что за первый квартал 2021 года злоумышленники провели 77% целенаправленных кибератак, из которых 82% были направлены на организации, а остальные – на частных лиц.

На сегодняшний день в корпоративных сетях компаний одной из главных задач является обеспечение управления доступом к информационным ресурсам. Стоит отметить, что в последнее время распространена концепция BYOD (Bring your own device) – сотрудники используют на рабочем месте в организации свои мобильные устройства вместо предоставляемых им официально [1].

Несмотря на удобства данной политики со стороны сотрудников, эта стратегия вызывает риски связанные с несанкционированным доступом к корпоративным данным. Необходимо учитывать, что при планировании и проектировании концепции защиты корпоративной инфраструктуры внутренний нарушитель является потенциально наиболее опасным и обладает более высоким потенциалом к выполнению различных сетевых атак на ресурсы организации [2]. К примеру, в случае с проводным подключением к сетевому коммутатору возможен риск подключения посторонних несанкционированных устройств к сетевым розеткам в кабинетах сотрудников.

Зачастую локальная вычислительная сеть компании устроена таким образом, что компьютер, который подключён к сетевой розетке, сразу же получает полный доступ ко всем ресурсам сети. В таком случае злоумышленнику остаётся только под каким-либо предлогом заполучить доступ в помещение компании, где есть подключенные рабочие станции, и подсоединить свой личный компьютер к сети, чтобы получить доступ к конфиденциальной информации, осуществить сетевую атаку либо загрузить в локальную сеть вредоносное программное обеспечение. Возможна ситуация при которой также в инфраструктуру организации может быть внедрён инсайдер, для осуществления несанкционированного доступа к закрытым данным.

В данной ситуации, в первую очередь, может защищать использование управляемых коммутаторов, установленных на уровне доступа с активированной технологией Port Security. Применение технологии Port security позволяет конфигурировать разрешение доступа для подключения к порту коммутатора устройствам с заданными администратором MAC-адресами.

Тем не менее, в случае с MAC-адресом сетевой карты устройства существует возможность его изменения на программном уровне, что позволяет злоумышленнику, зная

нужный MAC-адрес изменить его на своем устройстве и получить доступ к инфраструктуре.

Если же при подключении к сети доступ будет предоставляться только после выполнения процедуры аутентификации (с использованием логина и пароля пользователя либо по цифровому сертификату), то злоумышленник не сможет нарушить работу предприятия, поскольку не будет обладать необходимой информацией для подключения. Таким образом, обеспечивается защита от шпионажа и сетевых атак (в том числе и внутренних DoS-атак).

От атак рассматриваемого типа может применяться технология, регламентированная индустриальным стандартом IEEE 802.1x. Стандарт IEEE 802.1x регламентирует унифицированную архитектуру контроля доступа к портам с применением различных методов аутентификации клиентских устройств и обеспечивает аутентификацию конечных пользователей на канальном уровне модели OSI при разных типах подключения (как проводной тип подключения устройств, так и беспроводной) [3].

В стандарте IEEE 802.1x выделяется три основных компонента:

1) Супликант – подключаемое к корпоративной сети конечное устройство с предварительно установленным программным обеспечением для осуществления процесса аутентификации;
2) Аутентификатор – это сетевой коммутатор или беспроводная точка доступа – устройство, к которому непосредственно подключается супликант;
3) Сервер аутетификации - специальное программное обеспечение, установленное, как правило, на выделенном устройстве, которое содержит информацию о пользователях [4].

На рисунке 1 показана обобщенная схема функционирования технологии IEEE 802.1x.

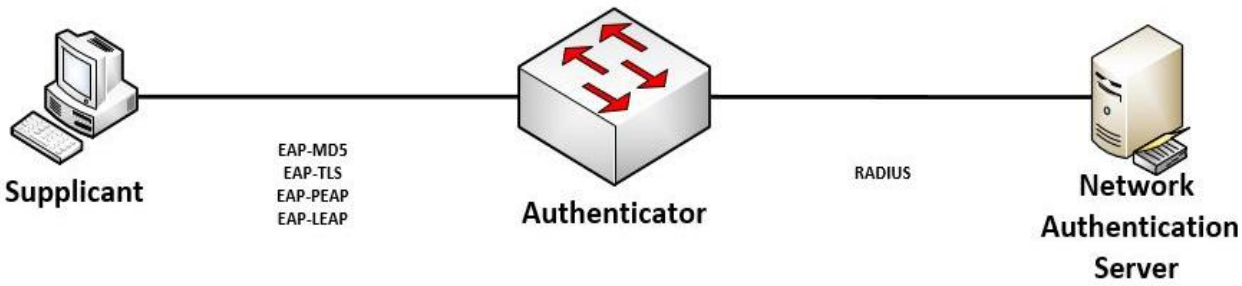


Рис. 1. Общая схема компонентов IEEE 802.1x

При подключении к порту коммутатора клиентского сетевого устройства, аутентификатор активирует логический порт для клиента, сразу переводя его в состояние "неавторизован" (англ. unauthorized). В результате данного процесса через клиентский порт сетевого коммутатора возможен обмен только служебным трафиком протокола IEEE 802.1x, а для всего остального пользовательского трафика этот порт коммутатора заблокирован.

После выполнения процесса аутентификации RADIUS сервер отправляет сообщение Radius-Accept (принять) либо Radius-Reject (отклонить) аутентификатору. Если получено сообщение Radius-Accept, то аутентификатор производит перевод порт, к

которому подключено клиентское устройство в состояние "авторизован" (англ. authorized)., и разрешается передача пользовательского траффика клиентом.

В качестве сервера аутентификации могут использоваться такие программные продукты как FreeRADIUS, Cisco ACS. FreeRADIUS является свободно распространяемым RADIUS сервером с открытым исходным кодом. Он является бесплатной альтернативой платным коммерческим RADIUS серверам [5].

Также в состав семейства серверных операционных систем Microsoft Windows Server, начиная с версии Windows Server 2008 R2 включена роль NPS (Network Policy Server), которая может использоваться в качестве сервера управления доступом [6].

Протокол RADIUS применяется для выполнения централизованной аутентификации пользователей. Он часто используется в инфраструктуре сетей интернет провайдеров и различных операторов связи при управлении доступом [7]. Протокол RADIUS является открытым и поддерживается многими известными производителями сетевого оборудования.

RADIUS протокол использует в своей архитектуре концепцию AAA (Authentication, Authorization, Accounting):

Authentication — процесс, который позволяет аутентифицировать (выполнить проверку подлинности) субъекта по его идентификационным данным, например, по его заданному логину (имя пользователя, номер телефона и т. д.) и паролю.

Authorization — процесс, определяющий полномочия идентифицированного субъекта для выполнения доступа к определённым ресурсам либо регламентированным сервисам.

Accounting — процесс, позволяющий осуществлять сбор сведений (учётных данных) об использованных ресурсах. Первичными данными (то есть, традиционно передаваемых по протоколу RADIUS) являются величины исходящего и входящего трафиков: в байтах/октетах (также с недавних пор в гигабайтах в связи с увеличением пропускной способности каналов передачи данных).

Стоит отметить, что рассматриваемый индустриальный стандарт IEEE 802.1x не предписывает в явном виде, какой протокол аутентификации необходимо использовать, и существуют альтернативные протоколы, аналогичные RADIUS. В качестве примеров можно привести такие протоколы как TACACS либо DIAMETER (также существует обновленная версия TACACS+) [8]. Протокол TACACS разработан компанией Cisco Systems и является закрытым. Протокол DIAMETER не получил такого широкого распространения и был создан как замена RADIUS в дальнейшей перспективе [9].

Используя роль NPS в Windows Server имеется возможность интеграции управления доступом с Microsoft Active Directory. Пользователи при прохождении процесса аутентификации могут использовать свои доменные учетные записи, зарегистрированные в системе [10].

Таким образом, на основе приведенного анализа можно сделать вывод, что при использовании технологии IEEE 802.1x риск несанкционированного доступа к локальной сети предприятия минимизируется для внутренних нарушителей. Также основными преимуществами являются поддержка как проводных, так и беспроводных Wi-Fi подключений и возможности масштабирования системы за счет поддержки стандарта известными производителями корпоративных решений.

СПИСОК ЛИТЕРАТУРЫ

1. Новожилов, Е.О. Компьютерные сети: Учебное пособие / Е.О. Новожилов. - М.: Academia, 2017. - 288 с.
2. Бортник, Д. А. Исследование способов защиты информации в распределенной корпоративной сети на основе внедрения технологии BYOD / Д. А. Бортник, А. С. Шабуров // Инновационные технологии: теория, инструменты, практика. – 2016. – Т. 1. – С. 259-265.
3. IEEE 802.1x-2010 : Port-Based Network Access Control – Revision of 802.1x-2004 [Электронный ресурс] / Institute of Electrical and Electronics Engineers. New York, 2010. URL: http://standards.ieee.org/getieee 802/download/802.1X-2010.pdf (дата обращения: 10.08.2015).
4. Гогуля, В. А. Исследование возможности использования централизованных политик доступа в корпоративной сети передачи данных / В. А. Гогуля, Г. В. Кравченко, Т. В. Минкина // Экономическое развитие регионов России в условиях трансформации информационной среды : Сборник научных статей по материалам Всероссийской научно-практической конференции, Ставрополь, 25–26 апреля 2018 года. – Ставрополь: Издательство "АГРУС", 2018. – С. 76-81.
5. Тагиров, В. К. Организация защиты передачи данных локальной вычислительной сети на основе перспективных технологий / В. К. Тагиров, Л. Ф. Тагирова, А. С. Милинов // Инновации, технологии, наука : сборник статей международной научно-практической конференции: в 4 частях, Пермь, 25 января 2017 года. – Пермь: Общество с ограниченной ответственностью "Аэтерна", 2017. – С. 158-162.
6. Реализация методики настройки системы защиты информации средствами Active Directory на базе Windows server 2012 R2 / Ю. А. Кузнецов, Е. И. Архалович, Д. В. Соколов, М. А. Бондарь // Состояние и перспективы развития современной науки по направлению «Информационная безопасность» : Сборник статей III Всероссийской научно-технической конференции, Анапа, 21–22 апреля 2021 года. – Анапа: Федеральное государственное автономное учреждение "Военный инновационный технополис "ЭРА", 2021. – С. 556-562.
7. Рыленков, Д. А. Применение технологии VLAN для повышения уровня защищённости корпоративных сетей / Д. А. Рыленков // XXXIV Международные Плехановские чтения : Сборник статей студентов В четырех томах, Москва, 29–31 марта 2021 года. – Москва: Российский экономический университет имени Г.В. Плеханова, 2021. – С. 129-132.
8. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей : Учебное пособие / О. М. Замятина. – 1-е изд.. – Москва : Издательство Юрайт, 2017. – 159 с. – (Университеты России). – ISBN 9785534003352.
9. Таненбаум, Э. С. Компьютерные сети / Э.С. Таненбаум, Д. Уэзеролл. - СПб.: Питер, 2018. - 512 с.
10. Баринов, Андрей Безопасность сетевой инфраструктуры предприятия / Андрей Баринов. - М.: LAP Lambert Academic Publishing, 2016. - 331 с

Бурдин В.А.
ПГУТИ, заведующий кафедрой, д.т.н., профессор,
burdin@psuti.ru
Губарева О.Ю.
ПГУТИ, начальник управления, к.т.н.,
o.gubareva@psuti.ru
Гуреев В.О.
ПГУТИ, аспирант,
v.gureev@psuti.ru

АЛГОРИТМ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ЗЛОУМЫШЛЕННИКА С ПОМОЩЬЮ DAS В 3-D ПРОСТРАНСТВЕ

ВВЕДЕНИЕ

Цифровая трансформация экономики характеризуется инновационными процессами внедрения информационных технологий во все сферы социально-политической и экономической жизни общества [1-3]. Основой цифровой экономики является сбор, передача и обработка цифровой информации. Внедряются технологии 5G, Интернет вещей, тактильный интернет и т.д. Как следствие резко возрастает плотность волоконно-оптических сетей передачи данных в зданиях, сооружениях, в том числе на объектах критической информационной инфраструктуры оптические кабельные сети зачастую строятся, используя технологию «волокно к рабочему месту». Только оптические волокна (ОВ) позволяют обеспечить пропускную способность, соизмеримую с требованиями технологий будущего [4, 5]. Это приводит к формированию компактных плотных волоконно-оптических сетей на объектах. Фактически это система распределенных и разнесенных в 3D-пространстве акустических сенсоров (DAS), что может приводить не только к хищению аудиоинформации, но и к идентификации местоположения пользователей сети, обслуживающего персонала и др.

ПОСТАНОВКА ЗАДАЧИ

На сегодняшний день практически все здания имеют сеть оптоволоконных линий связи. Очевидно, что свободные ОВ могут быть успешно использованы в качестве DAS для определения местоположения источника звука, и, в том числе, злоумышленника. По полученным данным предлагается выстроить цифровую 3D-карту объекта с наложением на систему видеонаблюдения для формирования адекватных моделей угроз, с использованием существующих на объекте средств выявления, идентификации и классификации угроз нарушения информационной безопасности для объектов различного вида и класса, а также для дополнения технологии идентификации пользователей на объекте.

Одними из наиболее перспективных способов поиска злоумышленника в помещении являются акустооптические способы [6-8]. Предлагаемый метод базируется на использовании DAS. Это системы акустического мониторинга с фазочувствительным оптическим рефлектометром (PH-OTDR) [9, 10], работающим во временной области, к которому подключено ОВ, служащее сенсором. DAS отличаются высокой чувствительностью и удовлетворительным разрешением.

ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ ИСТОЧНИКА АКУСТИЧЕСКОГО ВОЗДЕЙСТВИЯ НА ПЛОСКОСТИ С ЗАДАННОЙ ТОЧНОСТЬЮ

Положим, что злоумышленник своими действиями создает акустические колебания, воздействующие на ОВ внутри контролируемого помещения с системой DAS. Поскольку акустическое воздействие оказывается на множество точек сенсора, мы можем выделить на ОВ отдельные элементарные участки, длина которых равна калибровочной длине DAS. Тогда x_i, x_{i+1} – координаты начала и конца *i*-го элемента массива DAS; Δx – длина *i*-го элемента массива элементарных сенсоров DAS (калибровочная длина), определяемая как $\Delta x = x_{i+1} - x_i$.

На рис. 1 представлен принцип акустического воздействия на элементарные участки ОВ, где r_0 – кратчайшие расстояние от источника звука до ОВ.

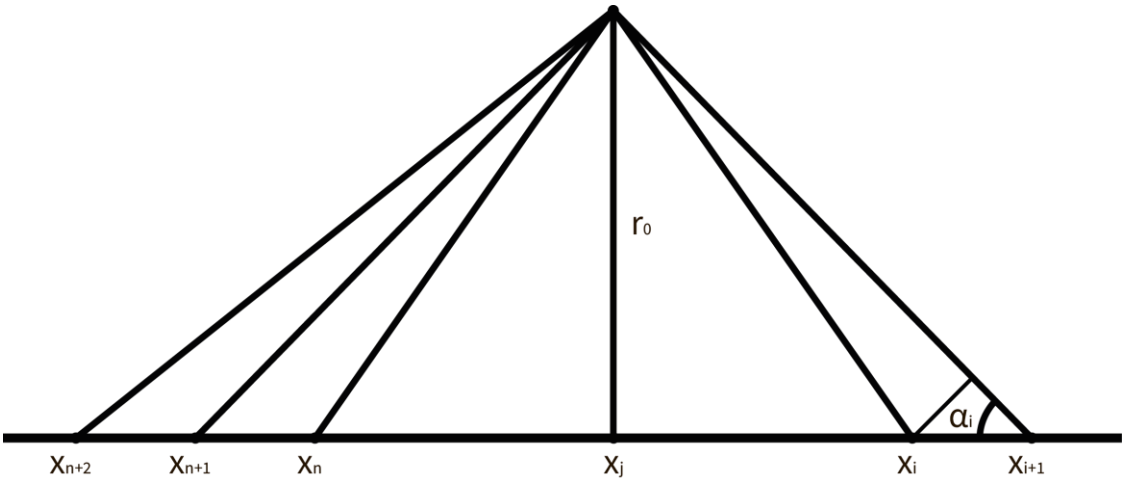


Рис. 1. Оценка расстояния от ОВ до источника акустического воздействия

Из рис. 1 следует, что α_i – угол падения луча акустического воздействия на *i*-й элементарный участок ОВ, тогда его значение можно определить как

$$\alpha_i = \arccos\left(\frac{\varphi_{i+1} - \varphi_i}{k \cdot \Delta x}\right), \quad (1)$$

где φ – фаза, получаемая при анализе характеристики обратного рассеяния ОВ, k – волновое число, Δx – калибровочная длина, λ – длина акустической волны, c – скорость звука в воздухе, f – частота звука.

Зная, что волновое число и скорость звука в воздухе рассчитываются следующим образом:

$$k = \frac{2\pi}{\lambda},$$

$$\lambda = \frac{c}{f}.$$

Определим кратчайшее расстояние до источника звука:

$$x_{0i} = \frac{x_i \cdot tg\alpha_i - x_{i+1} \cdot tg\alpha_{i+1}}{tg\alpha_i - tg\alpha_{i+1}}, \quad (2)$$

$$r_{0i} = x_{0i} \cdot tg\alpha_i . \quad (3)$$

Применяя метод Р. Нигматуллина [11], сделаем сортировку значений по убыванию с заданным ограничением, и получим, что $\langle x_{0i} \rangle \to \overset{1}{x}_0$.

В случае для двух ОВ на плоскости кратчайшее расстояние будет лежать на оси ординат, поэтому допускаем что $r_0 \approx y_0$, тогда $\langle y_{0i} \rangle \to \overset{1}{y}_0$.

Полученные выражения справедливы для двухмерного пространства, на практике же необходимо переходить к определению координат злоумышленника в 3-D пространстве, что связано с многоэтажностью большинства офисных помещений, а также с точностью вычислений.

ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ ИСТОЧНИКА АКУСТИЧЕСКОГО ВОЗДЕЙСТВИЯ В 3-D ПРОСТРАНСТВЕ С ЗАДАННОЙ ТОЧНОСТЬЮ

Для определения местоположения источника акустического воздействия (злоумышленника) на ОВ в трехмерном пространстве, необходимо использовать 3 ОВ, разнесенных в пространстве по разным плоскостям (рис. 2).

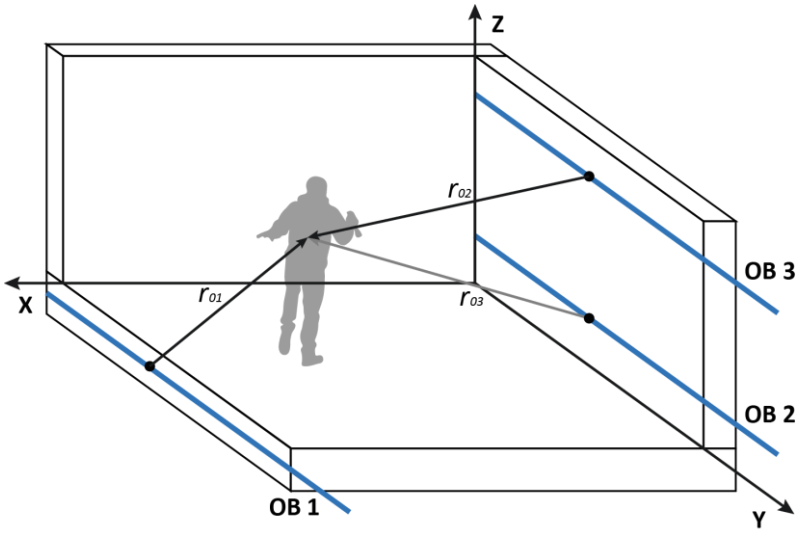


Рис. 2. Определение местоположения злоумышленника в 3-D пространстве

На рис. 2 изображено условное помещение, в котором имеются три оптических волокна (ОВ1, ОВ2, ОВ3) используемых в качестве DAS, последовательно подключенных к фазочувствительному импульсному оптическому рефлектометру, и злоумышленник, который оказывает некоторые звуковые колебания на ОВ.

Для трехмерного пространства кратчайшее расстояние от ОВ до источника звука будет определяться по формуле

$$r_0 = \sqrt{z_0^2 + y_0^2} , \quad (4)$$

где z_0 – кратчайшее расстояние до источника звука в плоскости *Z*, y_0 – кратчайшее расстояние до источника звука в плоскости *Y*.

Для каждого из трех ОВ определим значения x_{01}, x_{02}, x_{03}. Тогда на плоскости источник звука будет находится как пересечение трех

окружностей, радиусы которых равны r_{01}, r_{02}, r_{03} соответственно (рис.3). Далее разложим источник звука на спектральные характеристики и зададим обязательные условия $\Delta\varphi = \varphi_{i+1} - \varphi_i < 2\pi$, $k\Delta x < 2\pi$, таким образом все вычисления осуществляются только на низких частотах отсекая паразитные шумы и помехи.

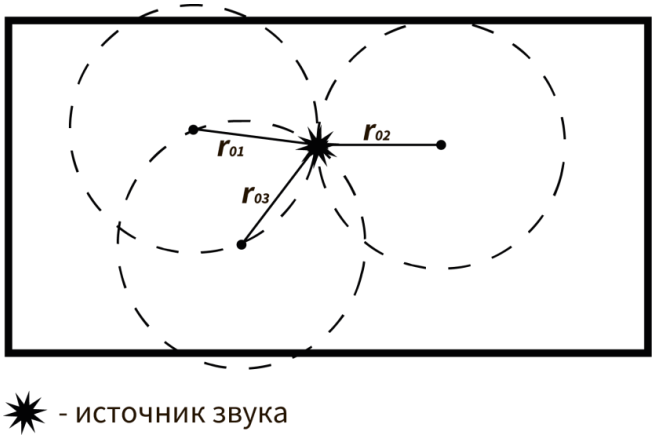


Рис. 3. Определение координат источника звука

Для типичных DAS калибровочная длина лежит в пределах 1.0–10 м [12]. Отклик *i*-го участка DAS запишется как [9, 10]:

$$s_i(t) = \int_{x_{i,0}}^{x_{i,1}} \eta(x) \cdot \varepsilon(x,t) dx, \tag{5}$$

где $\varepsilon(x,t)$ – деформация ОВ; $\eta(x)$ – коэффициент отклика, зависящий от условий прокладки кабеля, конструкции кабеля, положения ОВ в кабеле т.п.

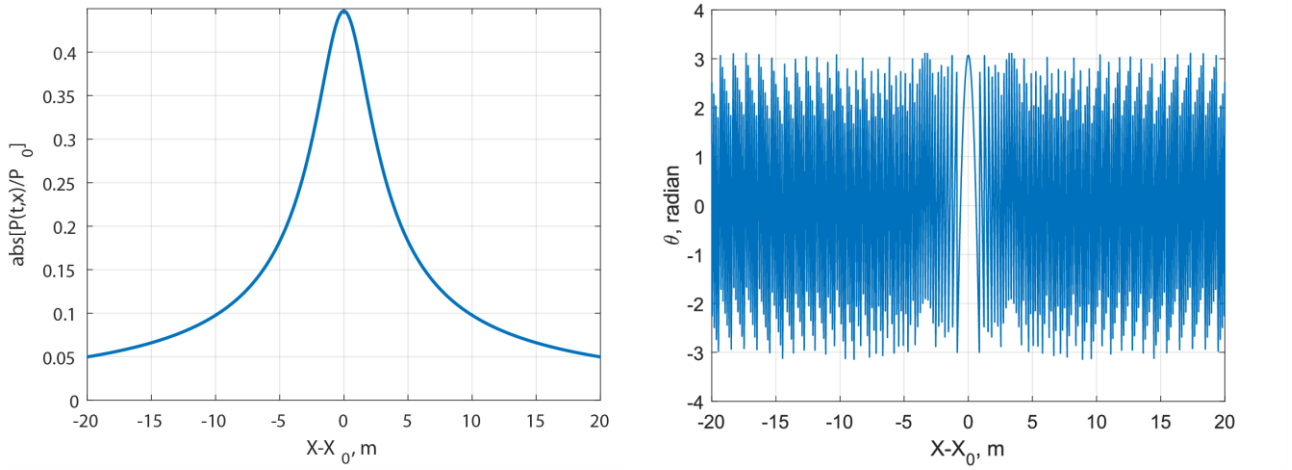
Коэффициент $\eta(x)$ в общем случае изменяется вдоль кабеля. Однако в первом приближении в пределах строительной длины кабеля его можно полагать постоянным.

Если ограничиться анализом для дальней зоны, полагая, что условия для такого допущения выполняются, то акустическое поле точечного источника, воздействующее на ОВ кабеля, описывается как [14]:

$$P(t,x) = \frac{P_0}{r} \exp\left[j(\omega t - kr) \right], \quad r = \sqrt{(z - z_0)^2 + (y - y_0)^2 + (x - x_0)^2}, \tag{6}$$

где x_0, y_0, z_0 – координаты источника акустических сигналов, x, y, z – координаты некоторой точки ОВ, ω – круговая частота, t – время; k – волновое число, P_0 – амплитуда акустического сигнала на выходе источника.

На рис. 4 приведены результаты вычислений распределений амплитуды и фазы отношения $P(t,x)/P_0$ вдоль ОВ при условии, что кабель проложен прямолинейно. При этом полагаем, что источник акустического сигнала и оптический кабель находятся в воздухе, $(z - z_0) = 1$ м, $(y - y_0) = 2$ м, частота акустического сигнала 2 кГц и скорость распространения звука в воздухе 331 м/с.



(а) (б)

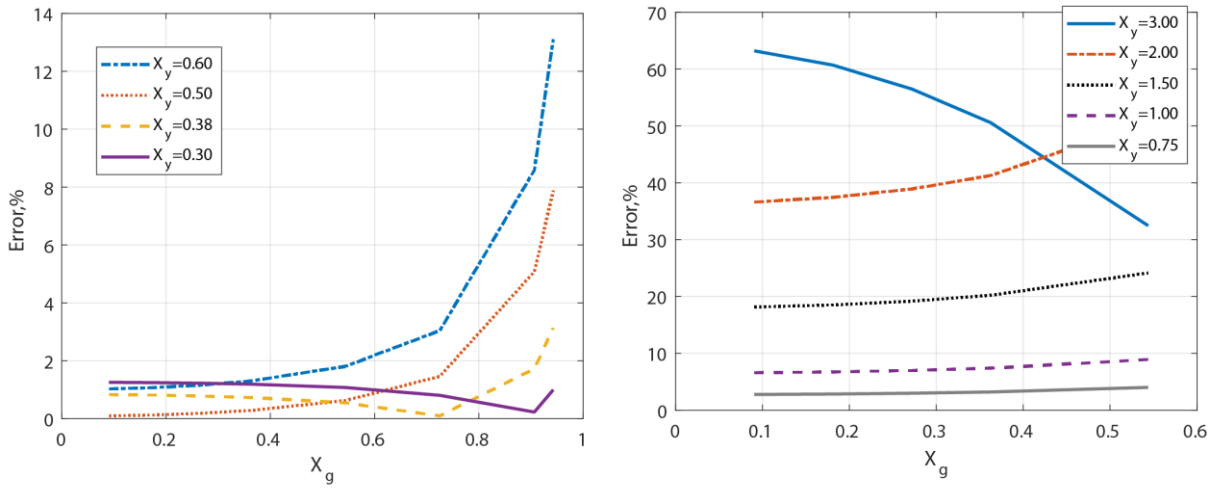
Рис. 4. Распределения амплитуды (а) и фазы (б) воздействующего акустического поля вдоль оптического волокна

С учетом (5)-(6) регистрируемый DAS сигнал с ОВ на элементарном участке кабеля описывается как

$$P_C(t,x_i) = P_0 \cdot \exp(j\omega t) \int_{x_{i,0}}^{x_{i,1}} \frac{\eta(x)}{r} \exp(-jkr)dx\,, \qquad (7)$$

На рисунке 4(б) представлены оценки распределений фазы отношения $P_C(t,x)/P_0$ в зависимости от координат *x* и *y*, рассчитанные по формуле (7) для рассмотренных выше условий при $\Delta x = 1$м и $\eta = 1$. Интеграл вычисляли численно методом трапеций.

