МТУСИ

ФУМО ВО ИБ

ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник научных трудов
по материалам всероссийской
научно-практической конференции

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ 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 сфере высшего образования по УГСНП 10.00.00 «Информационная безопасность»
(ФУМО ВО ИБ)

III Всероссийская научно-практическая конференция

ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8 ноября 2023 г.

СБОРНИК ТРУДОВ

Москва
2023

УДК: 004.056(082)

Теория и практика обеспечения информационной безопасности: сборник трудов III Всероссийской научно-практической конференции, Москва, 08 ноября 2023 года. – 2023. – 254 с.

ПРОГРАММНЫЙ КОМИТЕТ:

Леохин Юрий Львович, доктор технических наук, профессор, проректор по научной работе Московского технического университета связи и информатики (председатель);

Белов Евгений Борисович, заместитель председателя Федерального учебно-методического объединения в сфере высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (заместитель председателя);

Лось Владимир Павлович, доктор военных наук, профессор, президент МОО «Ассоциация защиты информации»;

Иевлев Олег Павлович, кандидат технических наук, декан факультета «Кибернетика и информационная безопасность» МТУСИ;

Шелухин Олег Иванович, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность» МТУСИ;

Кубанков Александр Николаевич, доктор военных наук, профессор, заведующий кафедрой «Безопасность телекоммуникаций» МТУСИ;

Крылов Григорий Олегович, профессор кафедры «Безопасность телекоммуникаций» МТУСИ, профессор Финансового университета при Правительстве Российской Федерации, доктор физико-математических наук, профессор;

Новиков Сергей Николаевич, доктор технических наук, доцент, заведующий кафедрой «Безопасность и управление в телекоммуникациях» Сибирского государственного университета телекоммуникаций и информатики;

Киреева Наталья Валерьевна, кандидат технических наук, доцент, декан факультета «Телекоммуникации и радиотехника» Поволжского государственного университета телекоммуникаций и информатики;

Красов Андрей Владимирович, кандидат технических наук, доцент, заведующий кафедрой «Защищенные системы связи» Санкт-Петербургского государственного университета телекоммуникаций имени профессора М.А. Бонч-Бруевича;

Безумнов Данил Николаевич, начальник отдела по реализации образовательных проектов МТУСИ (секретарь).

ISBN 978–5–6050465–7–8

СОДЕРЖАНИЕ

Секция 1

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И АНАЛИЗ СЕТЕВОГО ТРАФИКА

Секция 2

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Секция 3

ПРОБЛЕМЫ ЦИФРОВОГО СУВЕРЕНИТЕТА И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Секция 4

КИБЕРБЕЗОПАСНОСТЬ

Секция 1

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И АНАЛИЗ СЕТЕВОГО ТРАФИКА

Руководитель: **Панков Константин Николаевич,**
Московский технический университет связи и информатики, заведующий кафедрой «Теория вероятностей и прикладная математика», кандидат физико-математических наук, доцент

Секретарь: **Раковский Дмитрий Игоревич,**
Московский технический университет связи и информатики, ассистент кафедры «Информационная безопасность»

Цыгулев И.Н.,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
Светашев В.А.,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
Дебеева Е.Е.,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова

РАЗРАБОТКА WEB-ПРИЛОЖЕНИЯ ДЛЯ ПРОВЕДЕНИЯ СТАТИСТИЧЕСКИХ ТЕСТОВ ГЕНЕРАЦИЙ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Развитие информационных и телекоммуникационных технологий требует выявление новых задач кибербезопасности. Разработчикам криптографических приложений, необходимых для шифрования информации, нужен удобный инструментарий для исследования случайных чисел. Для того, чтобы анализировать степень случайности символов и повысить уровень безопасности, требуется обработка обширных объемов информации. По мере увеличения использования данных и вычислений, возникает необходимость в разработке новых приложений, способных эффективно выполнять сложные расчетные задачи. Одним из таких инструментов является NIST Statistical Test Suite, который предоставляет набор статистических тестов для оценки и качества работы генераторов случайных чисел. Модифицированная версия NIST Statistical Test Suite может быть скомпилирована для нескольких видов приложений. Однако, для проведения эффективных расчетов с использованием этого инструмента требуется значительная вычислительная мощность.

На сегодняшний день в РФ нет конкретно установленного стандарта для научных исследований, который регламентирует принципы и процедуру

тестирования и анализа случайных последовательностей. В связи с этим, было принято решение, установить в качестве основы хорошо описанные и в настоящее время действующие статистические тесты, созданные «Национальным институтом стандартов и технологии» (NIST) США. Данные тесты разработаны для оценки статистических свойств случайных чисел, используемых в различных криптографических и статистических приложениях. Эти тесты предоставляют возможность определить степень случайности последовательности чисел и её соответствие статистическим ожиданиям.

NIST SP 800-22 – общепринятый набор тестов, разработанный «Национальным институтом стандартов и технологии», состоит из 15 тестов для оценки случайности и качества генераторов случайных чисел [1]. Их можно разделить на четыре группы: первая включает в себя тесты с 1 по 4 это частотные тесты, вторая - тесты 5 и 6 это тесты повторяющихся паттернов, третья - тесты с 7 по 12 это тесты соответствия паттернам, и четвертая - тесты с 13 по 15 это тесты случайных блужданий [2].

NIST Statistical Test Suite представляет собой значимый инструмент для обеспечения безопасности и надежности информационных систем, использующих случайные числа. Применение данного метода выявляется в различных областях, таких как статистика, криптография и информационная безопасность.

Одной из фундаментальных проблем, с которой сталкиваются при проведении расчетов с использованием NIST Statistical Test Suite, заключается в масштабе данных. Тесты часто требуют анализа больших последовательностей случайных чисел, и в некоторых случаях данные могут быть слишком объемными, чтобы загрузить их целиком на обычный компьютер. Это порождает потребность в реализации масштабируемых вычислений.

В приведенной работе рассматривается разработка нового WEB-приложения, которое применимо для выполнения расчетов с использованием NIST Statistical Test Suite на мощных серверах. В процессе написания алгоритма приложения была выявлена проблема в необходимости анализа больших

объемов данных, которые невозможно полностью загрузить в базу. Альтернативой стало решение о загрузке данных частями с последующим комбинированием их в единый финальный отчет.

В данном исследовании для решения проблемы масштабирования вычислений было разработано WEB-приложение, способное работать на мощных серверах. Пользователи могут поэтапно загрузить свои данные, и каждый отдельный фрагмент анализируется независимо друг от друга. Такой способ позволяет использовать вычислительные мощности сервера максимально эффективно.

Разделение задачи позволяет проверять большие последовательности с большой скоростью. Высокопроизводительные серверы способны за минимальное количество времени рассчитывать статистическую значимость ряда в 100 тысяч или даже 1 миллион символов, совместно с многопоточностью данная реализация позволяет уменьшить время обработки и свести вычисления к простым и не большим числам, что создает меньшую нагрузку на вычислительные блоки машины.

В связи с использованием декомпозиции, встает вопрос о том, как объединить полученные результаты, а именно значение p-value (статистическая значимость). Для получения точных результатов, было принято решение использовать подход с оценкой равномерности распределения данных с использованием статистики хи-квадрат. Этот метод основывается на сравнении фактического распределения данных с ожидаемым равномерным распределением путем вычисления статистики хи-квадрат.

Оценивая эффективность выбранной методики, отдельно для каждого теста, мы можем использовать следующие формулы и процедуры:

1. Подготовка набора данных, а именно сбор в массив p-value посчитанных в выбранном тесте;

2. Оценка равномерности распределения данных, сопровождается вычислением ожидаемых частот для каждого интервала. Ожидаемая частота (E) для интервала i вычисляется как:

$$E_{[i]} = \frac{(\text{количество образцов в выборке})}{(\text{количество интервалов})}$$

3. Вычисление статистики хи-квадрат

$$\chi^2 = \sum \frac{(O_{[i]} - E_{[i]})^2}{E_{[i]}}$$

где:

O[i] - наблюдаемая частота (количество образцов в интервале i),

E[i] - ожидаемая частота (как определено в шаге 2),

Σ - сумма по всем интервалам.

4. Количество степеней свободы (df) в тесте хи-квадрат равно (количество интервалов - 1).

5. Полученная статистика хи-квадрат (χ^2) сравнивается с критическим значением из таблицы хи-квадрат для заданного уровня значимости и числа степеней свободы [3]. Если χ^2 больше критического значения, то это может указывать на то, что данные не соответствуют равномерному распределению.

6. В последним этапе выполняется статистический тест для определения, является ли отклонение χ^2 от ожидаемого случайным или статистически значимым. Этот этап включает в себя вычисление p-value и сравнение его с уровнем значимости alpha.

Основные шаги работы WEB-приложения включают:

1. Загрузку данных по частям: пользователи осуществляют загрузку данных в раздельной форме. Это особенно значимо в случаях, когда объем данных существенно превышает возможности целостной загрузки.

2. Анализ частей данных: каждая часть полученной информации анализируется с использованием NIST Statistical Test Suite. Это обеспечивает возможность распределить вычислительную нагрузку на сервер.

3. Комбинирование результатов: по завершении анализа каждого фрагмента данных, производится интеграция результатов в единый финальный отчет. Такой принцип позволяет пользователю получить полную картину оценки статистических свойств данных.

4. Отображение выводов: результаты анализа предоставляются перед пользователем в удобном формате, который способствует более наглядной интерпретации.

Применение WEB-приложения для масштабирования вычислений с использованием NIST Statistical Test Suite имеет несколько преимуществ:

- Эффективное использование серверных ресурсов предоставляет возможность обрабатывать большие объемы данных более эффективно, чем обычные компьютеры.

- Анализ информации по частям позволяет более равномерно распределить нагрузку на сервер, что способствует оптимальному использованию ресурсов.

- Пользователям предоставлена возможность осуществлять загрузку данных без предварительной необходимости их фрагментации, что упрощает процесс и делает его более удобным.

Для осуществления проекта был выбран язык программирования JavaScript, а для реализации серверной и клиентской части фреймворки Node JS и React JS соответственно. Данный язык программирования обладает всеми необходимыми инструментами и характеристиками для эффективной реализации WEB-приложений. Основные преимущества, которые делают его предпочтительным выбором, включают в себя:

1. Одноязычность JavaScript — использование одного языка программирования, JavaScript, как на серверной, так и на клиентской стороне, упрощает разработку и сопровождение приложения, в связи с тем, что технологии плотно переплетены, а написание кода ничем не отличается;

2. Node JS предоставляет высокую производительность на сервере благодаря асинхронной обработке запросов. Это позволяет быстро отвечать на запросы и обслуживать множество одновременных пользователей;

3. React JS — библиотека для построения пользовательского интерфейса: React.js — это библиотека для разработки пользовательского интерфейса, которая обеспечивает декларативный и компонентный подход к

созданию интерфейсов [4]. Это упрощает разработку, повторное использование компонентов и обеспечивает более эффективное управление состоянием. Данный фреймворк обладает огромной поддержкой сообщества, что дает возможность применять уже готовые мощные решения для построения графиков, таблиц и диаграмм;

4. Node JS и React JS позволяют разделить задачи между серверной и клиентской сторонами. Node JS обрабатывает логику сервера, обработку запросов и взаимодействие с базами данных, а React JS — создание пользовательского интерфейса и взаимодействие с пользователем. Это упрощает разработку и поддержку приложений;

5. Node.js обладает многопоточной архитектурой и событийной моделью, что делает его отличным выбором для обработки множества одновременных запросов, включая долгоживущие соединения, такие как веб-сокеты [4]. Данное преимущество позволяет в реальном времени загружать на сервер бинарные последовательности напрямую в обход компиляции в файл или другие хранилища данных;

6. REST API — технология позволяет не только связать клиентскую и серверную часть с помощью простых команд и WEB-запросов, но и использовать вычислительные мощности сервера напрямую из каких-либо дополнительных скриптов на любом языке программирования, способном выполнять отправку и прием WEB-запросов;

7. Для реализации сложных вычислений крупные компании предоставляют свои модули и библиотеки, доступные через пакетный менеджер NPM как для Node.js, так и для React.js, что упрощает разработку и позволяет быстро интегрировать сторонние решения, а также добиться высокой точности в расчетах.

Результатом проведенного анализа стала реализация методики и алгоритмов защиты, что отражено в схеме работы WEB-приложения (рисунок 1). Пользователь подключается к клиентской части с помощью WEB-браузера, взаимодействуя с UI-интерфейсом посредством POST запросов, передается

бинарная последовательность либо в файле, либо напрямую. Серверная часть производит расчет и возвращает результат на экран браузера для последующего анализа. Благодаря REST API помимо клиентского браузера с тестами могут работать сторонние программы, получившие доступ к серверу.

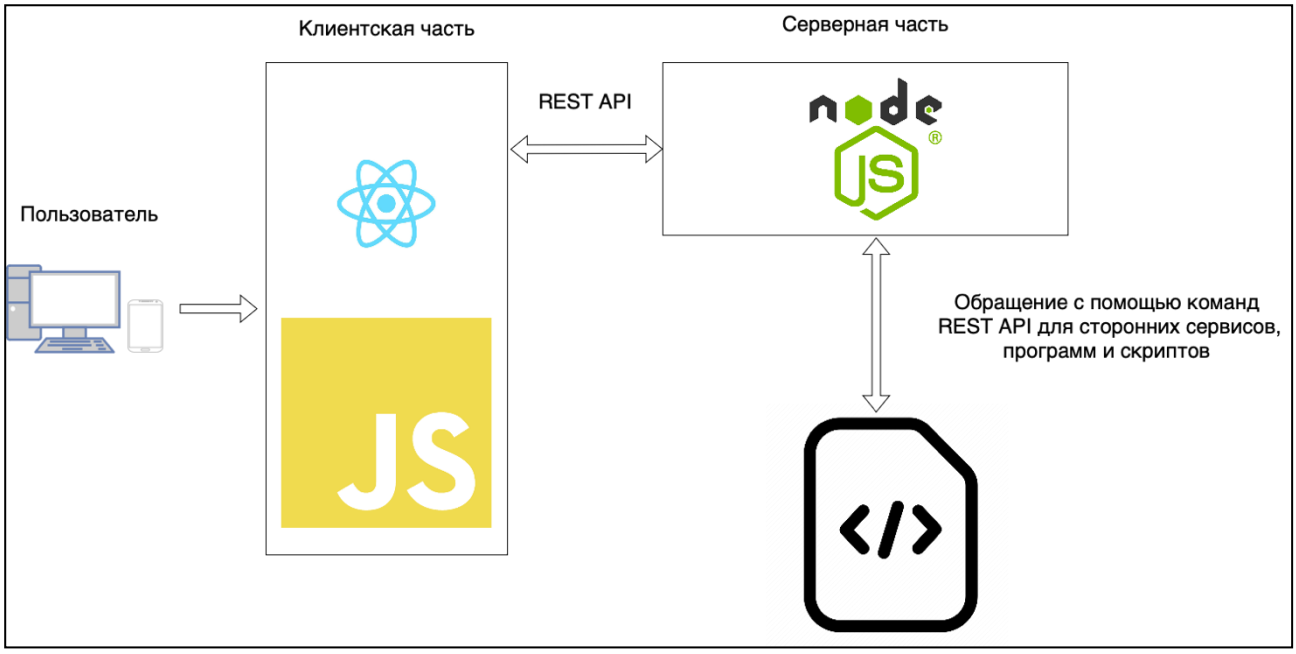

Рисунок 1 – Схема работы разработанного WEB-приложения

Предложенный авторский алгоритм и реализация методики тестирования позволяет использовать приложение, имеющее криптографическую направленность, в защите данных путем обработки больших масштабов информации. В дальнейшем, авторы намерены продолжить исследования по практическому применению приложения и более детальному изучению генерации случайных чисел.

СПИСОК ИСТОЧНИКОВ

1. Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray , San Vo A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Текст] / Andrew Rukhin, Juan Soto,

James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray , San Vo — 1a. — Gaithersburg: National Institute of Standards and Technology, 2010 — 131 c.

2. Rourab Paul, Hemanta DEy, Ranjan Ghosh, Amlan Chakrabarti NIST Statistical Test Suite / Rourab Paul, Hemanta DEy, Ranjan Ghosh, Amlan Chakrabarti [Электронный ресурс] // arxiv.org : [сайт]. — URL: https://arxiv.org/pdf/1609.01389v1.pdf (дата обращения: 17.10.2023).

3. Greenwood, P.E.; Nikulin, M.S. (1996). A guide to chi-squared testing. New York: Wiley. ISBN 0-471-55779-X.

4. Alex Banks, Eve Porcello Learning React: Functional Web Development with React and Redux [Текст] / Alex Banks, Eve Porcello — First Edition. — Boston: O'Reilly Media, Inc., 2016 — 151 c.

5. Ethan Brown Pro Express.js Master Express.js: The Node.js Framework For Your Web Development [Текст] / Ethan Brown — First Edition. — New York: Apress, 2014 — 343 c.

6. Шатило Е. Г., Элямского Н. В. Анализ методов статистической оценки качества псевдослучайных последовательностей. Информационные технологии, 2015, т. 21, № 4, с. 285-291.

7. Чернов Д. В., Протасевич В. И., Калинин В. И. Анализ статистических свойств последовательностей псевдослучайных чисел, полученных различными методами. Вестник Казанского технического университета, 2016, т. 19, № 13, с. 86-91.

8. Фомин В. Н., Попов А. П. Оценка качества псевдослучайных последовательностей на основе статистических тестов. Известия высших учебных заведений. Поволжский регион. Физико-математические науки, 2018, № 2, с. 24-35.

9. Ландин Д. В., Стоянова А. Ю. К вопросу о статистическом анализе качества генераторов псевдослучайных чисел. Наука и безопасность, 2017, т. 6, № 1, с. 39-44.

10. Иванов В. В. Программная реализация NIST SP 800-22 в контексте статистического тестирования групповых шифров. Компьютерные инструменты в образовании, 2017, т. 20, № 4, с. 7-13.

Чепурко И.А.
студент кафедры «Информационная безопасность» Южно-Российский государственный политехнический университет (НПИ).
ialexandrovich003@gmail.com
Лущаков М.А.
студент кафедры «Информационная безопасность» Южно-Российский государственный политехнический университет (НПИ).
lushakovmax123@gmail.com
Вахненко И.В.
Старший научный сотрудник НИО-1 НИЦ ВАС

ВЗАИМОСВЯЗЬ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ И АНАЛИЗА СЕТЕВОГО ТРАФИКА

Данная научная работа представляет собой обширный обзор ключевых аспектов криптографии, начиная с классических принципов и применений, и заканчивая передовыми тенденциями, такими как квантовая криптография. В работе подробно исследуются основные принципы криптографии, включая шифрование, асимметричные и симметричные ключи, а также основные алгоритмы, такие как RSA, AES, и 3DES. Особое внимание уделяется анализу и сравнительной оценке их эффективности и надежности в различных контекстах сетевого трафика.

КЛАССИЧЕСКАЯ КРИПТОГРАФИЯ

Классическая криптография – область криптографии, которая охватывает методы и техники шифрования данных, которые были разработаны и использовались до появления современных вычислительных методов и квантовой криптографии.

Основные элементы классической криптографии включают:

Шифры замены: методы шифрования, которые заменяют каждый символ или группу символов в открытом тексте другими символами в зашифрованном

тексте в соответствии с определенным правилом замены. Например, шифр Цезаря.

Шифры перестановки: методы шифрования, которые переставляют порядок символов в открытом тексте для создания зашифрованного текста. Например, шифр столбцов и шифр перестановки.

Простая и многократная замена: методы шифрования, которые используют несколько этапов замены или перестановки символов для создания более сложных шифров. Примером является шифр Виженера.

Классическая криптография, хотя и имеет длительную историю, столкнулась с рядом ограничений, таких как ограниченная безопасность из-за предсказуемости шифров и уязвимости к частотному анализу. С развитием современных компьютеров и криптоанализа классическая криптография постепенно уступает место современным методам криптографии, которые обеспечивают более высокий уровень безопасности и надежности.

ОСНОВЫ КВАНТОВОЙ КРИПТОГРАФИИ

Основы квантовой криптографии базируются на применении принципов квантовой механики для обеспечения безопасной передачи информации. Ключевая идея заключается в использовании квантовых свойств, таких как суперпозиция и запутанность, для создания криптографических протоколов, которые не могут быть взломаны классическими методами.

Принципы квантовой криптографии включают в себя:

Протокол квантового распределения ключей (QKD): это основополагающий протокол квантовой криптографии, который позволяет двум удаленным пользователям генерировать общий секретный ключ с абсолютной безопасностью. Это достигается благодаря принципу неопределенности Гейзенберга, который предполагает, что любая попытка измерения состояния квантовой системы приведет к его изменению. Поэтому любая попытка перехвата ключа будет обнаружена.

Квантовое шифрование: включает в себя использование квантовых свойств для создания криптографических алгоритмов, которые обеспечивают невозможность взлома при помощи классических методов. Одним из примеров является квантовое шифрование на основе однофотонных состояний, которое может быть использовано для защиты данных от криптоанализа.

Квантовая аутентификация: этот метод используется для проверки подлинности удаленных пользователей на основе квантовых свойств передаваемых частиц. Он обеспечивает более высокий уровень безопасности, чем классические методы аутентификации, так как любые попытки подделки будут немедленно обнаружены.

ПРЕИМУЩЕСТВА КВАНТОВОЙ КРИПТОГРАФИИ

Большинство современных систем защиты данных предпочитают квантовую криптографию перед классической по ряду важных причин:

Безусловная безопасность: квантовая криптография обеспечивает безусловную безопасность передачи ключей, что означает, что любые попытки перехвата ключей будут немедленно обнаружены. Это является принципиальным преимуществом перед классическими методами, которые подвержены криптоанализу и другим методам взлома.

Запрет квантового копирования: одним из фундаментальных принципов квантовой криптографии является запрет квантового копирования, что делает практически невозможным подделку или копирование передаваемых квантовых состояний. Это обеспечивает дополнительный уровень защиты, который отсутствует в классической криптографии.

Устойчивость к квантовым атакам: квантовая криптография разработана с учетом возможных квантовых атак, что позволяет системам быть устойчивыми к атакам, основанным на принципах квантовой механики. Это придает квантовой криптографии значительное преимущество в сравнении с классическими методами.

Будущее развитие технологии: в свете постоянного развития квантовых технологий и компьютеров, квантовая криптография представляет собой перспективное направление для обеспечения безопасности передачи данных в будущем. Это создает возможности для разработки новых методов и алгоритмов, которые могут улучшить безопасность информации в современном цифровом мире.

ЗАВИСИМОСТЬ АНАЛИЗА СЕТЕВОГО ТРАФИКА ОТ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Существует тесная связь между криптографическими алгоритмами и анализом сетевого трафика, особенно в контексте обеспечения безопасности и конфиденциальности данных. Примеры основных способов, в которых криптографические алгоритмы влияют на анализ сетевого трафика:

Шифрование данных: криптографические алгоритмы используются для шифрования данных, передаваемых по сети. Это может осложнить анализаторам сетевого трафика доступ к содержимому пакетов данных, так как они будут зашифрованы и недоступны для чтения без соответствующего ключа. В таких случаях анализаторы могут ограничиться анализом метаданных или статистических характеристик трафика, таких как размер пакетов, адреса и время отправки.

Аутентификация и целостность данных: криптографические алгоритмы также обеспечивают аутентификацию и целостность данных, передаваемых по сети. Проверка цифровых подписей и хэш-функций может быть использована для убеждения в том, что данные не были изменены во время передачи. Анализ сетевого трафика может включать проверку этих цифровых подписей и хэш-функций для установления подлинности данных и определения их целостности.

Мониторинг и управление безопасностью сети: Криптографические алгоритмы также могут быть использованы для мониторинга и управления безопасностью сети. Например, анализ шифрованных потоков данных может помочь в обнаружении подозрительной активности или нарушений политик

безопасности сети, что в свою очередь позволяет принимать соответствующие меры для защиты сети.

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В ЗАЩИТЕ СЕТЕВОГО ТРАФИКА

Применение криптографических алгоритмов играет ключевую роль в обеспечении безопасности сетевого трафика и защите цифровых данных. Вот несколько основных способов, в которых криптографические алгоритмы применяются для защиты сетевого трафика:

Шифрование трафика: одним из наиболее распространенных применений криптографии является шифрование данных, передаваемых по сети. Это позволяет обеспечить конфиденциальность информации путем преобразования данных в непонятный для посторонних вид. Популярные алгоритмы, такие как AES и RSA, используются для шифрования данных на различных уровнях сетевого стека.

Аутентификация и подлинность: криптографические алгоритмы применяются для обеспечения аутентичности данных и идентификации участников в сети. Цифровые подписи и алгоритмы хэширования используются для подтверждения подлинности передаваемых данных и участников обмена информацией.

Обеспечение целостности: криптографические хэш-функции часто используются для обеспечения целостности данных в сетевом трафике. Это позволяет обнаруживать любые изменения или повреждения данных, которые могут произойти во время их передачи, и предотвращать подделку данных.

Виртуальные частные сети (VPN): криптографические протоколы часто используются для создания защищенных туннелей в виртуальных частных сетях. Это позволяет организациям и пользователям обмениваться данными через общедоступные сети, такие как Интернет, с обеспечением конфиденциальности, целостности и аутентификации.

Цифровые сертификаты: криптографические алгоритмы используются для создания и проверки цифровых сертификатов, которые играют важную роль в аутентификации и безопасности в сетях. Это обеспечивает доверие между участниками сети и позволяет создавать защищенные каналы связи.

Применение криптографических алгоритмов в защите сетевого трафика играет ключевую роль в обеспечении конфиденциальности, целостности и аутентичности данных, а также в создании защищенных сетевых коммуникаций. Это необходимое условие для обеспечения безопасности информации в современных сетевых средах, особенно в контексте растущих угроз кибербезопасности.

ИССЛЕДОВАНИЕ

Исследование данной научной работы подразумевает анализ наиболее распространенных криптографических алгоритмов (AES, 3DES, RSA), которые используются для анализа сетевого трафика. Выбор лучшего.

AES (Advanced Encryption Standard):

Преимущества:

- Высокий уровень безопасности: AES обеспечивает высокий уровень защиты данных и широко применяется для шифрования конфиденциальной информации.

- Высокая производительность: AES хорошо оптимизирован для эффективного шифрования больших объемов данных и обеспечивает высокую производительность на современных вычислительных системах.

Недостатки:

- Нет особых недостатков, но выбор определенного режима работы (например, режим CBC или GCM) может зависеть от конкретных потребностей системы.

3DES (Triple Data Encryption Standard):

Преимущества:

- Высокий уровень безопасности: 3DES предоставляет более высокий уровень защиты по сравнению с оригинальным алгоритмом DES.

- Широкая совместимость: 3DES поддерживается во многих существующих системах и может быть использован в ситуациях, где требуется совместимость с устаревшим оборудованием.

Недостатки:

Сравнительно медленная производительность: 3DES требует больше вычислительных ресурсов по сравнению с более современными алгоритмами шифрования.