Введем обозначения $X_g = \Delta x/\lambda$, $X_y = \Delta x/y$. Здесь λ – длина акустической волны. На рис. 5 и 6 представлены зависимости оценок погрешностей от введенных величин X_g и X_y. На рис. 5 приведены зависимости погрешностей от X_g и отношения сигнал/помеха (SNR) при $X_y = 0.6$. Рассматривалась аддитивная помеха.



(а) (б)

Рис.5. Зависимости погрешностей от нормированных параметров калибровочной длины DAS

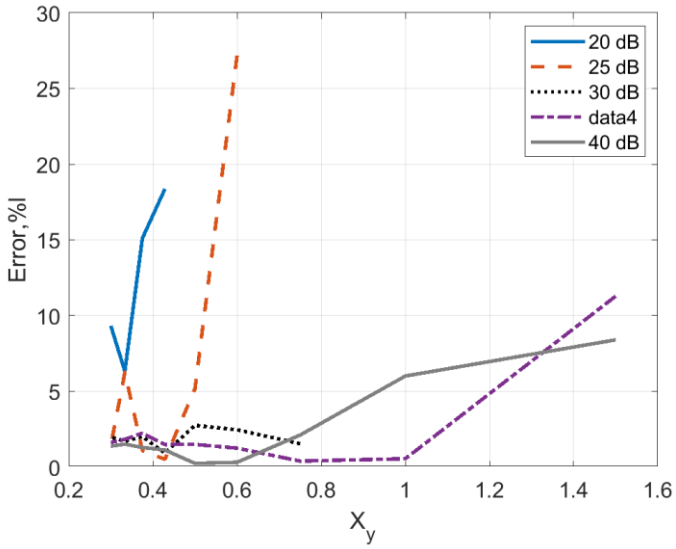


Рис.6. Зависимости погрешностей от уровня помех

Как показали результаты моделирования, области изменения параметров X_g и X_y, в которых погрешности приемлемы, невелики. Так, чтобы погрешности не превышали 10%, необходимо выполнение условий $X_g < 0.3-0.4$ и $X_y < 0.4-0.5$. Ограничения на X_g объясняются тем, что для реализации измерений необходимо, чтобы набег фазы на калибровочной длине не превышал 2π. Столь узкий диапазон изменений параметра X_g существенно ограничивает возможности выбора частоты акустического сигнала, что нежелательно в условиях помех. Это наглядно демонстрируют графики на рис. 5. Рост погрешностей с увеличением X_y ожидаем, так как при этом уменьшается зависимость набега фазы от координаты Y по сравнению с зависимостью от калибровочной длины.

ЗАКЛЮЧЕНИЕ

По результатам моделирования можно сделать вывод, что рассмотренный в работе алгоритм позволяет оценивать расстояние от ОВ до местоположения источника гармонического акустического воздействия (злоумышленника) с погрешностью до 10-15% и менее.

В данном случае параметр X_g нормированной калибровочной длины DAS не должен превышать 0.3-0.4, что существенно ограничивает диапазон допустимых частот источника вибро-акустического сигнала, а нормированный параметр калибровочной длины X_y не должен превышать 0.4 – 0.5.

Предлагаемая методика может быть использована для построения вспомогательных систем безопасности для исключения хищения информации и ценного имущества при помощи 3D-волоконно-оптических сетей в работе крупных офисов, государственных учреждений и коммерческих организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Yokoi, T. Digital vortex 2019. Continuous and Connected Change [Электронный ресурс] / T. Yokoi, J. Shan, M. Wade, J. Macaulay // Global Center for Digital Business Transformation. — 2019. — Режим доступа : https://www.imd.org/research-knowledge/reports/digitalvortex2019/.
2. Udovita, P.V. Conceptual Review on Dimensions of Digital Transformation in Modern Era / P.V. Udovita // International Journal of Scientific and Research Publications. — 2020. — 10(2). — 520-529.
3. Digital vortex 2021 [Электронный ресурс]. — Режим доступа : https://www.imd.org/research-knowledge/reports/digital-vortex-report-2021.
4. Abe, Y. Beyond 5G/6G White Paper / Y. Abe // NICT. — 2021. — 141.
5. Ranaweera, Ch. Rethinking of Optical Transport Network Design for 5G/6G Mobile Communication [Электронный ресурс] / Ch. Ranaweera, A. Nirmalathas, E. Wong, Ch. Lim, P. Monti, M. Furdek, L. Wosinska, B. Skubic, C.M. Machuca // IEEE Future Networks Tech Focus. — 2021. — 12. — Режим доступа : https://futurenetworks.ieee.org/tech-focus/april-2021/rethinking-of-optical-transport-network-design-for-5g-6g-mobile-communication.
6. Способ поиска трассы и определения места повреждения оптического кабеля: пат. 2656295 Рос. Федерация N 2017111420; заявл. 04.04.17; опубл. 04.06.18, Бюл. N16.
7. Способ поиска трассы прокладки оптического кабеля: пат. 2748310 Рос. Федерация N 2020135047; заявл. 26.10.20; опубл. 21.05.21, Бюл. N15.
8. Gureev, V.O. Optical cable location methods / V.O. Gureev, V.A. Burdin, O.V. Shaban // Proc. SPIE. — 2021. — 11793. — 117931A.
9. Muanenda, Y. Recent Advances in Distributed Acoustic Sensing Based on Phase-Sensitive Optical Time Domain Reflectometry / Y. Muanenda // Hindawi Journal of Sensors. — 2018. — 23(3897873). — 1-16.
10. Wang, Z. Recent Progress in Distributed Fiber Acoustic Sensing with Φ-OTDR / Z. Wang, B. Lu, Q. Ye, H. Cai // Sensors. — 2020. — 20(22). — 6594.
11. Nigmatullin, R.R. The General Theory of the Quasi-Reproducible Experiments: How to Describe the Measured Data of Complex Systems? / R.R. Nigmatullin, G. Maione, P. Lino, F. Saponaro, W. Zhang // Communications in Nonlinear Science and Numerical Simulation. — 2017. — 42. — 324-341.
12. Liang, J. Distributed acoustic sensing for 2D and 3D acoustic source localization / J. Liang, Z. Wang, B. Lu, X. Wang, L. Li, Q. Ye, R. Qu, H. Cai // Optics Letters. — 2019. — 44(7). — 1690 – 1693.
13. Hwang, J.-H. Position Estimation of Sound Source Using Three Otical Mach-Zehnder Acoustic Sensor Array / J.-H. Hwang, S. Soonwon, C.-S. Park // Current Optics and Photonics. — 2017. — 1(6). — 573-578.
14. Fenta, M.C. Fibre Optic Methods of Prospecting: A Compre-hensive and Modern Branch of Geophysics / M.C. Fenta, D.K. Potter, J. Szanyi // Surveys in Geophysics. — 2021. — 42. — 551-584.
15. Лепендин, Л.Ф. Акустика / Л.Ф. Лепендин. — М. : Высшая школа. — 1978. — 448.
16. Губарева, О.Ю. Потенциальные возможности оптических распределенных акустических сенсоров для определения местоположения злоумышленника / О.Ю.

Губарева, В.О. Гуреев, Г.Н. Чифранов // Инфокоммуникационные технологии. — 2021. — 19(2). — 239-249.

Студеникин А.В.
СКФУ, инженер-исследователь,
studentstavropol@mail.ru
Жук А.П.
СКФУ, профессор, к.т.н., профессор,
alekszhuk@mail.ru

ИССЛЕДОВАНИЕ УГРОЗ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ КОГНИТИВНОГО РАДИО

В последние годы во всем мире, и в Российской Федерации в том числе, отмечается взрывной рост пользователей беспроводной связи. Данное обстоятельство объясняется тем, что растет число пользователей беспроводной связью, растет число самих беспроводных сетей передачи данных, а также увеличивается количество пользовательских мобильных устройств, таких как смартфоны, планшетные компьютеры, ноутбуки, модемы и прочие, которым в большинстве случаев отдают предпочтение современные пользователи [1, 2].

Упомянутые тенденции свидетельствуют о необходимости использования все больших объемов частотного диапазона для осуществления беспроводного доступа пользователей к глобальной сети, который является ограниченным природным ресурсом, стоимость которого достаточно высока и соизмерима в отдельных странах со стоимостью самой беспроводной сети передачи данных. В силу этих обстоятельств в последнее десятилетие усилия ученых и инженеров направлены на разработку технологий, обеспечивающих повышение эффективности использования частотных ресурсов в беспроводных сетях передачи данных, одной из которых является технология когнитивного радио (КР). Идея когнитивного радио была впервые опубликована американским ученым Джозефом Митолой в 1999 году [3].

В силу основных принципов, заложенных в алгоритмы работы КР, по мнению исследователей в данной области, вероятность появления и реализации угроз безопасности информации в рассматриваемых сетях существенно возрастает [4, 5]. По этой причине успешное внедрение технологий КР зависит от разработки и внедрения основных механизмов безопасности для обеспечения надежности сетей и терминалов от атак безопасности.

Целью доклада является анализ угроз безопасности информации в сетях когнитивного радио и выявление наиболее опасных из них, а также анализ методов защиты информации от них.

Различают три основных вида архитектуры сети КР, которые имеют различные уровни уязвимости перед конкретными угрозами безопасности: совместная централизованная; совместная распределенная (децентрализованная); несовместная.

Уязвимости в системе безопасности сети КР будут возникать, когда какие-либо когнитивные радиокомпоненты не будут синхронизированы друг с другом. Централизованная архитектура в этом смысле является более эффективной, но с точки зрения надежности представляет собой единую точку отказа, что в случае сбоя основного элемента сети когнитивного радио приведет сразу к отказу всей сети.

Международным союзом электросвязи (МСЭ) в [6] определены восемь требований к безопасности: контролируемый доступ к ресурсам; надежность; защита конфиденциальности; защита целостности системы; защита целостности данных; соответствие нормативной базе; подотчетность: система должна гарантировать, что организация не может отрицать ответственность за любое из своих совершенных действий; проверка подлинности.

В работе [4] проведен анализ угроз безопасности информации в сетях когнитивного радио:

1) Подавление канала, используемого для распространения когнитивных сообщений.
2) Злонамеренное изменение когнитивных сообщений.
3) Маскировка под основного пользователя.
4) Злонамеренное изменение когнитивного радиоузла.
5) Внутренний сбой когнитивного радиоузла.
6) Маскировка под когнитивный радиоузел.
7) Появление скрытого узла.
8) Несанкционированное использование полосы частот спектра в монопольных целях.
9) Несанкционированное использование полосы частот спектра для DoS – атаки основными пользователями.
10) Насыщение канала когнитивного управления.
11) Прослушивание когнитивных сообщений.
12) Нарушение работы MAC или когнитивного механизма когнитивной радиосети.

Анализ работ [7, 8] показывает, что по сравнению с другими, угрозы злонамеренного изменения когнитивных сообщений и маскировки под основного пользователя считаются основными угрозами, поскольку они непосредственно влияют на функцию зондирования спектра, которая является первой фазой цикла КР.

Проведем анализ известных методов защиты, от этих типов угроз, которые сводятся к следующим [9-17]:

1) Методы защиты, основанные на репутации и доверии узлов сети КР.
2) Методы защиты, основанные на идентификации маскирующейся угрозы с помощью анализа сигнала пользователя сети КР.
3) Криптографические методы защиты когнитивных сообщений.
4) Методы защиты, основанные на использовании базы данных геолокации основных пользователей, для их более точной идентификации.

Первая группа методов защиты основана на понятиях репутации или доверия узлов КР (например, БС или терминального оборудования пользователей) [9-11].

Один из методов второй группы описан в работе [12] в котором для предотвращения угрозы маскировки под основного пользователя при объединении данных в процессе совместного зондирования спектра терминальным оборудованием сети КР используется рейтинг репутации терминального оборудования.

Идентификация узла КР посредством анализа переданного сигнала исследована в [13], где для увеличения характеристик специфических особенностей передатчика используется вейвлет-преобразование. Недостаток данного метода защиты заключается в

том, что ошибки в канале связи или эффекты распространения радиосигналов (интерференция, атмосферное поглощение и пр.) могут увеличить вероятность ложных решений. К этой же группе относится метод, основанный на использовании интегрированной базы данных, состоящей из достаточно объемных данных, таких как географические особенности, доступные услуги, спектральные правила, географическое местоположение и действия радиоустройств пользователей сети КР [14].

Еще один метод второй группы, описанный в [15], основан на применении схемы распознавания образов сигналов для идентификации приемопередатчиков пользователей сети КР с помощью электромагнитной сигнатуры. Недостатками данного метода является то, что используемый отличительный признак может меняться вместе со старением приемопередатчика.

Недостатками методов второй группы является низкая вероятность правильного решения при определении злонамеренных пользователей сети КР.

Третья группа методов основана на использовании криптографических преобразований когнитивных сообщений. Для снижения вероятности реализации угрозы злонамеренного изменения когнитивных сообщений в работе [16] предлагается использовать криптографический метод их шифрования с открытым ключом. Однако любое криптографическое преобразование сообщений приводит к неизбежным задержкам во времени доставки сообщений, необходимых для их шифрования и расшифрования, что негативным образом сказывается на устойчивости работы сети КР.

К четвертой группе относится метод защиты от угрозы маскировки под основного пользователя предложенный в [17], где описана процедура проверки передатчика при совместном зондировании спектра. Процедура проверки передатчика использует схему проверки геолокации передатчика, маскирующегося под основного пользователя.

Недостатком данного метода является его уязвимость к угрозе подмены навигационного сигнала, а также возможность потери навигационного сигнала в городских условиях в местах многоэтажной застройки.

Выводы:

К сетям когнитивного радио с точки зрения обеспечения безопасности передаваемой информации предъявляются такие же жесткие требования, как и к обычной беспроводной сети передачи данных.

Анализ известных угроз сети КР показывает, что угрозы злонамеренного изменения когнитивных сообщений и маскировки под основного пользователя считаются их основными угрозами, поскольку они непосредственно влияют на функцию зондирования спектра, которая является первой фазой цикла КР.

Для защиты от актуальных угроз сетей КР используется четыре группы методов защиты информации, однако их анализ показал, что их эффективность зависит от изменяющихся в сети факторов, которые снижают вероятность успешного отражения угроз при их использовании в системе защиты информации сети КР.

Выявленные недостатки известных методов защиты информации от актуальных угроз сети КР предопределяют дальнейшее развитие методов защиты информации, обеспечивающего гарантированное отражение угроз.

БЛАГОДАРНОСТИ

96Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта № 29/2020.

СПИСОК ЛИТЕРАТУРЫ

1. Roy, S.D. Cognitive radio CDMA networking with spectrum sensing / Sanjay Dhar Roy, Sumit Kundu, Gianluigi Ferrari and Riccardo Raheli // International journal of communication systems. –2014. –Vol. 27. –No. –P. 1582–1600.
2. Жук, А.П. О целесообразности использования ансамблей ортогональных сигналов с изменяющейся размерностью в системе CDMA / Жук А.П., Черняк З.В., Сазонов В.В. // Инфокоммуникационные технологии. –2008. –Т. 6. –№ 4. –С. 16-20.
3. Mitola, J. Cognitive radio: Making software radio more personal / J. Mitola, G.Q., Maguire Jr. // IEEE Personal Communication. –1999. –Vol. 6. –No. 4. –P. 13 – 18.
4. Baldini, G. Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead / Gianmarco Baldini, Taj Sturman, Abdur Rahim Biswas, Ruediger Leschhorn, Gÿozö Gódor, Michael Street // IEEE communications surveys & tutorials. –2012. –Vol. 14. – No. 2. –P. 355-379.
5. Perich, F. Policy-based spectrum access control for dynamic spectrum access network radios / F. Perich, and M. McHenry // Web Semantics: Science, Services and Agents on the World Wide Web. –2009. –Vol. 7, –Issue 1, Pages 21-27.
6. Требования к безопасности сетей электросвязи: рекомендация 2-й исследовательской комиссии Международного союза электросвязи (МСЭ-Т) ITU-T E.408 от 28 мая 2004 года // Рекомендации МСЭ-Т серии E. –2004. – 21 с.
7. Anand, S. An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks / S. Anand, Z. Jin andd K.P. Subbalakshmi // 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN'08). – USA. Chicago. –2008. –Vol. –No. –P. 1-6.
8. Safdar, G.A. Common Control Channel Security Framework for Cognitive Radio Networks / G.A. Safdar and M. O'Neill // 69th IEEE Vehicular Technology Conference, (VTC Spring 2009). –Spain. Barcelona. –2009. –Vol. –No. –P. 1-5.
9. Wenkai, W. Attack-proof collaborative spectrum sensing in cognitive radio networks / W. Wenkai, L. Husheng, S. Yan, and H. Zhu // 43rd Annual Conference on Information Sciences and Systems (CISS 2009). –USA. Baltimore. – 2009. –Vol. –No. –P. 130-134.
10. Wang, W. CatchIt: Detect Malicious Nodes in Collaborative Spectrum Sensing / W. Wang, H. Li, Y. Sun and Z. Han // IEEE Global Telecommunications Conference (GLOBECOM 2009). –USA. Hawaii. Honolulu. – 2009. –Vol. –No. –P. 1-6.
11. Kun, Z. Reputation-based cooperative spectrum sensing with trusted nodes assistance / Z. Kun, P. Paweczak, and D. Cabric // IEEE Communications Letters. –2010. –Vol.14. –No.3. –P. 226-228.
12. Chen, R. Robust Distributed Spectrum Sensing in Cognitive Radio Networks / R. Chen, J, M, Park, and K. Bian // The 27th IEEE Conference on Computer Communications (INFOCOM 2008). –USA. Phoenix. – 2008. –Vol. –No. –P. 1876-1884.
13. Zhao, C. A PHY-layer Authentication Approach for Transmitter Identification in Cognitive Radio Networks / Caidan Zhao; Liang Xie; Xueyuan Jiang; Lianfen Huang; Yan Yao // 2010 International Conference on Communications and Mobile Computing (CMC 2010). – China. Shenzhen. – 2010. –Vol. 2. –No. –P. 154-158.
14. Zhao, Y. Overhead Analysis for Radio Environment Map-enabled Cognitive Radio Networks / Y. Zhao, J. H. Reed, S. Mao, and K. K. Bae // 1st IEEE Workshop on Networking

Technologies for Software Defined Radio Networks, (SDR 2006). –Orlando, Florida. – 2006. – Vol. 2. –No. –P. 18-25.

15. Afolabi, O.R. On Secure Spectrum Sensing in Cognitive Radio Networks Using Emitters Electromagnetic Signature / O.R. Afolabi, K. Kiseon, Ahmad A. // Proc. of 18th International Conference on Computer Communications and Networks, (ICCCN 2009). –USA. San Francisco. – 2009. –Vol. –No. –P. 1-5.

16. Tingting, Z. A New Cooperative Detection Technique with Malicious User Suppression / Z. Tingting, Z. Yuping // IEEE International Conference on Communications, (ICC 2009). –Germany. Dresden. – 2009. –Vol. –No. –P. 1-5.

17. Chen, R. Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," / R. Chen, J.M. Park // 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, (SDR 2006). –USA. Florida. Orlando. – 2006. –Vol. –No. –P.110-119.

Студеникин А.В.
СКФУ, инженер-исследователь
studentstavropol@mail.ru

МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ НА ОСНОВЕ ХАОТИЧЕСКОГО ПРИМЕНЕНИЯ ОРТОГОНАЛЬНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

При создании современных беспроводных радиосетей возникают следующие проблемы, требующие решения: нехватка радиочастотного диапазона (спектра), обеспечение электромагнитной совместимости беспроводных систем, организация эффективного управления сетью и её элементами, обеспечение качественных показателей при передаче информации.

Вариантом решения данных проблем является применение систем КР, которые должны работать, не создавая помех и не требуя защиты от других РЭС [1].

К наиболее приемлемым технологиям физического уровня систем КР следующие: модуляция на основе синтезированного банка фильтров FBMC, OFDM с дополнительной фильтрацией (f-OFDM), обобщенное мультиплексирование с частотным разделением (GFDM) и мультиплексирование с частотным разделением и универсальной фильтрацией (UFMC). Вместе с тем к настоящему времени достаточно полно проработан вопрос применения в беспроводных радиосетях технологий радиодоступа на основе кодового разделения каналов (CDMA - Code Division Multiple Access) IS-95, cdmaOne, CDMA2000 и W-CDMA, которая имеет преимущества по сравнению с другими технологиями по помехоустойчивости, эффективности использования радиочастотного спектра, скрытности и другим показателям.

Анализ ряда работ по данной теме показал, что внедрение новых систем когнитивного радио создает новые угрозы безопасности информации, которые появляются в связи с концепцией динамического доступа к спектру, а также потребностями аутентификации элементов системы КР [2]. По этой причине решение вопросов защиты информации в системах когнитивного радио имеет актуальное значение.

Анализ существующих направлений повышения защищенности систем СС с КРК на основе структурной скрытности позволяет выделить следующие направления решения данной задачи.

Первое направление основано на автоматической смене известных структур ансамблей дискретных ортогональных сигналов (АДОС). [3-13].

Второе направление повышения структурной скрытности СС с КРК заключается в использовании в качестве расширяющих нелинейных псевдослучайных последовательностей ПСП [14].

Третье направление повышения защищенности СС с КРК на основе структурной скрытности, заключается в использовании ансамблей дискретных ортогональных последовательностей (АДОП), получаемых на основе векторного синтеза [3, 7-9, 15].

Четвертое направление основано на использовании функциональных преобразований псевдослучайных аргументов для синтеза и последующего хаотического использования систем дискретных квазиортогональных кодовых последовательностей (СДККП) в системах глобальной спутниковой навигации [16].

Пятое направление основано на использовании последовательностей де Брейна, изменяющихся по случайному алгоритму, обеспечивающему повышение уровня скрытности передачи СС с КРК [17].

Не смотря на разнообразие известных подходов повышения защищенности СС с КРК на основе структурной скрытности, они имеют существенные обобщенные недостатки, которые заключаются в следующем:

1) ограниченность количества используемых структур ансамблей (систем) ортогональных и квазиортогональных кодовых последовательностей в требуемом диапазоне размерностей;

2) несовершенство алгоритмов формирования ансамблей ортогональных кодовых последовательностей различных размерностей;

3) наличие у ансамблей ортогональных кодовых последовательностей сигналов низких корреляционных характеристик;

4) использование ансамблей многоуровневых ортогональных кодовых последовательностей сигналов возможно только в каналах связи с низким уровнем помех, которые в технике беспроводной связи практически отсутствуют.

С учетом выявленных недостатков известных подходов повышения защищенности СС с КРК на основе структурной скрытности можно сделать вывод об их ограниченности и необходимости поиска усовершенствованного способа повышения защищенности СС с КРК на основе структурной скрытности.

Анализ работ [6, 18-22] показывает, что наибольший показатель структурной скрытности рассматриваемых систем связи может обеспечить хаотическое применение АМОКП, получаемых на основе векторного синтеза при рассмотрении собственных векторов эрмитовых матриц (ЭМ). Однако вопросы разработки формирователя данных сигналов, алгоритма защищенного информационного обмена на основе применения АМОКП и структуры защищённой СС с КРК на основе хаотического применения АМОКП в них не рассматривались.

Целью статьи является повышение защищённости информации в СС с КРК на основе хаотического применения ортогональных кодовых последовательностей.

Задачей статьи является разработка алгоритмов синтеза и формирования АМОКП, а также алгоритма защищенного информационного обмена в СС с КРК на основе хаотического применения АМОКП.

Разработку алгоритма защищенного информационного обмена в СС с КРК на основе хаотического применения АМОКП по мнению автора целесообразно начать с решения задач их синтеза и формирования.

В работах [18, 23-25] показано, что решение задачи синтеза АМОКП необходимо осуществлять на основе множества собственных векторов (СВ) ЭМ вида (1).

Поскольку СВ ЭМ ортогональны между собой, то их можно использовать в качестве модели АМОКП [15].

$$Q=\begin{pmatrix} d_{1,1} & q_{1,2}\cdot e^{j\varphi_{1,2}} & \Lambda & q_{1,m-1}\cdot e^{j\varphi_{1,m-1}} & q_{1,m}\cdot e^{j\varphi_{1,m}} \\ q_{2,1}\cdot e^{j\varphi_{2,1}} & d_{2,1} & \Lambda & q_{2,m-1}\cdot e^{j\varphi_{2,m-1}} & q_{2,m}\cdot e^{j\varphi_{2,m}} \\ q_{3,1}\cdot e^{j\varphi_{3,1}} & q_{3,2}\cdot e^{j\varphi_{3,2}} & \Lambda & q_{3,m-1}\cdot e^{j\varphi_{3,m-1}} & q_{3,m}\cdot e^{j\varphi_{3,m}} \\ \text{M} & \text{M} & \text{M} & \text{M} & \text{M} \\ q_{n-1,1}\cdot e^{j\varphi_{n-1,1}} & q_{n-1,2}\cdot e^{j\varphi_{n-1,2}} & \Lambda & d_{n-1,m-1} & q_{n-1,m}\cdot e^{j\varphi_{n-1,m}} \\ q_{n,1}\cdot e^{j\varphi_{n,1}} & q_{n,2}\cdot e^{j\varphi_{n,2}} & \Lambda & q_{n,m-1}\cdot e^{j\varphi_{n,m-1}} & d_{n,m} \end{pmatrix}, \quad (1)$$

где $q_{k,i}\cdot e^{j\varphi_{k,i}}=q_{i,k}\cdot e^{j\varphi^*_{i,k}}$ - комплексно-сопряженные числа в показательной форме, модули которых равны $q_{k,i}=q_{i,k}$, а аргументы $\varphi_{k,i}=\varphi^*_{i,k}$ - коплексно-сопряжены, $d_{1,1}\text{K}\,d_{n,m}$ - вещественные числа.

В качестве примера для синтеза АМОКП выберем ЭМ четвертого порядка ($N=4$). В данной матрице коэффициенты второй диагонали примем равными $A_{12}=A_{21}=100e^{i\pi/2};\ B_{23}=B_{32}=0,01;\ C_{34}=C_{43}=100e^{i\pi}$, а остальные приравняем к нулю. В этом случае ЭМ примет вид, представленный ниже

$$Q=\begin{pmatrix} 0 & 100e^{i\pi/2} & 0 & 0 \\ 100e^{-i\pi/2} & 0 & 0,01 & 0 \\ 0 & 0,01 & 0 & 100e^{i\pi} \\ 0 & 0 & 100e^{-i\pi} & 0 \end{pmatrix}. \quad (2)$$

Для решения задачи на практике разработана программа моделирования и оценки свойств АМОКП и подробно описана в [23].

С помощью программы были рассчитаны СВ ЭМ (2), которые с учетом нормирования имеют следующий вид

$$\underset{\text{r}}{X}=\begin{pmatrix} 0,5e^{i\pi/2} & 0,5e^{i0} & 0,5e^{i0} & 0,5e^{i\pi} \\ 0,5e^{i0} & 0,5e^{i3\pi/2} & 0,5e^{i\pi/2} & 0,5e^{i3\pi/2} \\ 0,5e^{i3\pi/2} & 0,5e^{i\pi/2} & 0,5e^{i0} & 0,5e^{i0} \\ 0,5e^{i0} & 0,5e^{i\pi/2} & 0,5e^{i\pi/2} & 0,5e^{i\pi/2} \end{pmatrix}. \quad (3)$$

Если систему СВ ЭМ (3) отождествить с моделью АМОКП, то она графически может быть представлена следующим образом (Рис. 1).

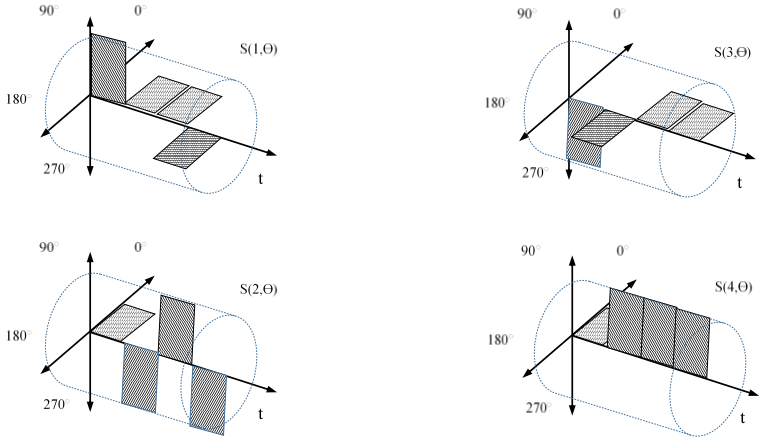


Рис. 1. Внешний вид АМОКП, описываемого системой (3)

Изменяя фазы диагональных коэффициентов ЭМ (2) в соответствии с их значениями на тригонометрической окружности, можно получать АМОКП, отличающиеся друг от друга фазовой структурой.

При использовании всего диапазона значений аргументов (фаз) диагональных коэффициентов ЭМ можно получить достаточно представительное множество систем СВ ЭМ вида (3) с различными значениями аргументов (фаз) у каждой координаты СВ [15].

Получаемые таким образом АМОКП имеют увеличенное по сравнению с известными количество неповторяющихся структур последовательностей, которое позволит в течение большего промежутка времени осуществить их хаотическое применение без повторений в СС с КРК.

Для формирования необходимого количества структур АМОКП, необходимого для обеспечения структурной скрытности СПИ с КРК, возможностей существующих устройств формирования последовательностей недостаточно.

Анализ известных устройств формирования ансамблей ортогональных последовательностей показал преимущества генератора функций Попенко – Турко (ГФПТ) [8] по сравнению с другими, который выбран за основу для построения универсального формирователя АМОКП.

Предлагается следующая структура универсального формирователя (Рис. 2).

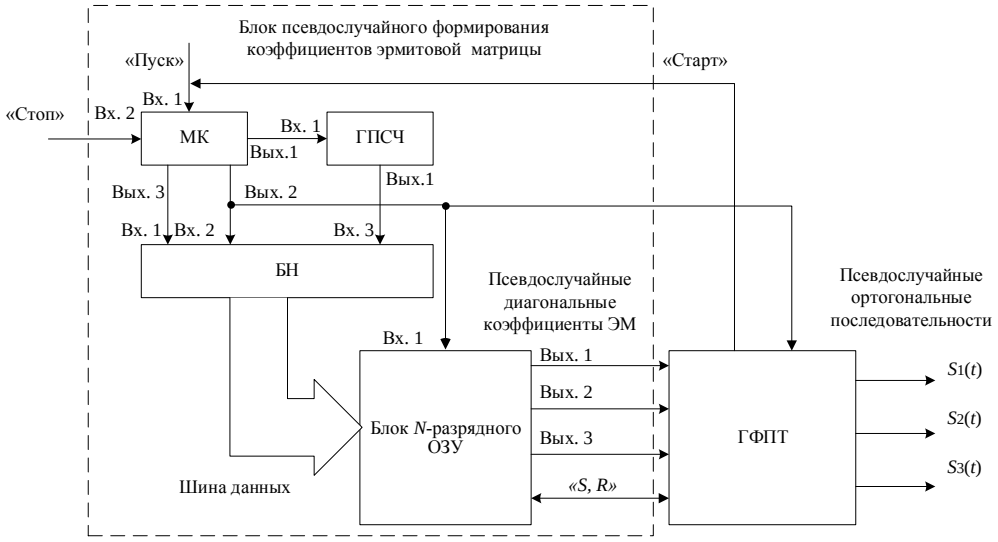


Рис. 2. Структура универсального формирователя АМОКП

Сущность предлагаемого решения заключается в том, что в исходный ГФПТ добавляется блок псевдослучайного формирования коэффициентов ЭМ, содержащий микропроцессор МК, генератор псевдослучайных чисел (ГПСЧ), блок накопителя (БН), блок разрядного оперативного запоминающего устройства (ОЗУ), а также обратную связь, наличие которой обеспечивает автоматизацию процесса хаотического формирования коэффициентов ЭМ.

В результате, генерируемые псевдослучайные АМОКП будут отличаться друг от друга по форме, а в случае их использования в качестве расширяющих последовательностей в СС с КРК будут обеспечивать повышенный уровень скрытности [18].

Анализ источников [5, 14] показывает, что вопросам построения и моделирования защищенного информационного обмена в СС с КРК в известных работах уделено недостаточно внимания.

Структура защищённой СС с КРК представлена ниже (Рис. 3).

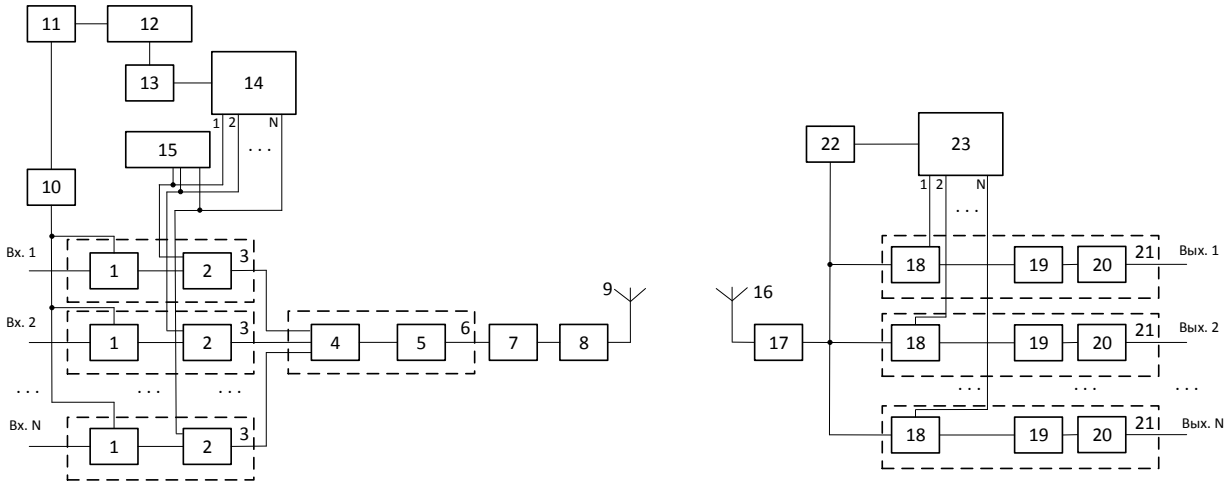


Рис. 3. Структура защищённой системы связи с кодовым разделением каналов

Алгоритм защищенного информационного обмена в СС с КРК на основе хаотического применения АМОКП реализуется следующим образом.

1. На первом этапе передающая аппаратура и приемная аппаратура СС с КРК вводится в цикловую фазу.

2. На втором этапе устанавливается синхронизм между передающей и приемной частью СС с КРК.

3. На третьем этапе осуществляется информационный обмен между канальными пользователями СС с КРК, причем в качестве сигнала-переносчика подлежащего передаче информационного символа используется сформированный в данный момент времени АМОКП.

4. На четвертом этапе на передающей и приемной стороне происходит синхронная смена исходных данных, необходимых для получения новой структуры АМОКП, используемых для передачи последующего информационного символа.

5. На пятом этапе осуществляется процесс информационного обмена за счет применения АМОКП новой структуры.

6. На шестом этапе с целью исключения повтора использования одного и того же АМОКП осуществляется проверка сформированных на предыдущих этапах ансамблей и используемого в данный момент времени.

7. На последующих этапах повторяются действия, описанные для 1-6 этапов алгоритма, до тех пор, пока процесс передачи информации не будет завершен, или нарушен по внешним или внутренними причинам.

Выводы:

1. Внедрение новых систем КР создает новые угрозы безопасности информации, которые появляются в связи с концепцией динамического доступа к спектру, а также потребностями аутентификации элементов системы когнитивного радио.

2. Не смотря на разнообразие известных подходов повышения защищенности систем связи СС с КРК на основе структурной скрытности, они имеют существенные недостатки, основным из которых является низкая структурная скрытность.

3. Наибольший показатель структурной скрытности СС с КРК может обеспечить хаотическое применение АМОКП, получаемых на основе векторного синтеза при рассмотрении СВ ЭМ.

4. Разработанный алгоритм синтеза АМОКП позволяет получить увеличенное количество их неповторяющихся структур по сравнению с известными подходами.

5. Предложенная структура универсального формирователя АМОКП и алгоритм его функционирования.

6. Алгоритм защищенного информационного обмена в СС с КРК на основе хаотического применения АМОКП реализуется на основе реализации семи основных этапов и позволяет повысить защищённость информационного обмена на основе структурной скрытности.

БЛАГОДАРНОСТИ

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта № 29/2020.

СПИСОК ЛИТЕРАТУРЫ

1. Тихвинский В. О. Динамическое управление радиочастотным ресурсом сетей 5G для различных видов доступа к РЧС // Электросвязь. № 7. 2019. С. 18–22.

2. Ермакова А. В., Бабенко К. А., Мирошникова Н. Е. Текущее состояние и перспективы развития сети 5G // Телекоммуникации и информационные технологии. 2021. Т. 8. № 1. С. 21–28.

3. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

4. Варакин Л. Е. Теория сложных сигналов. – М.: Советское радио, 1978. – 199 с.

5. Дядюнов Н. Г., Сенин А. И. Ортогональные и квазиортогональные сигналы. – М.: Связь, 1977. – 224 с.

6. Литюк В. И., Литюк Л. В. Методы цифровой многопроцессорной обработки ансамблей радиосигналов. – М.: Солон-Пресс, 2007. – 592 с.

7. Попенко В. С. Векторный синтез ансамблей ортогональных сигналов. Часть 2. – Ставрополь: МО РФ, 1993. – 131 с.

8. Попенко В. С., Турко С. А. Генератор функций Попенко-Турко // Патент на изобретение SU 1753464 A1, опубл. 06.03.1990. – URL: http://elibrary.ru/item.asp?id=23014440 (дата обращения 27.06.2020).

9. Попенко В. С. Оценка ширины спектра дискретных сигналов // Радиотехника. 1996. № 11. С. 57–59.

10. Системы широкополосной радиосвязи: учеб. пособие для студ. вузов. – Одесса: Наука и техника, 2009. – 344 с.

11. Goel S, Chen V Information security risk analysis – a matrix-based approach. Proceedings of the Information Resource Management Association (IRMA) International Conference. – Hershey, USA, 2005. – 9 p.

12. Golomb S. Digital communications with space applications. – Upper Saddle River NJ, Prentice-Hall, 1964. – 210 p.

13. Golomb S. Shift Register Sequences. – San Francisco: Holden-Day, 1967.

14. Сухарев Е. М. и др. Общесистемные вопросы защиты информации. Коллективная монография. Кн. 1. – М.: Радиотехника, 2003. – 296 с.

15. Пашинцев В. П. Малофей О. П., Жук А. П. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн: Монография – М.: ООО Издательская фирма «ФМЛ», 2010. – 196 с.

16. Орёл Д. В. Моделирование стохастических систем двоичных квазиортогональных кодовых последовательностей на основе метода функциональных преобразований: автореф. дис. ... канд. техн. наук: 05.13.18 / Орёл Дмитрий Викторович. – Ставрополь, 2013. – 19 с.

17. Косякин С. И., Москвитин И. А., Смирнов А. А. Способ передачи информации в системах с кодовым разделением каналов и устройство для его осуществления // Патент на изобретение RU 2234191 C2, опубл. 10.08.2004. – URL: http://elibrary.ru/item.asp?id=37941753 (дата обращения 28.06.2020).

18. Жук А. П., Студеникин А. В., Жук Е. П. Алгоритм и устройство формирования ансамблей псевдослучайных ортогональных последовательностей для систем передачи информации с кодовым разделением каналов // Системы управления, связи и безопасности 2020 № 3. С. 1-21. DOI: 10.24411/2410-9916-2020-10301.

19. Жук А. П., Белан Н. В., Карасев И. В., Луганская Л. А. Оценка количества ансамблей новых многофазных ортогональных сигналов // Инфокоммуникационные технологии. 2017. Том 15. № 2. С. 117-123.

20. Жук А. П., Сазонов В. В. Влияние коэффициентов второй диагонали эрмитовой матрицы на корреляционные и спектральные свойства определяемых ею ортогональных в усиленном смысле сигналов. // Физика волновых процессов и радиотехнические системы. 2007. Т.10. № 6. С. 52-54.

21. Жук А. П., Петренко В. И., Кузьминов Ю. В., Жук Е. П., Луганская Л. А. Совершенствование способов обмена информацией в высокоскоростных беспроводных информационных сетях с использованием новых типов ансамблей дискретных последовательностей // Современные проблемы науки и образования. 2013. № 5. С. 144.

22. Жук А. П., Жук Е. П., Трошков А. М. Способ передачи информации с псевдослучайной перестройкой формы сигналов для систем связи с кодовым разделением каналов // Информационная безопасность. 2012: материалы XII Международной научно-практической конференции. Ч. 1. – Таганрог: ТТИ ЮФУ. 2012. – С. 346.

23. Свидетельство об гос. регистрации программы для ЭВМ № 2020665609. Программа генерации стохастических ортогональных сигналов «Stohastic orthogonal signal generator (SOSG)», 2020 г. / Сухоруков С. Ю., Жук А. П., Тран Е. С., Шуляк Я. В., Жук Е. П., Студеникин А. В.; № 2020665609; заявл. 20.11.2020; опубл. 27.11.2020.

24. Студеникин А. В., Жук А. П., Жук Е. П. Математическое моделирование ансамблей дискретных ортогональных последовательностей // Инновационные векторы цифровизации экономики и образования в регионах России, март 10-11, Ставрополь,

Ставропольский государственный аграрный университет. Ставрополь: Изд-во Агрус Ставропольского гос. аграрного университета. 2021. – С. 799.

25. Студеникин А. В., Жук А. П., Тран Е. С. Программная модель синтеза увеличенных объемов систем дискретных ортогональных кодовых последовательностей // Сборник докладов II Всероссийской научной конференции (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации», Ноябрь 30, 2020, Ставрополь, Северо-Кавказский федеральный университет. – Ставрополь: Изд-во СКФУ, 2020. С. 227-232.

Груздев С. В.
СарФТИ НИЯУ МИФИ, старший преподаватель
Евстифеев А. А.
СарФТИ НИЯУ МИФИ, старший преподаватель
Казаков А. А.
СарФТИ НИЯУ МИФИ, старший преподаватель
Красильников Б. А.
СарФТИ НИЯУ МИФИ, заведующий лабораторией
dim010307@yandex.ru

ОЦЕНКА ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ SDR-ПРИЕМНИКА ДЛЯ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ

Угрозы утечки информации

В современном мире трудно представить обработку большого объема данных без применения средств вычислительной техники (СВТ). Однако при использовании СВТ для обработки конфиденциальной информации необходимо обеспечить её сохранность.

Одним из сценариев утечки информации является утечка информации по техническим каналам за счет возникающих в процессе функционирования СВТ физических полей, которые могут содержать информацию. Совокупность источника информации, несанкционированного приёмника и среды распространения называют техническим каналом утечки информации (ТКУИ).

Одним из потенциально опасных ТКУИ является побочное электромагнитное излучение (ПЭМИ), возникающее при протекании по цепям СВТ токов. Поскольку величина тока переносит информацию, излучение так же может быть модулировано ей.

Методы противодействия утечке информации по каналу побочного электромагнитного излучения

Для оценки эффективности применяемых мер противодействия необходимо оценить отношение сигнал/шум на границе контролируемой зоны. Данная задача решается при проведении специальных исследований (СИ). С целью получения достоверных и повторимых результатов, условия, при которых проводятся измерения, должны быть регламентированы. На практике это достигается использованием измерительных площадок с жестко заданными геометрическими характеристиками в соответствие с руководящими документами регулирующих органов, например, ФСТЭК России.

Особенности систем, построенных по модели SDR

На практике возможны случаи, когда объект защиты располагается стационарно и не может быть легко перенесен на измерительную площадку, или необходимо произвести измерения в условиях расположения объекта защиты с учетом всех принимаемых мер [1, 2]. Тогда встаёт вопрос создания портативного мобильного комплекса, который бы позволил проводить оценку эффективности мер противодействия утечке информации по каналу ПЭМИ. Основой такого комплекса может являться программно-определяемая радиосистема (SDR). В простейшем случае в качестве основного элемента такой системы используется АЦП, подключенный непосредственно к приёмной антенне (рис. 1).

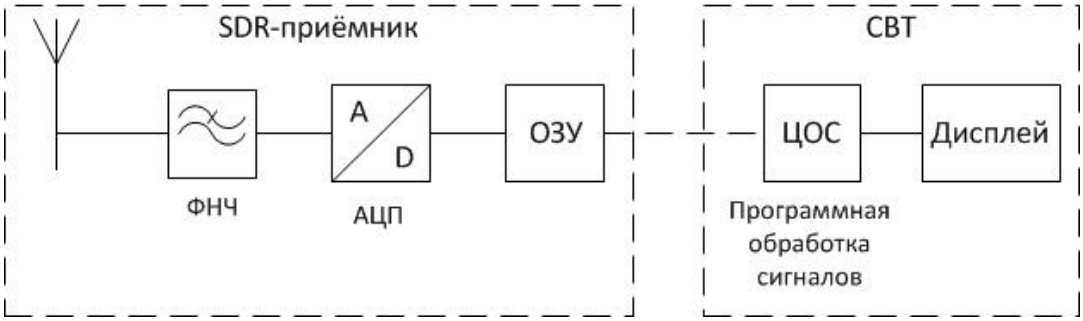


Рис. 1. Схема программно-определяемой радиосистемы

Для сравнения на рис. 2 приведена упрощенная структурная схема супергетеродинного приёмника, применяемого при проведении СИ:

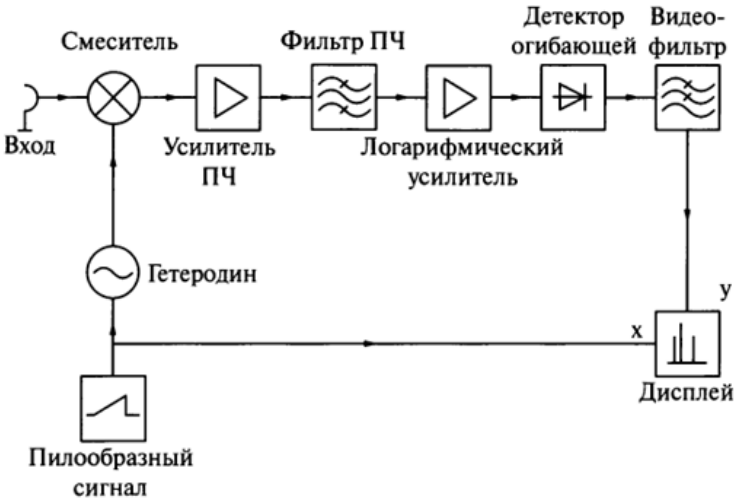


Рис. 2. Схема супергетеродинного приёмника

Особенностью супергетеродинного приёмника является использование гетеродина для переноса частоты. Данное решение обусловлено сложностью создания перестраиваемого полосового фильтра с допустимыми амплитудно-частотными характеристиками [3].

При использовании схемы, представленной на рис. 1, обработка сигналов осуществляется на СВТ, при этом методы цифровой обработки сигналов (ЦОС) позволяют создать фильтр любой требуемой характеристики. Однако, поскольку на вход АЦП поступает широкополосный сигнал, существует вероятность перегрузки входных каскадов в случае наличия мощной помехи на частоте, отличной от частоты исследуемого сигнала. Тогда восстановление исходного сигнала будет невозможно.

Таким образом, использование SDR-приёмника даёт возможность использовать методы ЦОС и отложенного анализа, а с другой стороны такой приёмник оказывается чувствительным к помехам, а его характеристики по уровню шума, согласованию с приёмной антенной и точности измерения амплитуды и частоты сигналов оказываются ниже. Также имеются ограничения, связанные с использованием быстрого преобразования Фурье (БПФ).

Описание используемого SDR-приёмника

В качестве измерительного приёмника используется доступный RTL-SDR, построенный на основе чипсета RTL2832. Микросхема содержит два 8-битных АЦП с

частотой дискретизации до 3,2 МГц и интерфейс USB для связи с компьютером. Эта микросхема на входе принимает I- и Q-потоки, источником которых является микросхема R820T. Она реализует радиочастотную часть, а именно буферный усилитель антенны, перестраиваемый широкополосный фильтр и квадратурный демодулятор с синтезатором частоты. Микросхема работает в диапазоне частот 24–1766 МГц.

Рис. 3. Внешний вид приёмника

Обзор используемого ПО для работы с SDR-приёмником

GNURadio. Позволяет проводить ЦОС полученных сигналов, при этом программа позволяет, как изменять характеристики существующих стандартных фильтров, так и создавать свои фильтры с заданной импульсной характеристикой. Это позволяет создавать оптимальные фильтры на основании априорных знаний об исследуемом сигнале. Также данное ПО позволяет обрабатывать полученный сигнал и создавать модуль с требуемым алгоритмом обработки сигналов. Для этой цели имеется возможность добавления своей библиотеки, написанной на языке Python, что позволяет автоматизировать процесс регистрации сигналов и реализовать, например, отложенный анализ или восстановление сигналов по нескольким реализациям с использованием их взаимной корреляции.

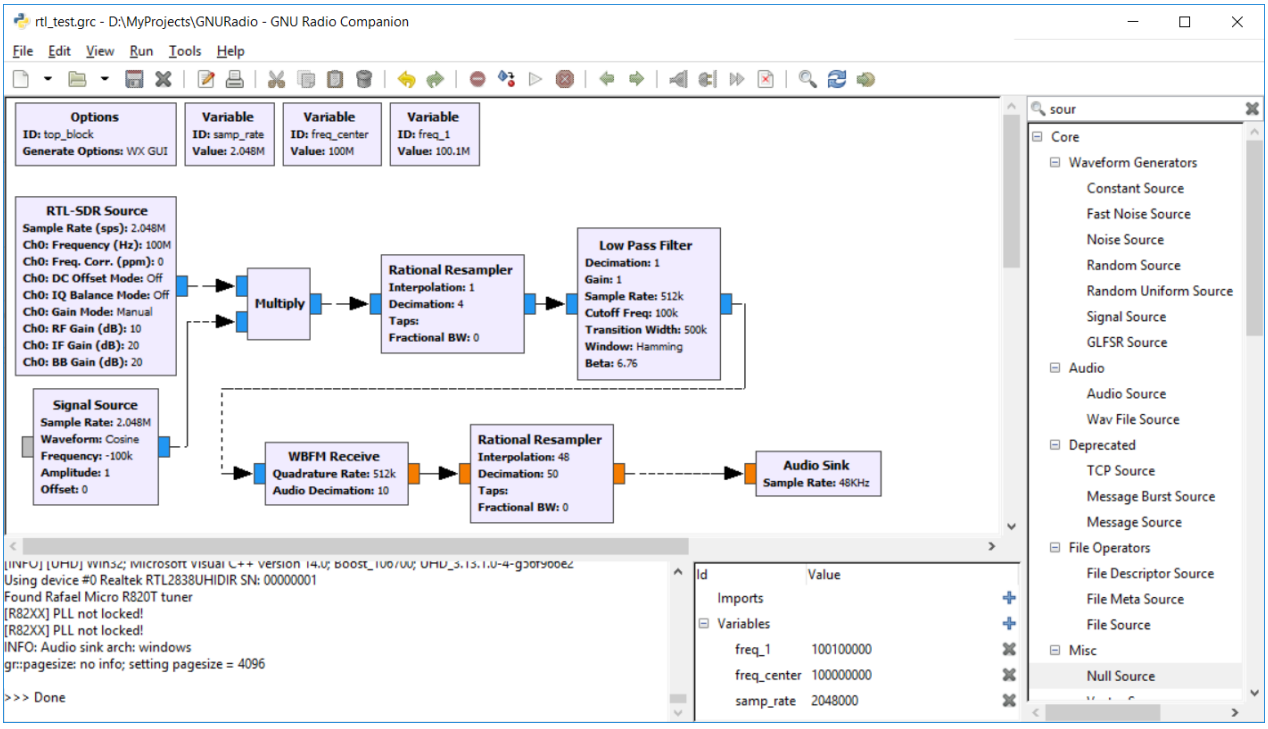


Рис. 5. Внешний вид интерфейса программы GNURadio

Особенности ПЭМИ интерфейсов СВТ

Сигналы ПЭМИ являются побочными, не предусмотренными разработчиком СВТ, что приводит к низкой мощности сигналов ПЭМИ в сравнение с сигналами функциональных каналов связи. Кроме того, в отличие от функциональных каналов связи, мощность полезного сигнала оказывается распределена в большом диапазоне частот. Поскольку информативные сигналы СВТ оказываются апереодическими, а зачастую могут быть даже импульсными, их спектр оказывается бесконечным и не дискретным. В таком случае спектр сигналов ПЭМИ определяется спектральной характеристикой излучающей системы, представленной межблочными кабелями и проводниковыми линиями. Поскольку на этапе разработки задачи эффективного излучения сигналов ПЭМИ не ставится, а зачастую даже наоборот, характеристики такой антенны оказываются не согласованными с характеристиками передаваемого сигнала. Таким образом, приём сигналов оказывается затруднен и предварительная оценка ожидаемого спектра сигналов является сложно выполнимой задачей. Все это приводит к тому, что поиск сигналов должен осуществляться чувствительной аппаратурой с широким частотным диапазоном и изменяемыми характеристиками фильтров [4-7]. На рисунке ниже представлены спектры сигналов ПЭМИ разных мониторов, полученные Маркусом Куном в его исследованиях [8].