RSA (Rivest-Shamir-Adleman):

Преимущества:

- Поддержка цифровых подписей: RSA широко используется для аутентификации и создания цифровых подписей, что делает его ценным инструментом в цифровой безопасности.

- Гибкость: RSA может использоваться для шифрования данных различной длины и может быть применен в различных сценариях, где требуется асимметричное шифрование.

Недостатки:

- Более сложный процесс ключевого управления: управление ключами в RSA может быть более сложным, особенно при обмене ключами между пользователями.

Чтобы определить, какой алгоритм лучше, необходимо тщательно оценить требования к безопасности, производительности, контекст применения и ограничения системы. Например, если системе требуется высокая производительность при шифровании больших объемов данных, то AES может быть предпочтительнее. Если система использует устаревшее оборудование, 3DES может быть предпочтительным вариантом. RSA может быть лучшим выбором для цифровых подписей и аутентификации.

ЗАКЛЮЧЕНИЕ

Из вышеизложенных данных становится ясно, что криптография играет решающую роль в обеспечении безопасности сетевого трафика и защите цифровых данных. Современные методы защиты сетевого трафика, основанные на криптографических алгоритмах, позволяют обеспечить конфиденциальность, целостность и аутентичность данных, а также создать защищенные каналы связи и сетевые соединения.

Тем не менее, необходимо учитывать, что современные криптографические алгоритмы постоянно развиваются, чтобы противостоять новым угрозам и атакам, связанным с развитием вычислительных возможностей. Поэтому для поддержания высокого уровня безопасности необходимо обеспечивать регулярное обновление и модернизацию криптографических методов, а также постоянно повышать осведомленность и квалификацию специалистов в области кибербезопасности.

СПИСОК ИСТОЧНИКОВ

1. Величко С.П. «Методы и средства защиты информации.», 2013.

2. Иванов, А. А., и Д. И. Петров. "Анализ методов криптографической защиты информации." Вестник Российского университета дружбы народов. Серия: Информационные системы и технологии 21, no. 1 (2017): 88-96.

3. Карпов, Д. Н. "Методы анализа сетевого трафика для обеспечения безопасности информационных систем." Научно-технический вестник информационных технологий, механики и оптики 20, no. 4 (2020): 573-579.

4. Смирнов, В. И., и О. Н. Попов. "Криптографические методы обеспечения безопасности информационных систем." Вестник Балтийского федерального университета им. И. Канта 25, no. 3 (2018): 442-446.

5. Петровский, С. В., и А. Г. Смирнов. "Анализ уязвимостей сетевых протоколов для защиты информационных систем." Информационные технологии и вычислительные системы 6, no. 2 (2019): 97-104.

6. Воронов, В. В., и Г. А. Петрова. "Основы криптографии и защиты информации." Издательство Юрайт, 2021. Григорьев, С. В. "Методы анализа и

защиты сетевого трафика." Информационные технологии и безопасность 2, no. 4 (2017): 54-61.

7. Никитин, В. А. "Технологии защиты сетевого трафика в информационных системах." Информационные технологии и безопасность 3, no. 2 (2018): 28-34.

8. Павлов, А. С. "Криптография и методы обеспечения информационной безопасности." Научно-технический вестник информационных технологий, механики и оптики 19, no. 3 (2019): 481-485.

9. Зайцев, Е. В., и В. И. Смирнов. "Анализ сетевого трафика для обнаружения и предотвращения кибератак." Информационные технологии и безопасность 1, no. 3 (2016): 16-22.

10. Медведев, И. П., и О. Г. Иванова. "Современные методы криптографической защиты данных." Издательство Лань, 2020.

Раковский Д.И.
Московский технический университет связи и информатики,
ассистент кафедры "Информационная безопасность"
Prophet_alpha@mail.ru,
Александров И.Д.
Московский технический университет связи и информатики,
студент кафедры "Информационная безопасность",
Боков А.Д.
Московский технический университет связи и информатики,
студент кафедры "Информационная безопасность"

СТЕНД ДЛЯ СБОРА ТЕЛЕМЕТРИИ МНОГОЗНАЧНЫХ КОМПЬЮТЕРНЫХ АТАК

Введение

Современные компьютерные атаки, совершаемые на корпоративные компьютерные сети (КС), характеризуются обходом статистических и сигнатурных средств защиты информации [1–3]. Для защиты таких систем применяются все более комплексные системы защиты информации [4,5].

Современные КС могут подвергаться нескольким компьютерным атакам одновременно [6]. Из-за ограниченности средств сбора телеметрии с хостов атакуемой КС, собранные дампы содержат записи, идентичные по всем атрибутам, но ассоциированные с разными компьютерными атаками. Указанные свойства являются проявлениями многозначности данных [7–9]. Актуальной задачей является разработка стенда для сбора телеметрии КС в условиях проведения многозначных контролируемых компьютерных атак.

Структура и схема функционирования стенда, формализация задачи

Пусть КС задается множеством из M упорядоченных наборов значений дискретно изменяющихся атрибутов КС [10]:

$$\boldsymbol{D}_{NM} = \left\{ \left(\boldsymbol{A}(n,\ ), set_n \right); \boldsymbol{A} = \left(a_{nm} \right), m = \overline{1,M}, n = \overline{1,N} \right\}, \quad (1)$$

где $\boldsymbol{A}(n,\ ) = (a_{n1}, a_{n2}, \ldots, a_{nM})$ - n-тый вектор-строка матрицы (таблицы) атрибутов экспериментальных данных $\boldsymbol{A}$, состоящая из M столбцов. Тогда элемент этой строки, $a_{ni} \in \boldsymbol{A}(n,\ )$, означает метрическое значение i-того атрибута на n-той строке экспериментальных данных ; set_n – классовая метка, ассоциированная с n-ной строке значений атрибутов записи экспериментальных данных; $\left(\boldsymbol{A}(n,\ ), set_n \right)$ - пара элементов типа «n-ная строка экспериментальных данных, соответствующая ей классовая метка»; N – количество записей экспериментальных данных; M – количество атрибутов в экспериментальных данных.

Пусть топология КС T исследуемой КС состоит из двух множеств хостов:

$$T = \left\{ VH_i; i = \overline{1,I} \right\} \cup \left\{ AH_j; j = \overline{1,J} \right\} \cup DAS \cup Router, \quad (2)$$

где VH_i – i-тый хост, имитирующий жертву (далее – атакуемый хост, от англ. *Victim host*); AH_j – j-тый хост, имитирующий машину злоумышленника (далее – атакующий хост, от англ. *Attack host*), проводящую контролируемую компьютерную атаку (ККА) на VH_i; *DAS* – сервер агрегации данных (англ. *data aggregation server*), аккумулирующий телеметрию с VH_i и AH_j.; Router – маршрутизатор, соединяющий множество атакуемых и атакующих хостов.

Зададим перечень компьютерных атак *AL* (англ. *Attack Library*), которые атакующие хосты AH_j реализуют на атакуемые хосты VH_i:

$$AL = \left\{ attack_k; k = \overline{1,K} \right\}. \quad (3)$$

Каждая компьютерная атака (3) обладает набором параметров, однозначно ее описывающих и общих для каждой реализации:

$$attack_k : \left\langle params_{l_k} \right\rangle; l_k = \overline{1,L_k}. \quad (4)$$

Конкретное множество параметров детализируется в зависимости от механизма реализации компьютерной атаки. Общее число параметров атаки - L_k - варьируется в зависимости от детализации атаки.

Зададимся рядом варьирующихся параметров реализации атаки из библиотеки *AL* (3) - AoI_k (англ. *Attack on Interval*):

$$AoI_k : \langle IS, IE, attack_k, ah, tar, dur, int, etcp \rangle, \quad (5)$$

где *IS* – параметр, точное время начала интервала атаки (англ. *Interval Start*); *IE* – параметр, точное время окончания интервала атаки (англ. *Interval End*); $attack_k$ - набор параметров атаки, общих для каждой реализации; *ah* – атакующий хост, реализующий экземпляр атаки в пределах указанных интервалов; *tar* – множество целей атаки для dur – длительность атаки в пределах указанных интервалов; *int* – интенсивность атаки в пределах указанных интервалов; *etcp* – множество иных варьирующихся параметров.

Отметим, что содержимое AoI_k может задаваться как фиксированными числами, так и законами распределения случайной величины, выбираемыми из библиотеки распределений $FL = \left\{ F_{lf}(\alpha_p); p = \overline{1, P_{lf}}, lf = \overline{1, LenF} \right\}$, где α_p - *p*-тый параметр *lf*-того закона распределения.

Для предотвращения уничтожения КС в следствие фатального воздействия компьютерных атак, предусмотрен механизм оценки максимально допустимого негативного воздействия на КС *i*-тый атакуемый хост VH_i - $MaxDamage_{VH_i}$ - со стороны атакующих хостов. Под $MaxDamage_{VH_i}$ понимается максимально допустимое время ответа *i*-того атакуемого хоста VH_i на синхронизирующий сигнал, поступающий с сервера агрегации данных *DAS*.

Взаимодействие между элементами КС (2) – *DAS*, VH_i и AH_j – осуществляется через программные агенты первого и второго типов, распространяемые на соответствующие хосты хосты - $PA = \left\{ prograg_{1,i}; i = \overline{1, I} \right\} \cup \left\{ prograg_{2,j}; j = \overline{1, J} \right\}$. Программные агенты первого типа - $prograg_{1,i}$ - осуществляют сбор телеметрической информации с атакуемых хостов VH_i. Программные агенты второго типа - $prograg_{2,j}$ - осуществляют сбор телеметрической информации с атакующих хостов AH_j. Программные агенты первого и второго типов связаны с сервером агрегации данных *DAS* через центральный пункт управления (ЦПУ).

На этапе проведения ККА, в момент реализации атаки, датчик псевдослучайных чисел *RND*, получая на вход закон распределения $F_{params_{l_k}}$ и установленные параметры, формирует окончательные параметры реализации атаки внутри каждого интервала *IS* - *IE*.

Опишем воздействие атакующими хостами AH_j на хосты-жертвы VH_i, вектором из W_k параметров AoI_k: $\vec{V}_k = \left(AoI_{kw}; w = \overline{1, W_k}\right)$, где W_k – количество раз, когда *k*-тая атака (3) планируется к реализации в течение эксперимента. Каждая тройка задается собственным набором параметров (5).

Множество экспериментальных данных (1), порождается в результате воздействия атакующими хостами AH_j на хосты-жертвы VH_i (2) тройками (5), объединенными в вектора. Конфигурация воздействия по каждой компьютерной атаке может быть представлена в виде итогового множества $CoA = \left(\vec{V}_k; k = \overline{1, K}\right)$ (англ. *Chronology of Attacks*).

Визуализация механизма работы стенда, формализованного посредством выражений (1) – (5) представлена на (рис. 1).

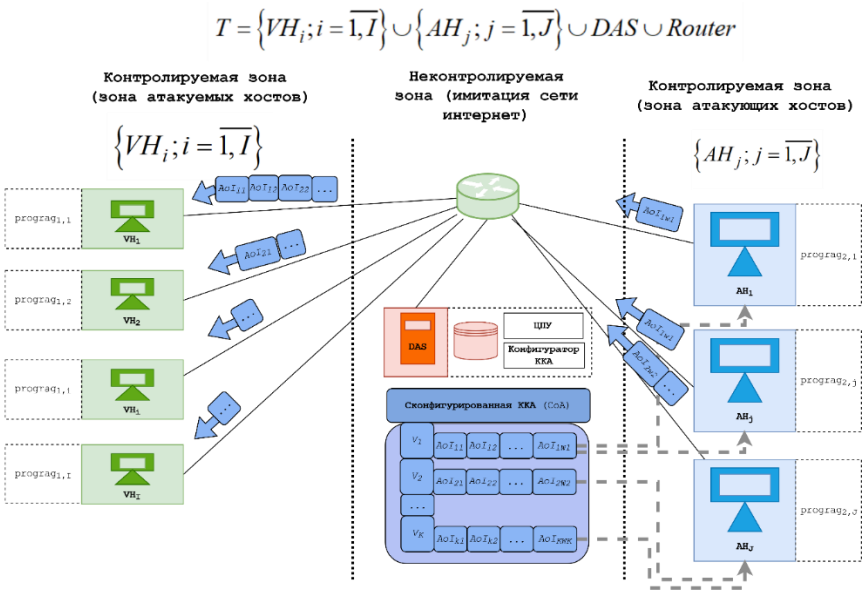

Рис. 1. Структурная и схема функционирования стенда

Топология исследуемой КС *T* (2) отражена на визуализации в виде двух контролируемых зон – зоны атакуемых хостов VH_i и зоны атакующих хостов AH_j. VH_i и AH_j разделены неконтролируемой зоной, имитирующей сеть

Интернет. На каждом из VH_i установлен программный агент первого типа $prograg_{1,i}$; на каждом AH_j установлен программный агент второго типа $prograg_{1,i}$; на сервере агрегации данных *DAS* расположена база данных для агрегируемый телеметрических данных с AH_j и VH_i; ЦПУ для контроля взаимодействия между программными агентами.

Программные агенты второго типа $prograg_{2,j}$ распространяется на атакующие хосты AH_j и необходим для формирования многозначных целевых столбцов – классовых меток наличия / отсутствия проведения ККА определенного типа с *j*-того атакующего хоста. Программный агент $prograg_{2,j}$, получая на вход расписание ККА от ЦПУ, осуществляет их проведение с учетом информации, поступившей из программных агентов первого типа.

Для реализации компьютерных атак, *DAS* посылает управляющие сигналы на атакующие хосты. Атакующие хосты реализуют компьютерную атаку.

В качестве демонстрации работоспособности стенда, была произведена многозначная ККА на один хост-жертву. Были выбраны атаки двух типов – «отказ в обслуживании» и «сканирование портов». Атака типа «отказ в обслуживании» реализована посредством утилиты *hping3*, «сканирование операционной системы» – *nmap*.

Интервалы проведения ККА были сконфигурированы таким образом, чтобы часть атак различных категорий происходила одновременно. Собрано 11.338 записей. Проведено 63 атаки: 13 атак типа «отказ в обслуживании» и 50 атак типа «сканирование операционной системы».

Итоговый набор данных, полученный в результате объединения всех таблиц всех баз данных, содержит 43 столбца (атрибута), включая 3 целевых столбца, из категорий «аппаратные атрибуты», «сетевая карта» и «диспетчер задач». Многозначные данные, снимаемые с диспетчера задач, объединены в одну строку операцией конкатенации.

На рис. 2 приведено частотное распределение целевых столбцов собранных данных.

Рис. 2. Частотное распределение целевых столбцов, собранных данных. Слева – распределение однозначных и многозначных записей. Справа – информация о частотном распределении каждого целевого столбца.

Полученный набор данных содержит 38% нормальных записей, и 62% записей, связанных с одной из двух компьютерных атак - «Отказ в обслуживании», «Сканирование ОС». Анализ полученных данных показывает, что доля многозначных данных, собранных за время эксперимента, составляла 5% от общего числа записей. Было найдено, что доля многозначных в множестве аномальных записей возрастает с ростом количества целевых столбцов.

Выводы

Новизна разработанного стенда заключается автоматизированной одновременной маркировке всех ККА, направленных на целевую КС.

Собраны демонстрационные экспериментальные данные. Эксперимент проводился в промежуток с 20:22:07 28.09.2023 по 09:40:04 29-09-2023. За указанное время собрано 11.338 записей. Проведено 63 атаки: 13 атак типа «отказ в обслуживании» и 50 атак типа «сканирование операционной системы».

Анализ полученных данных показывает, что доля многозначных данных, собранных за время эксперимента, составляет 5% от общего числа записей.

Данное исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта, Соглашение №. 40 469–21/23-К от 30.06.2023 г.

СПИСОК ИСТОЧНИКОВ

1. Sheluhin O.I., Osin A.V., Rakovsky D.I. New Algorithm for Predicting the States of a Computer Network Using Multivalued Dependencies // Aut. Control Comp. Sci. 2023. Т. 57, № 1. С. 48–60.
2. Аль-Ани М.м., Алшаиби А.Д., Костюченко Е.Ю. Эффективность Глубокого Обучения И Методы Машинного Обучения В Кибербезопасности // Проблемы Правовой И Технической Защиты Информации. 2021. № 9. С. 7–9.
3. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы Кибербезопасности. 2023. № 3 (55). С. 90–100. DOI:10.21681/2311-3456-2023-3-90-100.
4. Mozaffari M., Doshi K., Yilmaz Y. Self-Supervised Learning for Online Anomaly Detection in High-Dimensional Data Streams // Electronics. 2023. Т. 12, № 9. С. 1971.
5. Левшун Д.С. Иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак // Труды Учебных Заведений Связи. 2023. Т. 9, № 1. С. 105–115.
6. Шелухин О.И., Раковский Д.И. Многозначная классификация компьютерных атак с использованием искусственных нейронных сетей с множественным выходом // Труды Учебных Заведений Связи. 2023. Т. 9, № 4. С. 97–113.
7. Молодцов Д.А., Осин А.В. Новый метод применения многозначных закономерностей // Нечеткие Системы И Мягкие Вычисления. 2020. Т. 15, № 2. С. 83–95.

8. Sheluhin O.I., Ivannikova V.P. Comparative analysis of informative features quantity and composition selection methods for the computer attacks classification using the UNSW-NB15 dataset // T-Comm. 2020. T. 14, № 10. C. 53–60.
9. Riera T.S., Higuera J.-R.B., Higuera J.B., Herraiz J.-J.M., Montalvo J.-A.S. A new multi-label dataset for Web attacks CAPEC classification using machine learning techniques // Computers & Security. 2022. T. 120. C. 102788.
10. Шелухин О.И., Раковский Д.И. Многозначная классификация меток классов системных журналов компьютерных сетей. Сравнительный анализ эффективности классификаторов // Вопросы кибербезопасности. 2023. Т. 55, № 3. С. 62–77.

Липатников В.А.
Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного, старший научный сотрудник, д.т.н., профессор, lipatnikovanl@mail.ru
Мелехов К.В.
Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного, адъюнкт, kirill_melehov@bk.ru
Щукин А.В.
Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного, адъюнкт, kirill_melehov@bk.ru

МОДЕЛЬ ЦИФРОВОГО ПОТОКА СЕТИ ПЕРЕДАЧИ ДАННЫХ В УСЛОВИЯХ МНОГОЭТАПНЫХ АТАКАХ

Аннотация: для более детального рассмотрения процессов по управлению защищенностью сети передачи данных (СПД), предлагается исследовать особенности цифрового потока (ЦП) СПД в условиях многоэтапных атаках (МЭА). Модель должна учитывать структурно-функциональные параметры. Целью работы является повысить защищенность СПД путем создания модели ЦП СПД в условиях МЭА и её исследования. Для исследования использовался метод положения теории формальных грамматик. Результатом данного исследования будет считаться модель ЦП СПД в условиях МЭА с учетом взаимоувязанных параметров исследуемого объекта. Новизна модели ЦП СПД в условиях МЭА в отличии от известных учитывает выделение признаков ЦП

СПД, селекцию служебной информации, которая подлежит обработке, анализу и дальнейшему распознаванию элементов МЭА, определение мер защиты. Практическая значимость проведенного моделирования позволит разработать меры (способы) обеспечения защищенности СПД.

Ключевые слова – многоэтапная атака, теория формальных грамматик, защищенность, сеть передачи данных, цифровой поток, управление.

Введение

В наши дни технологии, которые обеспечивают передачу данных используются повсеместно [1]. При этом СПД отведена роль основного элемента в реализации данного процесса. Для устойчивого функционирования СПД требуется обеспечение её защиты [2]. Данная задача должна осуществляться в соответствии с новыми веяньями к исследованию ЦП, под которыми понимается взаимодействие определенных моделей сетевых протоколов на различных уровнях обеспечивающих передачу информации.

Вывод по обзору релевантных работ [3,4] заключается в том, что при разработке модели ЦП СПД недостаточно уделено внимание селекции управляющей информации. Одним из требований, является реализация способов обработки и определения возможного воздействия МЭА. Тем самым необходимость оценки защищенности СПД является актуальной.

Решение

Целостность модели функционально-логической архитектуры СПД (ФЛА СПД) подразумевающего объекта воздействия МЭА понимается взаимодействие определенных моделей сетевых протоколов на различных уровнях обеспечивающих передачу информации [5, 6]. При использовании нарушителем данного взаимодействия, только по единичным параметрам это возможно распознать. Одним из таких является ЦП, распространяющийся по сетевым каналам передачи данных**.** ФЛА СПД состоит из нескольких частных моделей. Одной из них является ЦП СПД. Данная модель раскрывает совместность соединений от одного объекта к другому объекту [7, 8]. Подразумевает выполнение задач по маркировке в цифровом потоке

признаков протоколов СПД, по селекции служебной информации, подлежащей обработке, анализу и дальнейшему распознаванию элементов МЭА и выработке предложений по защите защиты, а также определить иерархичность и взаимодействие сетевых протоколов.

ЦП возможно представить в виде последовательности двоичных чисел, которые являются значениями (0,1), передаваемых по каналам связи при реализации процедур установления, поддержания и ликвидации соединения для передачи данных (ПД) между двумя оконечными системами СПД. Соединения для ПД устанавливаются между объектами каждого логического уровня взаимодействующих оконечных систем: (N)-соединения. Таким образом, ЦП каждого (N)-соединения, за исключением соединения прикладного уровня переносит информацию как (N)-протокола, так и информацию (N+1)-протокола.

Вышеуказанные значения, которые присутствуют в ЦП соединения между объектами (N)-уровня сети. Это обуславливает использование определенного сетевого протокола, определённого уровня. Данный порядок именуется структурным элементам (СЭ) ЦП (N)-соединения ((N)-ЦПС).

Параметры содержатся в любом СЭ ЦП находящегося в логическом канале определенного уровня. Они устанавливаются в соответствии с задачами по безопасности СЕТИ от МЭА. СЭ подразделяются на отдельные биты и поля баз данных протокола (БДП), определенные комбинации по синхронизации, стаффингования и заполнения. В свою очередь они бывают сосредоточенными и составными (БДП, ЦП соединений высших уровней). Если рассматривать со стороны протокола или его режима, то они делятся на сосредоточенные и рассредоточенными. Без обнаружения, распознавания и установления взаимодействия СЭ ЦП сети не получится решить задачу по раннему обнаружению [9] преднамеренных МЭА.

Отношения строгого порядка, непосредственно связанные с цифровым потокам соединений в СПД. В данных условиях необходимо использование подходящих методов математического моделирования. В ходе анализа установлен, что формальные грамматики, позволят решить данную задачу. С

помощью вышеуказанного математического аппарата удастся избежать неоднозначности при описании. Он прост в реализации и эффективен в теории распознавания. При этом получится полностью учесть структурные свойства объекта [10].

ЦП (N)-соединения (ЦПС) СПД есть определенная на периоде существования соединения матемаьичская система (1)

$$A =< S, \{\oplus\}, \{R\} >, \quad (1)$$

где S - множество СЭ (N)-ЦПС; $\oplus$ - операция конкатенации на множестве структурных элементов; R - бинарное отношение на множестве СЭ в (N)-ЦПС.

Структура цифрового потока (N)-соединения СПД, описываемого алгеброй вида (1), есть отношение строгого порядка, определенное на множестве структурных элементов и существующее на интервале, равном длительности существования соединения, то есть (2)

$$R = \{\forall\left(s_i,\ s_j,\ s_k\right) \in S, s_i R s_j \neq s_j R s_i, i \leq j; s_i R s_j \wedge s_j R s_k \rightarrow s_i R s_k, i < j < k\}, \quad (2)$$

где $s_i,\ s_j,\ s_k$ - СЭ (N)-ЦПС канального уровня.

Отношение строгого порядка по определению есть бинарное отношение, обладающее свойствами антирефлексивности, антисимметричности и транзитивности.

(N)-ЦПС, переносящий команды и данные взаимодействующих объектов-пользователей услуг (N)-службы, состоит из элементов управления логическим каналом и различного типа (N)-БДП, в общем случае разделенных между собой элементами синхронизации ($\{s_i\}$). Перечисленные элементы являются структурными элементами (N)-ЦПС: $\{s_i\} \in S$.

В свою очередь (N)-БДП имеют соответствующую структуру, причем двоичные последовательности (N)-БДП, в общем случае, содержат адресные, управляющие, информационные и проверочные поля. Таким образом, сами (N)-БДП и их поля являются структурными элементами (N)-ЦПС.

Структура (N)-БДП любого типа, порядок обмена ими в ходе сеанса ПД, процедуры синхронизации и управления логическим каналом строго

регламентируется соответствующим (N)-протоколом управления. Поэтому между каждыми двумя соседними элементами существует строго определенное отношение порядка следования, которое нельзя изменить на обратное, то есть оно асимметрично. Этот порядок сохраняется и при двух одинаковых соседних СЭ, то есть соблюдается антирефлексивность. Транзитивность отношения порядка следования СЭ в (N)-ЦПС очевидна.

Многие (N)-протоколы СПД допускают конечное множество вариантов кодирования полей (N)-БДП и порядка следования (N)-БДП друг за другом в ходе сеанса ПД в зависимости от различных факторов: состояния канала связи, протяженности и пропускной способности линии связи, параметров оконечного оборудования данных, используемого (N-1)-протокола и др. В этом случае существует континиум $R_{(N)}=\{R_{(N)i}\}$, каждый СЭ соответствует конкретному режиму (N)-протокола.

Процесс обмена служебной информацией для управления на (N)-уровне (N=2..7) описывается цифровыми потоками соответствующих соединений между (N)-объектами сети с помощью алгебры вида:

$$A_{(N)} = \ < S_{(N)}, \{\oplus\}, \left\{R_{(N)}\right\} > . \qquad (3)$$

Размещение структурных элементов (N)-ЦПС адекватно описывается бинарными отношениями строгого порядка вида (3). Это утверждение справедливо как по отношению к последовательности передачи различных (N)-БДП в ходе сеанса ПД, так и к структуре самих (N)-БДП.

Иерархическая протокольная структура ЦП СПД может быть представлена алгеброй вида (4), где множество БДП каждого (N)-протокола является подмножеством СЭ БДП (N-1)-протокола:

$$A_{(N)} =< S_{(N)-БДП}, \{\oplus\}, \left\{R_{(N)}\right\} > \ ;$$

$$A_{(N)-БДП} =< \{S_{(N)-УИП}, S_{(N)-БДС}\}, \{\oplus\}, \left\{R_{(N)} S_{(N)-БДП}\right\} >; \qquad (4)$$

$$A_{(N)-БДС} =< S_{(N-1)-БДП}, \{\oplus\}, \left\{R_{(N-1)-БДС}\right\} > ;$$

$$A_{(N-1)} =< S_{(N-1)-БДП}, \{\oplus\}, \{R_{(N-1)}\} > \text{ и т.д.}$$

Выражения (5) представляют собой не что иное, как модель иерархии логических соединений в сквозном канале СПД между двумя оконечными системами. Для моделирования суммарного трафика необходимо рассматривать упорядоченное множество пар (*l*,*k*) оконечных систем СПД. Объединение алгебр всех ЦПС (каждая из которых определяется на периоде существования (*N*)-соединений данного сеанса ПД) на множестве каналов образуют модель трафика (алгебру трафика сети A_{TC}):

$$A_{TC} = \cup A_i(T_j)_{(l,k)}, \qquad (5)$$

где $A_i(T_j)_{(l,k)}$ - алгебра ЦПС *i*-го канала на периоде T_j существования *j*-го логического соединения между *l*-й и *k*-й оконечными системами СПД.