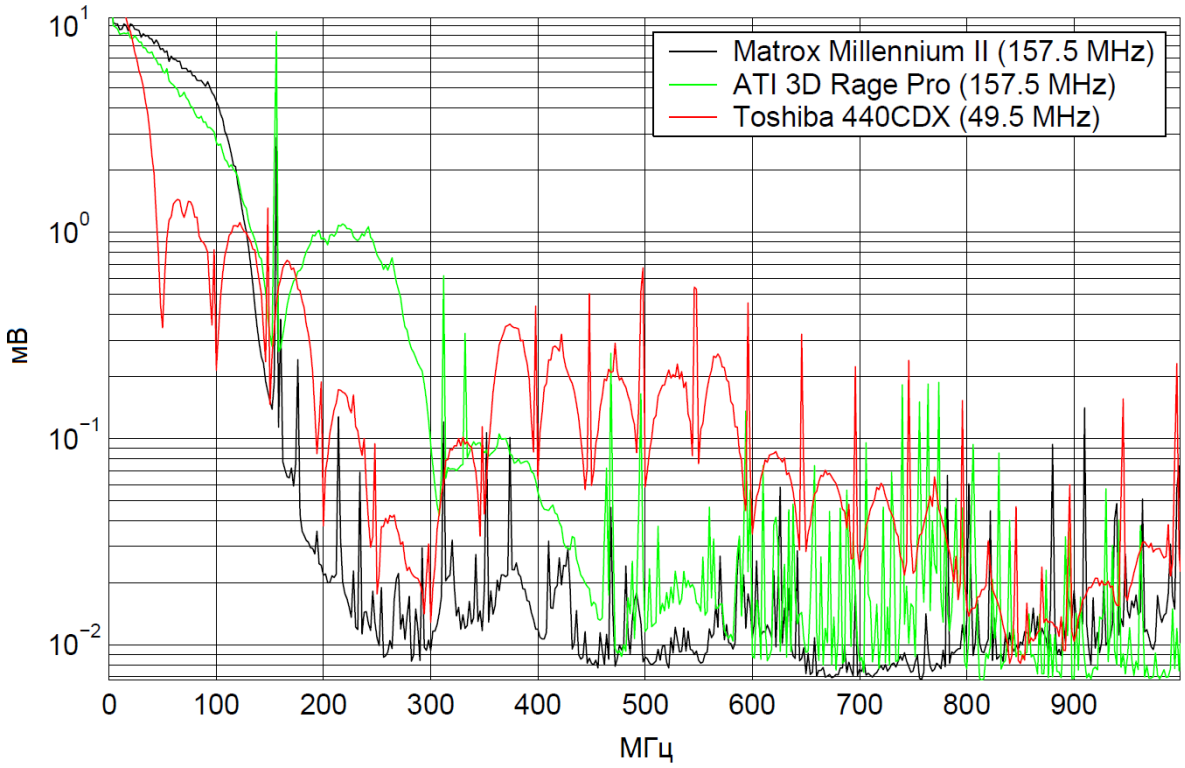


Рис. 6. Сравнение спектров сигналов ПЭМИ различных мониторов

Как видно, спектры сигналов ПЭМИ различаются для различных моделей мониторов, подсоединенных посредством интерфейса VGA значительно различаются даже при одинаковой частоте работы интерфейса.

Ни рис. 7 представлены спектры различных сигналов, а так же спектр сигналов ПЭМИ, полученные в рамках работы [9,10].

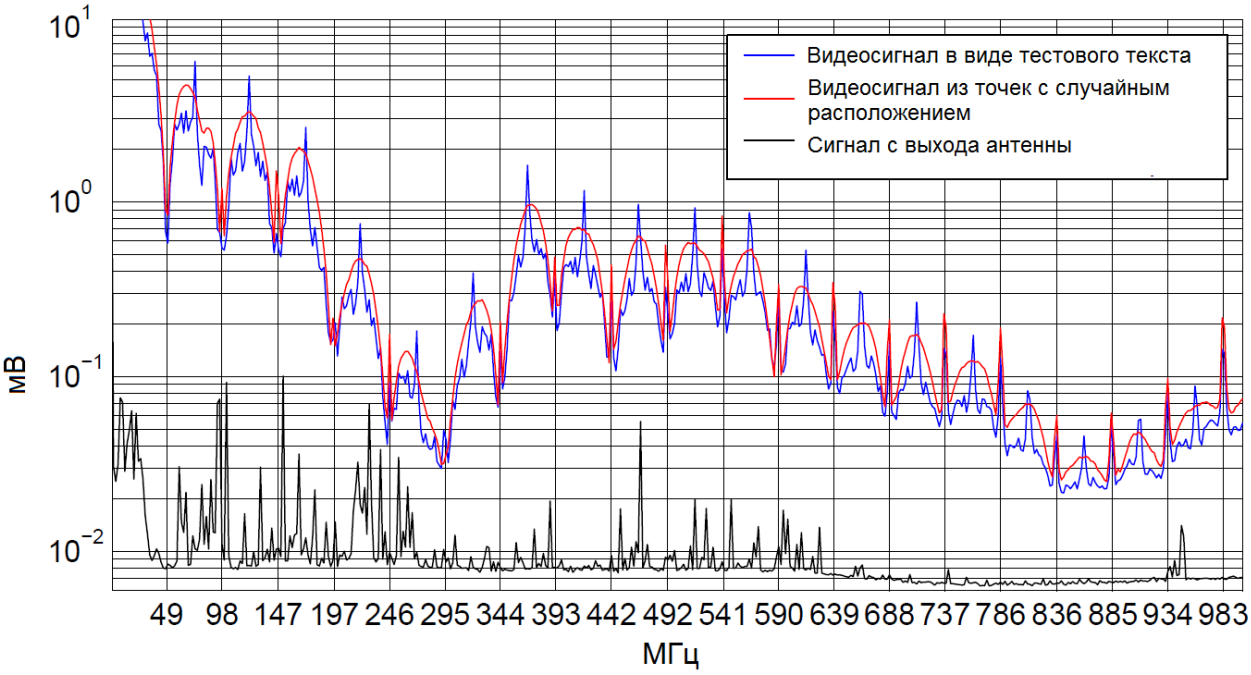


Рис. 7. Сравнение спектров различных сигналов

Как видно из рисунка, спектр исходного сигнала не совпадает со спектром ПЭМИ. Ранее было сказано, что спектр сигналов ПЭМИ определяется частотной характеристикой излучающей системы. Кроме того, данный график позволяет оценить величину напряжения на выходе приёмной антенны. Данные результаты получены при применении в качестве приёмной аппаратуры измерительного приемника, построенного по супергетеродинной схеме, а так же измерительных антенн.

Особенности использования SDR-приёмника для регистрации сигналов ПЭМИ

В процессе проведения СИ выполняется измерения уровней информативных сигналов. В соответствии с существующей нормативно-методической документацией измерения должны выполняться в соответствии с аттестованной методикой измерений поверенными средствами измерения, включенными в Федеральный информационный фонд по обеспечению единства измерений (ФИФ). В настоящий момент времени ни один из существующих SDR-приёмников не является средством измерений. Для обеспечения возможности их применения для проведения предварительных СИ производители данной аппаратуры должны внести ее в ФИФ. Однако, в рамках данной работы была проведена оценка возможности применения SDR-приёмника для приёма сигналов ПЭМИ.

Анализ полученных результатов

В рамках данной работы авторы использовали SDR-приёмник RTL820T2-SDR для приёма сигналов клавиатуры, мыши и VGA-кабеля, входящих в состав автоматизированного рабочего места. Результаты измерений обрабатывались в программе GNURadio. Результаты исследований показали, что сигнал ПЭМИ не был обнаружен. В то же время, при использовании в качестве измерительной аппаратуры измерительного приёмника и биконической измерительной антенны данные сигналы были обнаружены. Объект измерений располагался на высоте 1 м над подстилающей поверхностью. Измерения проводились на расстоянии 1 м. Кроме того, для SDR-приёмника измерения проводились так же на расстоянии 10 см. Это может объясняться как низкой чувствительностью самого SDR-приёмника и уровнем его собственного шума, так и неудовлетворительными характеристиками входящей в комплект антенны. Улучшение

характеристик использовавшегося средства измерений возможно за счет применения измерительных антенн, однако это осложняется необходимостью согласования входных каскадов SDR-приёмника, антенного кабеля и самой антенны, а так же установке разъема для подключения антенны, что выходит за рамки данной работы.

В рамках выполнения работы авторами показано, что использование SDR-приёмника для проведения СИ является перспективной задачей, однако требует доработки нормативно-методических документов, улучшения характеристик существующих приёмников и включения их в ФИФ.

СПИСОК ЛИТЕРАТУРЫ

1. Казаков А. А. Теоретическая модель распределенной системы средств активной защиты информации / А. А Казаков, Д. В. Лушкин, И. А. Николаева, В. Ю. Шишков // Математика и математическое моделирование. Сборник материалов XIV Всероссийской молодежной научно-инновационной школы.— 2020.— С. 143-144.
2. Казаков А. А. Исследование вопросов защиты информации от утечки по техническому каналу при использовании средств активной защиты / А. А Казаков, В. И. Ерошев // Математика и математическое моделирование. Сборник материалов XIII Всероссийской молодежной научно-инновационной школы.— 2019.— С. 61-62.
3. Евстифеев А. А. Разработка предложений по оценке защищенности информации технических систем от утечки по техническим каналам / А. А. Евстифеев, В. И. Ерошев, А. А. Казаков // Математика и математическое моделирование. Сборник материалов XII Всероссийской молодежной научно-инновационной школы.— 2018.— С. 15-16.
4. Шишкин, Г. Селекторы цифровых команд. Часть 2 / Г. Шишкин, Д. Николаев // Компоненты и технологии. – 2009. – № 8(97). – С. 112-116.
5. Шишкин, Г. Селекторы цифровых команд. Часть 3 / Г. Шишкин, Д. Николаев // Компоненты и технологии. – 2009. – № 9(98). – С. 116-120.
6. Схемотехническая реализация автомата / С. Гончаров, Д. Николаев, В. Никитин, В. Писецкий // Компоненты и технологии. – 2013. – № 2(139). – С. 126-128.
7. Исследование перспективных технических каналов утечки информации / А. А. Евстифеев, В. И. Ерошев, А. А. Казаков, Д. Б. Николаев // Математика и математическое моделирование : Сборник материалов XII Всероссийской молодежной научно-инновационной школы, Саров, 17–19 апреля 2018 года. – Саров: Саровский физико-технический институт НИЯУ МИФИ, 2018. – С. 12-13.
8. Markus G. K. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations / G. K. Markus, J. A. Ross // Information Hiding, IH’98, Portland, Oregon, Proceedings, LNCS 1525, Springer-Verlag.— 1998.— P. 124–142.
9. Исследование возможности создания программно формируемых технических каналов утечки информации / А. А. Евстифеев, В. И. Ерошев, А. А. Казаков, Д. Б. Николаев // XXIII Нижегородская сессия молодых ученых (технические, естественные, математические науки) : материалы докладов, Нижний Новгород, 22–23 мая 2018 года. – Нижний Новгород: Нижегородский государственный инженерно-экономический институт, 2018. – С. 85.

10. Исследование метода многопозиционного приема при обнаружении сигналов побочного электромагнитного излучения / А. А. Казаков, А. А. Евстифеев, В. И. Ерошев, Д. Б. Николаев // Математика и математическое моделирование : сборник материалов XI Всероссийской молодежной научно-инновационной школы, Саров, 11–13 апреля 2017 года / Национальный исследовательский ядерный университет МИФИ, Саровский физико-технический институт. – Саров: Б. и., 2017. – С. 16-17.

Белозубова А.И.
НИЯУ МИФИ, аспирант
aibelozubova@mephi.ru
Епишкина А.В.
НИЯУ МИФИ, к.т.н.
avepishkina@mephi.ru
Когос К.Г.
НИЯУ МИФИ, к.т.н.,
kgkogos@mephi.ru

ОГРАНИЧЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТЕВОГО СКРЫТОГО КАНАЛА ПО ВРЕМЕНИ С УЧЕТОМ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ СЛЕДОВАНИЯ ПАКЕТОВ В СЕТИ

Аннотация. Скрытым каналом называется непредусмотренный разработчиком информационной системы коммуникационный канал, который может быть применен для нарушения политики безопасности. Опасность скрытых каналов заключается в том, что при соблюдении определенных условий возможно построение необнаруживаемого скрытого канала. Возможность негласного использования особенностей протокола IP и широкое распространение IP-сетей придают масштабность проблеме утечки информации по скрытым каналам в IP-сетях. В связи со структурными особенностями IP-протокола становится возможной скрытая передача информации путем модуляции передачи пакетов: изменения битов заголовков, информационного наполнения и временных характеристик.

Настоящая работа посвящена разработке и исследованию способа противодействия утечке информации по скрытым каналам по времени в IP-сетях, заключающегося во введении случайных дополнительных задержек перед отправкой пакетов. Такое противодействие вносит ошибки в потенциальные скрытые каналы и заставляет злоумышленника преднамеренно понижать интенсивность передачи данных.

В рамках исследования оценивалось влияние предложенного способа противодействия на бинарный скрытый канал, основанный на изменении длин межпакетных интервалов. Рассмотрен случай, когда время следования пакетов в сети описывается нормальным законом распределения, и приведены формулы расчета пропускной способности сетевого скрытого канала с учетом временных характеристик трафика в сети.

Исследование выполнено при финансовой поддержке Министерства науки и высшего образования (грант аспирантам и молодым ученым на исследования, которые направлены на обеспечение информационной безопасности для задач цифровой экономики).

Ключевые слова: *скрытые каналы, информационная безопасность, пропускная способность, время движения пакетов, нормальное распределение.*

Введение

Термин «скрытый канал» впервые введен авторами [1] как коммуникационный канал, не предназначенный для передачи информации. В [2] утверждается, что скрытый канал — это коммуникационный канал, который не был предусмотрен разработчиком системы и который может быть использован для нарушения политики безопасности.

Возможность негласного использования свойств протокола IP и широкое распространение IP-сетей придают масштабность проблеме утечке информации по скрытым каналам в IP-сетях. Особую актуальность рассматриваемой угрозе придают результаты исследований показывающие, что если противнику известна схема контроля в системе защиты, то возможно построение невидимого для системы защиты скрытого канала управления программно-аппаратным агентом в компьютерной среде [3, 4].

Традиционно, по способу передачи информации скрытые каналы разделяются на каналы по памяти и каналы по времени [5]. Изменение полей заголовков пакетов (например, Fragment Offset, CheckSum, Time To Live, Time Stamp) и изменение длин передаваемых пакетов используется для передачи информации по скрытым каналам по памяти в IP-сетях [6-10]. Изменение скорости передачи пакетов, изменение длин межпакетных интервалов и переупорядочивание пакетов используются для построения скрытых каналов по времени в IP-сетях [8], [11 - 14].

Применяют три основных способа противодействия утечке данных по скрытым каналам: обнаружение, подавление и ограничение пропускной способности скрытых каналов. Способ обнаружения скрытых каналов позволяет эффективно использовать канал связи, но не гарантирует выявление всех возможных каналов утечки информации, так как нарушитель может использовать нетривиальную схему кодирования, чтобы сделать скрытый канал необнаруживаемым [3, 4]. Подавление скрытых каналов, состоящее в нормализации параметров IP-трафика (то есть, в передаче IP-пакетов фиксированной длины с фиксированными заголовками через равные промежутки времени), приводит к существенному снижению эффективности использования пропускной способности каналов связи. Способ ограничения пропускной способности скрытых каналов, заключающийся в контролируемом понижении пропускной способности скрытых каналов и, как следствие, несущественном увеличении дополнительной нагрузки на канал связи, позволяет гарантированно снизить объем данных, утечка которых возможна по скрытому каналу. Данный подход применим в случае, когда политика безопасности допускает существование в системе скрытых каналов с пропускной способностью не выше заданной, что рекомендуется в ГОСТ 53113.1-2008 [2], авторами TCSEC [5] и специалистами IBM [15]. Однако для принятия решения о введении любых мер противодействия необходимо точно оценить возможности противника и определить максимальную пропускную способность скрытого канала [2, 16]. В связи с этим настоящая работа посвящена исследованию способов оценки максимальной пропускной способности бинарного скрытого канала по времени с учетом характера времени следования пакетов в сети (далее — ВСП). Исследования проведены для случаев, когда время движения пакетов в сети определяется нормальным законом распределения. Пропускная способность скрытого канала оценивается как функция параметров скрытого канала и закона распределения ВСП в сети.

Далее статья организована следующим образом. Описание схемы работы исследуемого сетевого скрытого канала и рассмотрение факторов, влияющих на время следования пакетов в сети, приведены в разделе 1. Раздел 2 содержит описание математического аппарата, используемого для оценки пропускной способности скрытого канала в условиях, когда время следования пакетов в сети определяется нормальным законом распределения. В разделе 3 описывается метод противодействия утечке информации. В разделе 4 приводится описание способа расчета остаточной пропускной

способности скрытого канала в условиях введения метода противодействия. Обзор основных результатов, выводы и выявленные направления исследований представлены в заключении.

Направления исследований

В настоящем разделе представлено описание исследуемого сетевого скрытого канала по времени, а также условий в сети, в которых скрытые каналы могут функционировать.

Сетевой скрытый канал, основанный на изменении длин межпакетных интервалов

Отправитель и получатель определяют значения интервалов t_0 и t_1, которые обеспечивают высокую скорость передачи информации и допустимый уровень ошибок в скрытом канале. Передача пакета с межпакетным интервалом t_0 соответствует биту «0», а с интервалом t_1 соответствует биту «1». Пусть q — вероятность, с которой в закодированном отправителем сообщении появляется бит «0», а t — длина интервала между приемами пакетов на стороне получателя. Если $t \le t_{\text{гр}}$, то получатель декодирует бит «0», если $t > t_{\text{гр}}$, то получатель декодирует бит «1», где $t_{\text{гр}}$ — граничное значение длины межпакетного интервала, определяющееся как $t_{\text{гр}} = \dfrac{t_0 + t_1}{2}$. На рис. 1 показана передача сообщения «00110» с использованием скрытого канала.

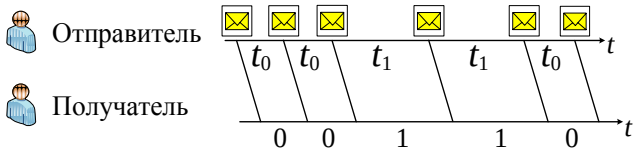


Рис. 1. Передача сообщения «00110» по сетевому скрытому каналу, основанному на изменении длин межпакетных интервалов

Время следования пакетов в сети

Следует принимать во внимание, что в сети возникают задержки, приводящие к возникновению ошибок или, другими словами, шума в скрытом канале. Выделяют задержки, вызванные следующими причинами [17]:

1. узловая обработка — время, необходимое маршрутизатору для чтения заголовка пакета и определения его дальнейшего маршрута;
2. очередь — время, которое пакет находится в очереди для дальнейшей передачи по линии связи;
3. передача — время, необходимое для перемещения пакета в линию передачи;
4. распространение — время передачи пакета по линии связи от источника к получателю.

Задержки передачи и распространения относятся к типу постоянных задержек. Задержка пакета в очереди и обработка на маршрутизаторе зависят от нагрузки в сети, размера и количества пакетов, полосы пропускания интерфейса. Поэтому время движения пакетов в сети от отправителя получателю непостоянно, однако подчиняется некоторым законам. Исследования авторов [18 - 20] показали, что время движения пакетов в сети хорошо аппроксимируется усеченным нормальным, гамма, логнормальным, экспоненциальным законами распределения и распределением Вейбулла. Далее

исследуется способ оценки максимальной пропускной способности скрытых каналов по времени с учетом характера движения пакетов в сети. В качестве базового случая была рассмотрена ситуация, когда пропускная способность скрытого канала рассчитывается в условиях предположения, что ВСП от отправителя к получателю равномерно распределено на некотором отрезке. Однако, в реальных условиях одни значения ВСП могут встречаться чаще других. На основании исследований авторов статей [18 - 20] дополнительно были рассмотрены случаи, когда ВСП принимает вид нормального и экспоненциального распределения.

Пропускная способность скрытого канала в условиях нормального распределения времени следования пакетов в сети

Пропускная способность скрытого канала с шумом может быть оценена по следующей формуле:

$$C = \max_{X} \frac{I(X,Y)}{T + t_{\text{п}}}, \tag{1}$$

где X и Y входные и выходные характеристики скрытого канала соответственно, T — средняя длина межпакетного интервала, $t_{\text{п}}$ — среднее время перемещения пакета в линию передачи.

Взаимная информация может быть оценена по следующей формуле:

$$I(X,Y) = H(Y) - H(Y \mid X), \tag{2}$$

энтропия рассчитывается по формуле:

$$H(Y) = -\sum_{y \in \{0,1\}} p_{\text{вых}}(y) \log_2 p_{\text{вых}}(y), \tag{3}$$

условная информация Y и X равна

$$H(Y \mid X) = -\sum_{x \in \{0,1\}} p_{\text{вх}}(x) \sum_{y \in \{0,1\}} p_{\text{вых}}(y \mid x) \log_2 p_{\text{вых}}(y \mid x), \tag{4}$$

где $p_{\text{вых}}(i)$ — вероятность распознавания символа «i», $p_{\text{вых}}(i \mid j)$ — вероятность распознавания символа «i» при отправке символа «j», $i, j \in \{0,1\}$. Далее будем считать, что биты «0» и «1», передаваемые по скрытому каналу, подаются на вход с вероятностями $p_{\text{вх}}(0) = q, p_{\text{вх}}(1) = 1 - q.$

Авторами была исследована локальная сеть и с использование утилиты ping были получены временные характеристики трафика – значения Round Trip Time (RTT) для более чем 10 тысяч IP пакетов. Сделано допущение, что ВСП от отправителя получателю (односторонняя задержка) равно половине значения RTT. Минимальное время движения пакета до сетевого устройства составило 1 мс, максимальное — 19 мс, среднее — 4,4 мс. Таким образом, максимальное отклонение ВСП от среднего значения составляет $d_{\max}$ = 14,6 мс, и значения ВСП от отправителя к получателю лежат в интервале (a;b), где a=1 мс, b=19 мс. Пусть в скрытом канале, основанном на изменении длин межпакетных интервалов, пакеты отправляются в середине интервала t_0=2$d_{\max}$, если необходимо послать значение «0», и в середине интервала t_1=6$d_{\max}$ — если значение «1». Таким образом, длина интервала, между двумя пришедшими пакетами на стороне получателя, лежащая в пределах (0; 4$d_{\max}$) соответствует «0», а лежащая в пределах (4$d_{\max}$; 8$d_{\max}$) — «1». Средний межпакетный интервал равен 4$d_{\max}$.

Обозначим $f(x)$ функцию распределения ВСП. Согласно исследованиям $f(x)$ может принимать форму нормального, экспоненциального, усеченного нормального, гамма, логнормального, закона распределения и их различных сумм и распределения Вейбулла [14-18]. Пусть функция $f(x)$ описывается нормальным законом распределения (НЗР) с функцией плотности вероятности:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}, \tag{5}$$

и функцией распределения:

$$F = \frac{1}{2}\left[1 + erf\left(\frac{x-\mu}{\sqrt{2\sigma^2}}\right)\right], \tag{6}$$

$$erf(m) = \frac{2}{\sqrt{\pi}}\int_0^m e^{-t^2} dt.$$

Здесь *erf x* — функция ошибок (функция Лапласа), которую нельзя получить за конечное число арифметических операций, поэтому применяется ее аппроксимация разложением в ряд Тейлора:

$$erf(m) = \frac{2}{\sqrt{\pi}}\sum_{n=0}^{\infty}\frac{(-1)^n m^{2n+1}}{n!(2n+1)}. \tag{7}$$

Полученный в результате эксперимента набор значений ВСП в сети был аппроксимирован. Были рассчитаны параметры μ,σ нормального распределения. На рис. 2 синим цветом представлен график распределения полученных значений ВСП от отправителя к получателю. Красным цветом обозначена плотность распределения с рассчитанными параметрами μ,σ, где значения по оси ординат рассчитывались по формуле (5).

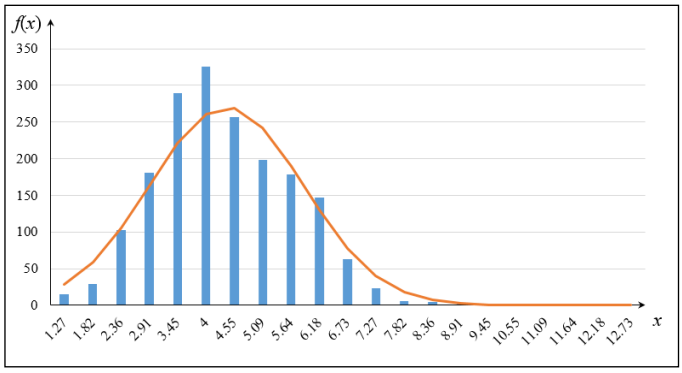


Рис. 2. График распределения ВСП в сети от отправителя до получателя

Чтобы определить условные вероятности $p(y|x)$ распознавания символа «*y*» при отправке символа «*x*» при введении задержек перед отправкой пакетов, необходимо рассмотреть условия выполнения следующих неравенств:

Табл. 1. Определение условных вероятностей

Условная вероятность	Неравенство
$p(0\|0)$	$t_0 - t_п + t_в \le t_{гр}$

$p(0\|1)$	$t_1 - t_п + t_в \le t_{гр}$
$p(1\|0)$	$t_0 - t_п + t_в \ge t_{гр}$
$p(1\|1)$	$t_1 - t_п + t_в \ge t_{гр}$

Для определения условной вероятности $p_{вых}(0|0)$ необходимо определить вероятность того, что соблюдается неравенство $t_в - t_п \le t_{гр} - t_0$, где $t_п$ и $t_в$ — величины, подчиняющиеся нормальному закону распределения. Пусть $z = t_в - t_п$, а $F'(z)$ — функция распределения разности двух случайных величин, каждая из которых подчиняется нормальному закону распределения. Нормальное распределение обладает свойством устойчивости, следовательно, функция $F'(z)$ также подчиняется нормальному закону распределения с параметрами $\sigma_z = \sqrt{2\sigma^2} = \sqrt{2}\sigma$ и $\mu_z = \mu - \mu = 0$:

$$F'(z) = \frac{1}{2}\left[1 + erf\left(\frac{z}{2\sigma}\right)\right]. \quad (8)$$

Следовательно,

$$p_{вых}(0\,|\,0) = \int_{-\infty}^{t_{гр}-t_0} f(z)dz = F'(t_{гр} - t_0). \quad (9)$$

Аналогично рассчитываются остальные условные вероятности:

$$\begin{aligned} p_{вых}(0\,|\,1) &= \int_{-\infty}^{t_{гр}-t_1} f(z)dz = F'(t_{гр} - t_1), \\ p_{вых}(1\,|\,0) &= \int_{t_{гр}-t_0}^{+\infty} f(z)dz = 1 - F'(t_{гр} - t_0), \\ p_{вых}(1\,|\,1) &= \int_{t_{гр}-t_1}^{+\infty} f(z)dz = 1 - F'(t_{гр} - t_1). \end{aligned} \quad (10)$$

При помощи полученных формул (1), (9), (10) и подбора параметров скрытого канала было установлено, что максимальная пропускная способность скрытого канала при условии распределения ВСП в сети по нормальному закону распределения и отсутствии противодействия достигает 404,52 бит/с при параметрах t_0=0 с, t_1=9,2 мс и q= 0,9465.

Таким образом, в данном разделе оценена пропускная способность бинарного скрытого канала, основанного на изменении длин интервалов между отправкой пакетов, при распределении ВСП в сети согласно нормальному закону распределения.

Метод противодействия утечке информации

Предлагаемый метод противодействия заключается во введении перед отправкой пакетов дополнительных задержек τ, значения которых равномерно распределены на интервале (0;d), где d — параметр противодействия. Таким образом в скрытый канал добавляется шум, что приводит к ошибкам и, как следствие, снижает его пропускную способность.

Ошибки в скрытом канале, основанном на изменении длин межпакетных интервалов, заключаются в том, что задержки, введенные перед отправкой пакетов, изменяют длины межпакетных интервалов на стороне получателя. Таким образом межпакетные интервалы, соответствующие биту «0», могут увеличиваться до длины, соответствующей биту «1», и наоборот [21].

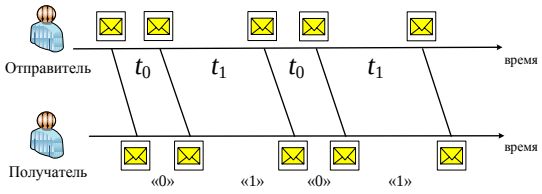


Рис. 3. Отправка сообщения «0101» в скрытом канале без введения метода противодействия

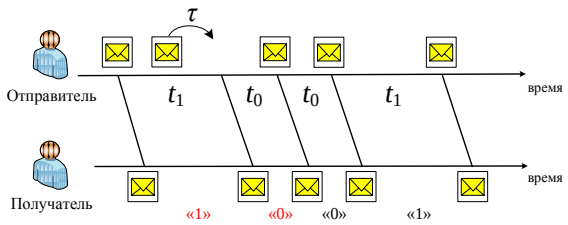


Рис. 4. Появление ошибок в скрытом канале из-за введения задержек перед отправкой пакетов

На рис. 3 показана отправка сообщения «0101» в скрытом канале, на рис. 4 — отправка того же сообщения и проиллюстрировано появление ошибок и распознавание получателем сообщения «1001» в результате введения задержки τ перед отправкой второго пакета.

Остаточная пропускная способность скрытого канала в условиях введения противодействия

Далее приведены неравенства, определяющие условные вероятности $p(y|x)$ распознавания символа «y» при отправке символа «x» при введении задержек перед отправкой пакетов.

Табл. 2. Определение условных вероятностей в условиях введения противодействия

Условная вероятность	Неравенство
$p(0\|0)$	$t_0 - t_{\text{п}} + t_{\text{в}} - \tau_{\text{п}} + \tau_{\text{в}} \le t_{\text{гр}}$
$p(0\|1)$	$t_1 - t_{\text{п}} + t_{\text{в}} - \tau_{\text{п}} + \tau_{\text{в}} \le t_{\text{гр}}$
$p(1\|0)$	$t_0 - t_{\text{п}} + t_{\text{в}} - \tau_{\text{п}} + \tau_{\text{в}} \ge t_{\text{гр}}$
$p(1\|1)$	$t_1 - t_{\text{п}} + t_{\text{в}} - \tau_{\text{п}} + \tau_{\text{в}} \ge t_{\text{гр}}$

Пусть $z = t_{\text{в}} - t_{\text{п}}$, где $t_{\text{п}}$ и $t_{\text{в}}$ – случайные величины, подчиняющиеся нормальному закону распределения. Тогда:

$$\begin{aligned} p(0\,|\,0) &= \int_{-\infty}^{t_{\text{гр}}-t_0+d_{\text{п}}-d_{\text{в}}} f(z)dz = F'(t_{\text{гр}} - t_0 + d_{\text{п}} - d_{\text{в}}), \\ p(0\,|\,1) &= \int_{-\infty}^{t_{\text{гр}}-t_1+d_{\text{п}}-d_{\text{в}}} f(z)dz = F'(t_{\text{гр}} - t_1 + d_{\text{п}} - d_{\text{в}}), \\ p(1\,|\,0) &= \int_{t_{\text{гр}}-t_0+d_{\text{п}}-d_{\text{в}}}^{+\infty} f(z)dz = 1 - F'(t_{\text{гр}} - t_0 + d_{\text{п}} - d_{\text{в}}), \\ p(1\,|\,1) &= \int_{t_{\text{гр}}-t_1+d_{\text{п}}-d_{\text{в}}}^{+\infty} f(z)dz = 1 - F'(t_{\text{гр}} - t_1 + d_{\text{п}} - d_{\text{в}}). \end{aligned} \qquad (11)$$

При этом вероятности того, что получатель в скрытом канале декодирует символы «0» и «1», определяются по формулам (11)**Ошибка! Источник ссылки не найден.**. И при помощи формул (1) - (4) определяется пропускная способность скрытого канала.

Используя полученные формулы и перебор параметров скрытого канала и метода противодействия, можно оценить наибольшее значение остаточной пропускной способности канала при введении задержек перед отправкой пакета. На рис. 5 представлен график зависимости пропускной способности скрытого канала при введении задержек перед отправкой пакетов от параметра противодействия.

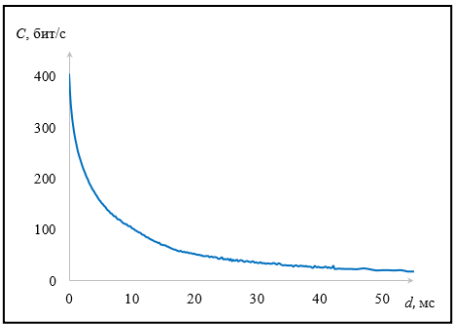


Рис. 5. График зависимости остаточной пропускной способности скрытого канала от параметра противодействия *d*

Рекомендации по ограничению пропускной способности скрытых каналов приводятся, например, специалистами IBM Knowledge Center и авторами критериев определения безопасности компьютерных систем (Trusted Computer System Evaluation Criteria): скрытые каналы с пропускной способностью выше, чем 100 бит/с, недопустимы в информационной системе [5, 15]. Таким образом, из графика на рис. 5 видно, что для снижения пропускной способности бинарного скрытого канала, основанного на изменении длин интервалов между отправкой пакетов, до значения 100 бит/с параметр противодействия *d* необходимо принять равным 10 мс.

Заключение

В работе был исследован способ оценки максимальной пропускной способности бинарного сетевого скрытого канала, основанного на модификации длин межпакетных интервалов, при распределении ВСП в сети согласно нормальному закону распределения. Предложен метод противодействия утечке информации, заключающийся во введении дополнительных случайных задержек перед отправкой пакетов и отличающийся тем, что он применим в случае, когда к защищаемому объекту предъявляются требования информационной безопасности, допускающие функционирование скрытого канала с пропускной способностью не выше заданной. Приведены формулы расчета пропускной способности скрытого канала при отсутствии противодействия и в условиях введения дополнительных задержек перед отправкой пакетов. При расчетах учитывается характер распределения ВСП. Точный расчет максимальной пропускной способности потенциального скрытого канала позволит принимать объективные решения о введении средств противодействия, а точная оценка остаточной пропускной способности сделает возможным выбор параметра метода противодействия с условием сохранения эффективной пропускной способности коммуникационного канала.

Оценка пропускной способности других типов скрытых каналов с учетом характера распределения ВСП в сети и введения мер противодействия представляет собой тему для дальнейшего исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Фамилия 1-го автора, И.О. Nonlinear iterative precoding algorithm for MIMO multiuser systems / И.О. 1-я фамилия, И.О. 2-я фамилия // Название журнала. — Год выпуска. — № журнала. — Страницы.
2. Lampson, B.W. A Note on the Confinement Problem // Communications of the ACM. — 1973. — vol. 16, No. 10. — pp. 613-615.
3. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. — Введ. 2009-10-01. — М.: Стандартинформ, 2009. — 12 с.
4. Грушо, А.А. Скрытые каналы и безопасность информации в компьютерных системах / А.А. Грушо // Дискретная математика. — 1998. — Том 10, выпуск 1. — С. 3–9. — Библиогр.: с. 9.
5. Грушо, А.А. О существовании скрытых каналов / А.А. Грушо // Дискретная математика. — 1999. — Том 11, выпуск 1. — С. 24–28. — Библиогр.: с. 28.
6. National Computer Security Center, Department of defense standard, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985.
7. Ahsan, K. Practical Data Hiding in TCP/IP / K. Ahsan, D. Kundur // Proceedings of the ACM Workshop on Multimedia Security. — 2002.
8. Zander, S. Covert Channels in the IP Time To Live Field / S. Zander, G. Armitage, P. Branch // Proceedings of the Australian Telecommunication Networks and Applications Conference. — 2006.
9. Zander, S. A Survey of Covert Channels and Countermeasures in Computer Network Protocols / S. Zander, G. Armitage, P. Branch // IEEE Communications Surveys and Tutorials. —2007. — vol. 9, No. 3. — pp. 44-57.
10. Epishkina, A. A random traffic padding to limit packet size covert channels / A. Epishkina, K. Kogos // Proceedings of the 2015 Federated Conference on Computer Science and Information Systems. —2015. — vol. 5. — pp. 1107-1113.
11. Epishkina, A. Covert channels parameters evaluation using the information theory statements / A. Epishkina, K. Kogos // Proceedings of the 5th International Conference on IT convergence and security. — 2015. — pp. 395-399.
12. Cabuk, S. “IP covert timing channels: design and detection / S. Cabuk, C.E Brodley, C. Shields // Proceedings of the eleventh ACM conference on computer and communications security. — 2004. — pp. 178-187.
13. Girling, C.G. Covert channels in LAN’s / C.G. Girling // IEEE Transactions on software engineering. —1987. vol. 13, no. 2. — pp. 292-296.
14. Shah, G. Keyboards and Covert Channels / G. Shah, A. Molina, M. Blaze // Proceedings of the 15th USENIX Security Symposium, 2006, pp. 59-75.

15. Sellke, S.H. Covert TCP/IP timing channels: theory to implementation / S.H. Sellke, C.-C. Wang, S. Bagchi, N.B. Shroff // Proceedings of the 28th conference on computer communications, 2009, pp. 2204-2212.
16. IBM Knowledge Center [Электронный ресурс] / Режим доступа: https://www.ibm.com/support/knowledgecenter/ssw_aix_71/security/taix_audit_bandwidth.html (дата обращения 15.09.2021).
17. ГОСТ Р 53113.2-2009. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов [Текст]. — Введ. 2009-12-01. — М.: Стандартинформ, 2010. — 12 с.
18. Liu, M. Research on the Distribution and Self-Similarity Characteristic of End-To-End Network Delay / M. Liu, Y. Xue, Y. Zhao, H. Guo // International Journal of Future Generation Communication and Networking. — 2015. — vol.8, No.3.
19. Elteto, T. On the distribution of round-trip delays in TCP/IP networks / T. Elteto, S. Molnar // Proceedings of the 24th Conference on Local Computer Networks. — 1999.
20. Karakas, M. Determination of network delay distribution over the internet / M. Karakas // Thesis submitted to the graduate school of natural and applied sciences of the Middle East Technical University. — December 2003.
21. Sukhov, A.M. Generating Function For Network Delay / A.M. Sukhov, N.Yu. Kuznetsova, A.K. Pervitsky, A.A. Galtsev,// Journal of High Speed Networks. — 2016. — vol. 22, no. 4. — pp. 321-333.
22. Huang, G. Measurement and Modeling of Network Delays for MS-Based A-GPS Assistance Delivery / G. Huang, D. Akopian, C. L. P. Chen // IEEE Transactions on instrumentation and measurement. — 2014. — vol. 63, No. 8.

Лапшичёв В.В.
ЮФУ, младший научный сотрудник
lapshichyov@sfedu.ru

МЕТОДИКИ ОБНАРУЖЕНИЯ ДАННЫХ СЕТИ TOR

1. Проблематика обнаружения сети Tor. Главными особенностями сети Tor является использование цепочки узлов, через которые проходит зашифрованный трафик между пользователем и сервером сети, реализуемой анонимными серверами [1]. Для применения законодательно установленной нормы, позволяющей применять санкции в отношении использования т.н. «анонимайзеров» (сетей, систем и программ, обеспечивающих анонимность пользователя), необходимо решить ряд вопросов, стоящих на пути реализации законного блокирования. Обнаружение и идентификация трафика сети Tor усложнены ввиду различных способов обеспечения анонимности ее пакетов, среди которых: использование с 2018 года обновленного протокола шифрования TLS версии 1.3, позволяющего шифровать не только передаваемые данные, но и сам процесс установления соединения в части, касающейся рукопожатия между клиентским и серверным программным обеспечением; использование обфускации (маскирования) пакетов между локальной машиной пользователя и сервером сети, делая «глубокий анализ пакетов» на оборудовании провайдеров средств связи бесполезным. Работы китайских ученых [2-4], занимающихся проблематикой обнаружения и идентификации сети Tor, говорят о том, что ими найдены решения для определения данных сети, в том числе в обфусцированном потоке, с применением нейронных сетей. Однако ими же выражается сомнение в универсальности разработанного ими метода в связи с успешной идентификацией данных сети Tor только в лабораторных условиях.

2. Средства обнаружения протокола TLS v1.2. Установление соединения по протоколу TLS версии 1.2 характеризуется отсутствием шифрования пакетов рукопожатия, что позволяет обнаружить и идентифицировать данные сети Tor. Анализ уникальности свойств пакетов, передаваемых в ходе рукопожатия TLS, позволил определить самоподписываемый сертификат X.509 пакета server_hello сервера сети Tor как главный предмет исследования в рукопожатии, обладающий признаком, позволяющим однозначно его идентифицировать в ряду других.

Опираясь на имеющийся научный опыт в данном направлении, первоначально были выбраны в качестве средства идентификации установления соединения с сетью Tor анализатор NetworkMiner, сертификат X.509 и совокупность значений характеристик сертификата в пакете server_hello: строка «details» анализатора содержит маску «TLS Certificate:CN=www.{произвольный набор цифр и латинских букв}.net /.com» и номер порта соединения: 443, 9001 или 8443. Третье значение было получено в ходе экспериментов по исследованию анализаторами Wireshark и NetworkMiner дампов сети Tor [5, 6].

Проведенные исследования выявили, что средством обнаружения и идентификации рукопожатия TLS версии 1.2 является анализатор Wireshark, пакет server_hello, содержащий сертификат, и значение строки пакета tls.handshake.certificate_length (размер сертификата рукопожатия TLS), находящееся в диапазоне от 400 до 600 байт.

3. Средства обнаружения протокола TLS v1.3. В 2018 году, в связи с введением в использование сетью Tor протокола TLS версии 1.3, шифрованию подвергся и пакет рукопожатия сервера server_hello. При этом следует отметить, что по-прежнему без шифрования передается пакет client_hello клиента сети в адрес входного узла сети Tor.

Проведенные дальнейшие исследования показали, что для использования в качестве средства обнаружения и идентификации установления соединения по протоколу TLS версии 1.3 вместе с анализатором Wireshark необходимо применять значение строки frame.len (размер пакета client_hello), находящееся в пределах 369-385 байт (для универсальности расширен до диапазона 369-399 байт). Также в состав средства входит параметр tls.handshake.extensions_server_name (параметр указывает, каким должно быть имя сервера при установлении соединения), содержащий значения «com» и «www» [7].

4. Обнаружение в условиях обфускации. Помимо усиления защиты за счет протокола TLS версии 1.3 в программном комплексе Tor предусмотрен ряд так называемых подключаемых транспортов, которые делают невозможным анализ пакетов за счет применения обфускации (маскирования), в том числе с пересборкой передаваемых пакетов [8-9].

С целью идентификации обфусцированного трафика сети Tor был проведен анализ, основанный на перехвате трафика анализатором Wireshark и исследовании сохраненных дампов с помощью сниффера SPID [10].

Исследование процесса анализа трафика сниффером Wireshark выявило возможность захвата пакетов программного комплекса Tor, передаваемых обфускатором через локальный хост 127.0.0.1 в браузер Firefox, включенный в состав комплекса. При перехвате таких пакетов виден только входящий и исходящий на локальный хост (127.0.0.1) трафик, без идентификации IP-адресов. Для такого трафика можно использовать средства обнаружения и идентификации – анализатор Wireshark, пакеты client_hello (TLS версий 1.2 и 1.3) и сертификатов Tor (TLS версии 1.2).

5. Методики обнаружения и идентификации. Алгоритм, разработанный с использованием средств обнаружения и идентификации данных сети Tor протокола TLS версии 1.2, учитывает содержание пакета server_hello с сертификатом и основан на проверке строки пакета tls.handshake.certificate_length (размер сертификата рукопожатия TLS). Для использования значений фильтрации Wireshark необходимо содержание фильтра выразить следующим образом: tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400

Алгоритм, разработанный для обнаружения и идентификации пакетов рукопожатия протокола TLS версии 1.3 основывается на анализе строк пакета client_hello, который единственный из всего потока данных остается незашифрованным. Для использования значения фильтрации Wireshark для версии TLS 1.3 необходимо содержание фильтра выразить следующим образом: tls && frame.len <= 399 && frame.len >=369 && tls.handshake.extensions_server_name contains com && tls.handshake.extensions_server_name contains www

6. Реализация результатов. Для программной реализации средств обнаружения и идентификации было разработано (в соавторстве) программное средство TerminaTOR, основанное на библиотеках и модулях Wireshark. Для проведения экспериментов был создан стенд (Рис. 1).

Рис. 1. Стенд для экспериментов

В соответствии с методиками обнаружения и идентификации обеих версий протокола TLS на АРМ был запущен анализатор сети Wireshark, и применены представленные ранее значения фильтрации (Рис. 2, 3).

tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400

	Time	Source	Destination	Protocol	Length	Info
286	179.932128	37.187.102.186	192.168.43.5	TLSv1.2	1051	Server Hello, Certificate, Se
326	181.025552	51.15.13.245	192.168.43.5	TLSv1.2	1067	Server Hello, Certificate, Se
1293	216.719908	193.23.244.244	192.168.43.5	TLSv1.2	1070	Server Hello, Certificate, Se
1297	216.758928	94.130.186.49	192.168.43.5	TLSv1.2	1063	Server Hello, Certificate, Se
1345	237.929663	195.201.26.209	192.168.43.5	TLSv1.2	1072	Server Hello, Certificate, Se
1349	238.044791	128.31.0.34	192.168.43.5	TLSv1.2	1064	Server Hello, Certificate, Se

Рис. 2. Результаты фильтрации рукопожатия TLS v1.2

Для протокола TLS версии 1.3 применялась соответствующая методика, алгоритм и средства обнаружения и идентификации. Также запущен программный комплекс Tor и в поле настройки фильтров Wireshark было указано значение фильтра для рукопожатия TLS версии 1.3 (Рис. 3).

Для применения методик обнаружения и идентификации рукопожатия по протоколу TLS версий 1.2 и 1.3 в условиях обфускации пакетов между пользователем и сервером в настройках Wireshark был выбран локальный интерфейс 127.0.0.1.

tls && frame.len <= 399 && frame.len >=369 && tls.handshake.extensions_server_name contains com && tls.handshake.extensions_server_name contains www

	Time	Source	Destination	Protocol	Length	Info
503	47.198972	192.168.0.11	51.15.151.31	TLSv1.3	388	Client Hello
504	47.199990	192.168.0.11	95.165.139.85	TLSv1.3	375	Client Hello
505	47.200327	192.168.0.11	37.147.200.2…	TLSv1.3	371	Client Hello
506	47.200455	192.168.0.11	185.220.101.…	TLSv1.3	378	Client Hello
507	47.200966	192.168.0.11	80.43.245.98	TLSv1.3	388	Client Hello
635	48.098055	192.168.0.11	37.147.200.2…	TLSv1.3	390	Client Hello

Рис. 3. Результаты фильтрации рукопожатия TLS v1.3

При этом можно отметить, что подключение было запрошено у 4 серверов из 6 указанных в настройках, а осуществлено лишь по одному адресу (Рис. 4). Предположительно это связано с тем, что два узла не принимают трафик с обфускацией.

(tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400) or (tls && frame.len <= 399 && frame.len >=369 && tls.handshake.extensions_server_name c

	Time	Source	Destination	Protocol	Length	Info
7230	17.196960	127.0.0.1	127.0.0.1	TLSv1.3	372	Client Hello
7234	17.233658	127.0.0.1	127.0.0.1	TLSv1.3	371	Client Hello
7400	18.047609	127.0.0.1	127.0.0.1	TLSv1.2	376	Client Hello
7448	18.428523	127.0.0.1	127.0.0.1	TLSv1.2	1047	Server Hello, Certificate, Server Key Exchange, Server Hello Done
7493	19.534078	127.0.0.1	127.0.0.1	TLSv1.3	373	Client Hello

Рис. 4. Фильтрация обфусцированного трафика на персональной ЭВМ

Применение программы TerminaTOR для обнаружения и идентификации сети Tor осуществляется в соответствии с методикой, путем внесения данных в строки окна настроек (Рис. 4): размеров пакета server_hello, содержащего сертификат, и размеров пакета client_hello. Адреса сети Tor не вносились, а был использован адрес, предоставляемый программному комплексу сетью. При этом на один IP-адрес пользователя выделяется один IP-адрес входного узла (Рис. 5).

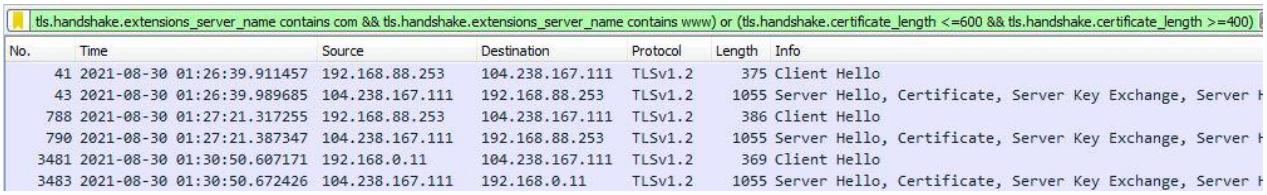


Рис. 5. Три последовательных подключения к адресу по умолчанию

Программное средство TerminaTOR выдало два результата обнаружения одного и того же IP-адреса Tor – с помощью средств обнаружения для обеих версий протокола, которые проанализировали пакеты client_hello и server_hello (Рис. 6).

Для анализа трафика в организации можно использовать коммутатор Mikrotik или другой управляемый гигабитный коммутатор с функцией зеркалирования (Рис. 7), включая его в разрыв между межсетевым экраном и коммутатором для зеркалирования трафика на АРМ специалиста, либо настроить на управляемом коммутаторе (если есть возможность) зеркалирование (Рис. 8).

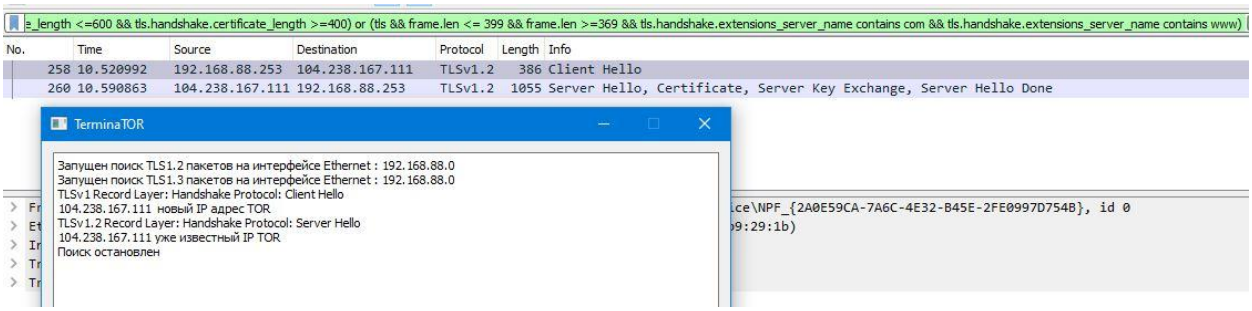


Рис. 6. Окно программы TerminaTOR с результатами фильтрации

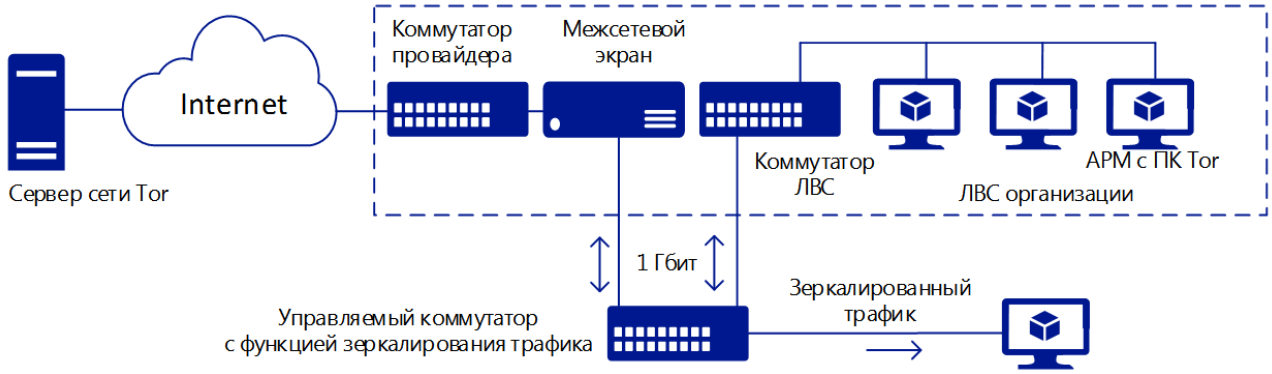


Рис. 7. Схема анализа в организации

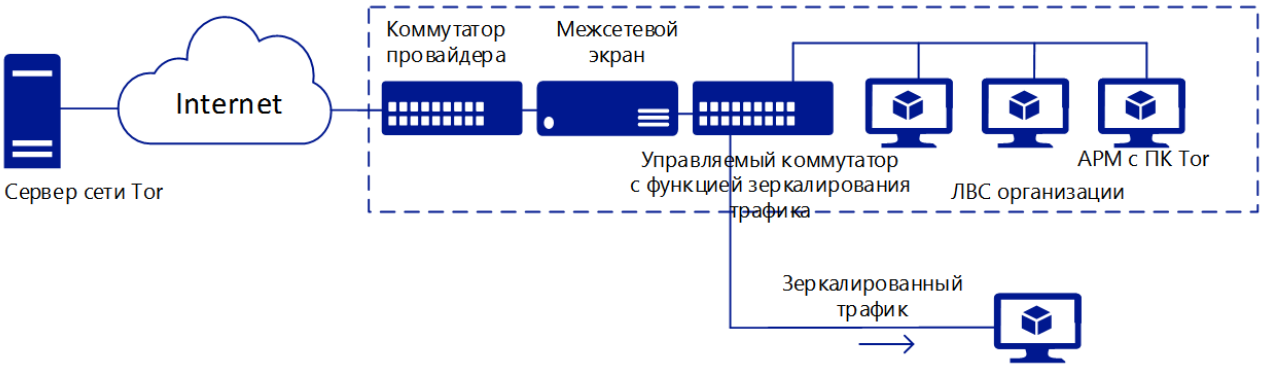


Рис. 8. Схема анализа с использованием коммутатора организации

7. Итоги. Таким образом, уже имеющиеся в научном обороте результаты исследований программного комплекса Tor дополнены новыми характеристиками протокола TLS-шифрования, используемыми для его обнаружения, прикладными методиками идентификации в сетях передачи данных программного комплекса Tor и деанонимизации его трафика с использованием особенностей рукопожатия протокола TLS версий 1.2 и 1.3. Работа выполнена при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта №23/2020.