Таким образом, свойства структуры цифрового потока, обеспечивают иерархическое взаимодействие сетевых протоколов на различных уровнях. В свою очередь это позволяет указывать местоположение и взаимосвязи структурных элементов ЦПС - носителей параметров протоколов, управляющей информации и данных пользователей [11]. Эти свойства предоставляют параметры для моделирования преднамеренных изменений функций сетевых протоколов сети по отображениям на ЦП логических соединений**.**

Заключение.

При моделировании ЦП СПД в условиях МЭА, рассмотрены переносящие команды управления и данные между взаимодействующими объектами. Представленная модель ЦП позволяет учитывать выделение в цифровом потоке признаков протоколов СПД. С целью их дальнейшей обработки осуществляется селекция в цифровом потоке служебной информации для управления. После чего определение воздействия МЭА, осуществляется за счет иерархии и взаимодействия сетевых протоколов.

Литература

1. Костарев С.В. Технологии защиты информации в условиях кибернетического противоборства./ С.В. Костарев, В,В, Карганов, В.А. Липатников // Санкт-Петербург, 2020.

2. Макеев А. С. Факторы, влияющие на эффективность управления информационной безопасностью / А. С. Макеев. — Текст: непосредственный // Молодой ученый. — 2016. — № 10 (114). — С. 66-69. — URL: https://moluch.ru/archive/114/29935/;

3. Липатников В.А. Устройство поиска информации./ В.А. Липатников, А.М. Плотников, В.В. Якимовец // Патент на изобретение RU 2100839 C1, 27.12.1997. Заявка № 95108104/09 от 18.05.1995.

4. Липатников В.А. Устройство поиска информации./ В.А. Липатников, А.М. Плотников, В.В. Якимовец // Патент на изобретение RU 2094845 C1, 27.10.1997. Заявка № 95103135/09 от 06.03.1995.

5. Sheth H. A survey on RBF Neural Network for Intrusion Detection System./ H.Sheth, B.Shah, S.Yagnik // Int. Journal of Engineering Research and Applications. 2014. vol. 4. Issue pp. 17–22.

6. Крибель А.М. Модель выявления аномалий в сетевом трафике сети передачи данных в условиях компьютерных атак / А.М. Крибель, Р.А. Перов, О.С. Лаута, С.Ю. Скоробогатов. — Текст: непосредственный // Научная электронная библиотека открытого доступа. URL: https://cyberleninka.ru/article/n/model-vyyavleniya-anomaliy-v-setevom-trafike-seti-peredachi-dannyh-v-usloviyah-kompyuternyh-atak

7. Задбоев В.А. Способ определения в сети передачи данных цепочки маршрутов до географического местоположения злоумышленника./ В.А. Задбоев, В.А. Липатников, К.В. Мелехов // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т. Санкт-Петербург, 2023. С. 512-517.

8. Мелехов К. В. Средство верификации модели процесса управления безопасностью сети передачи данных при многоэтапных атаках / К.В. Мелехов, В.А. Липатников, М.И. Петренко, А.А. Шевченко, В.А. Парфиров, И.А. Мелихов, М.Е. Мезенин // Свидетельство о регистрации программы для ЭВМ 2023664605, 05.07.2023. Заявка № 2023663624 от 27.06.2023.

9. Богачев, Д. Г. Анализ несанкционированного искажения протокольной информации в телекоммуникационных системах / Д. Г. Богачев, В. Т. Еременко // Известия Орловского государственного технического университета. Серия: Информационные системы и технологии. – 2007. – № 4-2. – С. 36-40.

10. Липатников В.А. Особенности сетевого контроля в сети передачи данных в условиях многоэтапных атак / В.А. Липатников, К.В. Мелехов, И.А. Мелихов // В сборнике: ТЕХНОЛОГИИ. ИННОВАЦИИ. СВЯЗЬ. Материалы научно-практической конференции. Санкт-Петербург, 2023. – С. 171-174.

11. Липатников В.А. Модель процесса обеспечения безопасности сети передачи данных в условиях информационного противоборства / В.А. Липатников, К.В. Мелехов, А.А. Шевченко, В.А. Парфиров // В сборнике: Актуальные проблемы защиты и безопасности. Труды XXVI Всероссийской научно-практической конференции. Санкт-Петербург, 2023. С. 569-572.

Секция 2

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Руководители: **Кубанков Александр Николаевич**,
Московский технический университет связи и информатики, заведующий кафедрой «Безопасность телекоммуникаций», доктор военных наук, профессор,

Булгакова Елена Валерьевна,
Московский технический университет связи и информатики, доцент кафедры «Безопасность телекоммуникаций», кандидат юридических наук, доцент

Задбоев В.А.
Военная академия связи имени С.М. Буденного, младший научный сотрудник
zadboev89@mail.ru
Робак В.А.
Санкт-Петербургский государственный университет аэрокосмического приборостроения, студент
molkorn999@gmail.com
Мелехов К.В.
Военная академия связи имени С.М. Буденного, адъюнкт
kirill_melehov@bk.ru

МОДЕЛЬ СРЕДСТВА КОНТРОЛЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ, РАННЕГО ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ АТАК

В наше время, когда важность информационной безопасности нельзя переоценить, вопрос обработки и анализа информации о многоэтапной атаке (МЭА) становится все более актуальным. Повышение эффективности системы выявления аномалий может быть полезным для улучшения процесса сохранения полученной из них информации и прогнозирования будущих аномалий.

Перед началом работы была разработана структура средства сетевого контроля сети передачи данных состояний системы, применяющей потоковые двухслойные РНС с управляемыми синапсами, для выявления аномалий, раннего обнаружения и классификации МЭА (Рис. 1).

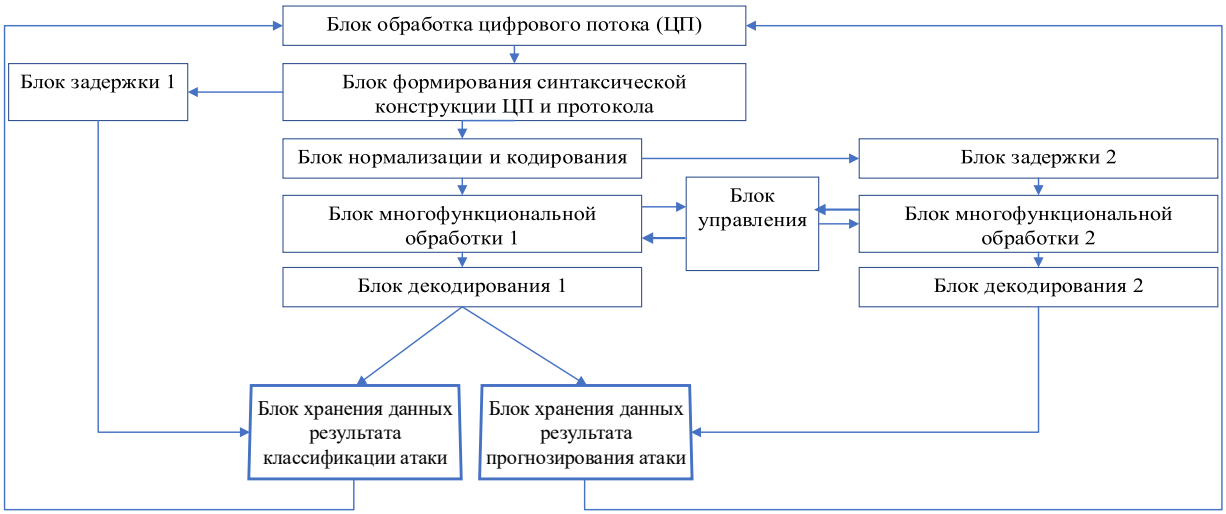

Рис.1 Структура средства сетевого контроля сети передачи данных

Структура поясняется следующим образом:

1. Цифровой поток об атаке поступает в систему. Происходит его обработка и анализ.

2. Формируется синтаксическая конструкция цифрового потока

3. Цифровой поток обрабатывается и преобразуется в нужный формат для лучшей работы нейросети.

4. Цифровой поток анализируется с помощью рекуррентной нейросети.

5. Нейросеть обновляет процесс обучения и принятия решений на основе работы моделей.

6. Происходит сохранение данных, полученных в результате работы нейросети.

Для расчета модели эффективности системы выявления аномалий в качестве решения был разработан граф состояний системы, применяющей потоковые двухслойные рекуррентные нейронные сети (РНС) с управляемыми синапсами, для выявления аномалий, раннего обнаружения и классификации многоэтапной атаки (МЭА).

Проведено исследования процесса выявления аномалий, раннего обнаружения и классификации МЭА с помощью потоковых двухслойных РНС с управляемыми синапсами.

На основе графа состояний была построена и решена система уравнений, с учетом нормировки $\sum_{k=0}^{m} P_k = 1$. Полученная система уравнений представлена в формуле (3) с учетом замен (1) и (2).

$$
\begin{cases}
a = \dfrac{\lambda_{0-1}}{\lambda_{1-2} + \lambda_{1-7}}, \\
b = \dfrac{\lambda_{0-1}\lambda_{1-2}}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})}, \\
c = \dfrac{\lambda_{0-1}\lambda_{1-2}(\lambda_{2-3} + \lambda_{11-3}\beta)}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})(\lambda_{3-4} + \lambda_{3-11})}, \\
d = \dfrac{\lambda_{0-1}\lambda_{1-2}\lambda_{3-4}(\lambda_{2-3} + \lambda_{11-3}\beta)}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})(\lambda_{3-4} + \lambda_{3-11})(\lambda_{4-5} + \lambda_{4-6})}, \\
e = \dfrac{\lambda_{0-1}}{(\lambda_{1-2} + \lambda_{1-7})\lambda_{5-0}}\left(\dfrac{\lambda_{1-2}\lambda_{3-4}\lambda_{4-5}(\lambda_{2-3} + \lambda_{11-3}\beta)}{(\lambda_{2-3} + \lambda_{2-8})(\lambda_{3-4} + \lambda_{3-11})(\lambda_{4-5} + \lambda_{4-6})} + \lambda_{1-7}\right), \\
f = \dfrac{\lambda_{0-1}\lambda_{1-2}}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})\lambda_{6-0}}\left(\dfrac{\lambda_{3-4}(\lambda_{2-3} + \lambda_{11-3}c)}{(\lambda_{3-4} + \lambda_{3-11})(\lambda_{4-5} + \lambda_{4-6})} + \dfrac{\lambda_{9-10}(\lambda_{2-8} + \lambda_{11-9}\beta)}{(\lambda_{9-10} + \lambda_{9-11})}\right), \\
g = \dfrac{\lambda_{0-1}\lambda_{1-7}}{(\lambda_{1-2} + \lambda_{1-7})\lambda_{7-5}}, \\
h = \dfrac{\lambda_{0-1}\lambda_{1-2}\lambda_{2-8}}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})\lambda_{8-9}}, \\
i = \dfrac{\lambda_{0-1}\lambda_{1-2}(\lambda_{2-8} + \lambda_{11-9}\beta)}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})(\lambda_{9-10} + \lambda_{9-11})}, \\
j = \dfrac{\lambda_{0-1}\lambda_{1-2}\lambda_{9-10}(\lambda_{2-8} + \lambda_{11-9}\beta)}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})(\lambda_{9-10} + \lambda_{9-11})\lambda_{10-6}}, \\
k = \dfrac{\lambda_{0-1}\lambda_{1-2}\beta}{(\lambda_{1-2} + \lambda_{1-7})(\lambda_{2-3} + \lambda_{2-8})}
\end{cases}
$$

(1)

$$
\alpha = \left(\frac{1}{1 + a + b + c + d + e + f + g + h + i + j + k}\right) \qquad (2)
$$

$$
\begin{cases}
P_0 = \alpha, \\
P_1 = a\alpha, \\
P_2 = b\alpha, \\
P_3 = c\alpha, \\
P_4 = d\alpha, \\
P_5 = e\alpha, \\
P_6 = f\alpha, \\
P_7 = g\alpha \\
P_8 = h\alpha \\
P_9 = i\alpha \\
P_{10} = j\alpha \\
P_{11} = k\alpha
\end{cases} \qquad (3)
$$

В качестве вероятности успешного выявления аномалий использовано нахождение системы в состояниях, когда система реализует сохранение результата классификации или сохранения результата прогнозирования атаки (P_5 и P_6) с последующим переходом к выявлению следующий аномалии, то есть система должна эффективно работать и в штатном режиме работы(P_0). Таким образом, вероятность успешного выполнения $P_A = P_0 + P_5$ или $P_A = P_0 + P_6$.

На основе системы уравнений (3) построены графики вероятности успешного сохранения данных результата классификации или прогнозирования атаки от времени обработки данных при различном времени кодирования и структурирования информации (Рис. 2-3).

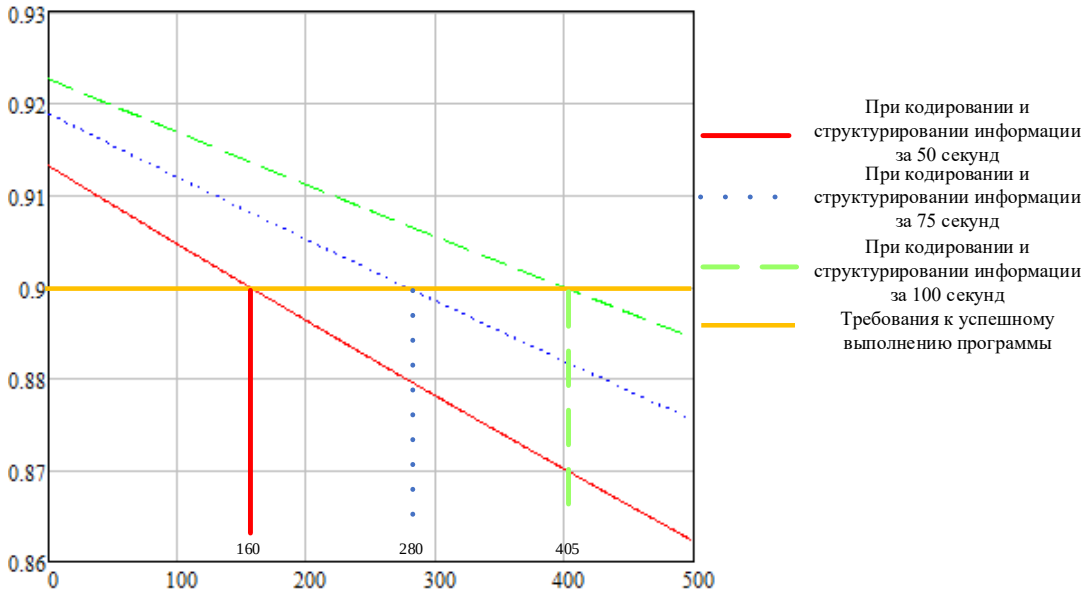

Рис. 2. Зависимости вероятности успешного сохранения данных результата классификации атаки от времени обработки данных при различном времени кодирования и структурирования информации

Исходя из вышеизложенных графиков, можно сделать вывод, что представленная модель средства сетевого контроля для выявления аномалий, раннего обнаружения и классификации атак является рациональной и эффективной.

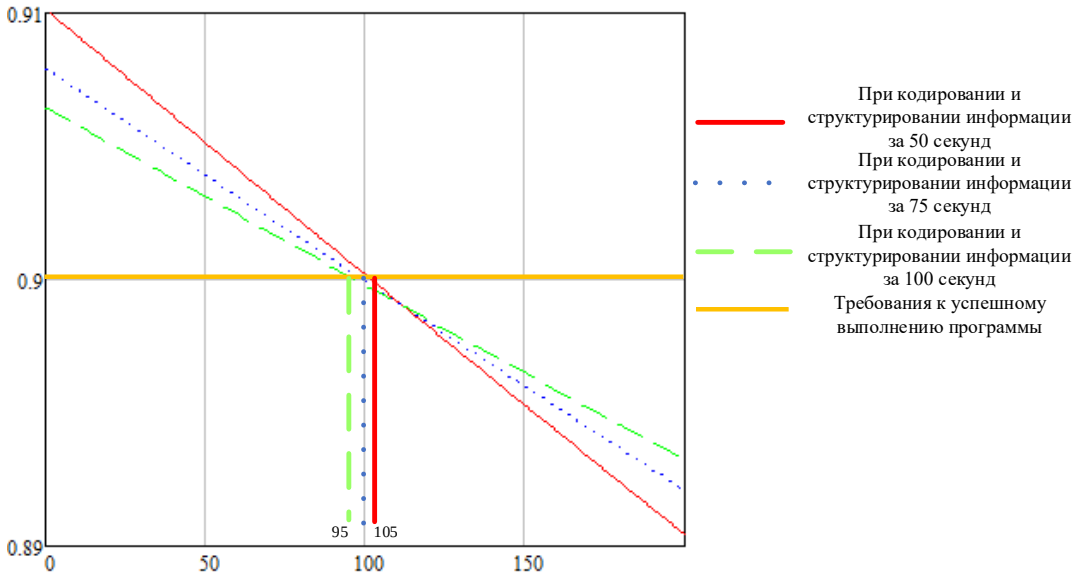

Рис. 3. Зависимости вероятности успешного сохранения данных результата прогнозирования атаки от времени обработки данных при различном времени кодирования и структурирования информации

Заключение

В ходе работы были выполнены все поставленные задачи, а именно:

1. Построена структура системы, применяющей потоковые двухслойные РНС с управляемыми синапсами, для выявления аномалий, раннего обнаружения и классификации МЭА.

2. Построен граф состояний системы, применяющей потоковые двухслойные РНС с управляемыми синапсами, для выявления аномалий, раннего обнаружения и классификации МЭА.

3. Описаны состояния системы, применяющей потоковые двухслойные РНС с управляемыми синапсами, для выявления аномалий, раннего обнаружения и классификации МЭА.

4. Проведены расчеты полученного графа состояний для расчета модели эффективности системы выявления аномалий, построены графики на основе результатов вычислений и сделаны соответствующие выводы по их результатам.

СПИСОК ЛИТЕРАТУРЫ

1. Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. № 4 (89). С. 67–76.

2. Липатников В.А., Мелихов И.А., Мелехов К.В. Особенности сетевого контроля в сети передачи данных в условиях многоэтапных атак. В сборнике: ТЕХНОЛОГИИ. ИННОВАЦИИ. СВЯЗЬ. материалы научно-практической конференции. Санкт-Петербург, 2023. С. 171-174.

3. Коршунов Г.И., Липатников В.А., Шевченко А.А., Малышев Б.Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя. Информационно-управляющие системы. 2018. № 4 (95). С. 61-72.

4. Макеев, А. С. Факторы, влияющие на эффективность управления информационной безопасностью / А. С. Макеев. – Текст: непосредственный // Молодой ученый. – 2016. – № 10 (114). – С. 66-69.

5. 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. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации. В сборнике: Технологии построения когнитивных транспортных систем. Материалы всероссийской научно-практической конференции с международным участием. 2019. -С. 207– 214;

7. Ломанов А. А., Косолапов В. С., Липатников В. А., Парфиров В. А., Шевченко А. А. Программный комплекс для распознавания аномалий в сетевом трафике на основе многокритериального классификатора в условиях угроз вторжений. Свидетельство о регистрации программы для ЭВМ 2022611916, 04.02.2022, Заявка № 2022610839 от 24.01.2022.

8. Липатников В.А., Шевченко А.А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. – 2016. – №2(94). – С. 128-140;

9. Липатников В.А., Тихонов В.А., Распознавание вторжений нарушителя при управлении кибербезопасностью инфраструктуры интегрированной организации на основе нейро-нечетких сетей и когнитивного моделирования // "Актуальные проблемы инфотелекоммуникаций в науке и образовании" VIII Международной научно-технической и научно-методической конференции сб. науч. ст. СПб. : СПбГУТ, 2018.

10. Липатников В.А., Косолапов В.С., Шевченко А.А., Сокол Д.С. Модель оценки процесса подготовки и реализации вторжений в сетях IP-телефонии. Информация и космос. 2021. № 4. С. 55-69.

Шевченко А.А.
Военная академия связи имени Маршала Советского Союза С.М. Буденного, старший научный сотрудник, к.т.н.,
alex_pavel1991@mail.ru
Роговой Н.А.
Военная академия связи имени Маршала Советского Союза С.М. Буденного, оператор роты (научной), kolyanike32@gmail.com

АНАЛИЗ ВОЗМОЖНОСТЕЙ ЗАРУБЕЖНЫХ СРЕДСТВ, ПРИМЕНЯЕМЫХ ДЛЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Введение. С развитием современных технологий информационная безопасность (ИБ) стала одним из приоритетных вопросов как для государственных, так и для частных организаций. Сети передачи данных (СПД) играют ключевую роль в современном обмене информацией, и их защита становится все более важной задачей. В виду того, что существует очень много решений, позволяющих контролировать защищенность СПД, необходимо провести анализ возможностей зарубежных средств защиты информации (СЗИ), применяемых для мониторинга ИБ СПД, для выбора наиболее подходящего продукта [1].

Решение. Для начала необходимо установить наиболее приоритетные задачи мониторинга ИБ СПД, а именно:

– контроль исключения использования заводских (простых) паролей доступа к телекоммуникационному оборудованию (ТКО), контроль за сменой паролей к ТКО СПД [2];

– контроль использования разрешенных *IP*-адресов для ТКО СПД;

– контроль легитимности подключения к ТКО СПД (с целью исключения подмены оборудования);

– контроль правильности настроек правил фильтрации, маршрутизации на ТКО СПД;

– контроль правильности настроек туннелирования на ТКО СПД;

– контроль корректности настроек *VLAN* (*VPN*) в СПД;

– контроль актуальности используемых учетных записей (настройка *DNS*-сервера и *ActiveDirectory*) в СПД;

– контроль отключения (блокированием) неиспользуемых портов ТКО СПД;

– контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через общедоступный сегмент СПД (с целью исключения передачи конфиденциальной информации);

– контроль качества каналов связи.

В целях решения вышеперечисленных задач мониторинга ИБ предприятия и организации, применяют *SIEM*-системы. Данные системы в режиме реального времени позволяют собирать информацию от систем аутентификации, СЗИ, прокси-серверов и специализированных приложений, а также из журналов событий различного ТКО, почтовых и файловых серверов и рабочих станций, в том числе из журналов аудита баз данных [3]. Такой охват информации об инфраструктуре организации позволяет *SIEM*-системам формировать наиболее объективные отчеты о защищенности информационного пространства [4]. Вся полученная информация от различных источников подвергается тщательному анализу с учетом правил, установленных администратором ИБ. Результаты анализа коррелируются с перечнем мер по нейтрализации угроз безопасности. *SIEM*-системы собирают, анализируют и уведомляют о событиях безопасности, но не предотвращают инциденты [5].

SIEM-системы являются основным инструментом в центрах мониторинга ИБ предприятий (*SOC*). Такие центры аккумулируют у себя всю информацию о инфраструктуре предприятия и о происходящих событиях ИБ в ней, проводят анализ, оповещают о нарушениях ИБ и формируют перечень необходимых мер по нейтрализации угроз.

В условиях мировой динамики ИБ следует обратить внимание на зарубежный рынок *SIEM*-систем. Зарубежные производители представляют широкий ассортимент продуктов и решений, ориентированных на обеспечение безопасности информации в СПД. Среди них выделяются несколько крупных и влиятельных компаний:

1. *IBM Security QRadar*;
2. *Splunk Enterprise Security*;
3. *Cisco SecureX*;
4. *McAfee Enterprise Security Manager*;
5. *SolarWinds Security Event Manager*.

Рассмотрим возможности некоторых *SIEM*-систем подробнее.

1. *IBM Security QRadar SIEM* – система представляет собой одно из ведущих решений на мировом рынке ИБ и предоставляет широкий набор функциональных возможностей для обнаружения и мониторинга угроз в СПД [6].

Основные преимущества и характеристики *IBM Security QRadar*:

– Сбор данных – *QRadar* может собирать данные из множества источников, включая журналы событий, сетевой трафик, системы сетевого оборудования, а также данные от конечных точек и приложений. Это позволяет системе иметь обширное представление о состоянии сети и активностях авторизированных пользователей.

– Корреляция событий – *QRadar* использует мощные алгоритмы корреляции для выявления связанных событий и инцидентов. Это помогает сократить количество ложных срабатываний и выявлять действительно важные угрозы.

– Обнаружение аномалий – система осуществляет анализ данных и выявляет аномальные паттерны, что позволяет быстро обнаруживать необычное поведение и потенциальные угрозы.

– Управление угрозами – *QRadar* предоставляет средства для классификации и приоритизации угроз, а также для реагирования на них. Система может автоматически блокировать потенциально опасные действия или отправлять уведомления администраторам.

– Соответствие стандартам безопасности – *QRadar* помогает организациям соблюдать требования стандартов безопасности и нормативных актов.

IBM Security QRadar SIEM имеет сертификат ФСТЭК России № 3354, подтверждающий выполнение функций мониторинга результатов регистрации событий безопасности и реагирования на них в соответствии с требованиями технических условий.

IBM Security QRadar SIEM представляет собой мощное решение для обеспечения безопасности информации в сетях передачи данных. Его функциональность позволяет организациям мониторить и защищать свои сети от разнообразных угроз, а также эффективно реагировать на инциденты.

Анализ возможностей IBM Security QRadar SIEM показал, что данный комплекс позволяет решать большую часть частных задач мониторинга ИБ, однако в данной системе не реализован контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через сети связи, а также контроль качества каналов связи.

2. *Splunk Enterprise Security* – это инструмент, позволяющий собирать, хранить, обрабатывать и анализировать данные от устройств и систем. Данную систему по большей части используют компании США и Европы, однако в последнее время её начинают применять организации по всему миру, включая Россию [7]. *Splunk Enterprise Security* отличает от других *SIEM*-систем то, что она способна черпать данные из практически любых источников, что и выводит её на передовые позиции мирового рынка средств мониторинга ИБ.

В связи с стремительным развитием технологий машинного обучения и искусственного интеллекта компанией *Splunk* был разработан модуль, который позволяет проводить расширенный анализ информации об ИБ, прогнозировать развитие воздействия, а также обнаруживать аномальную активности. Данный модуль успешно введён в состав *Splunk Enterprise Security*, что делает его ещё привлекательней для реализации мониторинга ИБ.

Преимущества *Splunk Enterprise Security* представлены на рисунке 1.

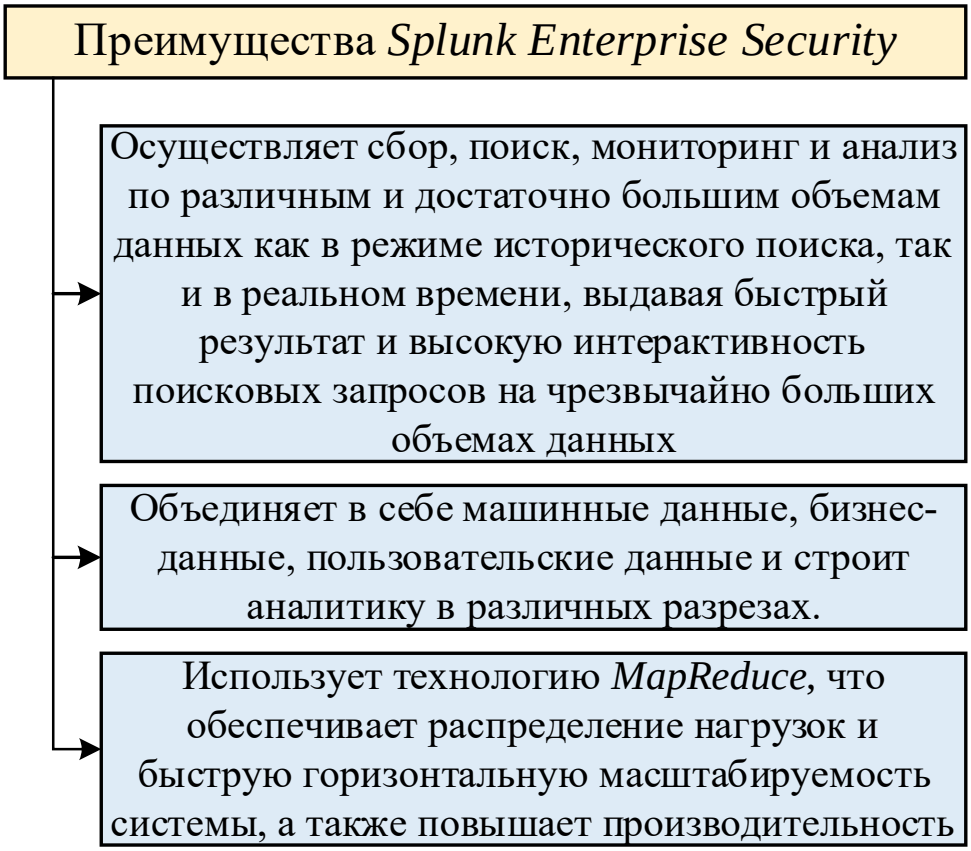

Рисунок 1 – Преимущества *Splunk Enterprise Security*

Анализ возможностей *Splunk* показал, что данный комплекс позволяет также решать большую часть частных задач мониторинга ИБ, однако в данной системе не реализован контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через сети связи, а также контроль качества каналов связи.

3. *McAfee Enterprise Security Manager* – инструмент, разработанный компанией *McAfee*, для организации мониторинга ИБ информационных систем и сетей [8].

McAfee Enterprise Security Manager (*ESM*) возможно приобрести в качестве программно-аппаратного комплекса, либо в качестве программного обеспечения. В сосав системы входит *ESM, Event Receiver* и *Enterprise Log Manager*. Каждый из компонентов системы могут быть развернуты отдельно друг от друга, так и вместе. Также данная компания представляет ряд дополнительных компонент: *Advanced Correlation Engine* – компонент, который выполняет контроль данных в режиме реального времени, использует две системы корреляции событий с целью обнаружения рисков и угроз до их возникновения; *Database Event Monitor* – компонент, отвечающий за сбор информации о транзакциях в базах данных без ущерба для быстродействия; *Application Data Monitor* – компонент, который выполняет выявление угроз на уровне приложения и *Global Threat Intelligence* – компонент, позволяющий работать с большими данными о безопасности организации.

Преимущества *McAfee Enterprise Security Manager* представлены на рисунке 2 [9].

McAfee SIEM имеет сертификат ФСТЭК России № 3353, подтверждающий выполнение функций мониторинга результатов регистрации событий безопасности и реагирования на них в соответствии с требованиями Технических условий.

Анализ возможностей *McAfee Enterprise Security Manager* показал, что данный комплекс позволяет также решать большую часть частных задач мониторинга ИБ, однако в данной системе не реализован контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через сети связи, а также контроль качества каналов связи [10].

Рисунок 2 – Преимущества *McAfee Enterprise Security Manager*

Заключение. Результаты анализа зарубежных средств, применяемых для мониторинга ИБ, говорят о том, что в последние годы зарубежные решения в области системы комплексной безопасности и мониторинга ИБ продемонстрировали значительное развитие и успешно конкурируют на глобальном рынке. Однако, они не в полной мере позволяют решать приоритетные задачи мониторинга ИБ, так как в них не реализован контроль содержания информационных сообщений и вложенных в них файлов, передаваемых через сети связи, а также контроль качества каналов связи. В связи с чем необходимо устанавливать дополнительные системы, что влечет избыточность, влияющую на объемы вычислительных мощностей, необходимых для эксплуатации всех продуктов, обеспечивающих ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Бутакова, Н.Г. Анализ интеграции средств мониторинга и аудита информационной безопасности корпоративной сети / Н.Г. Бутакова, А.А. Трунова // REDS: Телекоммуникационные устройства и системы. – 2017. – Т. 7, № 4. – С. 534-538.
2. Шевченко, А.А. Предложения по построению упреждающей системы управления информационной безопасностью информационной системы / А.А. Шевченко // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 14–15 октября 2020 года. – Санкт-Петербург: ФГКВОУВО «Военная академия связи имени Маршала Советского Союза С.М. Буденного» МО РФ, 2020. – С. 248-256.
3. Соколов, А.М. Современные решения в области информационной безопасности локальных сетей / А. М. Соколов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы XIII Межрегиональной научно-практической конференции, Брянск, 30 апреля 2021 года. – Брянск: Брянский государственный технический университет, 2021. – С. 244-248.
4. Липатников, В.А. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией / В.А. Липатников, А.А. Шевченко, А.Д. Яцкин, Е.Г. Семенова // Информационно-управляющие системы. – 2017. – № 4(89). – С. 67-76. – DOI 10.15217/issnl684-8853.2017.4.67.
5. Попов, С.В. Определение вероятностей состояний функционирования средства контентного анализа как элемента системы мониторинга инцидентов информационной безопасности / С.В. Попов, В.Н. Шамкин // Вестник Тамбовского государственного технического университета. – 2012. – Т. 18, № 1. – С. 27-37.
6. Липатников, В.А. Метод адаптивного управления защитой информационновычислительных сетей на основе анализа динамики

действий нарушителя / Г.И. Коршунов, В.А. Липатников, А.А. Шевченко, Б.Ю. Малышев // Информационно-управляющие системы. – 2018. – № 4(95). – С. 61-72. – DOI 10.31799/1684-8853-2018-4-61-72.

7. Нашивочников, Н.В. Применение аналитических средств в системе операционного мониторинга и анализа безопасности кибер-физических систем для предприятийтопливно-энергетического комплекса / Н. В. Нашивочников, А. А. Лукашин, А. А. Большаков // Математические методы в технике и технологиях - ММТТ. – 2019. – Т. 2. – С. 63-67.
8. Липатников, В.А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры / В. А. Липатников, А. А. Шевченко // Информационные системы и технологии. – 2016. – № 2(94). – С. 128-140.
9. Гончарова, Т.С. Сравнение и выбор средств мониторинга событий информационной безопасности / Т.С. Гончарова // Colloquium-Journal. – 2019. – № 28-2(52). – С. 20-22.
10. Бухарин, А.В. Способ прогнозирования состояния объектов связи и информации / А. В. Бухарин, А. С. Ишимов, П. И. Кузин [и др.] // Телекоммуникации. – 2023. – № 2. – С. 16-22. – DOI 10.31044/1684-2588-2023-0-2-16-22.

Борисова В.В., студент 3-го курса, Дальневосточный федеральный университет, borisova.vvl@dvfu.ru
Дегтярев Д.В., студент 2-го курса, Дальневосточный федеральный университет, degtyarev.dv@dvfu.ru
Макаров А.Г., к.ф.-м.н., доцент департамента информационной безопасности ИМКТ ДВФУ, научный сотрудник ИПМ ДВО РАН, makarov.ag@dvfu.ru
Боршевников А.Е., и.о. директора департамента информационной безопасности ИМКТ ДВФУ, borshevnikov.ae@dvfu.ru
Солдатов К.С., к.ф.-м.н., доцент департамента теоретической физики и интеллектуальных технологий ИНТиПМ ДВФУ,и.о. заведующего лабораторией вычислительной информатики ИПМ ДВО РАН, soldatov_ks@dvfu.ru
Нефедев К.В., д.ф.-м.н., профессор, директор департамента теоретической физики и интеллектуальных технологий ИНТиПМ ДВФУ, ведущий научный сотрудник ИПМ ДВО РАН , nefedev.kv@dvfu.ru

РЕАЛИЗАЦИЯ АЛГОРИТМА КВАНТОВОЙ ФАКТОРИЗАЦИИ ШОРА

Сегодня информационная безопасность постоянно меняется из-за новых угроз, и исследования в области квантовых вычислений становятся все более важными. Алгоритм квантовой факторизации Шора, разработанный Питером Шором в 1994 году, является одним из наиболее известных квантовых алгоритмов и имеет вероятностный характер. Он обеспечивает возможность эффективного разложения больших составных чисел на простые множители за полиномиальное время при использовании квантовых компьютеров [1].

Основная идея алгоритма Шора заключается в использовании квантового параллелизма и интерференции для эффективного нахождения периода функции, связанной с факторизуемым числом. Зная период, можно легко найти простые множители числа. Алгоритм Шора имеет огромное значение в области квантовых вычислений и криптографии, так как он представляет

потенциальную угрозу для современных криптографических систем, основанных на сложности факторизации больших чисел [2].

Разложение больших чисел на простые множители является вычислительной задачей, сложность которой растет экспоненциально с увеличением числа для классических алгоритмов [3]. Существует несколько эффективных классических алгоритмов факторизации, такие как метод квадратичных форм Шенкса и алгоритм Полларда-Штрассена, которые имеют временную сложность порядка $O(N^{1/5+\varepsilon})$ и $O(N^{1/4}\log^4 N)$ соответственно, где N – число, которое необходимо разложить на простые множители [4]. В то же время квантовый алгоритм Шора имеет временную сложность порядка $O(\log^3 N)$ на квантовом компьютере [5]. Таким образом, данный алгоритм значительно быстрее классических алгоритмов факторизации.

Реализация алгоритма Шора на квантовых компьютерах представляет свои сложности, так как требуется наличие достаточно большого и стабильного квантового компьютера с достаточным количеством кубитов и низким уровнем ошибок. Кроме того, необходимо разработать эффективные методы для управления и контроля квантовыми состояниями и операциями. На данный момент квантовые компьютеры находятся в разработке и не являются доступными для широкого использования.

Алгоритм Шора для факторизации больших чисел [6] состоит из двух частей: классической и квантовой. В классической части алгоритма выбирается случайное число a, которое должно быть взаимно простым с N, и вычисляется $\text{НОД}(a,\ N)$. Если $\text{НОД}(a,\ N)$ не равен 1, то a уже является нетривиальным делителем числа N, и факторизация завершена. Если $\text{НОД}(a,\ N)$ равен 1, то переходим к квантовой части алгоритма. В квантовой части алгоритма (Рис. 1), инициализируются два квантовых регистра x и y, применяется преобразование Адамара ко всем кубитам первого регистра, применяется модулярная функция $f(x) = a^x \bmod N$, используется управляемый унитарный оператор, который применяет операцию умножения на x к каждому состоянию первого регистра, в зависимости от значения второго регистра, выполняется фиктивное измерение

второго регистра, применяется обратное квантовое преобразование Фурье к первому регистру, и затем выполняется измерение первого регистра. После измерения состояний в регистре x, получаем случайное число x_0, которое содержит приближенное значение периода r функции $f(x)$. Приближенное значение периода r можно вычислить с использованием метода непрерывных дробей или других численных методов. После получения приближенного значения периода r, мы можем использовать это значение для определения множителей числа N с помощью классических алгоритмов [7], таких как алгоритм Евклида. Мы вычисляем НОД(N, $a^{r/2} \pm 1$), где a – случайное целое число, которое мы выбирали для создания модулярной функции. Если полученный НОД является нетривиальным делителем числа N, то мы нашли успешное разложение N на множители. Если $a^{r/2} \equiv -1 \, mod \, N$ или если полученный НОД не является нетривиальным делителем N, то мы возвращаемся к началу алгоритма, выбирая другое случайное a и повторяя процесс снова.

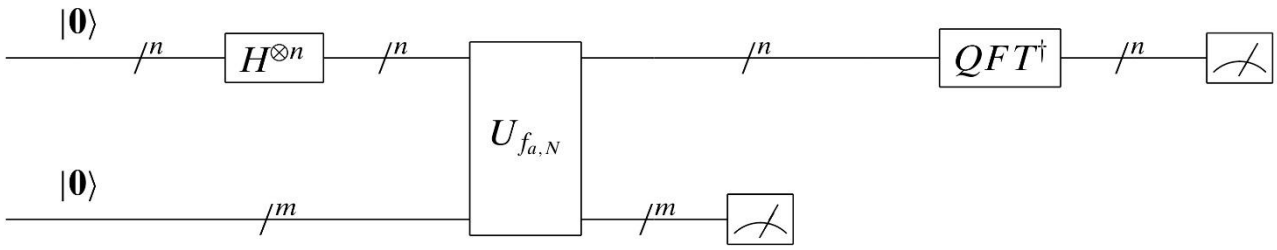

Рис. 1. Квантовая схема реализации алгоритма Шора

В результате исследования алгоритм Шора был реализован на эмуляторе 4-х кубитного квантового компьютера, написанном на языке программирования Python с использованием библиотеки Qiskit [8]. Было разложено число 15 на простые множители 3 и 5, получена схема для квантового компьютера, а также диаграмма результатов измерения состояния кубитов. Также алгоритм Шора был протестирован на реальном квантовом компьютере IBM [9].

На диаграмме результатов измерений состояний кубитов (Рис. 2) заметно, что период функции составляет 4, поскольку присутствуют четыре выраженных столбика вероятностей состояний кубитов. Важно отметить, что при взаимодействии различных путей вычисления в алгоритме Шора вероятности различных результатов могут накладываться друг на друга, вызывая интерференцию. Это может привести к тому, что некоторые столбики вероятностей будут выделяться, но в общем распределение вероятностей становится более равномерным.

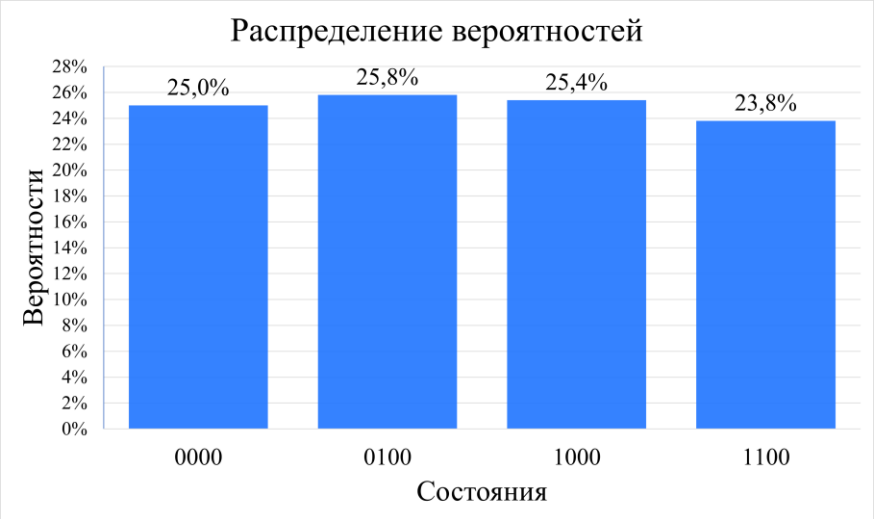

Рис. 2. Результаты измерений на эмуляторе

По результатам тестирования алгоритма Шора на реальном квантовом компьютере IBM была получена диаграмма (Рис. 3), которая отличается от диаграммы, полученной с помощью эмулятора.

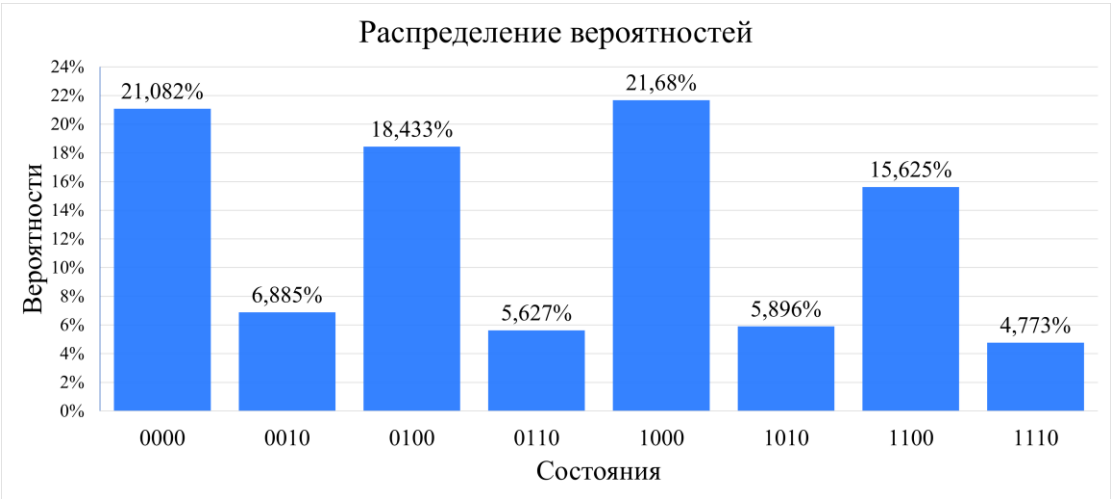

Рис. 3. Результаты измерений на реальном квантовом компьютере IBM

При сравнении с идеальными условиями, полученными при помощи эмулятора на языке Python, наблюдается добавление четырех дополнительных пиков с низкой вероятностью. Это объясняется высокой степенью погрешности, вызванной нестабильными состояниями кубитов, подверженных воздействию различных факторов окружающей среды. При увеличении числа, подлежащего факторизации, период также увеличится, что приведет к формированию более широкого распределения и увеличит количество столбиков вероятностей. Следовательно, процесс вычисления столбиков вероятностей становится более трудоемким, и точность измерений снижается, возможно, даже до такой степени, что это может привести к недостоверным результатам.

Проблема факторизации имеет большое значение в криптографии, так как многие криптографические протоколы основаны на сложности разложения на простые множители. Например, алгоритм RSA, широко используемый для шифрования данных, основан на трудности факторизации больших составных чисел [10]. Квантовые компьютеры могут быть использованы для взлома криптосистем, основанных на проблеме факторизации больших чисел. Для обеспечения безопасности в условиях наличия квантовых компьютеров необходимо разработать квантово-устойчивые алгоритмы шифрования, которые используют квантовые свойства для обеспечения безопасности передачи информации.

Проведенные исследования подтверждают эффективность алгоритма квантовой факторизации Шора на практике, который может использоваться для разложения больших чисел на простые множители, что недоступно для обычных компьютеров. В будущем планируется продолжить исследования и разработки, связанные с квантовым алгоритмом Шора. Рассматривается возможность увеличения числа кубитов на квантовых компьютерах, оптимизацию процессов подготовки кубитов, а также исследование новых областей применения алгоритма в криптографии, включая разработку более надежных методов шифрования и дешифрования, устойчивых к атакам с

использованием квантовых компьютеров. Эти разработки будут способствовать обеспечению безопасности данных и информации, особенно учитывая будущее влияние квантовых вычислений на криптографию.

СПИСОК ЛИТЕРАТУРЫ

1. Сысоев, С.С. Введение в квантовые вычисления. Квантовые алгоритмы: учеб. пособие / С.С. Сысоев // СПб.: Изд-во С.-Петерб. ун-та. - 2019. - 144 с.
2. Калачев, А.А. Квантовая информатика в задачах: учеб.-метод. пособие / А.А. Калачев // Казань: Казан. ун-т. — 2012. — 48 с.
3. Нильсен, М. Квантовые вычисления и квантовая информация / Н. Нильсен, И. Чанг; Пер. с англ. М.Н. Вялого; под ред. П.М. Островского // М.: Мир. — 2006. — 824 с.
4. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко // М.: МЦНМО. — 2003. — 328 с.
5. Hayward, M. Quantum computing and Shor’s algorithm / M. Hayward // Sydney: Macquarie University Mathematics Department. — 2008. — V. 1.
6. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P.W. Shor // Foundations of Computer Science: Conference Publications. — 1997. — P. 1484-1509.
7. Дасгупта, С. Алгоритмы / С. Дасгупта, Х. Пападимитриу, У. Вазирани; Пер. с англ. А.С Куликова; под ред. А. Шеня // М.: МЦНМО. — 2014. — 320 с.
8. Душкин, Р.В. Квантовые вычисления и функциональное программирование / Р.В. Душкин // Москва: ДМК Пресс. — 2015. — 232 с.
9. Вахний, Т.В. Выполнение простейших вычислений на квантовом компьютере IBM Q System One / Т.В. Вахний, А.К. Гуц, А.В. Овчинников // Математическое и компьютерное моделирование: сборник. - 2021. - 328 с.
10. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо // Москва: Постмаркет. — 2001. — 328 с.

Звежинский С.С.,
д.т.н., профессор кафедры «Информационная безопасность» МТУСИ,
zwierz@rambler.ru
Альбов Н.А.,,
магистрант МТУСИ,
albov2000@yandex.ru

ВИДЕО РАСПОЗНАВАНИЕ ЛИЦ ЛЮДЕЙ В СЛОЖНЫХ УСЛОВИЯХ

Общие положения

Распознавание (идентификация) людей по их лицам, в сравнении с другими биометрическими технологиями (отпечатки пальца, радужка и сетчатка глаза и пр.), имеет определенные преимущества вследствие незаметного и дистанционного съема информации, быстроты принятия решений, высокой функциональной надежности работы в типовых условиях. Интеллектуальные системы видео распознавания играют большую роль в создании городской системы безопасности, обеспечивая бесконтактные платежи и пр. Ведущими мировыми производителями систем интеллектуального видео являются Китай и Великобритания, - последняя предпочитает построение систем безопасности с упором именно на видео, а не охранную сигнализацию или систему контроля и управления доступом (СКУД), как в России.

Система распознавания лиц людей - это, по сути, программно-аппаратный комплекс (ПАК), сопоставляющий текущую информацию с видеокамер (ВК) с эталонной информацией из базы данных (БД), хранящей биометрические признаки людей – фото лиц или их математические образы. Типично такой ПАК состоит из двух основных компонентов:

- «железа» в виде IP-ВК и сервера (персонального компьютера);
- «софта» в виде общефункциональной платформы (Windows, Linux) и СПО, реализующего интеллектуальный алгоритм распознавания образов (лиц).

Видео распознавание подразделяется на 2D- (двумерное) и 3D- (трехмерное). Первые хранят в БД и используют обычные «плоские» фотоизображения, полученные с одной ВК. Вторые используют объемные образы лиц, полученных с помощью 2-х ВК и соответствующего математического преобразования. Более перспективной общепризнана 3D-технология, однако из-за её повышенной стоимости 2D-системы также находят применение, хотя по функциональной надежности они принципиально хуже.

С каждым годом системы видео распознавания используют все более «продвинутые» математические алгоритмы: от практически ручного поиска ключевых точек на лице (в 1960-х гг.) до современных алгоритмов, основанных на искусственных нейронных сетях (ИНС). При этом возросли не только точность распознавания, но и объем обрабатываемой информации, реализуя системы безопасности с тысячами ВК. Это обеспечило повышенное внимание не только государственных, но и частных компаний-инвесторов; например, за 2022 г. спрос на распознавание лиц со стороны финансового, страхового, промышленного и телеком бизнеса вырос в 1,5 раза [1].

У этой IT-технологии имеется серьёзный недостаток – существенное снижение точности распознавания при частично закрытых или измененных лицах (медицинские маски, грим и пр.), а также неблагоприятных факторах сцены (плохое освещение, ракурс и пр.). Ведущие разработчики продолжают непрерывные усилия по улучшению СПО, ниже представлен анализ алгоритмов распознавания лиц людей при неблагоприятных факторах.

История развития алгоритмов распознавания лиц

Первые попытки создания устойчивого алгоритма распознавания частично закрытых лиц относятся к 2010-13 гг. Они основывались либо на обнаружение текстур, присущих ключевым точкам лица (фильтры Габора), либо на использовании вероятностных моделей, фиксирующих взаимосвязь между значениями пикселей и соответствующими ключевыми точками. Удачным продуктом стал алгоритм *State-of-the-art*, основанный на двухэтапном

процессе идентификации обнаруженных элементов лиц [2]:

1. Изображение делилось на несколько сегментов, каждый определялся как часть лица, формируя набор областей для дальнейшего распознавания.

2. Набор областей сравнивался с теми же наборами областей эталонных лиц посредством метода локальных бинарных шаблонов. Далее использовалась метрика хи-квадрат (χ^2) для подтверждения сходства объектов.

Данный алгоритм достиг показателя точности порядка 67%, что уступало (примерно на 20%) в сравнении с результатами распознавания «открытых» людей для выбранного набора данных. Другие попытки, основанные на классических «жестких» решениях, приводили к аналогичным результатам.

Точность распознавания алгоритмов заметно возросла только после внедрения технологии свёрточных нейроных сетей (CNN) - архитектуры ИНС, предложенной в 1988 г. В 2017 г. был представлен нейросетевой алгоритм *Spartial Fusion* с повышенной точностью распознавания частично закрытых лиц, основанный на выявлении 14-и ключевых точек лица (рис.1а) [3]. После этого алгоритм строит геометрический образ, соединяя точки между собой и создавая шаблон (набор) углов, отражающих характерные черты лица человека (рис.1б). Далее вычисляется суммарная разница между углами на эталонном и полученном изображении, и если она не превышает порога, то делается вывод, что изображения (текущее и эталонное) принадлежат одному лицу.