СПИСОК ЛИТЕРАТУРЫ

1. History. Tor Project (2021). Retrieved from: https://www.torproject.org/ru/about/history.
2. An active de-anonymizing attack against tor web traffic / Yang Ming, Gu Xiaodan, Ling Zhen [и др.]. // Tsinghua Science & Technology. — 2017. — № 22(6). — С. 702-713.
3. Rao, Z., Niu, W., Zhang, X. S., & Li, H. (2017). Tor anonymous traffic identification based on gravitational clustering. Peer-to-Peer Networking and Applications, 11(3), 592–601. doi:10.1007/s12083-017-0566-4
4. Bai, X., Zhang, Y., & Niu, X. (2008). Traffic Identification of Tor and Web-Mix. In Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications (Vol. 1, pp. 548-551). IEEE Computer Society. doi:10.1109/ISDA.2008.209
5. Lapshichyov, V. V. TLS certificate as a sign of establishing a connection with the network Tor / V. V. Lapshichyov, O. B. Makarevich // The 12th International Conference on Security of Information and Networks (SIN 2019): Proceedings of the 12th International Conference on Security of Information and Networks, Sochi Russia, 12–15 сентября 2019 года / Edited by Oleg Makarevich, Ludmila Babenko, Maxim Anikeev, Atilla Elgi, Hossain Shahriar. – Sochi Russia: Published by Association of Computing Machinery, New York, USA, 2019. – P. 92-97. – DOI: 10.1145/3357613.3357628.
6. Lapshichev, V. V. TLS Certificates of the Tor Network and Their Distinctive Features / V. V. Lapshichev // International Journal of Systems and Software Security and Protection. – 2019. – Vol. 10. – No 2. – P. 20-43. – DOI 10.4018/IJSSSP.2019070102.

7. Лапшичев, В. В. Набор признаков установления https-соединения TLS v1.3 программным комплексом Tor / В. В. Лапшичев, О. Б. Макаревич // Известия ЮФУ. Технические науки. – 2020. – № 5(215). – С. 150-158. – DOI: 10.18522/2311-3103-2020-5-150-158.
8. Wenliang, Xu Obfuscated Tor Traffic Identification Based on Sliding Window / Xu Wenliang, Zou Futai. .// Security and Communication Networks . — 2021. — № 3. — С. 1-11 .- DOI: 10.1155/2021/5587837.
9. Di, Liang Obfs4 Traffic Identification Based on Multiple-feature Fusion / Liang Di, He Yongzhong. // In Proceedings of 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS). — Shenyang : IEEE, 2020. — С. 323-327. - DOI: 10.1109/ICPICS50287.2020.9202018.
10. Лапшичев, В. В. Деанонимизация трафика сети тор в условиях обфускации данных / В. В. Лапшичев, О. Б. Макаревич // Современные компьютерные технологии : Сборник статей Научно-методической конференции, Таганрог, 25–29 февраля 2020 года / Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Таганрог: Южный федеральный университет, 2020. – С. 52-57. – DOI: 10.18522/mod.comp.tech.2020.1.8.

Буханов Д.Г.
БГТУ им. В.Г. Шухова, старший преподаватель

ИССЛЕДОВАНИЕ МЕТОДОВ АНАЛИЗА СЕТЕВОГО ТРАФИКА И РАЗРАБОТКА СИСТЕМЫ ВЫЯВЛЕНИЯ АНОМАЛИЙ ТРАФИКА В КОМПЬЮТЕРНЫХ СЕТЯХ С ПРИМЕНЕНИЕМ ИСКУССТВЕННЫЙ НЕЙРОННЫХ СЕТЕЙ АДАПТИВНО-РЕЗОНАНСНОЙ ТЕОРИИ

Аннотация. Проведен анализ подходов к повышению безопасности в компьютерных системах. Выявлено, что наиболее полно решают задачу повышения безопасности в компьютерных системах системы обнаружения вторжений. В качестве метода анализа параметров сетевой активности предложено использовать искусственные нейронные сети адаптивно-резонансной теории с иерархической структурой памяти. На основе особенности структуры памяти сетей адаптивно-резонансной теории в работе была разработана модель обнаружения вторжений. Разработан алгоритм выполнения классификации в параллельном режиме работы. Проведены экспериментальные исследования разработанного способа классификации СКС в последовательном и параллельном режимах работы. В среднем скорость классификации в параллельном режиме была на 60% выше, чем в последовательном.

Ключевые слова: системы обнаружения вторжений, информационная безопасность, адаптивно-резонансная теория.

Введение

Современные условия жизни человека привели к увеличению роста сотрудников, работающих удаленно. Согласно отчету Cisco [1] рост числа сотрудников, работающих с использованием сетей Internet, увеличился в среднем на 50%, что позволило злоумышленникам использовать все более новые технологии для проведения атак. В соответствии с отчетом компании Positive Technologies за 2018 год, количество информационных систем в которых были обнаружены критические уязвимости выросло в два раза [2]. Эти сведения демонстрируют об актуальности проведения исследований в области повышения безопасности.

Наряду с ростом количества нарушений информационной безопасности происходит и развитие технологий повышения безопасности компьютерных систем (КС). Наиболее часто используемыми являются: системы туннелирования трафика, антивирусные системы, межсетевые экраны и другие. Большинство из них позволяют защитить от тех атак, которые были ранее выявлены. Для выявления новых видов атак в КС используются системы обнаружений вторжений (СОВ). В виду развития и роста информационных систем, использующих компьютерные сети наибольший интерес, имеют сетевые СОВ (ССОВ) [3]. Основной задачей ССОВ является выявления факта вторжения в КС. В качестве признаков обычно используются данные, полученные из сетевого трафика. Назовем наличие или отсутствие соответствующей сетевой атаки в некотором промежутке времени состоянием компьютерной сети (СКС). Своевременное определение (СКС) позволяет повысить безопасность КС.

ССОВ представляет собой программный или программно-аппаратный комплекс, расположенный внутри сети, либо на ее внешнем периметре. Основной задачей любой

СОВ является реализация способа определения СКС. СОВ можно разделить на два типа. К первому типу относятся СОВ, которые выявляют известные признаки (сигнатуры) состояний компьютерной сети. Недостатком таких систем является невозможность определить новый вид сетевой атаки. Ко второму типу относятся те, которые выявляют отклонение значений сетевых параметров от нормы (которые могут выявлять аномалии сетевого трафика). Недостатком таких систем является большое количество ложных срабатываний, но в отличие от систем первого типа, они могут выявлять новые виды атак. В качестве методов анализа параметров сетевой активности в таких СОВ хорошо себя зарекомендовали методы интеллектуального анализа данных (МИАД) [4]. К ним можно отнести методы, основанные на кластерном анализе, нечеткой логике, байесовском выводе, многоагентных системах, алгоритмах построения деревьев решений и искусственных нейронных сетях (ИНС).

При выявлении заранее определенных классов состояний сетевого трафика хорошие результаты достигнуты в работах, в которых используется байесовский вывод [5–7].

В работе [4] используется кластерный анализ. Для определения СКС было предложено использовать алгоритм k-means. Наилучшие результаты точности выявления были получены при количестве выходных кластеров равном количеству определяемых состояний компьютерной сети, которое составило 81,61%. Недостатком такого подхода является то, что заранее необходимо знать количество определяемых состояний. Это затрудняет своевременное определение новых видов сетевых атак, а также увеличивает время переобучения системы, так как может потребоваться переобучение всего классификатора.

В работе [8] авторы предлагают использовать нейро-нечеткую систему (Neuro-fuzzy system) для классификации данных, которая по сравнению с другими нейро-нечеткими системами классификации: Radial Basis Function Neural Network и Adaptive Neuro-Fuzzy Inject System, показывает значительно лучшие результаты. Но недостатком таких систем является недостаточная скорость работы для использования в системах реального времени, необходимость переобучения, необходимость добавления новых правил и проверки затем непротиворечивости и полноты базы знаний.

В работах [9–11] используются методы, основанные на многоагентных системах, данные методы хотя и позволяют решать задачу повышения информационной безопасности в частности, но на текущий момент не могут предоставить решение задачи в общем случае.

Одними из наиболее перспективных методов классификации состояния компьютерной сети стали методы и подходы, использующие различные архитектуры искусственных нейронных сетей [12–21]. В работе [18] авторы приводят данные экспериментов при использовании многослойных перцептронов и сетей Кохонена для выявления аномального поведения внутри сети. Их исследования показывают высокие результаты, по некоторым типам атак, не считая dos атаки типа smurf и neptune, выявление которых происходит по 2-3 параметрам, точность которых превышает 80 %. Это выше результатов подобных экспериментов других авторов. В работе [21] для увеличения эффективности классификации состояния компьютерной сети предлагается использовать предобработку входных данных мониторинга. После предобработки данные посылаются в классификатор на основе сети Кохонена. Проводимые ими исследования показывают

высокие результаты. Но недостатками рассмотренных систем является то, что при появлении новых типов сетевых атак требуется переобучить весь классификатор, что может привести к неспособности используемой архитектуры нейронной сети классифицировать новый образ. Это может привести к пересмотру архитектуры ИНС.

В работе предлагается структура ССОВ, использующая в качестве механизма интеллектуального анализа данных ИНС адаптивно резонансной теории, а именно, АРТ-2, которая способна работать с непрерывными входными сигналами. Общие положения об архитектуре АРТ-2 изложены в работах [22, 23]. В работе [24] предложена модификация структуры памяти сети АРТ-2 в поле F2, которая дает возможность организовать древовидную структуру памяти.

Разработка структуры СОВ

Ввиду гетерогенности и распределенности целевой системы для обеспечения безопасности структура ССОВ должна иметь распределенный характер. Предлагается использовать модель распределенной ССОВ, которая предполагает два вида программных агентов.

Один вид агентов обеспечивает сбор данных для анализа, второй выполняет непрерывный анализ полученных данных. Для снижения нагрузки на вычислительные узлы предлагается использовать распределенный анализ, при котором агент анализа получает сведения только от близлежащих программных агентов сбора данных. После, агенты анализа могут выполнять синхронизацию своих структур памяти [25].

Разработка классификатора состояния компьютерной сети

Ядром любой ССОВ является модуль анализа. Основная его цель —определение текущего СКС. Для определения СКС предлагается использовать метод классификации на основе адаптивно-резонансной теории с иерархической структурой памяти (АРТ-2m). В работе [24] предложена структура такой сети. Основными преимуществами применения такой сети являются:

- возможность гарантированного дообучения;
- возможность синхронизации участков памяти разных классификаторов;
- возможность распараллеливания вычислений не только в поле F1, но и в поле F2.

На рис. 1 представлен процесс работы классификатора СКС на основе АРТ-2m при параллельном режиме работы.

Вектор S, представляет собой кортеж из N параметров, описывающих текущее СКС. После его регистрации он передается на вход блока F1_clone. F1_clone выполняет создание вычислителя F1(c), где c — количество вычислительных потоков в поле предобработки F1, который выполняет нормирования сигналов вектора S. Полученные нормализованные значения синхронно записываются в очередь нормализованных значений. Для синхронизации записи и чтения из этой очереди был использован мьютекс (A0).

Для обработки новых значений, поступивших в очередь, используются вычислительные потоки поля F2, алгоритм работы которых предполагает выполнение следующих шагов:

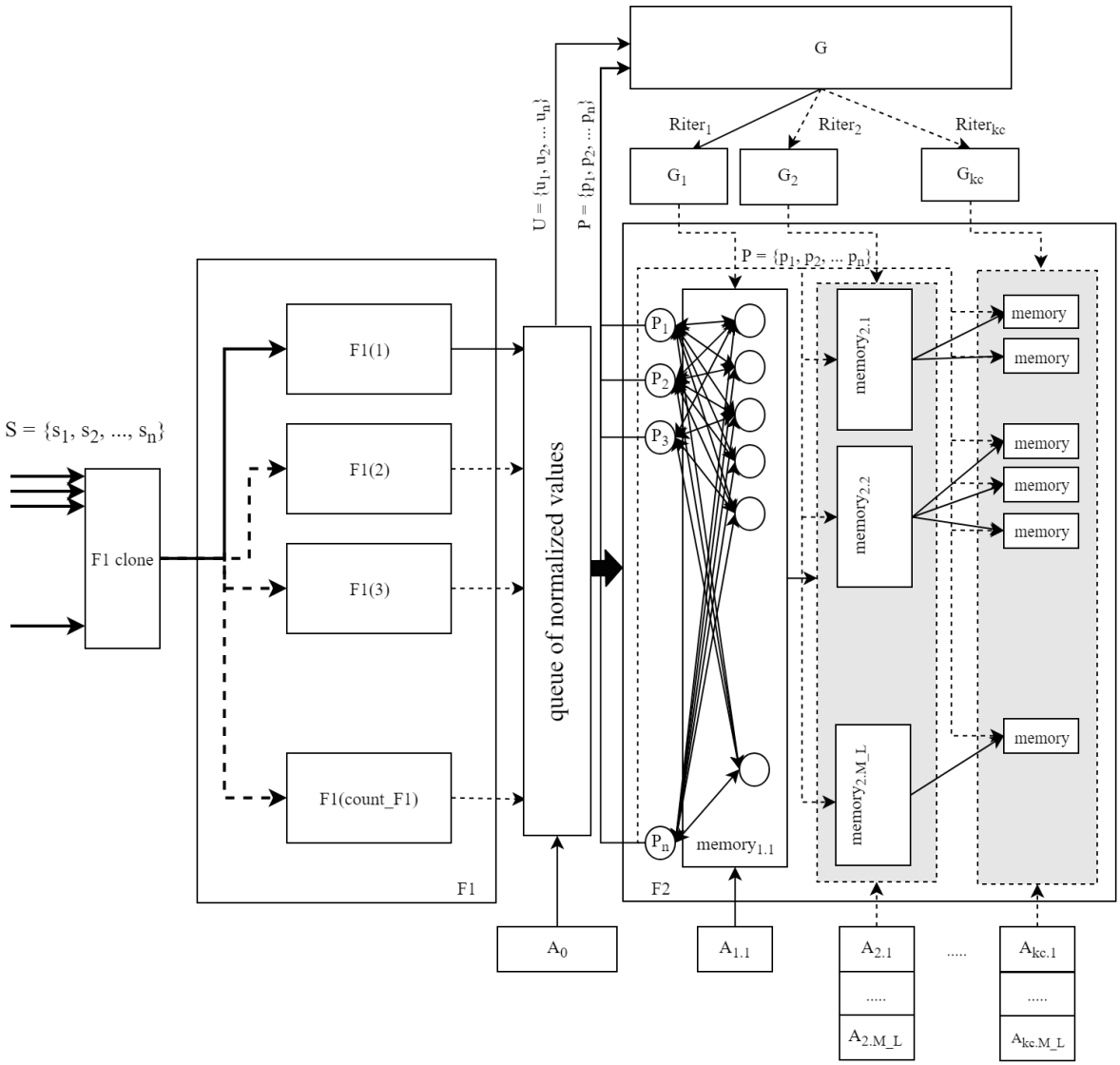


Рис. 1. Процесс работы классификатора в параллельном режиме

Шаг 1.1. Блокировка доступа на основе использования арбитров (мьютексы, A_{jk}) текущего $memory_{jk}$. Нахождение соответствующего выходного нейрона для текущего уровня памяти $memory_{jk}$, где $k=1..M\_L$ (M_L – количество выходных нейронов на j-ом уровне памяти). Соответствующим нейроном памяти называется такой нейрон, сигналы которого резонируют с нормированными данными, считанными с очереди. Если такой нейрон найден и если текущий уровень памяти j не последний, то переход к следующему **шагу 1.2**. Иначе, если текущий уровень памяти j, не последний, но не найден соответствующий нейрон, то происходит создание нового нейрона в текущем $memory_{jk}$ и переход к **шагу 2**, или если уровень памяти последний то происходит создание нового нейрона в текущем $memory_{jk}$ и установка его весов.

Шаг 1.2. Выполнение дообучения весов найденного соответствующего выходного нейрона уровня j, предоставление доступа к $memory_{jk}$, переход к следующему $memory_{j+1}$, переход к **шагу 1.1.**

Шаг 2. Создание нового уровня памяти $j+1$, его блокирование, нахождение текущего значения ($Riter_j$) параметра сходства (в работе была использована следующая

рекуррентная зависимость: $Riter_{j+1}=Riter_j+0.75(1-Riter_j)$), создание нейрона памяти в текущем уровне *j+1* и инициализация его весов, затем переход к **шагу 3**.

Шаг 3. Предоставление доступа к $memory_{j+1}$. Переход к **шагу 1.1**, считая уровень памяти *j+1* текущим.

Модель обнаружения новых видов сетевых атак

Помимо вышеуказанных преимуществ использование такого классификатора позволяет получить дополнительные сведения при обнаружении аномалии в трафике. Рассмотрим модель [26] обнаружения новых видов СКС.

Ранее была предложена новая модель выявления вторжений. Она состоит из выполнения следующих операций: получение и регистрация выделенных признаков сетевой активности в виде векторов, нормирование векторов в блоке «Предобработка» и затем определение СКС.

При определении СКС возникают следующие ситуации. Найден активный нейрон в выходном слое. При обучении нейроны выходного слоя помечаются желаемым СКС. Другая возможная ситуация может быть, когда в выходном слое нет помеченного нейрона состоянием компьютерной сети. В этом случае администратор в ручном режиме обязан указать тип возможного состояния. Для определения текущего СКС администратору предлагается в качестве дополнительной информации поддерево памяти (рисунок 5) активных нейронов разных уровней памяти. Поддерево визуально демонстрирует информацию о похожести определенного текущего СКС к данным ранее записанных в память классификатора. После принятия решения администратором происходит обучение.

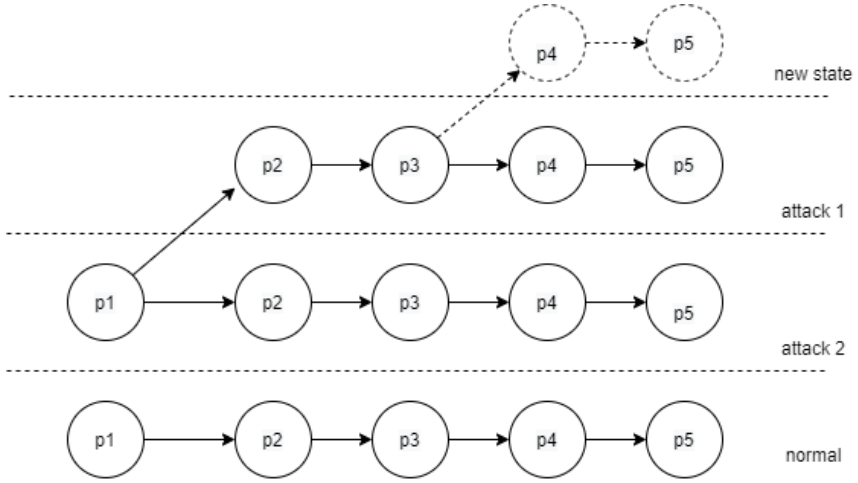


Рис. 2. Структура участка памяти классификатора на основе APT-2m

В случае возникновения аномалии администратору системы предлагаются сведения о близости нового СКС к уже существующим. Как показано на рисунке выше, после регистрации СКС администратор может изменить принадлежность new state к attack 1.

Экспериментальные исследования

В качестве тестовых данных для формирования обучающих и тестовых образцов атак была использована выборка сигнатур NSL KDD-2009 [28], которая основывается на базе данных KDD’99 [29].

Данные представленные в KDD являются эталонными для проверки решений задач определения СКС. На основе проведенных экспериментов были получены следующие результаты (рис. 3) работы классификации СКС при последовательном и параллельном режимах работы.

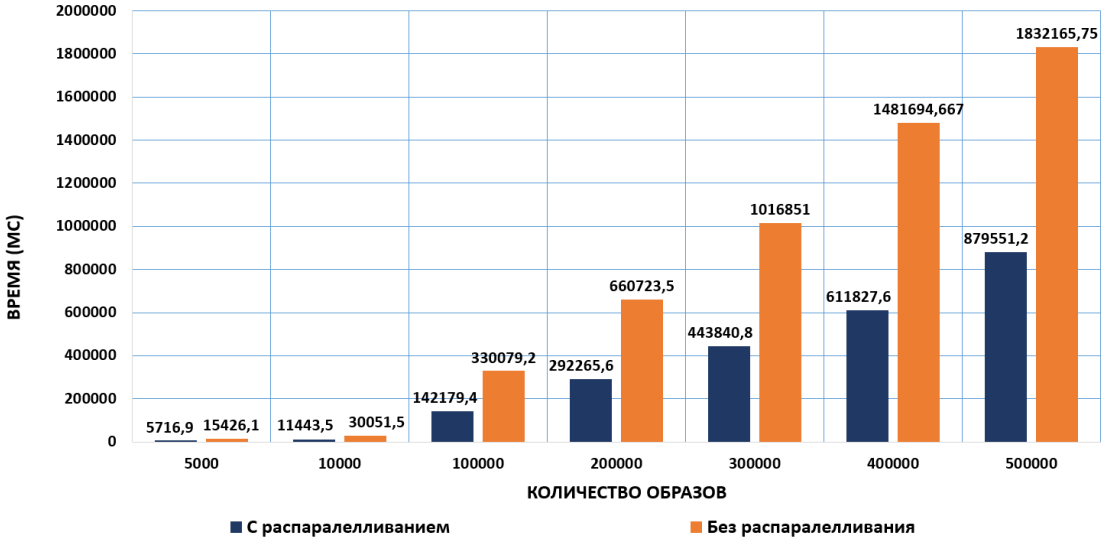


Рис. 3. Временные характеристики при последовательном и параллельном режимах работы

Из результатов эксперимента видно, что прирост скорость происходит после 10000 образов. Это связано с тем, что при распараллеливании вычислений используются дополнительные структуры и дополнительные проверки, связанные с синхронизацией потоков.

На рис. 4 изображены значения точности классификации на основе методики, изложенной в работе [30].

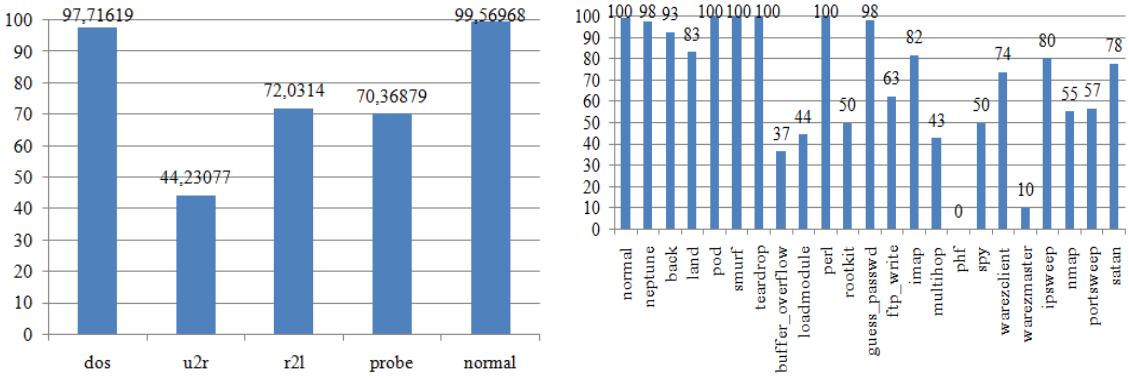


Рис. 4. Результаты оценки качества классификации СКС

На рис. 4. изображена точность определения различных классов (рисунок слева) и типов (рисунок справа) СКС. При бинарной классификации, без уточнения вида состояния значение точности было получено 95,88. Эти результаты являются сопоставимыми с результатами авторов других работ Проведенные эксперименты показывают сопоставимые результаты. Но в отличии от других методов интеллектуального анализа данных использование классификатора на основе ART-2m позволяет гарантированно выполнять дообучение.