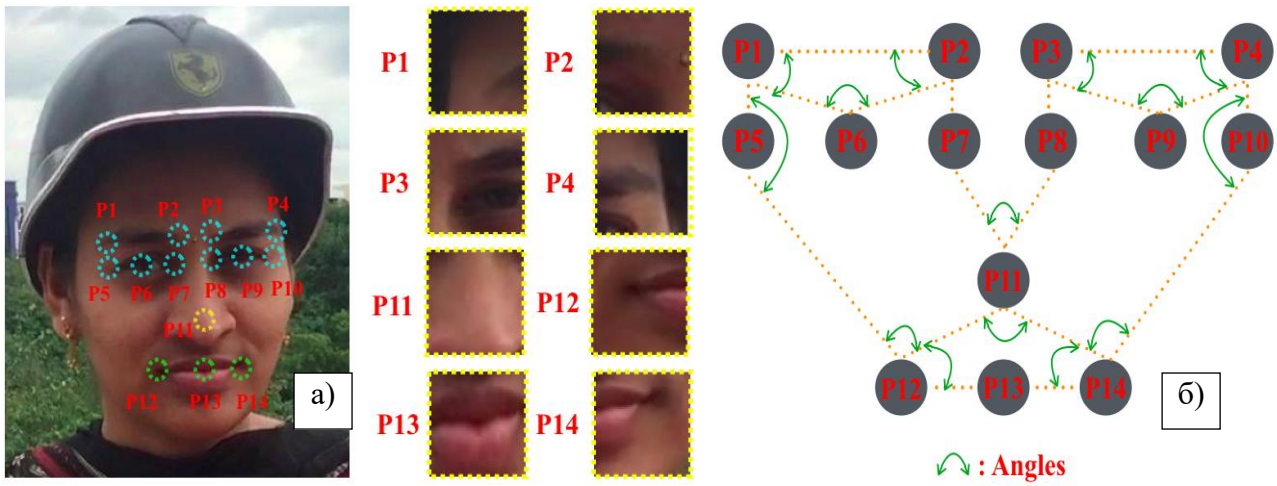

Рисунок 1 – Алгоритм Spartial Fusion: а) ключевые точки; б) шаблон

Точность работы *Spartial Fusion* по сравнению с аналогами повысилась примерно на 15 %, однако распознавание на контрастном фоне, при частичном повороте или закрытии лиц оставляло вопросы. Тем не менее, этот алгоритм выявил «генеральную линию» дальнейшего совершенствования алгоритмов распознавания лиц, основанных именно на *CNN*, прежде всего, путем увеличения числа ключевых точек.

В 2019 г. был предложен алгоритм, разделяющий изображение на его общепринятые части (глаза, щёки, губы и т.д.) с помощью т.н. предобученной модели *VGGF model* [4]. Обнаруженные элементы лица классифицировались с помощью метода опорных векторов или меры косинусной близости. Результаты этой и последующих работ показали, что алгоритмы CNN удовлетворительно распознают человека, имея информацию о половине и более лица, и показали значительное снижение точности при повороте (более 50 град.) даже незакрытого лица (рис.2).

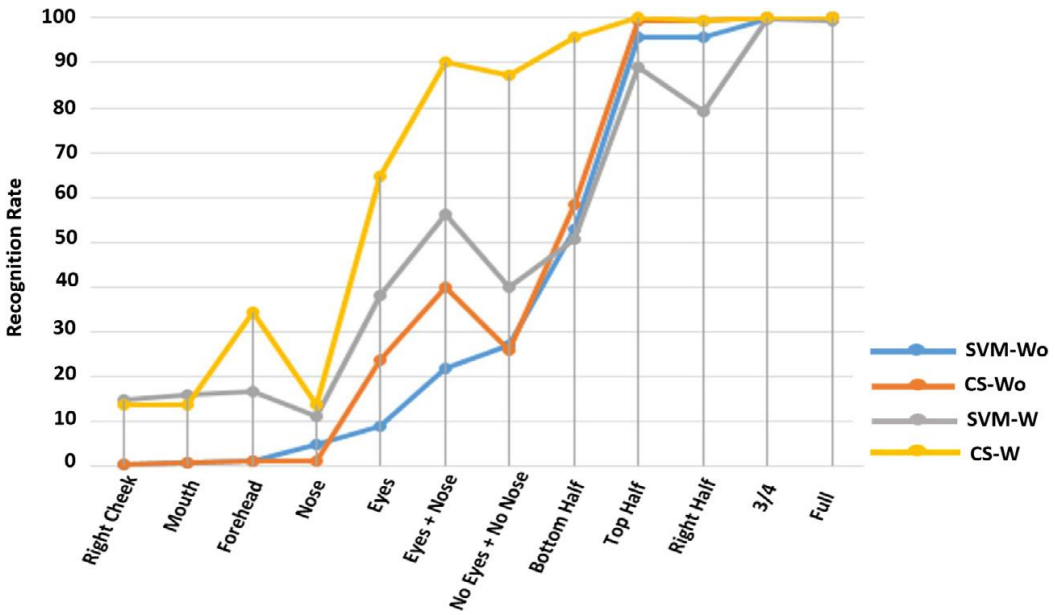

Рисунок 2 – Точность распознавания 4-х CNN в зависимости от доступной информации о лице

Тем не менее, алгоритмы CNN, показывая в типовых условиях сцены (хорошее освещение, фас и пр.) высокую функциональную надежность

(точность более 98%), стали внедряться по всему миру. Проблема явно обозначилась при введении тотального масочного режима во время эпидемии COVID-19, было выявлено влияние и таких потенциальных сложностей, как плохие освещение, качество съемки и пр. Разработчики СПО получили возможность наработать и исследовать огромную реальную БД «особых случаев», которую невозможно было собрать в предыдущие годы. Это продвинуло и кратно увеличило число исследований по видео распознаванию.

Таким образом, к 2021 г. было предпринято множество попыток создания алгоритма распознавания, близкого к идеальному с точностью не менее 99%, способного работать с «неидеальными» данными, которые заложили основу для современных нейросетевых алгоритмов. В 2021-22 гг. появилось несколько публикаций, в которых переосмыслен опыт пандемии и предложены новые подходы к распознаванию лиц в масках.

Новейшие алгоритмы распознавания частично закрытых лиц

У разработчиков СПО теперь наличие маски или частичное закрытие лица, как правило, предполагается в тестах на оценку функциональной надежности. Тем не менее, пока единого методического подхода к решению не выявлено, и новые СПО используют различные математические модели. Предпочтение в целом отдается свёрточным нейронным сетям (CNN), а разница заключается в способах захвата изображения и его предобработки.

В 2021 г. был предложен метод распознавания (и соответствующий алгоритм), основанный на объединении 2-х подходов: большее значение придавалось зоне лица вокруг глаз, а изображение по-прежнему обрезалось на уровне верхней границы маски [5]. Такой подход стал возможен благодаря внедрению в структуру сети т.н. CBAM-блоков, увеличивающих веса отдельных нейронов. Алгоритм позволил увеличить точность распознавания лиц в масках, при отсутствии оригинального «чистого» изображения, до 83%.

В том же году был предложен подход, являющийся сочетанием метода главных компонент для восстановления полного образа лица без маски, с

применением CNN [6]. Захваченное изображение разделялось на зону с маской и без неё, и для каждой (по подготовленному заранее набору лиц) вычислялось «среднее». Собственные вектора, найденные для открытой части, применялись для реконструкции закрытой части лица, после чего изображения объединялись. Для дальнейшего распознавания лиц использовалась нейросеть *FaceNet*, которая увеличила точность до 90±5% против 80%.

Альтернативный подход был предложен в 2023 г., и позволил еще немного улучшить точность распознавания [7]. Его суть состоит в добавлении к изначальному набору «эталонных лиц» изображения маски, и дальнейшей классификации лиц с помощью CNN. Данный алгоритм, по уверениям авторов, позволил добиться точности 95% при распознавании лиц в масках. Это, однако, требует расширения апробации алгоритма в разнообразных условиях сцены.

Таким образом, на настоящий момент времени видео распознавание лиц в сложных условиях сцены приблизилось к точности 95%. С точки зрения построения СКУД это непозволительно, и на порядки уступает другим биометрическим технологиям (например, по радужке глаза). Однако для комплексной безопасности, в качестве системы поддержки принятия решения, достигнутый уровень надежности уже можно считать вполне приемлемым.

Перспективы и проблемы технологии видео распознавания лиц

Перспективы технологии видео распознавания основаны на том, что:

- стоимость требуемого оборудования («железо») продолжает снижаться с каждым годом, и оно становятся более доступным;
- она находит применение не только в городской системе безопасности, но и на объектах с масочным режимом, - поликлиниках, вредном производстве;
- ее интегрирование с другими технологиями, даже не очень надежными, но дешевыми (например, по голосу), позволяет увеличить в целом надежность работы ПАК.

Можно выделить некоторые проблемы (недостатки), присущие современным интеллектуальным алгоритмам видео распознавания:

- проблема близнецов не может быть решена, хотя имеются обнадеживающие результаты, связанные с термограммами лиц;
- на текущий момент уже существуют решения, позволяющие создать 3D-маску, практически идентичную оригинальному лицу человека;
- не выработано единого методического подхода к оптимальному распознаванию лиц в масках (не доказано, что CNN – лучшее решение);
- менеджмент компании может собирать биометрические данные сотрудников и посетителей без их согласия, и в случае взлома БД эти люди могут подвергаться слежке со стороны злоумышленников.

Внедрение распознавания лиц и особенности российского рынка

При внедрении видео распознавания необходимо учитывать то, что:

- обеспечение безопасного хранения биометрических персональных данных повышает требования к системе ИБ в целом;
- перед проектированием ПАК полезно ознакомиться со стандартом BSEN 62676-4:2015, - в отечественном законодательстве аналога нет [8];
- особенности сцены съемки пока еще играют большую роль, и для максимальной точности следует располагать ВК на высоте 1,5…2,0 м (уровне глаз человека);
- желательно, чтобы модель ВК для «эталонных» изображений была идентичной тем, которые используются для получения текущего изображения;
- необходим тщательный подбор порога решения, обеспечивающего известный компромисс между ошибками 1-го и 2-го рода [9].

За последнее время в России достигнут существенный прогресс в сфере IT-технологий обеспечения безопасности, что не обошло стороной и распознавание лиц. Особенности российского рынка следующие:

- В России имеются около 10-и компаний-разработчиков СПО в сфере распознавания видео образов, конкурирующих на рынке с мировыми брэндами Google, Apple и пр.

- Основной спрос на видео распознавание приходится на государство; так московская мэрия применяет в метро технологии компании NtechLab.
- Российская законодательная база в данной области находится в процессе разработки, уже существуют закон о хранении биометрических данных [10], но этого явно недостаточно.
- Вне Москвы и нескольких крупных городов (Санкт-Петербург, Казань и др.) данная технология внедряется низкими темпами, поэтому в провинции имеются большие потенциальные возможности для развития этого бизнеса.
-

Заключение

За последнее десятилетие предприняты многочисленные попытки улучшения качества видео распознавания лиц в сложных условиях: к 2023 г. в лучших из них, основанных на сверточных нейронных сетях, достигнута точность порядка 95%. Однако так и не было определено, где предел надежности этой технологии (например, максимум точности). Тем не менее, технология продолжает внедряться в системы безопасности крупных городов России, реагируя на вводимые условия масочного режима. К ее недостаткам можно отнести пока еще зависимость точности от условий сцены, остро стоит также вопрос защиты обрабатываемых биометрических данных.

В России перспективы видео распознавания лиц связаны, прежде всего, с крупными городами, где имеется метро. Появляются нормативные акты, регулирующих данную IT-сферу, упрощающие проектирование и согласование. Можно спрогнозировать существенный рост этого сегмента российского рынка, чего нельзя сказать о повышении его качества. По-видимому, точность распознавания в неблагоприятных условиях (в т.ч. людей в масках) не превысит величину 97…98%, а этого недостаточно для его использования в СКУД.

СПИСОК ИСТОЧНИКОВ

1. Корнев Т., Мерцалова А. Распознавание лиц требует ясности // «Коммерсантъ», 29.03.2023.

2. Martinez B. et al. Local evidence aggregation for regression-based facial point detection // IEEE Trans. on Pattern Analysis and Machine Intelligence. 2013. 35(5).

3. Singh A., Patil D., Reddy G. Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network // IEEE Int. conf. on Computer Vision Workshops. 2017.

4. Elmahmudi A.A., Ugail H. Deep face recognition using imperfect facial data // Future Generation Computer Systems. 2019. № 99.

5. Li Y. et al. Cropping and attention based approach for masked face recognition // Applied Intelligence: Dordrecht. 2021.

6. Malakar S. et al. Masked Face Recognition Using Principal component analysis and Deep learning // Int. conf. on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). 2021.

7. Abbas S.M., Abdulameer M.H. Masked Face Recognition Using Convolutional Neural Networks // Jour. of Kufa for Mathematics and Computer. 2023. № 10.

8. BS EN 62676-4:2015: Video surveillance systems for use in security applications. Application guidelines. 2015.

9. https://www.videonet.ru/rekomendaczii-po-nastrojke-raspoznavaniya-licz.html.

10. Федеральный закон РФ от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных…», 2022.

Секция 3

ПРОБЛЕМЫ ЦИФРОВОГО СУВЕРЕНИТЕТА И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Руководители: **Крылов Григорий Олегович**,
Московский технический университет связи и информатики, профессор кафедры «Безопасность телекоммуникаций», Финансовый университет при Правительстве Российской Федерации, профессор, доктор физико-математических наук, профессор

Буряков Виктор Михайлович,
Московский технический университет связи и информатики, ассистент кафедры «Безопасность телекоммуникаций»

Пахомов М.А.
ФГАОУ ВО «СПбПУ»,
Институт компьютерных наук и кибербезопасности,
аспирант,
pahomov.ma@yandex.ru
Павленко Е.Ю.
ФГАОУ ВО «СПбПУ»,
Институт компьютерных наук и кибербезопасности,
к.т.н., доцент
pavlenko_eyu@spbstu.ru
Сорокин А.А.
ФГАОУ ВО «СПбПУ»,
Институт компьютерных наук и кибербезопасности,
студент,
sorokin2.aa@edu.spbstu.ru

РАЗРАБОТКА ПРОТОКОЛА БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ MANET-СЕТЕЙ

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки молодых российских ученых - кандидатов наук МК-3861.2022.1.6

Развитие мобильных технологий привело к созданию отрасли, производящей доступные мобильные устройства с унифицированными стандартами беспроводной связи. Их повсеместное распространение приводит к формированию интереса исследования самоорганизующихся сетей, которые способны функционировать без каких-либо требований к инфраструктурным решениям.

Физическая открытость сетей, организованных беспроводными каналами связи, а также невозможность исключить вероятность появления внутреннего

нарушителя, формулируют широкий спектр задач, которые должны решаться протоколом безопасной маршрутизации MANET-сетей.

Атаки, связанные с воздействием на участников сети для нарушения корректного функционирования протокола маршрутизации, делятся на пять категорий [1]. Сравнительный анализ подходов к обеспечению безопасной маршрутизации и их возможности противодействия классам атак представлен в Табл.1.

Табл. 1. Сравнение подходов к обеспечению безопасной маршрутизации

Класс атак	**Предотвращение**	**Обнаружение**	**Обозначение**
Атаки на идентифицирующую информацию	+	-	A1
Модификация управляющего трафика	+	+	A2
Подделка управляющих сообщений	+	-	A3
Удаление пакетов	-	+	A4
Ретрансляция управляющего трафика	-	+	A5

Из сравнительного анализа следует, что подход с предотвращением атак не реализует защиту от внутреннего нарушителя. Таким образом, в ходе дальнейшего исследования для формирования общего решения рассмотрены протоколы, реализующие описанные подходы к обеспечению безопасности маршрутизации MANET-сетей.

Механизм управления ключами в MANET-сети должен отвечать следующим требованиям [3]:

– отказоустойчивость;

– безопасность;

– доступность.

В Табл. 2 представлен сравнительный анализ рассмотренных протоколов предоставления инфраструктуры для применения криптографии с открытым ключом.

Табл. 2. Сравнительный анализ протоколов управления ключами

Протокол	**Схема управления ключами**	**Особенности**
Распределённая криптосистема	Доступ к единому закрытому ключу при обращении к k узлам.	Требуется механизм взаимодействия с узлом-комбинатором
Управление в рамках кластеров		Организация шифрования с закрытым ключом внутри кластера
SEKM		Динамическая схема смены конфигурации АС и пересоздания общего сертификата
Полностью распределённый CA	Формирование сертификата при обращении к k узлам	Каждый узел выполняет роль CA
Иерархический CA		Разделение на сообщества
Автономное управление ключами		Уровни доверия сертификату; Динамическая схема смены конфигурации АС
Самоорганизованное управление ключами	Самостоятельное формирование сертификатов	Узлы попарно устанавливают факт доверия сертификатам

По результатам сравнения рассмотренных протоколов управления ключами в распределённой сети сделан вывод, что наибольший интерес представляют протоколы, реализующие одноранговую распределённую систему, так как обслуживание централизующих узлов является неактуальным при частых разрывах соединений.

Подходы к предотвращению атак реализуются за счёт обеспечения целостности информации внутри сети. Для сравнения протоколов предложены критерии: использование одноранговой системы управления ключами (К1), аутентификация узлов (К2), контроль целостности пакетов (К3), невозможность отказа от авторства (К4) [4]. Табл. 3 показывает соответствие протоколов критериям.

Табл. 3. Сравнительный анализ протоколов противодействия атакам

Протокол	**Критерий**			
	К1	**К2**	**К3**	**К4**
ARAN	+	+	+	+
SRP	-	+	+	-
SEAD	+	+	-	+
ARIANDE	-	+	+	+
SAODV	+	+	-	-
SRPRBF	+	+	+	-

По результатам проведённого сравнения сделан вывод, что наиболее подходящим для формирования общего решения безопасной маршрутизации MANET-сетей является протокол ARAN [5]. Однако ARAN не предоставляет механизмов борьбы с внутренними нарушителями.

Подход предотвращения атак не позволяет защититься от внутренних угроз [6]. С целью решения данной проблемы представлены методы, ориентированные на анализ трафика для выявления аномального поведения

узлов и пресечения развивающейся атаки [7]. Для их сравнения предложены следующие критерии:

– К2 – протокол не использует особенности реализаций аппаратного обеспечения устройств;

– К3 – протокол учитывает энергетические ресурсы участника сети;

– К4 – протокол реализует механизм распределения оценки вредоносности узла;

– К5 – протокол включает механизм устойчивости к клевете;

– К6 – протокол использует информацию о свойствах интерфейсов беспроводной связи при выполнении оценки вредоносности узла.

В Табл. 4 представлено сравнение исследуемых протоколов на основе предложенных критериев.

Табл. 4. Сравнительный анализ протоколов обнаружения атак

Протокол	**Критерий**						
	A4	**A5**	**K2**	**K3**	**K4**	**K5**	**K6**
CONFIDANT	+	+	-	-	+	-	-
T2AR	+	+	-	+	-	-	+
FPNT-OSLR	+	+	-	+	+	-	+
ReTEAODV	+	+	+	-	+	+	-
TSQRS	**+**	**+**	**+**	**+**	**+**	**+**	**+**

По результатам проведённого сравнения сделан вывод о том, что протокол TSQRS [8] в полной мере соответствует требованиям общего решения безопасной маршрутизации. Эффективное применение протокола требует анализа параметров сети, так как использует в решении задачи классификации обширный набор взвешенных параметров. Далее предложено улучшение протокола.

По результатам исследования сформулирован состав протокола защиты от известных классов атак. В Табл. 5 представлены избранные компоненты прототипа протокола безопасной маршрутизации.

Табл. 5. Ключевые компоненты протокола безопасной маршрутизации.

Класс атаки	**Избранные методы противодействия**	**Избранные подходы к реализации**	**Избранные компоненты**
Атаки на идентифицирующую информацию	Аутентификация узлов	С помощью сертификата открытого ключа	Аутентификация и контроль целостности пакетов на основе ARAN
Модификация управляющего трафика	Контроль целостности пакетов	Использование электронной подписи пакетов	
Подделка управляющих сообщений	Невозможность отказа от авторства		
Удаление пакетов	Наблюдение за выполнением операций сети	Вычисление и распространение оценки вредоносности узла	На основе TSQRS
Ретрансляция управляющего трафика			

Протокол TSQRS является расширением реактивного протокола AODV, которое ориентировано не только на обеспечение безопасности, но и на улучшение качества выполнения операций сети [8].

Вычисление уровня доверия к соседнему узлу вычисляется по формуле (1).

$$T_i = w_1 * CRF_i + w_2 * DRF_i + w_3 * IL_i + w_4 * RE_i + w_5 * LQ_i + w_6 * CQ_i \quad (1)$$

где CRF - относительное число переданных управляющих пакетов, DRF - относительное число переданных пакетов с данными, IL - уровень близости, RE - уровень энергетических ресурсов узла, LQ - качество соединения, CQ - качество канала, $w_{1...6}$ - используемые веса.

Решение о вредоносности узла i принимается, если рассчитанное значение T_i оказывается меньше некоторого порогового. Выбор этого значения, а также весов является сложной задачей, требующей анализа для конкретной конфигурации сети. Для решения данной задачи предлагается использование методов машинного обучения.

В рамках ограничений вычислительных ресурсов, которые свойственны устройствам MANET-сетей, необходимо учитывать мощность, требуемую для эффективного применения методов машинного обучения. Поэтому при его выборе уместно обратиться к опыту IoT [9], который свидетельствует о том, что наибольшую точность при решении задачи классификации для беспроводных сетей показывает алгоритм случайных деревьев.

Для разрабатываемого протокола безопасной маршрутизации предлагается использование алгоритма случайного леса. Входными параметрами модели являются: CRF, DRF, IL, RE, LQ, CQ.

На Рис. 1 представлено взаимодействие компонентов разработанного протокола безопасной маршрутизации.

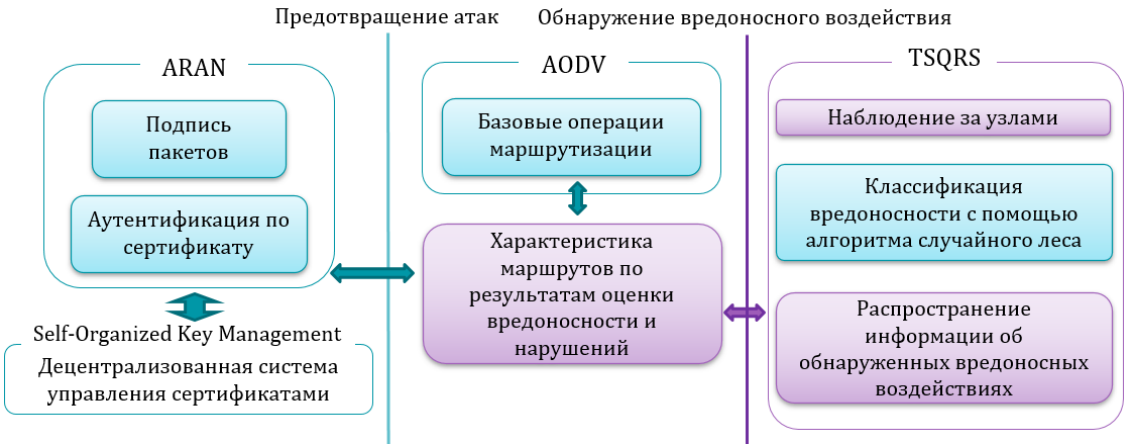

Рис. 1. Компоненты разработанного протокола

В рамках разработки предлагаемого прототипа протокола безопасной маршрутизации MANET-сетей выполнено сравнение результатов решения задачи оценки вредоносности узлов для следующих протоколов:

– Предлагаемой модификации TSQRS на основе алгоритма случайного леса;

– TSQRS;

– ReTEAODV [10].

В среде симуляции реализован сбор данных, которые узлы получают в ходе наблюдения для следующих сценариев [11]:

– реализация black hole атаки;

– реализация grey hole атаки;

– реализация воронки;

– реализация Wormhole.

В Табл. 8 представлены результаты сравнения рассматриваемых подходов к решению задачи оценки вредоносности узла для реализованных атак.

Табл. 8. Сравнение результатов решения задачи классификации вредоносности

	Случайный лес	**TSQRS**	**ReTEAODV**
Black hole			
$Accuracy$	0,86	0,70	0,77
$Precision$	0,70	0,46	0,57
$Recall$	0,76	0,60	0,68
$F_{\text{мера}}$	0,73	0,53	0,63
Grey hole			
$Accuracy$	0,71	0,61	0,65
$Precision$	0,48	0,34	0,40
$Recall$	0,60	0,44	0,48
$F_{\text{мера}}$	0,53	0,38	0,44

	Случайный лес	TSQRS	ReTEAODV
Воронка			
$Accuracy$	0,73	0,57	0,55
$Precision$	0,51	0,33	0,34
$Recall$	0,69	0,52	0,32
$F_{\text{мера}}$	0,56	0,41	0,33
Worm hole			
$Accuracy$	0,52	0,44	0,43
$Precision$	0,40	0,33	0,25
$Recall$	0,36	0,25	0,27
$F_{\text{мера}}$	0,38	0,29	0,26

Результат сравнительного анализа точности решения задачи классификации вредоносного воздействия узла на сеть показал, что предлагаемый подход в рамках эксперимента демонстрирует большее число корректно принимаемых решений, а также меньшее число ошибок.

Для проведения оценки способности разработанного протокола противодействовать рассмотренным классам атак в среде, реализованной для проведения предыдущего эксперимента, были осуществлены дополнительные атаки со стороны внешнего нарушителя. В Табл. 9 представлено сравнение реализованных атак рассматриваемых классов и компонента протокола, который отреагировал на неё.

Табл. 9. Сравнение атак и отреагировавших компонентов протокола

Класс атаки	**Атака**	**Реакция протокола**
A1	Сивилла	ARAN: ошибка аутентификации узла
A2	Подмена адресата	ARAN: нарушение целостности
	Клевета	

Класс атаки	Атака	Реакция протокола
A3	Воронка	TSQRS (модификация): узел определён вредоносным
A4	Black hole	
	Grey hole	
A5	Wormhole	

По результатам проверки сделан вывод о том, что разработанный прототип протокола безопасной маршрутизации MANET-сетей способен противодействовать рассматриваемым классам атак.

В данной работе исследованы протоколы, организующие маршрутизацию MANET-сетей, рассмотрены проблемы обеспечения их безопасности и классы атак.

В результате исследования разработан прототип протокола безопасной маршрутизации MANET-сетей, который состоит из механизма распределённого управления сертификатами открытых ключей, компонента аутентификации, контроля целостности, а также комплекса оценки узлов с алгоритмом случайного леса.

СПИСОК ИСТОЧНИКОВ

1. Banerjee B., A brief overview of security attacks and protocols in MANET / Neogy S. // INDICON. – 2021. – С. 1- 6

2. Datta R. Security for mobile ad hoc networks // Handbook on securing cyber-physical critical infrastructure. – 2012. – С. 147-190.

3. Selim B. Key management for the manet: A survey / Yeun C. Y. // 2015 International Conference on Information and Communication Technology Research (ICTRC). – IEEE, 2015. – С. 326-329

4. Vijayakumar K. Study on reliable and secure routing protocols on manet / Somasundaram K. // Indian Journal of Science and Technology. – 2016. – Т. 9. – №. 14. – С. 1-10

5. Sanzgiri K. Authenticated routing for ad hoc networks // IEEE Journal on selected areas in communications. – 2005. – Т. 23. – №. 3. – С. 598-610.

6. Priya N. D. S. Trust Management Schemes for Secure Data Transfer in MANETs: A Survey / Parameswaran T. //. – 2017.

7. Kalime S. A review: secure routing protocols for mobile adhoc networks (MANETs) / Sagar K. // Journal of Critical Reviews. – 2021. – Т. 7. – С. 8385-8393

8. Pathan M. S. et al. An efficient trust-based scheme for secure and quality of service routing in MANETs // Future Internet. – 2018. – Т. 10. – №. 2. – С. 16.

9. Sethuraman P. Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET / Kannan N. // Wireless Networks. – 2017. – Т. 23. – С. 2227-2237.

10. Hasan M. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches // Internet of Things. – 2019. – Т. 7. – С. 100059.

11. Tiruvakadu D. S. K. Confirmation of wormhole attack in MANETs using honeypot / Pallapa V. // Computers & Security. – 2018. – Т. 76. – С. 32-49.

Гололобов Н.В.
ФГАОУ ВО «СПбПУ»,
Институт компьютерных наук и кибербезопасности,
аспирант,
neptu133@gmail.com
Павленко Е.Ю.
ФГАОУ ВО «СПбПУ»,
Институт компьютерных наук и кибербезопасности,
к.т.н., доцент
pavlenko_eyu@spbstu.ru

ВЫЯВЛЕНИЕ АТАК НА РАСПРЕДЕЛЁННУЮ АВТОМОБИЛЬНУЮ КИБЕРФИЗИЧЕСКУЮ СИСТЕМУ НА ОСНОВЕ НЕРОЙННОЙ СЕТИ С ДОЛГОЙ КРАТКОСРОЧНОЙ ПАМЯТЬЮ

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки молодых российских ученых - кандидатов наук МК-3861.2022.1.6.

Состояние киберустойчивости системы во много определяется спецификой ее функционирования, степенью изоляции, количеством входных узлов и многими другими факторами. Длительность интервала безотказной работы зависит от большого числа факторов, точно предсказать которые невозможно, поэтому, отказ или нарушение безопасности обычно считают случайным событием. Киберустойчивость принято характеризовать вероятностью отказа в работе или нарушения состояния защищенности киберфизических систем (КФС) в течение определенного отрезка времени.

Основными группами элементов киберфизической системы являются группа элементов обработки информации и группа элементов передачи информации [1, 2]. Для каждой группы ненадежность определяется в соответствии с функциональными требованиям группой элементов [2].

Ненадежность элементов обработки информации, может заключаться как в полном отказе работы, в изменении функциональности (стабильном получении неверных результатов), так и в частных сбоях [3].

Современные транспортные средства, оснащенные большим количеством электронных компонентов, датчиков, приводов и широкими возможностями подключения, являются классическим примером КФС [4]. Для обеспечения безопасности передаваемых данных обычно используются именованные сети передачи данных (Named data network, NDN) [5]. В основе таких сетей лежит принцип помещения содержимого в центр коммуникации и обеспечение защиты содержимого.

Типичная инфраструктура автомобильной КФС (АКФС) включает в себя автомобили, интеллектуальные дорожные знаки, информационные табло и многое другое. Логические узлы данной киберфизической системы подключаются через беспроводные и проводные средства связи.

Внедрение связи в транспортных средствах для передачи информации по сети увеличило возможности кибератак на автомобильные системы. Целью этих атак является получение доступа к информации, а также контроль над физическими операциями автомобильной системы. К таким атакам относятся:

- вызов отказа в обслуживании;
- атаки на путь следования данных;
- атаки типа «человек посередине»;
- атака посредством вредоносного обновления;
- внедрение кода, команды или пакета;
- нарушение целостности передаваемых сообщений;
- мимикрия и атака воспроизведением.

Основной характеристикой NDN является использование цифровых подписей в Data- и Interest-пакетах. До выполнения отправки пакета каждый пакет данных подписывается. В некоторых случаях пакет Interest также может быть подписан частичным именем, включая метку времени, префикс «NONCE»

и любые другие элементы имени. Подпись связывает имя с содержимым и его провайдером.

Тем не менее, NDN имеют ряд специфичных только для них атак, а именно:

1. Отравление содержимым: проверка подписи содержимого не требуется для промежуточных серверов или маршрутизаторов. В этом случае у злоумышленников появляется возможность использовать этой опции для распространения вредоносного или недопустимого содержимого, в том числе содержимого с недействительной подписью в сетевых кэшах.

2. Загрязнение кэша: эта атака основана на сговоре и фальсификации местоположение кэша. В результате действительно популярное содержимое удаляется из кэша из-за ложного повышения популярности недопустимого содержимого, что серьезно влияет на производительность.

3. Cache Snooping: этот метод используется для получения информации о кэшированном содержимом. Злоумышленник отправляет запрос с разными именами, опциями исключения и областью действия вместе с анализом времени отклика запроса, чтобы определить конфиденциальность содержимого и статус доступа для запуска других атак.

4. Атака на маршрутизацию: маршрутизация в NDN зависит исключительно от объявленных префиксов имен и заполнения структуры FIB этими опубликованными префиксами имен. В результате атаки, сообщение, перенаправленное на эти префиксы, направляется на вредоносный узел или узлы, которые могут вернуть вредоносное содержимое или перенаправляют запрос в сетевые зоны с недоступным содержимым.

В задачах распознавания киберугроз отклонение от номинального уровня функциональности киберфизической системы распознается как аномальное поведение. В свою очередь это позволяет одновременно реагировать на угрозы, не допуская снижения уровня функциональности до минимально допустимого [6]. Данный подход позволяет снизить как

финансовые, так и функциональные издержки при восстановлении киберфизической системы [7].

Одним из наиболее перспективных направлений в распознавании аномалий является использование нейронных сетей с долгой кратковременной памятью [8, 9]. Их отличительной особенностью является связь между элементами, которая образует направленную последовательность. Таким образом, становится возможной обработка серии событий во времени [10].

Предлагаемый метод распознавания состоит из ряда операций:

1. Для АКФС задаются номинальный и минимально допустимый уровень функциональности, а также максимально допустимое время работы в условиях минимального уровня функциональности.

2. Модель проходит обучение на типовом для АКФС наборе данных, содержащем как показатели нормального функционирования, так и показатели в условиях повышенного «кибердавления».

3. В ходе функционирования обученная модель осуществляет мониторинг показателей функциональности АКФС в момент времени T и на основе наблюдаемых значений производит прогнозирование значений в момент времени T+1.

4. В случае выявления значительного отклонения между прогнозируемым и фактическим значением – аномалии – производится подготовка к восстановлению системы для избежания каскадного эффекта при отказе, однако восстановление на данном этапе не производится.

5. При превышении максимально допустимого значения времени работы в условиях минимального уровня функциональности немедленно запускаются процессы восстановления работоспособности.

6. При невозможности восстановления функциональности системы до номинального уровня производится перерасчёт пограничных показателей, относительно которых далее будет оцениваться отклонение прогнозируемого значения от фактического.

В общем случае автомобильную киберфизическую систему можно представить как однонаправленный граф без петель. Вершины графа определяются приоритетом в соответствии с алгоритмом определения эффективного пути, реализация которого зависит от конкретной АКФС. Ребра графа задают не только направления передачи пакетов, но и максимально допустимую нагрузку на отрезке между транзитными узлами, превышение которой сигнализирует о снижении функциональности АКФС.

Скорость изменения топологии в АКФС сравнима со скоростью изменения топологии в MANET-сетях, что накладывает необходимость выполнения двух условий для успешного применения метода:

1. Обеспечение каждого узла механизмом для балансировки нагрузки на сеть.

2. Обеспечение каждого узла механизмом восстановления в случае выявления факта снижения функциональности.

В рамках предложенной архитектуры в случае обнаружения DoS- и DDoS-атак при обнаружении угроз из-за большого трафика запросов через определенный интерфейс или конкретный домен префикса имени NDN, компонент, обеспечивающий устойчивость предпринимает следующие действия, не нарушая нормальную работу системы:

1. Снижение скорости трафика, связанного с конкретным префиксом имени или входящим интерфейсом.

2. Сообщение другим маршрутизирующим узлам (в частности, пограничным) об атаке и соответствующей информации, включая префикс имени, интерфейс, скорость и т. д. Это позволяет ограничить атаку и направить ее обратно к источнику или источникам.

3. Включение префикса или интерфейса в черный список на определенный срок, который зависит от серьезности атаки.

4. Отбрасывание запросов, относящихся к конкретному домену или полученных от конкретного входящего интерфейса, и удаление из структуры FIB префикса имени.

Использование рекуррентных нейронных сетей, в частности сетей с долгой кратковременной памятью позволяет не только оперативно реагировать на возникающие атаки, а также своевременно их предотвращать, но и захватывать контекст состояния АКФС для минимизации ошибок при принятии решений [11]. Обучение нейронных сетей должно проводиться на основе набора данных, экземпляры в котором имеют значения, приближенные к реальным показателям. Это обеспечит не только большую точность прогнозов, но и значительно ускорит процесс обучения.

Дальнейшие исследование в данном направлении должны быть посвящены имплементации разработанного метода, а также повышению его универсальности для противостояния различным типам атак и оценке его эффективности в рамках моделируемой АКФС. Кроме этого, предварительно должна быть разработана система оценки киберустойчивости АКФС, на основе которой и будет производиться оценка эффективности.

СПИСОК ИСТОЧНИКОВ

1. X.800: Security architecture for Open Systems Interconnection for CCITT applications // – (22.03.1991) – [Электронный ресурс]. – Режим доступа: https://www.itu.int/rec/t-rec-x.800-199103-i/en.

2. Стандарты информационной безопасности распределенных систем // Информационная безопасность. – (26.02.2016). – [Электронный ресурс]. – Режим доступа: https://informationsecurityweb.wordpress.com/2016/05/26/стандарты-информационной-безопасно-2/.

3. Рекомендации X.800 для распределенных систем // deHack.ru. – [Электронный ресурс]. – Режим доступа: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/rekomendatsii_x_800_dlja_raspredelennyx_sistem/?p=3.

4. Акопов, А. С. Моделирование динамики дорожно-транспортных происшествий с участием беспилотных автомобилей в транспортной системе

"умного города" / А. С. Акопов, Л. А. Бекларян // Бизнес-информатика. – 2022. – Т. 16, № 4. – С. 19-35. – DOI 10.17323/2587-814X.2022.4.19.35. – EDN BWZYIV.

5. Named Data Networking's Intrinsic Cyber-Resilience for Vehicular CPS / S. H. Bouk, S. H. Ahmed, R. Hussain, Y. Eun // IEEE Access. – 2018. – Vol. 6. – P. 60570-60585. – DOI 10.1109/ACCESS.2018.2875890.

6. Januário, F. A Distributed Multi-Agent Framework for Resilience Enhancement in Cyber-Physical Systems / F. Januário, P. Gil, A. Cardoso // IEEE Access. – 2019. – Vol. 7. – P. 31342-31357. – DOI 10.1109/ACCESS.2019.2903629.

7. R. A. Becker et al. Increasing scientific confidence in adverse outcome pathways: Application of tailored Bradford-Hill considerations for evaluating weight of evidence // Regulatory Toxicol. Pharmacol. — 2015. — Vol. 72, N. 3. — P. 514–537. doi: 10.1016/j.yrtph.2015.04.004.

8. Chen, J. GC-LSTM: graph convolution embedded LSTM for dynamic network link prediction / J. Chen, X. Wang, X. Xu // Applied Intelligence. – 2021. – DOI 10.1007/s10489-021-02518-9. – EDN CAJUBN.

9. Attention-based Conv-LSTM and Bi-LSTM networks for large-scale traffic speed prediction / X. Hu, T. Liu, X. Hao, Ch. Lin // The Journal of Supercomputing. – 2022. – Vol. 78, No. 10. – P. 12686-12709. – DOI 10.1007/s11227-022-04386-7. – EDN AOJVZL.

10. Казакова, Д. А. Пример прогнозирования временных рядов с помощью рекуррентной нейронной сети LSTM / Д. А. Казакова // Проблемы теории и практики современной науки: материалы Международной (заочной) научно-практической конференции, Нефтекамск, 21 ноября 2022 года / Научно-издательский центр «Мир науки». – Нефтекамск: Научно-издательский центр "Мир науки" (ИП Вострецов Александр Ильич), 2022. – С. 27-30. – EDN POUNMJ.

11. Бачалдина, О. Д. Информационная безопасность киберфизических систем на примере "умных" автомобилей / О. Д. Бачалдина, Е. В. Коренюгин, Е. К. Щелокова // Молодежная научная школа кафедры "Защищенные системы связи". – 2020. – Т. 1, № 2(2). – С. 4-9. – EDN KMLNIV.

Самарин Н.Н.
ФГУП «НИИ «Квант»,
начальник научно-исследовательского отделения,
к.т.н,
samarin_nik@mail.ru

АНАЛИЗ ВОЗМОЖНОСТЕЙ НАПРАВЛЕННОГО ФАЗЗИНГ-ТЕСТИРОВАНИЯ В ЗАДАЧАХ ПОИСКА ОШИБОК В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Поиск и исправление ошибок в программном обеспечении (ПО) имеет большое значение при обеспечении безопасности информационной системы, в которой оно применяется. Согласно отчету, опубликованному компанией по кибербезопасности Veracode в 2017 году [1], наблюдается тенденция к увеличению числа использований методик гибкой разработки и применения ПО с открытым исходным кодом. В среднем, 75% ПО исходит из компонентов с открытым исходным кодом, поэтому уязвимости в этих компонентах создают огромный риск для безопасности. Применяемые в такого рода системах безопасности методы сосредоточены только на известных уязвимостях и практически не могут выявлять потенциальные уязвимости, скрытые в бинарном коде.

Фаззинг-тестирование — это технология тестирования безопасности, которая базируется на генерации большого множества входных данных для приложения и использует инструментированную программу в качестве индикатора для обнаружения возможных уязвимостей [2]. Направленный фаззинг — это технология обнаружения уязвимостей, которая основана на местоположении цели в заданной пользователем программе. В основном он делится на DSE (Direct Symbolic Execution, направленное символьное исполнение) и DGF (Direct Greybox Fuzzing, направленный фаззинг серого ящика). В ходе жизненного цикла ПО происходят его изменения и доработки.

Основным фактором, на который необходимо обращать внимание - не приведут ли эти изменения к появлению уязвимостей. Направленный фаззер использует это изменение в качестве целевого местоположения для сканирования, чтобы обнаружить потенциальные уязвимости и предотвратить их распространение.

В отличие от ненаправленных фаззеров, направленные фаззеры тратят много времени на поиск конкретного целевого местоположения вместо того, чтобы тратить много времени на несвязанные программные модули. Направленный фаззинг нацелен на определение областей входных данных, попадания в которые могут повлиять на чувствительные к безопасности точки программы, и фокусируется на изменении этих начальных значений для выявления дефектов и уязвимостей.

Большинство направленных фаззеров основаны на символьном исполнении [3]. Одним из наиболее перспективных подходов к фаззинг-тестированию является использование фаззера на основе «пятен». Его целью является идентификация и фаззинг конкретных входных байтов в исходном коде для получения определенного значения в заданном месте программы, например, нулевое значение в знаменателе оператора деления [5] и др. Это, в свою очередь, может значительно сократить пространство поиска, однако оставляет необходимость предоставления начального ввода.

Направленное символьное исполнение

Символьное исполнение изначально использовалось в области компиляторов, отладки и т. д. [6]. Основная идея состоит в том, чтобы обозначить входные данные программы символами и выполнить эти символьные переменные в качестве входных данных, собрать ограничения предикатов для оценки условия ветвления и, наконец, использовать решатель для получения новых тестовых входных данных [7].

Наиболее часто встречающимся типом символьного исполнения является статическое символьное исполнение. Входная переменная обозначается символом, после чего с помощью программы статического анализа символ

преобразуется в промежуточное представление. В ходе исполнения переменная модифицируется, тем самым изменяя и значение символизированной переменной.

Сочетание традиционного статического символьного исполнения с фактическим исполнением называется динамическим символьным исполнением [8]. Динамическое символьное выполнение поддерживает два состояния: одно — состояние фактической переменной, а другое — символизированное состояние. Фактическое состояние отображает случайно сгенерированные значения в переменные, тогда как символизированное состояние символизирует переменные. Динамическое символьное исполнение сначала выполняется в соответствии с фактическим состоянием, собирает ограничения символизации переменных. Затем ограничение инвертируется, и обрабатываются ограничения альтернативной трассы. Процесс повторяется до тех пор, пока не будут исследованы все трассы или не достигнуты установленные пользователем ограничения. Таким образом, исключается проблема, связанная с тем, что ограничение не может быть идентифицировано или решено. Новые входные данные генерируются путем решения ограничений, полученных конечным автоматом. Этот подход не только находит возможные уязвимости с учетом трассы, но также идентифицирует возможные уязвимости с учетом объектов управления доступом [9].

Направленное символьное исполнение переводит проблему достижимости в итеративную задачу решения ограничений. Поскольку большинство путей неосуществимы, поиск обычно является итеративным, заключаясь в поиске возможного пути к промежуточной цели. Как только возможная трасса, которая действительно может достичь целевого местоположения, определена, апостериорно генерируется тестовый пример как решение соответствующего ограничения трассы.

Эффективность направленного символьного исполнения компенсируется его производительностью [10]. Данный метод требует много времени для анализа программы и решения ограничений. Во время каждой итерации

используется анализ программы для выявления тех ветвей, которые необходимо отменить, чтобы приблизиться к цели, создавая соответствующие условия пути на основе последовательности инструкций используя решатель ограничений для проверки выполнимости этих условий. условия.

Направленное символьное исполнение применяется для доступа к опасным местам в программе, перезаписи изменений в исправлении, перезаписи ранее обнаруженных элементов программы для увеличения охвата, проверки отчетов статического анализа, внезапного обнаружения и воспроизведения сбоев на местах.

Направленное фаззинг-тестирование серого ящика

При фазинге серого ящика применяется подход на основе покрытия. Он предназначен для генерации входных данных, которые могут обеспечить максимальное покрытие кода и наиболее глубокое исследование трасс программы. Направленное фаззинг-тестирование серого ящика сопоставляет проблему достижимости с задачей оптимизации и использует специальный метаэвристический алгоритм для расчета минимального расстояния, на котором генерируется начальное число переходов до цели [11].

В процессе направленного фаззинг-тестирования серого ящика тестировщики используют инструменты, которые генерируют случайные данные и отправляют их в приложение для проверки его реакции. Таким образом, выявляются ошибки в обработке данных и другие уязвимости, которые могут привести к нарушению безопасности.

Для проведения направленного фаззинг-тестирования серого ящика необходимо иметь достаточно подробное представление о том, как работает приложение и какие данные оно обрабатывает. Это поможет определить, какие типы данных следует использовать при генерации тестовых данных.

Также важно учитывать, что направленное фаззинг-тестирование серого ящика может быть достаточно ресурсоемким процессом, поэтому его проведение может занять некоторое время. Однако, благодаря этому методу,

можно получить ценную информацию о безопасности приложения и защитить его от потенциальных угроз.

Направленное фаззинг-тестирование серого ящика сохраняет эффективность обыкновенного фаззинг-тестирования серого ящика, поскольку весь анализ программы происходит на этапе компиляции. В то же время его можно легко распараллелить, что позволяет выделить больше вычислительной мощности для быстрого и эффективного обнаружения уязвимостей. По сравнению с направленным символьным вычислением [12], направленное фаззинг-тестирование серого ящика не требует анализа программы и решения ограничений в связи с тем, что облегченный анализ программы выполняется во время компиляции.

Заключение

Оба рассмотренных в настоящей статье метода могут достичь указанного пользователем места в программе. Однако направленное символьное выполнение имеет более сложный программный анализ, чем направленный фаззинг серого ящика. В будущем можно будет интегрировать направленный фаззинг белого ящика и направленный фаззинг серого ящика на основе символьного исполнения, а также воспользоваться преимуществами точного анализа символьного исполнения и множественного входа генерации фаззинга серого ящика. В то же время, выбирая выполнение тест-кейсов, возможно интегрирование алгоритмов машинного обучения для определения сильных и слабых сторон тест-кейсов, а также порядка приоритета их выполнения на основе моделей, извлеченных из прошлого опыта.

Тем не менее, фаззинг-тестирование также имеет определенные ограничения. Например, при фаззинг-тестировании невозможно выявить уязвимости, связанные с контролем доступа. Кроме этого, фаззинг-тестирование не позволяет определить, связана ли обнаруженная проблема с проблемой безопасности при выявлении нарушений контроля доступа. Многоэтапные уязвимости безопасности также не могут быть выявлены при

проведении фаззинг-тестирования. В будущем, возможно, эти ограничения могут быть нивелированы с использованием методов направленного нечеткого анализа.

СПИСОК ИСТОЧНИКОВ

1. Software Security Report [M]. Veracode. 201 7
2. Honghui Li, Jia Qi, Feng Liu. Research on Fuzzy Testing Technology[J]. Science in China, 2014, 44 (10): 1305-1322.
3. Liang H, Pei X, Jia X, et al. Fuzzing: State of the Art[J]. IEEE Transactions on Reliability, PP (99):1-20.
4. Website. 2017. Peach Fuzzer Platform. http ://www.peachfuzzer.com/produ cts/peach-platform/. (2017).
5. Website. 2017. SPIKE Fuzzer Platform. http://www.immunitysec.com. (2017).
6. Website. 2017. Zzuf: multi-purpose fuzzer. http://caca.zoy.org/wiki/zzuf. (2017).
7. Jared D. DeMott, Richard J. Enbody, and William F. Punch. 2007. Rev- olutionizing the Field of Grey-box Attack Surface Testing with Evolu- tionary Fuzzing. (2007).
8. Fabien Duchene. 2013. Fuzz in the Dark: Genetic Algorithm for Black-Box Fuzzing. In Black Hat 2013. Black Hat, Sao Paulo, Brazil. https: //hal.inria.fr/hal- 00978844.
9. Duran J. W., Ntafos S. A report on random testing //Proceedings of the 5th international conference on Software engineering. – 1981. – C. 179-183.
10. Forrester, J.E. and Miller, B.P. An empirical study of the robustness of Windows NT applications using random testing. In Proceedings of the 4th USENIX Windows System Symp., Seattle, (Aug. 2000).
11. A. Takanen, J. D. DeMott, C. Miller, and A. Kettunen, Fuzzing for Software Security Testing and Quality Assurance, 2nd ed. Artech House, 2018.

12. U. Erlingsson, L. Lozano, and G. Pike, “Enforcing forward-edge control-flow integrity in gcc & llvm,” in Proceedings of the USENIX Security Symposium, 2014, pp. 941–955.

Щербинина И.А.
Морской государственный
университет им. адм. Г.И. Невельского,
г.Владивосток, декан физико-
технического
факультета, к. п. н., доцент,
shcherbinina@msun.ru
Потапова К.А.
Морской государственный
университет им. адм. Г.И. Невельского,
г.Владивосток, аспирант,
smirnovaksenia2018@inbox.ru

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИМЕНЕНИЯ RFID-ТЕХНОЛОГИЙ ПРИ ИДЕНТИФИКАЦИИ КОНТЕЙНЕРОВ

Объём внешнеторгового оборота – ключевой показатель мировой экономики, в частности, отношений между странами. Существует несколько способов транспортировки грузов. Для перевозки больших объёмов товаров на дальние расстояния самый экономически выгодный – морской транспорт, что обуславливает его востребованность во все времена. Согласно данным Росморречфлота, грузооборот морских портов России на 2022 года повысился на 0,7 % в сравнении с 2023 годом и составил примерно 842 млн тонн. В том числе, объем перевалки сухих грузов составил примерно 405 млн тонн (-2,0%), наливных грузов – 437 млн тонн (+3,4%) [6].

Члены экипажей, работающих на судах торгового флота, утверждают, что вопрос безопасности данных о грузе остаётся открытым до сих пор.

В данной статье рассматриваются проблемы безопасности при перевозке грузов, возникающие при применении RFID-технологий.

Доля морских перевозок в мировом грузообороте по оценкам различных агентств варьируется от 62% до 91%. Ясно, что при таких показателях безопасности морских перевозок грузов уделяется особое внимание [4].

Вопросы обеспечения информационной безопасности морских перевозок являются очень важными, т.к. нацелены на нахождение возможности снижения отрицательного воздействия злоумышленников на эффективность и исправность работы, имущество, имущественные интересы, а также окружающую среду и здоровье, как обслуживающего персонала, так и населения в районах осуществления производственной и коммерческой деятельности.

Повышение устойчивости к угрозам безопасности информационной инфраструктуры морских портов является одним из приоритетов субъектов критической информационной инфраструктуры [1].

Возникающие угрозы, а также нетрадиционные атаки на информационную инфраструктуру морского порта, выявили пределы традиционной оценки рисков и усилий по снижению риска. Некоторые угрозы не могут быть предвидены, а снижение всех возможных рисков на минимально возможном уровне не всегда экономически выгодно.

Технология, которая может решить вопрос хранения и защищенности данных о грузе на этапах погрузки, транспортировки и выгрузки, – радиочастотная идентификация.

Радиочастотная идентификация (RFID) - новейшая технология, состоящая из трех ключевых деталей: RFID-меток (миниатюрных чипов); RFID-считывателей; и системы сбора, распространения и управления данными, которая может определить или сканировать информацию с повышенной скоростью и точностью [10].

Эта система в основном состоит из следующих компонентов.

– транспондер (RF-метка);

– трансивер (считыватель) с декодером;

– антенна.

На рисунке 1 показана модель базовой RFID-системы.

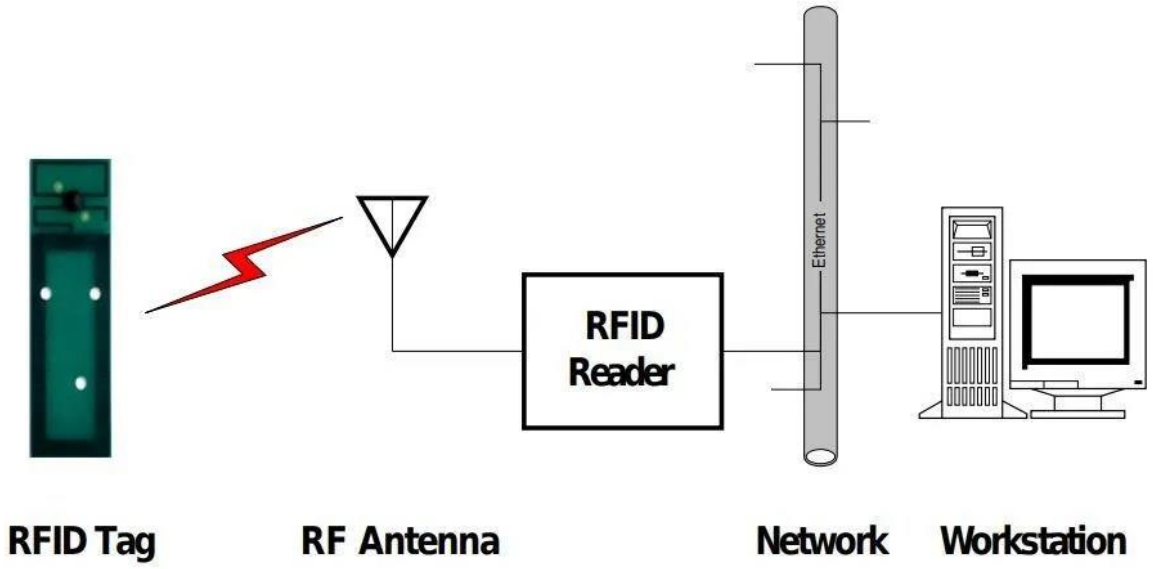

Рис. 1. Модель базовой RFID-системы [3]

Активные и пассивные RFID-метки - это два типа RFID-меток, которые обычно используются. Активные RFID-метки передают информацию непосредственно считывателю без использования внешней батареи или источника, тогда как пассивные метки для работы требуют внешнего питания.