Заключение

В работе предложена иерархическая структура памяти для искусственной нейронной сети типа АРТ-2. Данная организация памяти позволяет устранить недостатки классической нейронной сети адаптивно-резонансной теории, а именно, ускорить поиск резонирующего нейрона и предоставить возможность организации вычислений в параллельном режиме. Также это позволяет повысить точность распознавания путем добавления новых уровней памяти с более жестким параметром сходства. Был предложен алгоритм работы сети АРТ-2m в параллельном режиме. Результаты проведенных экспериментов позволяют сделать вывод о возможности использования АРТ-2m в системах обнаружения вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. Cisco Secure. Как защищаться от наиболее важных угроз. – 2021. – С. 41.
2. Positive Technologies. Уязвимости корпоративных информационных систем. – 2018. – С. 21.
3. Петренко С.А. Методы обнаружения вторжений и аномалий функционирования киберсистем / С.А. Петренко // Труды Института системного анализа Российской академии наук. 2009. – Vol. 61. – P. 194–201.
4. Duque S. Using Data Mining Algorithms for Developing a Model for Intrusion Detection System (IDS) / S. Duque, M.N. Bin. Omar // Procedia Comput. Sci. – 2015. – Vol. 61, – № 1. – P. 46–51.
5. Abd-Eldayem M.M. A proposed HTTP service based IDS / M.M. Abd-Eldayem // Egypt. Informatics J. Ministry of Higher Education and Scientific Research. – 2014. – Vol. 15, – № 1. – P. 13–24.
6. Altwaijry H. Bayesian based intrusion detection system / H. Altwaijry // J. King Saud Univ. - Comput. Inf. Sci. – 2012. – Vol. – 24, – № 1. – P. 1–6.
7. Зубков Е.В., Белов В.М. Методы интеллектуального анализа данных и обнаружение вторжений / Е.В. Зубков, В.М. Белов // Вестник СибГУТИ. – 2016. – № 1. – P. 118–133.
8. Ghosh S. A novel Neuro-fuzzy classification technique for data mining / S. Ghosh, S. Biswas, D. Sarkar, P. P. Sarkar // Egypt. Informatics J. – 2014. –Vol. 15. – № 3. – P. 129–147.
9. Бешта А.А. Многоагентная эволюционирующая система как средство контроля над внутренними злоумышленниками / А.А. Бешта // Вестник Волгоградского государственного университета. – 2012. – № 6. – С. 93–97.
10. Косенко М.Ю. Многоагентная система обнаружения и блокирования ботнетов путем выявления управляющего трафика на основе интеллектуального анализа данных / Косенко М.Ю // Челябинск, 2017. – 149 с.
11. Никишова А.В. Интеллектуальная система обнаружения атак на основе многоагентного подхода / А.В. Никишова // Вестник Волгоградского государственного университета. – 2011. – № 5. – С. 35–37.
12. Adil S.H. An improved intrusion detection approach using synthetic minority over-sampling technique and deep belief network / S.H. Adil, S.S. Ali, K. Raza, A.M. Hussaan // Frontiers in Artificial Intelligence and Applications. – 2014. – P. 94–102.
13. Jiang X. Application of Improved SOM Neural Network in Anomaly Detection / X. Jiang,

K. Liu, J. Yan, W. Chen // Phys. Procedia. – 2012. – Vol. 33, – № 1. – P. 1093–1099.
14. Абрамов Е.С. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на web-сервисы / Е.С. Абрамов, Я.В. Тарасов // Инженерный вестник Дона. – 2017. – Т. 46, – № 3. – Р. 1–17.
15. Абрамов Е.С. Нейросетевой метод обнаружения низкоинтенсивных атак типа «Отказ в обслуживании» / Е.С. Абрамов, Я.В. Тарасов, Е.П. Тумоян // Известия ЮФУ. – 2016. – Т. 182. – № 9. – С. 58–71.
16. Большев А.К. Применение нейронных сетей для обнаружения вторжений в компьютерные сети / А.К. Большев, В.В. Яновский // Вестник Санкт-Петербургского университета. – 2010. – Т. 1. – № 1. – С. 129–135.
17. Васильев В.И. Интеллектуальная система обнаружения атак в локальных беспроводных сетях / В.И. Васильев, И.В. Шарабыров // Вестник Уфимского государственного авиационного технического университета. – 2015. –Т. 19–4, – № 70. – С. 95–105.
18. Емельянова Ю.Г. Неросетевая технология обнаружения сетевых атак на информационные ресурсы / Ю.Г. Емельянова, А.А. Талалаев, И.П. Тищенко, В.П. Фраленко // Программные системы теория и приложения. – 2011. – Т. 3. – № 2. – С. 3–15.
19. Марков Р.А. Исследование нейросетевых технологий для выявления инцидентов информационной безопасности /Р.А. Марков, В.В. Бухтояров, А.П. Попов, Н.А. Бухтоярова // Молодой ученый. – 2015. – № 23 (103), – С. 55–60.
20. Тимофеев А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевых атак / А. Тимофеев, А.А. Браницкий // Int. J. Inf. Technol. Knowl. – 2012. – Т. 6, – № 3. – С. 257–265.
21. Idhammad M. Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques / M. Idhammad, K. Afdel, M. Belouch // Procedia Comput. Sci. – 2018. – № 127. P. 35–41.
22. Carpenter G.A. ART 2: Stable self-organization of pattern recognition codes for analog input patterns / G.A. Carpenter, S. Grossberg // Appl. Opt. – 1987. – Vol. 26, – № 23. P. 4919–4930.
23. Carpenter G.A. ART 2-A: An adaptive resonance algorithm for rapid category learning and recognition / G.A. Carpenter, S. Grossberg, D.B. Rosen // Neural Networks. – 1991. – Vol. 4, – № 4. – P. 493–504.
24. Буханов Д.Г. Сеть адаптивно-резонансной теории с многоуровневой памятью / Д.Г. Буханов, В.М. Поляков // Научные ведомости БелГУ. – 2018. – Т. 45, – № 4. – С. 709–717.
25. Bukhanov D.G., Polyakov V.M. Detection of network attacks based on adaptive resonance theory / D.G. Bukhanov, V.M. Polyakov // J. Phys. Int. Conf. Inf. Technol. Bus. Ind. – 2018. – P. 1–9.
26. Буханов Д.Г. Модель выявления вторжений в компьютерные сети на основе искусственных нейронных сетей адаптивно-резонансной теории / Д.Г. Буханов // Информация и безопасность. – 2020. – Т. 4, – № 2. – С. 225–234.
27. Bukhanov D.G., Polyakov V.M. An Approach to Improve the Architecture of ART-2 Artificial Neural Network Based on Multi-Level Memory / D.G. Bukhanov, V.M. Polyakov // Fuzzy Technol. intheindustry. – 2018. – Vol. 2. – P. 235–242.

28. The NSL- KDD Data Set [Электронный ресурс]. Режим доступа: http://www.unb.ca/cic/datasets/nsl.html
29. KDD Cup 1999 Data [Электронный ресурс] – Information and Computer Science University of California, Irvine, 1999. Режим доступа: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
30. Оценки классификаторов [Электронный ресурс] // Режим доступа: https://learnmachinelearning.wikia.org/ru/wiki/Оценки_классификаторов.

Смирнов В.И.
ПГТУ, старший преподаватель,
s_mir_vl@mail.ru

МЕТОДИКА ИСПОЛЬЗОВАНИЯ ФИЗИЧЕСКИХ ЭФФЕКТОВ ПРИ ПРИМЕНЕНИИ СИСТЕМНОГО ПОДХОДА К ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЕ РЕЧЕВОЙ ИНФОРМАЦИИ

Разработана методика, которая реализуется на основе исследования составляющих системного подхода при разработке систем информационной безопасности. Предложенная методика развивает теоретические основы использования физических эффектов (ФЭ) при технической защите речевой информации. Она учитывает иерархии элементов технических средств и ФЭ, реализует анализ/выявление максимально возможного количества уязвимостей в каналах речевой коммуникации и позволяет настроить механизмы защиты за счет ослабления/устранения нежелательных результатов воздействия ФЭ.

Любые технические средства несанкционированного съёма речевой информации в технических каналах утечки вызывают некоторые изменения физических параметров в окружающей среде. Первопричиной этих изменений являются ФЭ, проявляющиеся при утечке конфиденциальной информации. Известны сотни ФЭ [1, 2], которые описывают проводимость, модификацию и преобразование звукового поля, а также изменяют свойства физического объекта при тех или иных основных и дополнительных воздействиях. Различные совместимые и объединённые ФЭ, используемые в технических каналах утечки информации (ТКУИ), определяют их специфику.

Впервые возможность применения систематизированных знаний о ФЭ при исследовании физических основ технических средств обеспечения информационной безопасности была показана в работах А.Н. Соболева и В.М. Кириллова [2, 3]. Вопросы, связанные с изучением ФЭ и законов утечки речевой информации по техническим каналам, рассматриваются в публикациях [4-6]. Однако в сборнике рекомендаций [4] представлено небольшое число ФЭ, связанных с акустоэлектрическими преобразователями, в статье [5] сведения о ФЭ в акустических каналах представлены в качестве справочного материала, а в учебном пособии [6] нет новых решений по использованию знаний о ФЭ в вопросах инженерно-технической защиты речевой информации.

А.Н. Соболевым и В.М. Кирилловым выделены следующие составляющие системного подхода при разработке систем информационной безопасности [2]:

«1. Стадии жизненного цикла источника информации.

2. Связь источника информации с компонентами окружающей среды.

3. Анализ физических основ технических средств создания, передачи, приёма и использования информации.

4. Учет направлений развития технических средств.

5. Взаимосвязь и взаимозависимость технических средств перехвата информации, противодействия перехвату и контроля состояния системы информационной безопасности.

6. Комплексный подход к созданию системы информационной безопасности».

Таким образом, показано, что необходимо развитие теоретических основ использования ФЭ при применении системного подхода для разработки системы информационной безопасности. При совершенствовании защиты речевой информации от утечки по техническим каналам с учётом особенностей проявления ФЭ необходимо учитывать особенности речевой информации как формы защищаемой информации и классы ТКУИ.

Первая и вторая составляющие затрагивают человека (как источник речевой информации) и среду распространения речевого сигнала. Третья и четвёртая составляющие связаны с техническими средствами передачи, обработки, хранения и отображения информации (ТСПИ), вспомогательными техническими средствами и системами (ВТСС) и техническими средствами разведки (ТСР) в акустических каналах. Исследование последних двух составляющих направлено на выявление взаимосвязей компонент ТКУИ с техническими средствами противодействия перехвату и контроля состояния защищённости речевой информации. На Рис. 1 предложена соответствующая схема для ТКУИ.

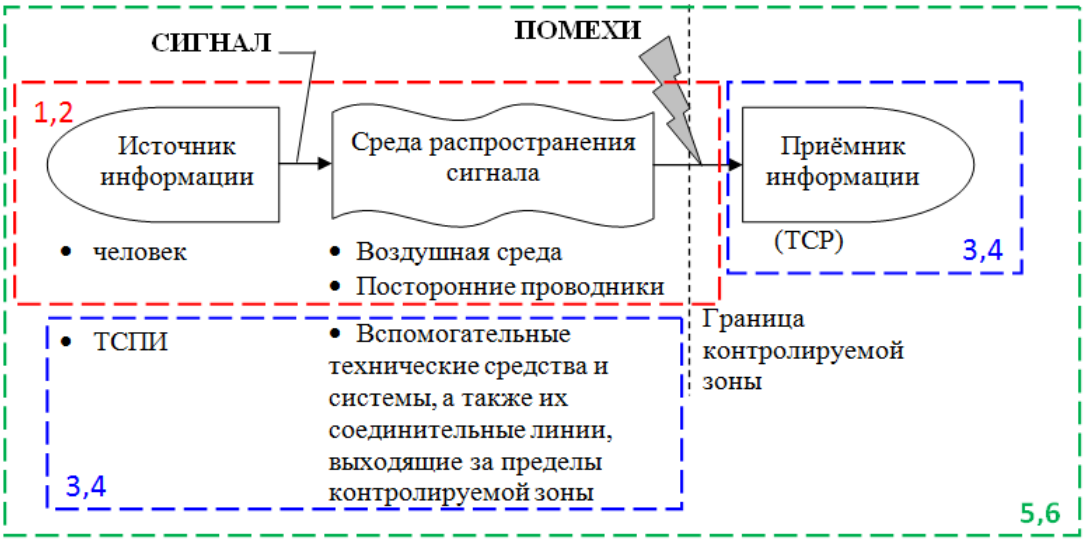


Рис. 1. Схема ТКУИ и составляющие системного подхода (указаны шесть составляющих и связанные с ними компоненты ТКУИ)

Стадии жизненного цикла источника речевой информации. Исследование составляющей предлагается подразделить на следующие этапы:

Этап 1. Описание источника речевой информации как системы.

Этап 2. Анализ стадий жизненного цикла источника речевой информации.

При рассмотрении источника речевой информации (человека) как системы различают три основных уровня [7]: клеточный (элементно-системный), уровень систем органов (компонентно-системный) и целостный организм человека (макросистемный). Человеческий организм является элементом более сложной системы (надсистемы), включающей в себя внешнюю среду и влияющей на структуру и функционирование данного организма. Умственные и психические возможности человека как системы и части надсистемы описываются внутренними (физиологическими) и внешними (психические и социальные) информативными признаками [8], которые представлены в Табл. 1.

Табл. 1. Информативные признаки человека

№	Группа признаков	Описание
1	Физиологические признаки	По сведениям, полученным о состоянии здоровья человека по химическому, хемилюминесцентному, электрическому, магнитному, инфракрасному, радиотепловому и акустическому каналам передачи внутренних информативных признаков, можно выделить: здоровых, практически здоровых и больных хроническими заболеваниями людей (в стадии компенсации, субкомпенсации или декомпенсации).
2	Психические признаки	1. Национально-психологические признаки отражают общие информативные признаки, характерные для представителей одного этноса. 2. Индивидуально-личностные признаки: а) По признакам, основанным на взаимосвязи телосложения и характера человека: эндоморфы, мезоморфы и эктоморфы. б) По темпераменту характера: сангвиники, флегматики, холерики и меланхолики. в) По акцентуациям характера: с демонстративным, с застревающим, с возбудимым, с боязливым, с экзальтированным и с эпилептоидным типом характера. г) К персональным признакам относятся общие, физические, функциональные, интеллектуальные и персонографические. Общие признаки: жизненные привычки, взгляды и их устойчивость, отношение к происходящим событиям, отношение к различным аспектам жизни, национализм, отношение к себе, увлечения и др. Физические признаки: рост, телосложение, вес, глаза, волосы, зубы, рот, кожа и особые приметы. Функциональные признаки: походка, жестикуляция, мимика, улыбка, голос, речь и динамика изменения кожи. Интеллектуальные признаки: уровень мышления и его критичность, сообразительность, практичность, проницательность, интеллект, эрудиция, способность к анализу событий и др. Персонографические признаки: ФИО, дата и место рождения, реальная национальность, состояние здоровья, место работы и служебные обязанности, перспективы карьеры, награды и др. 3. Групповые признаки характеризуют признаки социальных групп, в которые входит человек. 4. По восприятию информации можно выделить три группы людей: визуалисты, кинестики и аудиалисты. 5. Признаки морально-психологического состояния проявляются на физиологическом, поведенческом и коммуникативном уровнях, а также в моторной, эмоциональной и когнитивной сферах. 6. Признаки зависимости характеризуют аддикцию к еде, курению,

		азартным играм, Интернету, покупкам и др.
3	Социальные признаки	Характеризуют прирождённый (статус, полученный при рождении), приобретённый (статус, достигнутый благодаря умственным и физическим усилиям человека) и предписанный статусы людей (статус, приобретаемый вне зависимости от желания самого человека).

Важнейшей чертой системного подхода является рассмотрение системы (человека) в режиме функционирования. Специалист по защите информации должен иметь в виду, что источник речевой информации представляет собой систему с жизненным циклом. Поскольку источником речевой информации является человек, часть стадий происходит в головном мозге.

На первых трёх стадиях жизненного цикла (создания, переработки и хранения речевой информации) человек формирует основное содержание речевого сообщения. Информация (идея, план и др.) возникает в мозге человека в абстрактной форме (кодирование), может перерабатываться (переосмысление) и храниться в кратковременной/долговременной памяти.

В процессе речеобразования (извлечение из памяти) информация трансформируется в акустическое речевое колебание. Личное общение между людьми считается наилучшим средством связи, поскольку речевые колебания одновременно передают несколько видов информации: смысловую (текст сообщения), информацию о говорящем лице (признаки, позволяющие узнать его по голосу) и информацию об эмоциональных факторах (интонационные признаки). Интонационные признаки определяют повествовательный, директивный или вопросительный характер сообщения и позволяют говорить о настроении собеседника.

Поскольку получателем речевой информации является человек, стадии переработки (переосмысление), хранения (хранение в кратковременной и долговременной памяти), использования (извлечение из памяти) и утилизации (забывание) также происходят в головном мозге. На стадии использования она может быть представлена в другой форме защищаемой информации (документированная, телекоммуникационная и др.).

Для прогнозирования образования ТКУИ (выявления основных угроз и вероятных злоумышленников) необходимо формировать более полный анализ стадий жизненного цикла источника речевой информации. Следует отметить, что выделенное количество стадий жизненного цикла и их наименование влияет на матрицу взаимосвязи с компонентами окружающей среды.

Выявлено, что стадии передачи и приёма речевой информации наиболее интересны злоумышленнику (недобросовестные конкуренты, преступные сообщества и др.), поскольку перехват конфиденциальной информации осуществляется в момент её

озвучивания. На этих стадиях содержание речевой информации становится известно широкому кругу лиц и увеличивается количество технических систем (ТС), с которыми может осуществляться взаимодействие источника информации. Всё это усложняет инженерно-техническую защиту речевой информации.

Связь источника речевой информации с компонентами окружающей среды. При использовании системного подхода А.Н. Соболев и В.М. Кириллов выделяют следующие компоненты окружающей среды [2]: человек, техническая среда, физическая среда, биологическая среда, а также организации, предприятия и фирмы. Для исследования составляющей предлагаются два этапа:

Этап 1. Построение матрицы взаимосвязи источника акустической (речевой) информации с компонентами окружающей среды. Строками и столбцами матрицы являются стадии жизненного цикла и компоненты окружающей среды соответственно.

Этап 2. Описание всех выявленных взаимосвязей. На пересечении строк и столбцов отмечаются характерные взаимосвязи и ключевые ФЭ (Табл. 2).

Табл. 2. Матрица взаимосвязи с компонентами окружающей среды

	предприятие, фирма или организация	человек	техн. среда	физ. среда	биол. среда
замысел создания	взаимосвязь$_{1}$	взаимосвязь$_{2}$	взаимосвязь$_{3}$	взаимосвязь$_{4}$	взаимосвязь$_{5}$
переработка	взаимосвязь$_{6}$	взаимосвязь$_{7}$	взаимосвязь$_{8}$	взаимосвязь$_{9}$	взаимосвязь$_{10}$
хранение	взаимосвязь$_{11}$	взаимосвязь$_{12}$	взаимосвязь$_{13}$	взаимосвязь$_{14}$	взаимосвязь$_{15}$
передача	взаимосвязь$_{16}$	взаимосвязь$_{17}$	взаимосвязь$_{18}$	взаимосвязь$_{19}$	взаимосвязь$_{20}$
приём	взаимосвязь$_{21}$	взаимосвязь$_{22}$	взаимосвязь$_{23}$	взаимосвязь$_{24}$	взаимосвязь$_{25}$
переработка	взаимосвязь$_{26}$	взаимосвязь$_{27}$	взаимосвязь$_{28}$	взаимосвязь$_{29}$	взаимосвязь$_{30}$
хранение	взаимосвязь$_{31}$	взаимосвязь$_{32}$	взаимосвязь$_{33}$	взаимосвязь$_{34}$	взаимосвязь$_{35}$
извлечение из памяти	взаимосвязь$_{36}$	взаимосвязь$_{37}$	взаимосвязь$_{38}$	взаимосвязь$_{39}$	взаимосвязь$_{40}$
хранение	взаимосвязь$_{41}$	взаимосвязь$_{42}$	взаимосвязь$_{43}$	взаимосвязь$_{44}$	взаимосвязь$_{45}$
забывание	взаимосвязь$_{46}$	взаимосвязь$_{47}$	взаимосвязь$_{48}$	взаимосвязь$_{49}$	взаимосвязь$_{50}$

Рассмотрим для примера (кратко) взаимосвязь источника речевой информации с технической средой на стадии передачи (взаимосвязь$_{18}$). Передача речевой информации может осуществляться в защищаемом (выделенном) помещении, в транспорте и на открытой местности. При передаче речевой информации основными критериями качества каналов речевой коммуникации являются разборчивость, громкость и натуральность речи. Воздействие технической среды на источник речевой информации многообразно. Для

каждой задачи будет свой перечень ТС, которые злоумышленник может использовать для формирования акустического канала утечки. Источник речевой информации, в свою очередь, может влиять на функционирование ТС, модулировать их электромагнитное излучение, предъявлять требования к защищенности и т.д.

При заполнении матрицы взаимосвязи источника речевой информации с компонентами окружающей среды возникают следующие ситуации:

1. Специалист по защите информации не может выделить взаимосвязь. В этом случае ячейка таблицы может оставаться пустой или заполняться каким-либо символом (например, можно использовать символ длинного тире).

2. Специалист по защите информации находит взаимосвязь и она совпадает с одной из предыдущих. В этом случае ячейка таблицы заполняется аналогично предыдущей (совпавшей).

3. Специалист по защите информации находит взаимосвязь и она не совпадает с другими. В этом случае ячейка заполняется уникальными данными.

Поскольку матрица взаимосвязи на практике получается громоздкой, для удобства ячейки могут нумероваться или заполняться различными символами, а пояснения к взаимосвязям даются после таблицы. Количество заполненных ячеек и полнота представленной информации зависят от знаний специалиста по защите информации. Предложенная матрица взаимосвязи позволяет определить с какими компонентами источник акустической (речевой) информации чаще всего взаимодействует и какие ТС необходимо проанализировать на предмет возможности формирования потенциального ТКУИ.

Анализ физических основ технических средств приёма, обработки, хранения и передачи речевой информации. Предлагаются следующие этапы анализа ТС, относящихся к ТСПИ и ВТСС:

Этап 1. Предварительный анализ ТС осуществляется табличным методом, предложенным в работе [4]: в шапке таблицы размещаются наводящие вопросы и специалист пытается подробно и объективно ответить на них (Табл. 3). По результатам предварительного анализа выбираются для дальнейшего анализа конкретные ТС, которые необходимо защитить от возможной утечки речевой информации.

Табл. 3. Пример предварительного анализа ТС

№	Название ТС?	Преобразователь?	Среда распространения преобразования?	Наиболее опасное состояние (режим работы ТС)?
1.	Извещатель пожарный дымовой (ИП 212-45)	Оптико-электронный (фотодиод) преобразователь, шлейф пожарной сигнализации	Шлейф пожарной сигнализации (связь с пультом)	Рабочий режим
2.	Светильник	Дроссель, стартер	Электрическая сеть, зоны индукции от дросселя	Рабочий режим, подключение к электрической сети

№	Название ТС?	Преобразователь?	Среда распространения преобразования?	Наиболее опасное состояние (режим работы ТС)?
3.	Телефонный аппарат	Вызывное устройство, микрофонный капсюль, телефонный капсюль	Телефонная сеть, зоны индукции от катушек и проводников	Ожидание вызова
4.	Система конференц-связи	Громкоговоритель, микрофон, усилитель	Линия связи	Рабочий режим, самовозбуждение усилителей
5.	Холодильник	Электродвигатель компрессора, трансформатор, пускозащитное реле, реле температуры	Электрическая сеть, зоны индукции от трансформатора и реле	Рабочий режим, подключение к электрической сети
…	…	…	…	…

Этап 2. Определяются входные/выходные параметры и рассматривается модель «чёрного ящика» (Рис. 2) для каждого выбранного ТСПИ/ВТСС.

Рис. 2. Модель чёрного ящика ТСПИ/ВТСС

Этап 3. Описание каждой ТСПИ/ВТСС как системы. На данном шаге приводятся характеристики и изображения каждой ТСПИ/ВТСС с указанием структурных элементов.

Этап 4. Определяется функциональное назначение и взаимосвязь структурных элементов. Затем заполняется Табл. 4. При заполнении таблицы можно использовать специализированные базы данных по ФЭ.

Табл. 4. Разбиение ТСПИ/ВТСС на элементы

№	Элементы	Основное воздействие ($A_{осн}$)	Дополнительное воздействие ($A_{доп}$)	Результат воздействия (C_i)	Название ФЭ
1	Элемент_1	A_1	$A_{доп1}$	C_1	$ФЭ_1$
2	Элемент_2	A_2	$A_{доп2}$	C_2	$ФЭ_2$
…	…	…	…	…	…
N	Элемент_N	A_N	$A_{допN}$	C_N	$ФЭ_N$

Этап 5. Для каждого структурного элемента соответствующие ФЭ представляем в виде модели чёрного ящика (Рис. 3) с указанием результатов воздействия.

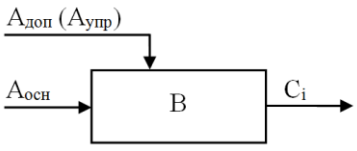


Рис. 3. Модель чёрного ящика ФЭ

Этап 6. Используя полученные на четвёртом и пятом этапах данные о структурных элементах ТСПИ/ВТСС, разрабатываем физические схемы (ФСх) трёх типов (ФСх ТСПИ/ВТСС, ФСх ТСПИ/ВТСС с побочными результатами воздействий и ФСх ТСПИ/ВТСС при воздействии звукового поля).

Этап 7. По ФСх ТСПИ/ВТСС с побочными результатами воздействий определяем те результаты воздействий, которые влияют на возможность формирования ТКУИ.

Анализ ТСР осуществляется по методике, предложенной в работе [9]. Методика позволяет выявлять управляющие воздействия для ФЭ, что влияет на обнаружение демаскирующих признаков ТСР. Также с её помощью производится поиск альтернативных вариантов физической основы перспективных ТСР.

Таким образом, предлагаемая последовательность этапов анализа физических основ технических средств приёма, обработки, хранения и передачи речевой информации позволяет принять решение о необходимости тех или иных мер по защите конкретных ТС для противодействия утечке речевой информации по техническим каналам.

Учёт направления развития технических средств акустической разведки, ТСПИ и ВТСС в ТКУИ. Предлагаемые этапы исследования возможных направлений развития технических средств акустической разведки и технических каналов утечки речевой информации:

Этап 1. Определение исходных данных. В качестве исходных данных для разработки/модификации ТС (ТКУИ или ТСР) даются длина цепочки синтеза совместимых ФЭ, входное и выходное воздействия.

Этап 2. Решение задач информационного поиска по ФЭ. Чтобы разработать ФСх новой ТС, необходимо последовательно решать определенного класса задачи информационного поиска (обычно слева направо). При создании или исследовании ТС для решения таких задач рекомендуется использовать специальные таблицы поиска или экспертную систему (рекомендующую возможные совместимые ФЭ). Примеры специальных таблиц поиска представлены в приложениях (Табл. П 1 и Табл. П 2) работы [2].

Этап 3. Оцениваются разработанные варианты ФСх по совместимости полученных ФЭ. Опираясь на работы [1, 2], была разработана онтология ФЭ в программе Protégé [10], которая учитывает вид воздействия, вид результата воздействия, возможности применения, возможности проявления на одном физическом объекте в разных агрегатных состояниях и др. Разработанная онтология может быть полезна для информационного поиска проявляющегося ФЭ при создании или исследовании ТС.

Этап 4. Анализ возможности преобразования оставшихся ФСх в техническое решение. Для таких целей предлагается использовать метод синтеза технических решений на основе ФСх, представленный в работе [1]. В таком случае полезна база данных по ФЭ и свойствам веществ и материалов.

Новые потенциально возможные решения (ТСР и ТКУИ) по их ФСх можно охарактеризовать такими признаками, как наличие новых ФЭ, новый состав известных ФЭ, уменьшение/увеличение количества ФЭ, изменение последовательности ФЭ и наличие дополнительных цепочек ФЭ. Таким образом, предлагаемая последовательность этапов исследования направлена на поиск новых ТС, которые могут использовать злоумышленники для несанкционированного получения речевой информации.

Взаимосвязь и взаимозависимость технических средств перехвата речевой информации, противодействия перехвату и контроля состояния системы информационной безопасности. На Рис. 4 предложена схема представления взаимосвязи и взаимозависимости ТС при решении задач противодействия ТКУИ. ТС могут работать по различным физическим полям.

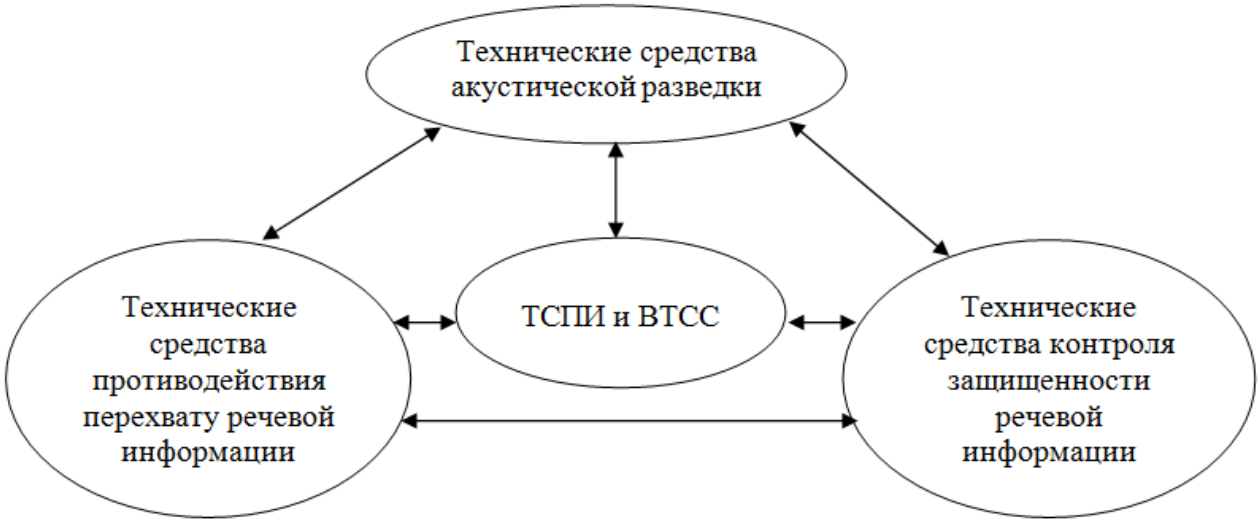


Рис. 4. Взаимосвязь ТСР, противодействия перехвату и контроля защищенности речевой информации

Предлагаемые этапы исследования взаимосвязи и взаимозависимости ТСР, противодействия перехвату и контроля состояния системы информационной безопасности:

Этап 1. Построение матрицы взаимодействий (Табл. 5).

По диагонали матрицы отражены взаимодействия между ТС одной категории, а в остальных ячейках – взаимодействия между ТС разных категорий, направленные в обе стороны. Матрица позволяет найти взаимосвязи, которые специалист по защите информации не учёл при исследовании предыдущих составляющих системного подхода при разработке системы информационной безопасности.

Табл. 5. Матрица взаимодействий ТС в акустических каналах утечки

	ТСПИ	ВТСС	ТСР	ТС противодействия перехвату акустической информации	ТС контроля состояния защищённости акустической информации
ТСПИ	взаимо-связи$_1$	взаимо-связи$_2$	взаимо-связи$_3$	взаимосвязи$_4$	взаимосвязи$_5$
ВТСС	взаимо-связи$_6$	взаимо-связи$_7$	взаимо-связи$_8$	взаимосвязи$_9$	взаимосвязи$_{10}$
ТСР	взаимо-связи$_{11}$	взаимо-связи$_{12}$	взаимо-связи$_{13}$	взаимосвязи$_{14}$	взаимосвязи$_{15}$
ТС противодействия	взаимо-связи$_{16}$	взаимо-связи$_{17}$	взаимо-связи$_{18}$	взаимосвязи$_{19}$	взаимосвязи$_{20}$

перехвату акустической информации					
ТС контроля состояния защищённости акустической информации	взаимо-связи$_{21}$	взаимо-связи$_{22}$	взаимо-связи$_{23}$	взаимосвязи$_{24}$	

Этап 2. Анализ с использованием ФЭ средств противодействия перехвату речевой информации и контроля состояния системы информационной безопасности (аналогично методике анализа ТСР [9]).

Этап 3. Построение ФСх ТКУИ при воздействии звукового поля. Анализ полученной ФСх и предложение механизмов защиты.

Важным является вопрос систематизации знаний по физическому анализу технических средств перехвата информации, противодействия перехвату и контроля состояния системы информационной безопасности (создание специализированных баз данных). При рассмотрении ТС противодействия перехвату и контроля состояния системы информационной безопасности используется «Государственный реестр сертифицированных средств защиты информации». Классификация ТКУИ [11] является неотъемлемой частью методологии изучения вопроса, поскольку позволяет систематизировать все известные методы и средства защиты информации от утечки по техническим каналам на основе исследования проявления ФЭ.

Комплексный подход при создании системы защиты речевой информации. Комплексное применение методов и средств защиты речевой информации предполагает согласованное применение различных мер при разработке целостной системы информационной безопасности, перекрывающей все существенные уязвимости в каналах речевой коммуникации и не содержащей слабых мест на стыках отдельных её компонентов.

Для раскрытия всех исследованных составляющих системного подхода при разработке систем информационной безопасности предлагается разработка и реализация программного комплекса, включающего:

– специализированную базу данных по ФЭ;

– подсистему выделения структурированной информации по ФЭ и обновления баз данных из текстов открытых источников (при участии эксперта);

– экспертную систему по решению задач информационного поиска по ФЭ;

– базу данных по систематизации знаний по результатам физического анализа технических средств перехвата информации, противодействия перехвату и контроля состояния системы информационной безопасности.

Для однозначного описания и понимания предлагаемой методики, опишем её как модель, используя методологию IDEF0, поскольку «нотация IDEF0 принята в России в качестве стандартного средства моделирования» [12]. Модель IDEF0 позволит понять, какая защищаемая информация, какие ТС и связи служат входом для проведения процедуры анализа безопасности компонент технического канала утечки речевой информации с позиций системного подхода, какие результаты получаются, что является

управляющими факторами и что для этого необходимо (ресурсы). На рисунках показаны контекстная диаграмма A0 первого уровня (Рис. 5) и декомпозиция этой диаграммы (Рис. 6).

Рис. 5. Контекстная диаграмма A0 «Провести процедуру анализа безопасности компонент технического канала утечки речевой информации с позиций системного подхода»

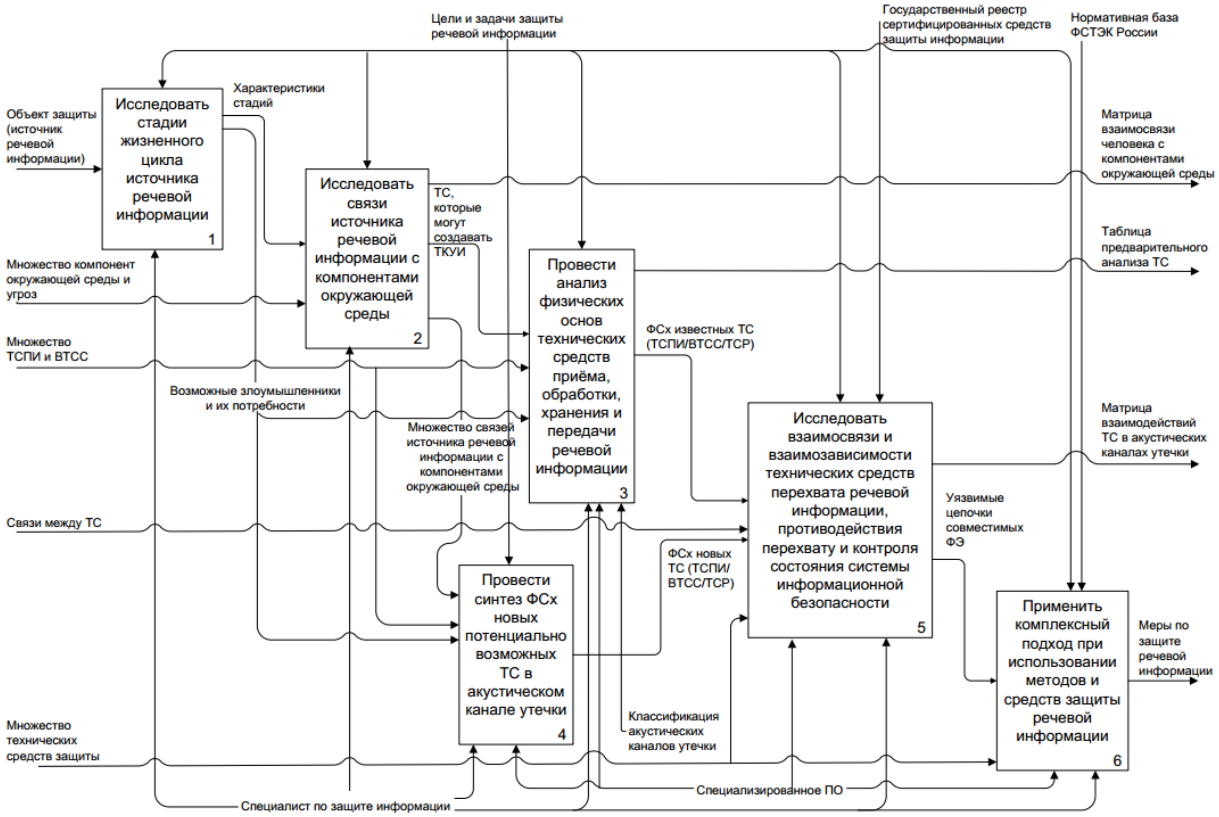


Рис. 6. Декомпозиция диаграммы A0

Выводы. Предлагаемая методика позволяет проводить аналитические действия с ТС и совместимыми ФЭ для выявления соответствия или несоответствия требованиям защищенности речевой информации ФСх ТКУИ. В работе показана последовательность основных этапов исследования составляющих системного подхода для совершенствования защиты речевой информации и представлена модель IDEF0 для однозначного описания и понимания предлагаемой методики.

Стадии жизненного цикла источника речевой информации и связи с компонентами окружающей среды определяют потребности вероятных злоумышленников и ТС, которые используются для формирования потенциальных акустических каналов утечки. Для остальных составляющих системного подхода при разработке систем информационной безопасности важную роль играют аналитический и синтетический методы исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Соболев, А. Н. Физические эффекты : научное издание / А. Н. Соболев. — Йошкар-Ола : МарГТУ, 2001. — 168 с.
2. Соболев, А. Н. Физические основы технических средств обеспечения информационной безопасности : учеб. пособие / А. Н. Соболев, В. М. Кириллов. — Йошкар-Ола : МарГТУ, 2004. — 232 с.
3. Соболев, А. Н. Физические основы перспективной вычислительной техники и обеспечение информационной безопасности : учеб. пособие / А.Н. Соболев, В.М. Кириллов, А.В. Киселев. — М. : Гелиос АРВ, 2012. — 256 с.
4. Аминов, В. П. Блокировка акустоэлектрических преобразователей в электронных технических средствах и системах общего применения : сборник рекомендаций «Z-9» / В. П. Аминов, И. В. Коровин, В. И. Рыбальченко. — М. : Гелиос АРВ, 2010. — 224 с.
5. Петраков, А. В. Физические эффекты и законы утечки аудио-видеоинформации техническими каналами / А. В. Петраков, Ю. С. Федяев, Н. П. Шепурев // Спецтехника и связь. — 2013. — № 5 — С. 23-28; — № 6 — С. 20-27.
6. Сагдеев, К. М. Физические основы защиты информации : учеб. пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. — 2-е изд., испр. и доп. — Санкт-Петербург : Интермедия, 2017. — 408 с.
7. Туревский, И. М. Формирование психомоторных способностей : учеб. пособие для среднего профессионального образования / И. М. Туревский. — М. : Издательство Юрайт, 2019. — 353 с. — (Серия: Авторский учебник).
8. Новиков, В. К. Средства, технологии, системы и технические каналы утечки информации для осуществления киберслежки за человеком и его деятельностью / В. К. Новиков, М. Г. Краснов, И. С. Рекунков. — М. : Горячая линия – Телеком, 2021. — 160 с.
9. Смирнов, В. И. Методика анализа технических средств разведки с использованием физических эффектов / В. И. Смирнов, И. Г. Сидоркина // Вестник Чувашского университета. — 2017. — № 3. — С. 273-281.
10. Васильева, Е. С. Разработка онтологии по физическим эффектам в программе Protege / Е. С. Васильева, А. И. Сосорева; науч. рук. В. И. Смирнов // Инженерные кадры – будущее инновационной экономики России: материалы VI Всероссийской студенческой конференции. — Йошкар-Ола : ПГТУ, 2020. — Ч. 4: "Информационные

технологии – основа стратегического прорыва в современной промышленности". — С. 27-31.
11. Сидоркина, И. Г. Уточнение классификации технических каналов утечки информации по физической природе носителя с учётом физических эффектов / И. Г. Сидоркина, В. И. Смирнов // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. — 2020. — №1 (45). — С. 37-46.
12. Прокушев, Я. Е. Моделирование процессов проектирования систем защиты информации в государственных информационных системах / Я. Е. Прокушев, С. В. Пономаренко, С. А. Пономаренко // Computational nanotechnology. — 2021. — Т. 8. — № 1. — С. 26–37.

Полещук Е. М.
МГУ им. адм. Г.И.Невельского, аспирант,
poleshuk@msun.ru
Щербинина И. А.
МГУ им. адм. Г.И.Невельского, декан, к.п.н., доцент,
shcherbinina@msun.ru

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ BLOCKCHAIN ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДОКУМЕНТАЛЬНОМ СОПРОВОЖДЕНИИ ЛОГИСТИЧЕСКИХ ПРОЦЕССОВ МОРСКИХ ГРУЗОПЕРЕВОЗОК

Цифровизация морского транспорта сопряжена с рядом очевидных особенностей перевозок на судах, которые затрудняют или вообще не позволяют осуществлять обмен данными с потребителями сервисов и ситуационными центрами. Соответственно необходимо разработать технологию нивелирующую данные недостатки.

Особенности инфраструктуры, условий работы таможни и других контролирующих органов, инспекционных комплексов, систем видеонаблюдения, автоматизации процедур, информационных систем также необходимо учитывать при переводе системы документирования процессов логистики на технологию блокчейн.

В связи с чем, актуальным и востребованным является создание модели безопасной децентрализованной системы документального сопровождения при организации морских перевозок на основе распределённого реестра. Для достижения поставленной цели необходимо реализовать следующие задачи:

изучение основных направлений законодательного регулирования документооборота на морском транспорте;

изучение особенностей обеспечения информационной безопасности при организации документооборота на морском транспорте;

классификация участников морских грузоперевозок и определение их роли в системе документирования морской логистики;

разработка модели угроз информационной безопасности для различных участников морских перевозок;

определение направлений внедрения технологии Blockchain, как инструмента информационной безопасности;

разработка протокола взаимодействия участников морских перевозок в рамках разрабатываемой распределенной информационной системы.

Анализ основных направлений законодательного регулирования документооборота на морском транспорте позволяет сформировать перечень основных документов при организации контейнерных перевозок, который включает:

Сертификат груза;

Договор морских перевозок;

Грузовой план;

Погрузочный ордер;

Штурманская расписка;

Манифест груза;

Коносамент;

Претензия о несоответствии груза;

Акт порчи груза;

Морской протест;

Приёмо-сдаточный ордер;

другие документы.

В России предприятия транспортной отрасли попадают под действие Федерального закона №187-ФЗ от 19.07.2017 «О безопасности критической информационной инфраструктуры». При проведении работ по защите логистических процессов возникает необходимость в модернизации существующей инфраструктуры для поддержания высокого уровня информационной безопасности.

Таким образом, в индустрии морских контейнерных перевозок задействовано большое количество организаций и посредников, что отражается на документообороте, в общем смысле. Сведения в документах могут представлять ценность для злоумышленников и подлежат защите.

Информационная инфраструктура морских портов представляет собой совокупность наземных информационно-измерительных и вычислительных средств с требуемым математическим обеспечением, предназначенных для организации услуг морских перевозок. Ключевой интерес представляют объекты инфраструктуры морских портов, так или иначе связанные с информационными технологиями [2].

Весь массив потенциальных источников угроз безопасности информации морских портов можно разделить на внутренние источники, к которым относятся структурные элементы системы, в том числе аппаратное и программное обеспечение, а также персонал, и внешние источники [3].

Цели злоумышленников можно определить следующим образом:

нарушение конфиденциальности;

нарушение целостности;

нарушение доступности;

нарушение работоспособности всей системы, подсистем или отдельных компонентов объектов информационной инфраструктуры морского порта.

Способы реализации наиболее вероятных угроз безопасности информационной инфраструктуры морских портов:

анализ сетевого трафика при его передаче между объектами информационной инфраструктуры морских портов;

изменение, искажение и модификация данных, обрабатываемых объектами информационной инфраструктуры морских портов;

перехват сеанса взаимодействия компонентов объекта информационной инфраструктуры морского порта;

реализация парольных атак;

атаки на прикладном уровне;

DOS-атаки;

атаки «IP-спуфинг». [4]

Реализация угроз информационной безопасности возможна в случае образования канала между источником угрозы и носителем данных. В отношении наличия легального

доступа к объектам критической информационной инфраструктуры морских портов все нарушители делятся на две группы: внешние и внутренние нарушители.

Внешние нарушители – это лица, не имеющие законного доступа к информационным ресурсам морских портов.

Внутренних нарушителей морского порта можно классифицировать по уровню возможностей, предоставляемых им системой контроля и управления доступом.

На основании проведенного анализа составлен перечень актуальных угроз информационной безопасности объектов критической инфраструктуры типового морского порта:

угроза незаконного получения паролей и других реквизитов разграничения доступа систем морского порта с дальнейшим их использованием;

угроза разглашения, передачи или утраты атрибутов разграничения доступа систем морского порта;

угроза перехвата конфиденциальной информации по сети систем морского порта;

угроза несанкционированного использования терминалов пользователей морского порта, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи;

угроза реализации скрытого канала передачи данных морского порта;

угроза внедрения программных «закладок» и «вирусов» в информационную инфраструктуру морского порта;

угроза внедрения агентов в число персонала информационных систем морского порта;

угроза вывода из строя подсистем обеспечения функционирования сети морского порта;

кража, модификация, уничтожение информации морского порта;

несанкционированное отключение средств защиты систем морского порта;

угроза неправомерного ознакомления с защищаемой информацией морского порта;

угроза несанкционированного создания учётной записи пользователя систем морского порта;

угроза повышения привилегий систем морского порта.

Анализ уязвимостей и угроз информационной безопасности морских портов позволяет провести оценку факторов активности потенциального злоумышленника при организации морских перевозок.

Качественная разработка модели защиты системы документирования морских перевозок включает разработку протокола взаимодействия участников информационной системы. При этом необходимо учитывать особенности документооборота морской логистики. В частности, в процессе морских перевозок существуют такие документы, без которых груз не сможет даже выйти из порта. К ним относятся коносамент и чартер [5].

В коносамент должны быть включены множество пунктов о транспортировке груза, в том числе и безопасность [6].

Все эти требования направлены на обеспечение не только безопасности экипажа, но и безопасности доставки сохранного груза получателю. Поэтому коносамент, как вид документа, является наилучшим первоначальным объектом в разработке модели системы защищенного документооборота морских перевозок.

Согласно Международным правилам толкования торговых терминов «Инкотермс» (публикация Международной торговой палаты 1990 г., N 460), коносамент исполняет три основные функции: является доказательством передачи товара на борт судна, доказательством заключения договора перевозки, а также средством для передачи во время транзита прав на товар третьим лицам [7].

Поскольку коносамент является товарораспорядительным документом, смарт-контракт морского коносамента должен обеспечивать обязательную идентифицируемость участников системы. Это реализуется посредством ассиметричной криптографии. В сети формируются узлы пользователей, на которых создаются профили участников в соответствии с матрицей разрешений. На этом этапе для пользователя также формируется открытый и закрытый ключи (протокол RSA), которые служат для взаимной аутентификации и обеспечения юридической значимости документов. Множество транзакций состоит из отправок пользователями i ($1 \leq i \leq n$), где n – количество авторизованных пользователей. В качестве хэша множества транзакций используется дерево Меркла.

Защищённая система документооборота морской логистики должна обеспечивать приватность данных и защиту от несанкционированного доступа. Отправка секретных параметров в системе происходит в зашифрованном виде на основе доказательства с нулевым разглашением, для реализации которого используется протокол Фиата-Шамира. Стойкость данного протокола основывается на сложности извлечения квадратного корня по модулю достаточно большого составного числа n, факторизация которого неизвестна.

Отправка документа, участвующего в процессе цепочки поставки, от пользователя A к пользователю B осуществляется через доверенную сторону T. Сначала пользователь подписывает документ своим закрытым ключом и шифрует сообщение на открытый ключ T. В данную транзакцию также включается секретный параметр пользователя A, сгенерированный для конкретной цепочки поставки. Сторона T должна иметь возможность расшифровать сообщение для подтверждения идентификации пользователя A. После этого доверенная сторона T может переслать подписанный документ получателю.

Требование к множественности оригинальных экземпляров коносамента обеспечивается за счёт того, что, согласно принципу технологии блокчейн, у каждого пользователя хранится копия реестра. Все действия в сети записываются в блокчейн в соответствии с политикой одобрения и соответствующего типа транзакции. В случае инцидента информационной безопасности, виновная сторона может быть идентифицирована, а инцидент обработан в соответствии с условиями модели управления.

В цепочке взаимодействия важную роль играет проверяющий узел PD (personal direction). Этот узел формируется на этапе инициализации сети и содержит список авторизованных пользователей и матрицу разрешений доступа к документам морской логистики. Поэтому именно узел PD осуществляет проверку секретных параметров пользователей. Результат проверки отправляется обратно доверенной стороне T. Если проверка завершается успешно, в сети формируется блок B, являющийся заключительным в рамках конкретной цепочки поставки. В противном случае, функция, реализующая данный шаг, вернёт ошибку и блок не будет сформирован до получения результата успешной проверки.

Для орагнизации испытаний разработанного смарт-коносамента используется модульное тестирование, состоящее из юнит-тестов. Для каждой вызываемой функции чейнкода написан отдельный тест. Данные функции тестирования имеют вид «go test», в них указывается, какая именно функция вызывается, поскольку на каждом узле вызывается определённый набор команд [8].

Рассматриваемый чейнкод смарт-коносамента реализует специально разработанный протокол консенсуса, и написан на языке программирования Golang на базе распределённой платформы Hyperledger Fabric.

В таблице 1 приведены функции, реализованные в чейнкоде морского коносамента, а также их определения. Для каждой функции чейнкода приведена функция тестирования и результат её выполнения.

Таблица 1. Тестирование функций чейнкода морского коносамента

Функция чейнкода	Результат функции
CreateGenesisBlock	Формирование нулевого блока
TestCreateGenesisBlock(t *testing.T)	OK Command-line arguments 0.248 s
SendDeliveryParametrs	Отправка параметров цепочки поставки
TestSendDeliveryParametrs(t *testing.T)	OK 2.193 s
GenerateKeyPair	Генерация ключевой пары
TestGenerateKeyPair(t *testing.T)	OK 1.991 s
SendPublicKey	Отправка открытого ключа
TestSendPublicKey(t *testing.T)	OK 0.089 s
SignTransactionsAndGenerateBlockQ	Подписание транзакций и генерации блока
TestSignTransactionsAndGenerateBlockQ(t *testing.T)	OK 0.097 s
GenerateUserID	Генерация параметра пользователя сети
TestGenerateUserID(t *testing.T)	OK 0.083 s
SendGenerAndPublicKey	Отправка сгенерированного параметра и публичного ключа в зашифрованном виде
TestSendGenerAndPublicKey(t *testing.T)	OK 0.120 s
SendUsersID	Отправка списка идентификаторов пользователей в зашифрованном виде

TestSendUsersID(t *testing.T)	OK 0.087 s
GenerateListOfSignedDocuments	Формирование списков подписанных документов
TestGenerateListOfSignedDocuments(t *testing.T)	OK 1.177 s
SendPrivateKey	Отправка закрытого ключа
TestSendPrivateKey(t *testing.T)	OK 0.175 s
VerifySignedDocuments	Проверка подписанных документов
TestVerifySignedDocuments(t *testing.T)	OK 21.839 s
ResendSignedDocumentAndGeneratedParametr	Пересылка пользователям зашифрованных подписанных документов и сгенерированных параметров
TestResendSignedDocumentAndGeneratedParametr(t *testing.T)	OK 0.096 s
SendGeneratedParametrs	Отправка сгенерированных параметров пользователей
TestSendGeneratedParametrs(t *testing.T)	OK 0.519 s
SendDocumentAndGeneratedParametr	Отправка подписанного документа и сгенерированных параметров пользователей в зашифрованном виде
TestSendDocumentAndGeneratedParametr(t *testing.T)	OK 0.139 s
ZKP_Proof	Запрос верификации секретного значения s.
TestZKP_Proof(t *testing.T)	OK 0.101 s
ZKP_Verify	Верификация значения секретного s в доказательстве с нулевым разглашением
TestZKP_Verify(t *testing.T)	OK 0.127 s

В результате был написан и протестирован смарт-контракт, реализующий договор морского коносамента Smart-konosament. Тесты для проверки работы каждой функции объединены в конфигурационный файл Smart-konosament_Test, взаимодействующий со смарт-коносаментом напрямую с использованием инструментов языка программирования Golang, что в целом положительно сказалось на скорости тестирования чейнкода.

Положительный результат тестирования позволяет сделать вывод об исполняемости смарт-коносамента. Данный смарт-контракт может быть использован для организации процессов документирования морских перевозок в электронном виде на базе

технологии распределенного реестра. Также данный контракт может быть взят за основу для дальнейшей разработки других форм документов морской логистики.

СПИСОК ЛИТЕРАТУРЫ

1. https://customsforum.ru/news/opinion/blokcheyn-platforma-zagvozdka-v-tom-gotov-li-biznes-delitsya-konfidentsialnymi-dannymi-553048.html
2. Приказ N 475от 7.12.2017 «Об утверждении Перечня объектов инфраструктуры морского порта» // [Электронный ресурс], Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71760828/ (Дата обращения: 14.12.2020).
3. Банк данных угроз безопасности информации// [Электронный ресурс], Режим доступа: http://bdu.fstec.ru/ (Дата обращения: 14.12.2020).
4. Sokolov, S.S., Glebov, N.B., Antonova, E.N., Nyrkov, A.P. The Safety Assessment of Critical Infrastructure Control System// Proceedings of the 2018 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2018.
5. Алексеев С. С. Гражданское право: учебник//Москва: Проспект, 2015.
6. "Кодекс торгового мореплавания Российской Федерации" от 30.04.1999 N 81-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017)//"Российская газета", N 85-86, 01-05.05.1999.
7. Международные правила толкования торговых терминов "Инкотермс 2000" http://www.consultant.ru/document/cons_doc_LAW_57195/
8. Testing Smart Contracts — Режим доступа: https://yos.io/2020/07/09/testing-smart-contracts/ (дата обращения: 20.08.2021)

ТиПОИБ-2021

МОСКВА 2021