Программное обеспечение управляет взаимодействием между RFID-считывателем и RFID-метками.

RFID-метки обычно называют транспондером, который действует как передатчик, а также как приемник в системе RFID. Три основные детали RFID-метки являются антенна, микрочип (память) и герметизирующий материал. Различают две разновидности RFID-меток:

1. Тег только для чтения (микрочип или память сохраняются один раз, во время производственного процесса, а информация и серийный номер на метке неизменны).

2. Тег чтения-записи (в процессе производства сохраняется только серийный номер, остальные блоки могут быть пересохранены пользователем).

RFID можно разделить на: фиксированный RFID и мобильный RFID. Фиксированный RFID записывает метки в стационарном положении. Мобильный RFID, считается в том случае если считыватель или метка являются мобильными [8].

RFID позволяет защитить рассматриваемые логистические процессы путем их автоматизации: отраженный от метки радиосигнал передается на считыватель, затем полученные данные отправляются в сетевое хранилище.

Со временем возникли различные проблемы конфиденциальности и безопасности. Одна из самых больших проблем состоит в том, что любой, у кого есть способный считыватель RFID, может прочитать RFID-метки, если они находятся поблизости (например, за пределами склада). Это можно сделать даже без ведома сотрудников.

Однако, как упоминалось ранее, важным элементом экосистемы RFID является база данных. Да, некоторые бирки имеют уникальные серийные номера, которые может прочитать любой считыватель. Но если читатель не подключен к базе данных, в которой хранится его информация, эта информация будет бесполезна. Более того, поскольку большинство RFID-меток не обладают вычислительной мощностью, злоумышленник не сможет декодировать зашифрованную информацию.

При этом метки должны быть совместимы со считывателем. В большинстве случаев считыватели RFID создаются специально для работы с метками определенной категории. Например, считыватели низкочастотного диапазона могут считывать только низкочастотные метки.

Чтобы избежать любого потенциального нарушения безопасности меток, следует убедиться, что назначенное место на складе защищено и находится вне досягаемости снаружи.

Наконец, существуют также проблемы конфиденциальности, связанные с RFID-чипами в таких документах, как электронные паспорта. Как правило, чипы паспортов обладают базовыми возможностями контроля доступа, что означает, что они обладают вычислительной мощностью для декодирования

зашифрованной информации, например личной информации о владельце паспорта [7].

Однако эти данные можно прочитать только с помощью считывателей пограничного контроля. Сотрудники пограничного контроля используют считыватель не только для подтверждения личности владельца паспорта, но и действительности самого паспорта.

Возможные сценарии работы злоумышленника [5]:

– злоумышленник находит физический доступ к помещению, где находится метка и пересохраняет её;

– считыватель злоумышленника сканирует данные с плохо защищённого тега;

– считыватель извлекает данные с поддельных меток (в системе две одинаковые метки);

– злоумышленник перехватывает движение между считывателем и сетевым хранилищем;

– злоумышленник получает доступ к хранилищу, где сохраняются считанные данные.

Рекомендации по безопасности:

– физическое ужесточение мер безопасности на объекте (охрана протяженности, установка видеонаблюдения и системы контроля и управления доступом и другое в зависимости от параметров объекта);

– перезапись и смена ACCESS-пароля после каждой логистической операции или цепочки операции, что более разумно;

– временная или постоянная (до следующего пересохранения) дезактивирования метки;

– внедрение датчиков, для определения удаленности считывателя от метки; данный встроенный алгоритм определяет объем разрешенной информации для выдачи считывателю в зависимости от его отдаленности от метки;

– введение бита конфиденциальности в связке «метка – считыватель»; так, например, при нулевом значении бита считыватель распознаёт только ID метки, если же значение равно единице, то выдаётся полная информация;

– криптографическая защита канала связи при передаче считанных данных в сетевое хранилище;

– принятие мер по повышению защищённости баз данных, в том числе, минимизация угрозы SQL-инъекций, распределенное хранение.

Внедрение дополнительных датчиков и алгоритмов в RFID-метки влияет на её энергопотребление. Поэтому нет чётких указаний к мероприятиям по защищённости RFID-систем: это индивидуально с учётом особенностей конкретного объекта и условий внешней среды.

Список литературы

1. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» от 27.06.2006 (ред. от 29.12.2022 N 604-ФЗ)
2. Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы Цифровая экономика Российской Федерации»
3. Radio Frequency Identification Technology [Электронный ресурс]. — Режим доступа: https://krazytech.com/technical-papers/radio-frequency-identification-technology
4. Безопасность морских грузоперевозок [Электронный ресурс]. — Режим доступа: https://novelco.ru/press-tsentr/bezopasnost-morskikh-gruzoperevozok/?ysclid=lnvmc3jxmh115714600
5. Банк данных угроз безопасности информации. Список уязвимостей. [Электронный ресурс]. — Режим доступа: https://bdu.fstec.ru/vul (дата обращения: 13.10.2023)
6. Грузооборот морских портов России в 2022 году вырос на 0,7% [Электронный ресурс]. — Режим доступа: https://tass.ru/ekonomika/16788943?ysclid=lnvmadkmh5728877270

7. Логунова И.В., Трощенко Д.В. Модель логистической системы предприятия в условиях цифровой экономики // Экономинфо. 2019. № 16−2−3. С. 81−86.

8. Применение технологии RFID в повседневной жизни [Электронный ресурс]. — Режим доступа: https://rfidunion.com/information/rfid-technology-in-everyday-life.html

9. Сердюкова Л.О., Баширзаде Р.Р.к., Пахомова А.В. Формирование инновационной транспортно-логистической системы на цифровой платформе // Научно-технические ведомости СПб-ГПУ. Экономические науки. 2020. № 2. С. 64–78. DOI: 10.18721/JE.13206

10. Технология радиочастотной идентификации (RFID) в логистике [Электронный ресурс]. — Режим доступа: https://www.axelot.ru/smi/tehnologiya-radiochastotnoj-identifikaczii-rfid-v-logistike/?ysclid=lnvf6nn9cf731548268

Жуков С.В.
каф. ГИиИБ, ст. преп.
Самарский университет
svzhukov@ssau.ru
Марченко Е.А.
студент
Самарский университет
katyushenkamarchenko@mail.ru

ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ В DLP-СИСТЕМЕ ДЛЯ АНАЛИЗА ДАННЫХ

За последний год утекло больше 40 миллионов записей с персональными данными. Большие компании не могут рисковать такой статистикой. С одной стороны, они должны соответствовать нормативным требованиям и защищать чувствительные данные. С другой стороны, компании должны адаптироваться к современным реалиям и технологическим изменениям, которые, в свою очередь, подразумевают большую мобильность сотрудников, использование облачных приложений. Появилось больше свободы, а это значит, увеличивается количество способов утечки данных из организации. Технология применения нейронных сетей помогла бы оптимизировать работу систем контроля утечки данных.

DLP-системы на основе нейросетевых технологий являются ключевым инструментом в сфере информационной безопасности, предотвращающим утечку конфиденциальных данных. Они объединяют в себе преимущества DLP и нейросетевых методов, позволяя создавать интеллектуальные системы анализа данных, способные автоматически обнаруживать потенциальные угрозы и предотвращать утечку данных. DLP (Data Loss Prevention) - это область информационной безопасности, которая ставит своей задачей защиту

ценных данных организаций от несанкционированного доступа, модификации, уничтожения и распространения [1].

Нейросетевые технологии, в свою очередь, основаны на искусственных нейронных сетях и представляют собой совокупность методов и алгоритмов, способных обучаться на больших объемах данных, что позволяет применять их в информационной безопасности и эффективно бороться с угрозами, предотвращая утечку конфиденциальных данных [2].

Объединение DLP и нейросетевых технологий дает возможность создавать более интеллектуальные системы, способные анализировать поведение пользователей и контента для обнаружения потенциальных угроз. Такие системы могут быть настроены для реагирования на различные сценарии и предупреждать организации о возможных рисках. Они способны автоматически обнаруживать аномальное поведение пользователей, несанкционированные попытки доступа к конфиденциальным данным, а также обнаруживать утечку информации через различные каналы связи [3].

Предлагаемое программное обеспечение разрабатывается с учётом поддержки только операционной системы Windows. Этот выбор обусловлен тем, что Windows широко используется. Однако, несмотря на наличие различных программ для работы с ресурсами Windows, не все из них могут предоставить необходимые данные и расширить функциональность по нашим требованиям. При сборе информации о системе и действиях пользователя важно учитывать загрузку системных ресурсов. Поэтому необходимо использовать инструменты, предоставляемые операционной системой Windows. Это позволит нам собирать отчеты по различным логическим группам данных, которые мы определим [4, 5].

В операционной системе Windows существует множество данных, которые необходимо собирать. Например, мы можем получить информацию о загрузке процессора, использовании памяти, состоянии дискового пространства и сетевых подключениях. Эти данные помогут нам анализировать производительность системы и выявлять потенциальные проблемы. Кроме

того, мы можем собирать данные о действиях пользователя, такие как запущенные приложения, посещенные веб-сайты и активность в социальных сетях. Это позволит нам отслеживать использование ресурсов пользователя и обнаруживать возможные угрозы безопасности.

Таким образом, было необходимо создать мониторинговую систему, которая позволит собирать отчеты по некоторым выделенным логическим группам данных [6]. В ОС Windows будут собираться и анализироваться следующие данные:

- общую информацию о системе;
- содержимое лог-файлов и системную информацию, содержащие сведения о конфигурации и событиях безопасности;
- сведения об установленном программном обеспечении на рабочую станцию;
- сведения о текущей конфигурации клиентских настроек доступа к данным (Data Access Client Experience);
- сведения об распознаваемых жестких дисках, о конфигурации хранилищ и их мета-данные;
- сведения о настройках DNS-клиента;
- сведения о всех событиях, провайдеры которых зарегистрированы в операционной системе;
- сведения о конфигурации сети, информацию о существующих и установленных подключениях, адаптерах, устройствах, соседних подключениях, данные IPSec и другие данные, относящиеся к сетевой информации;
- сведения о подключенных устройствах; сведения о работающих процессах, сервисах, запланированных задачах и другая информация;
- видео-информация, собираемая путем выполнения снимков экрана рабочей станции;
- сведения о WMI-объектах и их конфигурации.

Администратору безопасности важно знать не только что пользователь делал, но видеть более широкий контекст: с каких устройств заходил, откуда подключался к сети, и так далее. Это необходимо для того, чтобы эффективно фильтровать нормальную активность от потенциально опасной. Например, для определения скомпрометированной учетной записи, которую может использовать злоумышленник, администратору полезно знать, с каких устройств пользователь заходил и откуда подключался к сети. Если в компании запрещено использование посторонних устройств, система должна сигнализировать, если пользователь авторизовался на чужом компьютере, даже если его собственная машина продолжает работать. Часто такие случаи связаны со скомпрометированной учетной записью, которая пытается распространиться на другие устройства или аутентифицироваться на них для получения доступа к данным, включая учетные записи других пользователей.

Существуют различные подходы к использованию моделей угроз в области информационной безопасности. Один из них - это статический подход. В этом случае система реагирует на определенные события, например, аутентификацию администратора на клиентской машине. Этот список администраторов может быть заранее задан или система сама может выделять администраторов без участия пользователя.

Модели угроз также могут быть автоматическими. В этом случае мониторинговая интеллектуальная система определяет типичное поведение пользователя, анализирует действия пользователей с аналогичными обязанностями, учитывает другие факторы и создает модель поведения. Исходя из этого профиля, система может определить, что пользователь не должен был получать доступ или копировать определенные данные с определенного ресурса.

Однако, ложные срабатывания являются серьезной проблемой для администратора безопасности. Каждый аналитик, работающий в департаменте кибербезопасности, может проверить только ограниченное количество оповещений. Если количество оповещений значительно превышает доступные

ресурсы, они ставятся в очередь. Очередь оповещений может продолжать расти, а затем сбрасываться, так как нет другого выхода из ситуации.

Другой подход заключается в добавлении исключений вручную. Например, можно массово удалить записи DNS для предотвращения доступа к определенным ресурсам. Таким образом, администратор безопасности должен иметь доступ к разнообразной информации, чтобы эффективно отслеживать и контролировать действия пользователей. Использование моделей угроз и различных подходов позволяет более точно определять потенциально опасную активность и принимать соответствующие меры для обеспечения безопасности компании.

С самообучением систем есть одна проблема: одни и те же действия могут несколько раз быть распознаны как вполне легитимные, но в какой-то момент подобная активность окажется действием злоумышленника. Например, пользователь 100 раз выполняет поиск файлов в одной и той же папке, система «учится» считать это действие нормальным, а на 101-ый раз пользователь начинает массово копировать оттуда файлы (особенность работы в Windows состоит в том, что зачастую поиск и копирование файлов неотличимы). Обученная система считает исход успешно проанализированным, что на самом деле является неверным выводом [7].

В завершение хотелось бы отметить, что при удаленной работе поведенческий анализ становится еще более необходимым. Расплывающиеся границы компании приводят к тому, что защитить учетные записи сотрудников от взлома становится сложной задачей. Поэтому компании нужно не только обнаруживать признаки атаки на систему, но и анализировать, какие цели мошенники преследовали и были ли их действия прекращены вовремя.

Важным аспектом является также анализ активности внутренних сотрудников. Проведение автоматического анализа поведения сотрудников на ресурсах компании позволяет выявлять отклонения от привычного поведения. Это помогает выявлять потенциальные угрозы со стороны инсайдеров, которые

могут злоупотреблять своими привилегиями, особенно во время их свободного времени.

Существует процесс обеспечения кибербезопасности, направленный на анализ поведения пользователей и связанный с обнаружением внутренних угроз, целевых атак и финансового мошенничества - User Behavior Analytics.

Первое, что предполагает под собой этот подход – анализ истории активности пользователя на рабочем персональном компьютере. Так формируются нормальные и вредоносные модели поведения.

Также, работая с различными типами данных, технология выявляет их на основе прошлых и текущих сессий. Это могут быть позиции и должности сотрудников, геоданные, роли для доступа, активность в сети и оповещения о безопасности. Важными факторами являются продолжительность сессии и затронутые пользователем интернет-ресурсы.

Технология UBA подразумевает визуализацию приоритетных данных. С помощью неё отлично распознаются достоверные аномалии в числе многочисленных рисков, оценивается уровень потенциального негативного влияния пользователя на систему организации. Таким образом, специалисты по информационной безопасности могут расставлять приоритеты для решения проблем и предотвращения последствий [8, 9].

Кроме того, с точки зрения информационной безопасности такой анализ имеет большое значение. Предотвратить угрозы и посягательства на активы компании гораздо дешевле, чем восстанавливаться после атаки и ликвидировать последствия. Поэтому инвестиции в решения поведенческого анализа оправданы и помогают обеспечить безопасность и защиту конфиденциальной информации компании [10].

СПИСОК ИСТОЧНИКОВ

1. Гречанная, А.Ю. DLP-системы и их роль в защите от утечек конфиденциальной информации / А.Ю. Гречанная, А. Д. Тастенов // Наука и техника Казахстана. — 2015. — №3-4 — С. 23-27 — URL: https://cyberleninka.ru/article/n/dlp-sistemy-i-ih-rol-v-zaschite-ot-utechek-konfidentsialnoy-informatsii (дата обращения: 16.10.2023).

2. Сокол, Д.С. Использование искусственных нейронных сетей для выбора DLP-систем [Электронный ресурс] / Д.С. Сокол, А.Р. Айдинян, О.Л. Цветкова // Символ науки. — 2016. — №1. — С. 94-97. — URL: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennyh-neyronnyh-setey-dlya-vybora-dlp-sistem (дата обращения: 16.10.2023).

3. Писаренко, И.В. Нейросетевые технологии в безопасности [Электронный ресурс] / И.В. Писаренко // Информационная безопасность. — 2009. — № 4. — С. 34-35. — URL: https://lib.itsec.ru/articles2/Oborandteh/neyrosetevye-tehnologii-v-biznese (дата обращения: 16.10.2023).

4. Алексеев, И.В. Программная реализация модуля DLP-системы для мониторинга и анализа трафика корпоративной сети с использованием машинного обучения [Электронный ресурс] / И.В. Алексеев, М.А. Митрохин, Е.А. Кольчугина // Безопасность информационных технологий. — 2020. — Т. 27, №1. — С. 28-39. — URL: https://bit.mephi.ru/index.php/bit/article/view/1252 (дата обращения: 16.10.2023).

5. Арзамасцев, Н.А. Особенности использования искусственных нейронных сетей в сфере информационной безопасности [Электронный ресурс] / Н.А. Арзамасцев // StudNet. — 2022. — №5. — URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-iskusstvennyh-neyronnyh-setey-v-sfere-informatsionnoy-bezopasnosti (дата обращения: 16.10.2023).

6. Шабуров, А.С. Технические аспекты внедрения DLP-системы на основе Falcongaze Secure Tower [Электронный ресурс] / А.С. Шабуров, Е.Е.

Журилова, В.С. Лужнов. —// Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. — 2015. — №4. — С. 57-67. — URL: https://ered.pstu.ru/index.php/elinf/article/view/2709 (дата обращения: 16.10.2023).

7. Бархатов, Н.А. Возможности применения нейронных сетей в информационной инфраструктуре предприятия [Электронный ресурс] / Н.А. Бархатов, Е.А. Ревунова, И.С. Ундалова // Инновационная экономика: перспективы развития и совершенствования. — 2020. — Т. 6, № 48. — URL: https://cyberleninka.ru/article/n/vozmozhnosti-primeneniya-neyronnyh-setey-v-informatsionnoy-infrastrukture-predpryatiya (дата обращения: 16.10.2023).

8. Савенков, П. А. Использование методов и алгоритмов анализа данных в мобильной UEBA/DSS-системе для решения задач информационной безопасности [Электронный ресурс]/ П. А. Савенков // Известия ТулГУ. Технические науки. 2019. №12. — URL: https://cyberleninka.ru/article/n/ispolzovanie-metodov-i-algoritmov-analiza-dannyh-v-mobilnoy-ueba-dss-sisteme-dlya-resheniya-zadach-informatsionnoy-bezopasnosti (дата обращения: 16.10.2023).

9. Нашивочников, Н. В. Топологические методы анализа в системах поведенческой аналитики [Электронный ресурс] / Н. В. Нашивочников, В. Ф. Пустарнаков // Вопросы кибербезопасности. — 2021. — №2(42). — URL: https://cyberleninka.ru/article/n/topologicheskie-metody-analiza-v-sistemah-povedencheskoy-analitiki (дата обращения: 16.10.2023).

10. Лисунова, М. Е. Разработка систем поведенческого анализа [Электронный ресурс] / М. Е. Лисунова // Молодой ученый. — 2019. — № 19 (257). — С. 9-10. — URL: https://moluch.ru/archive/257/58848/ (дата обращения: 16.10.2023).

Секция 4

КИБЕРБЕЗОПАСНОСТЬ

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

Секретарь: **Рыбаков Сергей Юрьевич**,
Московский технический университет связи и информатики, ассистент кафедры «Информационная безопасность»

Затеев С. В.
Научно-инжиниринговый центр
«Доверенные системы на основе АПК» ТУСУР, техник
zateev.stanislav@gmail.com

ПРОДЛЕННАЯ АУТЕНТИФИКАЦИЯ НА ОСНОВЕ АНАЛИЗА КЛАВИАТУРНОГО ПОЧЕРКА

В современном мире цифровые технологии применяются во всех сферах нашей жизни. Огромное количество информации личного характера и информации иных видов, требующих соблюдения ее конфиденциальности, хранится в цифровом виде. Как показывает практика [1 – 3], огромное количество конфиденциальных данных сливаются в сеть, утечка крупного пула данных не редкость.

Для соблюдения конфиденциальности информации требуется применение необходимых средств защиты. Одними из наиболее распространенных СЗИ являются средства идентификации и аутентификации пользователей. Этот же вид СЗИ является одним из самых действенных.

Как известно аутентифицировать пользователя можно тремя основными способами: то, что пользователь знает (пароль); то, что пользователь имеет (токен) или биометрические данные пользователя. Очевидно, что первые 2 способа уступают в надежности 3-му, т.к. ключ относительно просто скомпрометировать. 3-й способ гораздо более надежный, однако, он требует серьезных затрат (в основном на оборудование для считывания биометрических данных). Одним из типов биометрических данных, которые можно использовать для аутентификации пользователя (как показывают исследования [4 – 6]), но при этом не требуется дорогостоящего оборудования для считывания, является клавиатурный почерк, который определяется специфическими особенностями в динамике работы с клавиатурой компьютера.

Также следует понимать, что стандартные средства идентификации и аутентификации пользователя являются рубежным средством защиты информации, т.е. разовый подбор злоумышленником ключа предоставит ему дальнейшую свободу действий. Вышеописанную проблему решают средства продленной аутентификации пользователя – СЗИ выполняющие процесс аутентификации все время нахождения пользователя в системе. СЗИ именно такого типа можно выстроить при помощи анализа клавиатурного почерка.

Итак, для построения подобной системы необходимо собрать данные о работе пользователей с клавиатурой, выделить признаки, на основе которых можно было бы определить пользователя, и построить классификатор, который мог бы эту работу провести.

В распоряжении имеются данные о работе с клавиатурой 25 пользователей. При этом для каждого пользователя имеется примерно 200 – 250 тысяч записей. Каждая запись описывает одно произошедшее событие и представляет из себя вектор из 5 значений: идентификатор пользователя, идентификатор сеанса (каждый пользователь записывался в несколько сеансов), идентификатор клавиши, тип события (нажатие или отпускание клавиши) и временная метка события.

Затем необходимо выделить признаки, которые бы могли охарактеризовать динамику работы пользователя с клавиатурой. Вполне логичным выбором было бы выделение общих признаков, характеризующих работу с клавиатурой: общее время интервала, процент ошибок с учетом и без учета затраченного времени, скорости spm, netto, brutto*, степень аритмичности и другие признаки, какие были, например, предложены в работе [7]. Но как показывает практика [8, 9] наибольшую точность работы выдает анализ определенных конструкций (сочетаний) клавиш. Также этот способ позволяет выделить большое количество признаков. Однако, необходимо понимать, что если вероятность постоянного использования всех клавиш (в первую очередь соответствующих буквам) в процессе написания текста достаточно велика, то вероятность использования большинства их сочетаний либо критически низка

(что приводит к статистической незначительности самих параметров), либо исключена вовсе (например, сочетания «аь», «оъ», «ааа» и т.д.).

Это приводит к тому, что количество признаков становится избыточным, а подавляющее большинство признаков являются неинформативными. Следовательно, стоит проблема сокращения признакового пространства. В качестве способа сокращения в итоге был использован банальный выбор наиболее часто употребляемых конструкций. Как показывают исследования [10], для достижения приемлемой точности достаточно ограниченного количества сочетаний клавиш. Также в процессе работы использовался метод главных компонент для сокращения признакового пространства, однако, он не улучшил качество работы модели, поэтому было решено от него отказаться.

Отдельного упоминания заслуживает выбор признаков сочетаний клавиш. Если для одиночной клавиши признак всего один и он очевиден: это продолжительность нажатия клавиши (рассчитывается как время между нажатием и отпусканием клавиши), то для сочетаний клавиш эти признаки необходимо выделять отдельно для каждого типа сочетаний (сочетания, состоящие из 2-х, 3-х и т.д. клавиш), при этом необходимо выделить их таким образом, чтобы они полностью (однозначно) описывали конструкцию, но при этом не были избыточными.

Для биграмм (сочетание из двух клавиш) этот набор признаков представляет из себя следующее: время между нажатием первой клавиши и нажатием второй, время между нажатием первой клавиши и отпусканием второй и время между отпусканием первой клавиши и нажатием второй. Данные признаки наглядно изображены на схеме, представленной на рисунке 1.

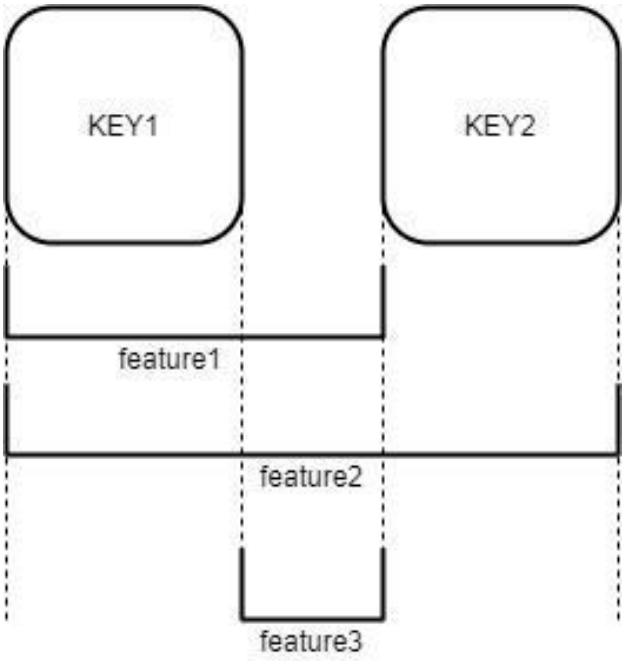

Рис.1 – Признаки нажатия биграмм

Для конструкций, содержащих более 2-х клавиш, можно определить набор признаков рекурсивным способом. Схему данного выделения признаков можно увидеть на рисунке 2. На рисунке 2 KEY(1)...KEY(N) – N-грамма, которая имеет свои (2*N - 1) своих признаков, KEY(N+1) – дополнительная клавиша, которая вместе с предыдущей N-граммой образует (N+1)-грамму. Принцип определения 2-х недостающих признаков представлен на рисунке.

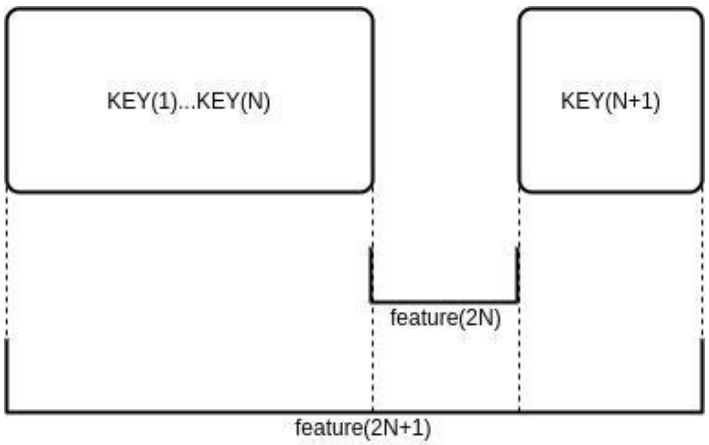

Рис 2. – Признаки нажатия N-грамм

Для формирования набора данных для работы классификатора был выбран следующий принцип. Весь поток событий разбивается на группы фиксированного размера (окна). В каждом окне для каждой конструкции вычисляется набор значений признаков, описанных выше. Но так как конструкция может встретиться в окне несколько раз, то в набор характеристик окна идут не значения выделенных выше признаков, а статистические характеристики выборки значений признаков в пределах окна: среднее выборочное значение, среднеквадратичное отклонение и коэффициент асимметрии. Таким образом формируется вектор признаков, описывающих окно. Из таких векторов и формируется итоговый датасет.

Подобный принцип формирования данных определяет набор настраиваемых параметров, которые влияют на качество работы модели.

Первый такой параметр – типы изучаемых сочетаний. В рамках описываемой модели использовались наиболее часто употребляемые одиночные клавиши, биграммы и триграммы. В процессе изучения вопроса также использовались тетраграммы, пентаграммы и слова (конструкции от пробела до пробела). Однако, в рамках ограниченного интервала вероятность хотя бы разовой встречи таких конструкций крайне мала, поэтому приличная часть признаков оказывалась неинформативной, но очень удобной для классификатора, что приводило к его переобучению. Поэтому от этих конструкций было решено отказаться.

Второй параметр – количество используемых сочетаний для каждого типа. Выбор малого количества конструкций может привести к недостатку информативных признаков, которые могут сильно повлиять на качество работы модели, выбор чрезмерного количества конструкций приведет к переобучению моделей, как описывалось выше. В рамках описываемой модели использовалось 30 одиночных клавиш, 70 биграмм и 20 триграмм.

Третий и четвертый параметры – размер окна и процент перекрытия между окнами (отношение количества событий, принадлежащим обоим соседним окнам, к размеру окна). Малый размер окна приводит к нарушению

статистической точности, большой размер окна позволяет охватить больше событий, но при этом замедляет работу системы. Перекрытие же окон позволяет им учитывать контекст друг друга. В рамках описываемой модели исследовалась зависимость качества работы модели от данных параметров. В качестве размера окна использовались значения 1000 и 2000 событий. Процент перекрытия варьировался от 0% до 75% с шагом в 25%.

В качестве классификатора использовались решающие деревья и случайные леса. В процессе работы настраивались следующие параметры: критерий (энтропия Шеннона и индекс Джини), глубина дерева (от 5 до 10), минимальный размер листа (10, 20 и 30), минимальный размер узла для разбиения (10, 20 и 30) и для лесов – количество деревьев (60, 70 и 80). Было выполнено обучение деревьев и лесов на тренировочных данных с применением кросс-валидации (количество выборок для кросс-валидации – 4).

Результаты работы модели сведены в таблицы, представленные на рисунках 3 и 4. Рисунок 3 – результаты работы деревьев, рисунок 4 – результат работы лесов. В таблицах указаны точность предсказания модели на тестовых данных (данных, которые модель не видела в процессе обучения) в графе accuracy, затем указаны оптимальные параметры классификатора из числа варьируемых (описаны выше). Также в последних 2-х столбцах указаны размер окна и шаг между первыми событиями в 2-х соседних окнах, который определяет процент перекрытия.

cv	accuracy	criterion	max_depth	min_samples_leaf	min_samples_split	size	step
4	0,859045	entropy	7	20	40	2000	2000
4	0,879498	entropy	8	20	30	2000	1500
4	0,88355	entropy	8	20	50	2000	1000
4	0,919498	entropy	9	20	20	2000	500
4	0,844565	entropy	9	20	30	1000	1000
4	0,876432	entropy	9	20	40	1000	750
4	0,887668	entropy	9	20	30	1000	500
4	0,923024	entropy	10	20	40	1000	250

Рис. 3 – Результаты работы решающих деревьев

cv	accuracy	n_estimators	criterion	max_depth	min_samples_leaf	min_samples_split	size	step
4	0,987791343	70	entropy	8	10	10	2000	2000
4	0,993305	80	entropy	8	20	10	2000	1500
4	0,996043	70	entropy	9	10	10	2000	1000
4	0,996574	80	entropy	9	10	10	2000	500
4	0,994565	80	entropy	8	10	10	1000	1000
4	0,995908	80	entropy	9	10	30	1000	750
4	0,997803	60	entropy	9	10	30	1000	500
4	0,996533	60	entropy	9	10	10	1000	250

Рис. 4 – Результаты работы случайных лесов

Таким образом, в очередной раз подтверждается, что динамика работы пользователя с клавиатурой пригодна для его аутентификации. Причем точность аутентификации достаточно высока (особенно у лесов), что подтверждают результаты работы созданной модели. Разработанный принцип формирования признаков для обучения и предсказания пригодны для использования в реальном времени, что очень важно для продленной аутентификации, в прозрачном для пользователя режиме.

СПИСОК ИСТОЧНИКОВ

1. Письма с конфиденциальной информацией украдены [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/utechki - informatsii/desyatki-tysyach-pisem-s-konfidentsialnoy-informatsiey-ukradeny (дата обращения 20.10.2023).
2. Утечки из сферы ИТ в первом полугодии 2023 года | Персональные данные [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/ analytics/daydzhesty-i-obzory/personalnye-dannye-utechki-iz-sfery-it-v-i-polugodii-2023-goda (дата обращения 20.10.2023).
3. Хакеры украли данные 7 млн студентов [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/utechki-informatsii/khakery-ukrali-dannye-semi-millionov-studentov (дата обращения 20.10.2023).
4. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической

аутентификации – [Электронный ресурс] – Режим доступа: http://docs.cntd.ru/document/1200048922 (дата обращения 20.10.2023).

5. ГОСТ Р 54412-2011/ISO/IEC/TR 24741:2007. Информационные технологии (ИТ). Биометрия. Обучающая программа по биометрии – [Электронный ресурс] – Режим доступа: http://docs.cntd.ru/document/1200094221 (дата обращения 20.10.2023).
6. ГОСТ ISO/IEC 24713-1-2013 Информационные технологии (ИТ). Биометрические профили для взаимодействия и обмена данными. Часть 1. Общая архитектура биометрической системы и биометрические профили – [Электронный ресурс] – Режим доступа: http://docs.cntd.ru/document/1200107284 (дата обращения 20.10.2023).
7. Тушканов Е.В. Разработка методов и алгоритмов повышения защищенности информации на основе анализа клавиатурного почерка: дис. канд. тех. наук: 05.13.19 – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, 2016
8. Казачук М.А. Динамическая аутентификация пользователей на основе анализа работы с клавиатурой компьютера: дис. канд. физ.-мат. наук: 05.13.11. – МГУ им. М.В. Ломоносова, Москва, 2019
9. Kang P. Keystroke dynamics-based user authentication using long and free text strings from various input devices / P. Kang, S. Cho //Information Sciences. – 2015. – Т. 308. – С. 72-93.
10. Al Solami E. User-representative feature selection for the keystroke dynamics. / E. Al Solami, C. Boyd, A. Clark, I. Ahmed // Proceedings of 2011 5th International Conference on Network and System Security. Institute of Electrical and Electronics Engineers Inc., United States – 2011. – С. 229-233.

Романова Н.Н.
Петербургский государственный университет путей сообщения, аспирант
romanova.nadezhda.00@mail.ru
Грызунов В.В.
Петербургский государственный университет путей сообщения,
Доцент кафедры Информатики и информационной безопасности
доктор технических наук, доцент.
viv1313r@mail.ru

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ЗЛОУМЫШЛЕННИКАМИ OSINT: СИСТЕМАТИЧЕСКИЙ ОБЗОР ЛИТЕРАТУРЫ

Аннотация

В данной статье рассматривается процесс поиска литературы для изучения проблемы обеспечения безопасности персональных данных при использовании злоумышленниками OSINT методом систематического обзора литературы. В процессе обзора определяются исследовательские вопросы, поисковые запросы, критерии включения и исключения, оценки качества найденных источников. Из отобранных источников литературы даются ответы на поставленные вопросы исследования.

Ключевые слова: OSINT, систематической обзор литературы, информационная безопасность, персональные данные.

Annotation

This article discusses the literature search process to study the problem of ensuring the security of personal data when OSINT is used by attackers using a systematic literature review. The review process identifies research questions, search queries, inclusion and exclusion criteria, and assessments of the quality of the sources

found. From selected literature sources, answers to the research questions are provided.

Key words: OSINT, systematic literature review, information security, personal data.

Определение систематического обзора литературы

В любом научном исследовании неотъемлемым и важным этапом является обзор литературы, в ходе которого необходимо изучить основные области главной теории, а также другие разработанные теории и их критику [1].

В данной статье рассматривается систематический обзор литературы (Systematic Literature Reviews – SLR). Он представляет собой методологию, используемую для идентификации, анализа и интерпретации соответствующих исследований для решения конкретных исследовательских вопросов [2].

Основными характеристиками SLR являются [3]:

1. Четкая постановка исследовательского вопроса, на который должно ответить исследование.

2. Поисковые запросы, включающие все связанные исследования, которые соответствовали бы критериям приемлемости.

3. Оценка качества выбранных исследований.

4. Систематическое представление и обобщение извлеченных данных из выбранных исследований.

5. Предоставление результатов исследования в распоряжение для научных целей и принятия решений.

Постановка исследовательского вопроса

Цель работы – идентификация угроз и существующих методов и средств обеспечения безопасности персональных данных пользователя и его репутации при использовании злоумышленниками OSINT, идентификация основных проблем при защите ПД пользователя с учетом OSINT.

С этой целью в нашем SLR рассматриваются следующие три исследовательских вопроса:

1. Какие существуют угрозы для безопасности персональных данных (ПД) пользователя и его репутации при использовании злоумышленниками OSINT?

2. Какие существуют методы и средства обеспечения безопасности ПД противодействующие OSINT?

3. Какие возникают проблемы при разработке методов и средств защиты ПД противодействующих OSINT?

Процесс поиска источников

На данном этапе необходимо определить стратегию поиска данных, которая помогает определить подходящую строку поиска и идентифицировать соответствующие базы данных для сбора соответствующей документации [4]. Количество баз данных для поиска в значительной степени определяется характером тематической области [5].

Определение цифровых библиотек

Для библиотек были определены следующие критерии:

1. Содержит материалы русских авторов.
2. Содержит материалы зарубежных авторов.
3. Часто обновляется.
4. Содержит материалы на тему информационная безопасность.

Для поиска были выбраны две системы: eLIBRARY и Google Scholar.

Формирование поисковых запросов

Было определено три поисковых запроса (Табл. 1). Ключевые слова «персональные данные» и «репутация» использовались для конкретизации вида защищаемой информации. «Угрозы», «средства защиты», «проблемы» и их синонимы определяют основную тему каждого поискового запроса. «OSINT» ограничивает поиск по конкретной технологии. Для составления поисковых

запросов использовались логические операторы И (&) для сужения области поиска, ИЛИ (|) для добавления результатов содержащих похожие данные.

Табл. 1 Поисковые запросы

№	Содержание поискового запроса
ПЗ1	(персональные данные | репутация) & (угрозы | уязвимости | риски) & OSINT
ПЗ2	(средства защиты | методы защиты | способы защиты) & (персональные данные | репутация) & (против | противодействующих) & OSINT
ПЗ3	(проблемы | риски | трудности) & (разработка | создание | проектирование) & (средства защиты | методы защиты | меры защиты | способы защиты) & (против | противодействующих) & OSINT

Результаты поиска. Промежуточный результат

Мы получили 320 статей по первому поисковому запросу из двух источников, 611 – по второму, 724 – по третьему (Табл. 2).

Табл. 2 Результаты поисковых запросов

№ поискового запроса	Количество найденных исследований в eLIBRARY	Количество найденных исследований в Google Scholar
ПЗ1	136	184
ПЗ2	196	315
ПЗ3	79	445
Итого	1355	

Критерии включения и исключения

Для получения первичного списка исследований были определены следующие критерии включения и исключения:

1. Первый этап отбора – отбор по названиям, ключевым словам:

1.1. (Исключение) Это не первичное исследование. Обзоры литературы отбрасываются.
1.2. (Исключение) Это не статья для журнала, конференции или семинара.
1.3. (Исключение) Статья написана до 2020 года.
1.4. (Исключение) Статья описывает не техническую составляющую процесса.

2. Второй этап отбора – отбор по аннотациям, полным текстам:
   2.1. (Включение) В исследовании рассматриваются угрозы безопасности ПД возникающие при использовании злоумышленниками OSINT.
   2.2. (Включение) В исследовании рассматриваются способы защиты ПД от OSINT.
   2.3. (Включение) В исследовании рассматриваются проблемы, возникающие при защите ПД против OSINT.

На первом этапе отбора с помощью встроенных в используемые поисковые машины фильтры мы исключили 942 исследования. После исключения повторяющихся источников ручной проверкой, было получено 228 исследований для дальнейшего анализа.

После второго этапа – было отброшено 135 результатов. Таким образом, для дальнейшего анализа было отобрано 93 исследования (Табл.3).

Табл. 3 Результаты поисковых запросов после отбора

№ поискового запроса	Количество найденных исследований в eLIBRARY	Количество найденных исследований в Google Scholar
Первый этап отбора		
ПЗ1	16	55
ПЗ2	7	143
ПЗ3	7	185
Итого	413	

Без дубликатов	228
Второй этап отбора	
Итого	93

Оценка качества источников

На данном этапе необходимо полностью ознакомиться с текстом исследования из списка результатов и ответить на вопросы оценки качества:

1. Ясно ли сформулированы цели и задачи исследования?
2. Сравнивается ли исследование со связанными работами?
3. Имеют ли выводы четкое изложение и теоретическую поддержку?
4. Были ли использованы правильные методы исследования?
5. Учтены ли ограничения исследования?
6. Журнал публикации статьи входит в перечень ВАК?

Для каждого вопроса предусмотрены три варианта ответа и числовые коэффициенты: «Да» = 1, «Частично» = 0.5, «Нет» = 0.

После ответа на все вопросы для каждого результата была получена количественная оценка качества. Все исследования, получившие оценку 3 и меньше были отброшены. Таким образом, мы отбросили 43 исследования и получили 50 источников для дальнейшего анализа.

Сбор данных

Все результаты, получаемые в п.3 и п.4, заносились в электронную таблицу Excel. В ней сохранялись полные ссылки источников для последующего цитирования, также отдельно были вынесены тип публикации, год, вопросы оценки качества и конечная оценка качества каждого источника. Таблица с результатами исследования представлена в приложении А.

Анализ данных

На основании собранных данным можно сделать вывод, что изучаемый вопрос стал активно исследоваться относительно недавно (Рис.1), количество публикаций значительно выросло в 2022 году (20 публикаций), по сравнению с предыдущими годами (2020 год – 7 публикаций, 2021 год – 8). За первое полугодие 2023 года количество публикаций достигло 14.

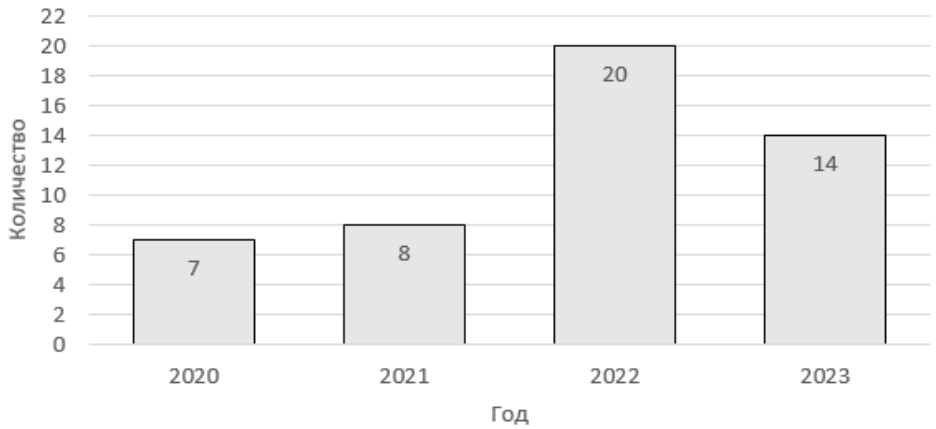

Рис. 1 Соотношение количества результатов к году их публикации

Что касается соотношения типов публикаций (Рис.2), то больше всего было опубликовано статей (31), чем материалов конференций (19).

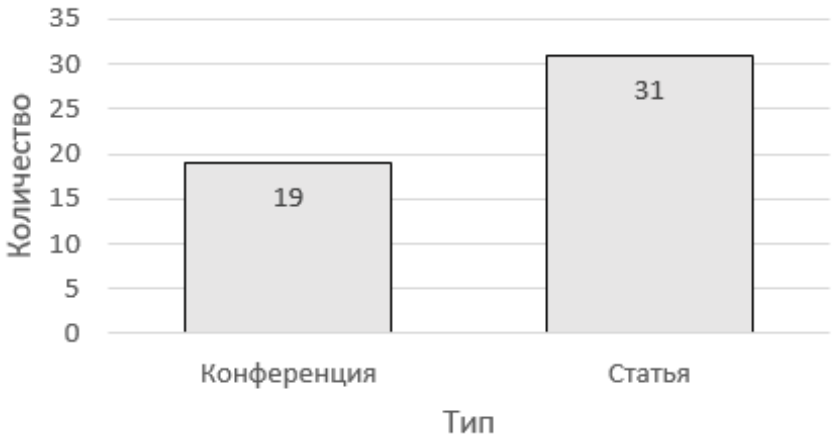

Рис. 2 Соотношение типов публикаций

Данные, полученные из результатов поиска

Какие существуют угрозы для безопасности персональных данных (ПД) пользователя и его репутации при использовании злоумышленниками OSINT?

Разведка по открытым источникам [6] (англ. Open source intelligence, OSINT) - включает в себя поиск, выбор, сбор и анализ информации из общедоступных источников. К «открытому источнику разведывательных данных» можно отнести: СМИ; публичные данные (правительственные отчеты, официальные данные о бюджетах и демографии и др.); «серая литература» (материалы научных, политических, социально-экономических и военных дисциплин и др.) [7].

OSINT можно категорировать следующим образом [7]: широкодоступные данные и информация; целевые коммерческие данные; мнение отдельных публичных экспертов; «серая литература», доступ к которой возможен только для определенной аудитории.

При использовании злоумышленниками OSINT нарушается одно из основных свойств информационной безопасности – конфиденциальность. Раскрытые конфиденциальные данные могут привести к следующим угрозам информационной безопасности:

1. Целевой атаки. Целевой фишинг отличается от обычного тем, что атака нацелена на конкретную жертву (конкретная организация/сотрудник/человек), отправляемые электронные письма более персонализированы, что повышает уровень доверия и, таким образом, успех атаки [8]. В данном случае, OSINT используется для сбора данных о жертве, на которых создаются / правдоподобные артефакты, заманивающие жертв к выполнению желаемого действия. К этой категории также относятся целевые атаки с использованием социальной инженерии, а также в целях доксинга (сбора и публикации персональной информации о человеке, часто из соображений мести) [9].

2. Нарушение работы информационных, производственных или других ресурсов организации [9]. С помощью OSINT можно осуществить сканирование IP-адресов, открытых портов, номеров телефонов, неправильно

настроенных хранилищ данных в облаке и других данных, которые позволяют обнаружить уязвимости организации и воспользоваться ими.

3. Взлом аккаунтов в социальных сетях с последующими правонарушениями. Зная персональные данные пользователей, злоумышленники могут попытаться взломать их аккаунты в онлайн-сервисах или социальных сетях [10]. Это может привести к утечке личной информации, финансовым потерям или даже краже личности.

4. Шантаж, вымогательство, нанесение ущерба репутации. Собрав достаточное количество персональной информации, злоумышленник может шантажировать жертву угрозой распространения информации в общем доступе [11]. В частности, такие атаки нацелены на публичных, популярных личностей, раскрытие персональных данных которых, может привести к угрозе для жизни.

Какие существуют методы и средства обеспечения безопасности ПД противодействующие OSINT?

Для защиты от атак, совершаемых с помощью OSINT можно использовать:

1. Обучение и повышение осведомленности. Часто исследуемые атаки происходят с помощью социальной инженерии и нацелены на человеческий фактор [8]. Необходимо проводить тренинги, на которых повышается осведомленность сотрудников об новых способах атак, о важности публикуемой в сети информации личной или о компании.

2. Контрразведка – OSINT против OSINT. Специалисты по информационной безопасности обычно прибегают к OSINT для оценки защищенности объекта, определению поверхности атаки для более успешного противодействия угрозам, выявлению утечек данных, идентификации готовящихся угроз, их источников и векторов, расследованию киберинцидентов и атрибуции атак [12].

3. Минимизация возможного ущерба. В случае OSINT достаточно сложно полностью защитить себя, но возможно уменьшить ущерб от атаки. Для этого

необходимо заранее установить и настроить средства защиты информации как для организации (сегментация сети, политики безопасности, разделение прав доступа и др.), так и для пользователя (сильные пароли, многофакторная аутентификация, настройки приватности и др.) [13].

4. Зашумление информации. Возможно запутать атакующего, добавив ложную/искажению информацию: чем больше информации у исследователя, тем сложнее определить достоверность данных с помощью OSINT. В этом случае требуется время и дополнительные усилия для выявления ложной информации и отбора надежных данных, что может оказаться нецелесообразным для злоумышленника [7].

Какие возникают проблемы при разработке методов и средств защиты ПД противодействующих OSINT?

Можно определить следующие трудности при построении средств защиты информации (СЗИ) от атак, совершаемых с помощью OSINT:

1. Большой объем данных получаемый от разведки по открытым источникам требует соразмерной вычислительной мощности или улучшенных алгоритмов обработки информации. Кроме того, важен корректный учет формализованных связей между данными, содержащимися в публикуемом пользователем контенте, и результатами, полученными с помощью разработанных инструментов оценки ряда идентификационных параметров личности нарушителя (источника угрозы). [12].

2. Человеческий фактор. Невозможно построить средство защиты полностью исключающее воздействие человеческого фактора.

3. Невозможность использовать иностранное программное обеспечение для разработки СЗИ из-за санкций и возможности внедрения недекларированных возможностей в исходный код зарубежного ПО [14], что усложняет процесс разработки комплексных систем защиты от рассматриваемых атак.

СПИСОК ИСТОЧНИКОВ

1. Бейкер М. Дж Написание обзора литературы // Пространство экономики. 2014. №3. URL: https://cyberleninka.ru/article/n/napisanie-obzora-literatury (дата обращения: 16.10.2023).

2. Alfonso I. et al. Self-adaptive architectures in IoT systems: a systematic literature review //Journal of Internet Services and Applications. – 2021. – Т. 12. – №. 1. – С. 1-28.

3. Mengist W., Method for conducting systematic literature review and meta-analysis for environmental science research / T. Soromessa, G. Legese //MethodsX. – 2020. – Т. 7. – С. 100777.

4. del Amo I.F., Erkoyuncu J.A., Roy R., Palmarini R., Onoufriou D. A systematic review of Augmented Reality content-related techniques for knowledge transfer in maintenance applications. Comput. Ind. 2018; 103:47–71. [Google Scholar].

5. Papaioannou D., Sutton A., Carroll C., Booth A., Wong R. Literature searching for social science systematic reviews: consideration of a range of search techniques. Health Info. Libr. J. 2010;27(2):114–122. [PubMed] [Google Scholar].

6. Соколов А.С. Разработка методики анализа защищенности информационной системы организации на основе открытых источников информации / А.В. Никитенко // Семьдесят пятая всероссийская научно-техническая конференция студентов, магистрантов и аспирантов с международным участием. Сборник материалов конференции. В 3-х частях. Ярославль, 2022. С. 188-191.

7. Сидорова, М. Е. Разведка по открытым источникам данных и ее применение для решения задач кибербезопасности / М. Е. Сидорова, А. Р. Кузьмин // Вестник Российского нового университета., Серия: Сложные системы: модели, анализ и управление. – 2023. – № 1. – С. 61-74. – DOI 10.18137/RNU.V9187.23.01.P.61. – EDN KKCSVG..

8. Матецкий М.А. Инструменты безопасности данных организации //Школа молодых новаторов. – 2023. – С. 80-83.

9. Дворянкин О.А. Современные технологии поиска информации в открытых источниках / Е.Н. Клочкова // Информационная безопасность: вчера, сегодня, завтра. Сборник статей по материалам VI Всероссийской научно-практической конференции., Москва, 2023. С. 64-68.

10. Hubbard J., IPASS: A Novel Open-Source Intelligence Password Scoring System / G. Bendiab, S. Shiaeles //2022 IEEE International Conference on Cyber Security and Resilience (CSR). – IEEE, 2022. – С. 90-95.

11. Дворянкин О. А. OSINT, PENTEST и несталкинг – информационные технологии интернета //Национальная ассоциация ученых. – 2022. – №. 84-2. – С. 6-13.

12. Гладнев В.В. Идентификация источников угроз информационной безопасности государственных информационных систем на основе открытых данных в интернете / М.В. Малый, К.Л. Стойчин, О.А. Пономарева // Безопасность информационного пространства. дополнение к сборнику научных трудов XXI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2023. С. 31-34.

13. Hwang Y. W. et al. Current status and security trend of osint //Wireless Communications and Mobile Computing. – 2022. – Т. 2022.

14. Воложанина Д.Н. Пересмотр процедуры оценки защищенности методами OSINT в условиях нестабильной международной политической обстановки //Актуальные проблемы авиации и космонавтики. – 2022. – С. 261-264.

15. Бондаренко Н.А. Характеристика OSINT и эффективность его использования / Т.М. Гусева // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики., Материалы XXII Международной научно-практической конференции. Ростов-на-Дону, 2022. С. 322-327.

Иванов Д.А.,
кандидат технических наук, преподаватель 1 кафедры филиала ВУНЦ ВВС «ВВА» в г. Челябинске.
Яцук К.В.,
доцент, преподаватель 23 кафедры филиала ВУНЦ «ВВС» в г. Челябинске.
Яковлев С.В.,
студент филиала высшего учебно-научного центра военно-воздушных сил «военно-воздушная академия» в городе Челябинске.

БЕЗОПАСНОСТЬ И ЕЕ ТЕОРЕТИЧЕСКИЕ ОСНОВЫ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Широкое применение компьютерных технологий в автоматизированных системах обработки информации и управления привело к обострению проблемы защиты информации, циркулирующей в компьютерных системах, от несанкционированного доступа. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жестко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно очень большое число угроз информации, которые могут быть реализованы как со стороны внешних нарушителей, так и со стороны внутренних нарушителей. В области защиты информации и компьютерной безопасности в целом наиболее актуальными являются три группы проблем:

1. нарушение конфиденциальности информации;
2. нарушение целостности информации;
3. нарушение работоспособности информационно-вычислительных систем.

Защита информации превращается в важнейшую проблему государственной важности.

Основы защиты информации в информационно-телекоммуникационных сетях

Защита информации превращается в важнейшую проблему государственной безопасности, когда речь идет о государственной, военной секретной информации. Огромные массивы такой информации хранятся в электронных архивах, обрабатываются в информационных системах и передаются по телекоммуникационным сетям. Основные свойства этой информации - конфиденциальность и целостность, должны поддерживаться законодательно, юридически, а также организационными, техническими и программными методами. Степень конфиденциальности выражается некоторой установленной характеристикой (особая важность, совершенно секретно, секретно, для служебного пользования, не для печати и т.п.), которая субъективно определяется владельцем информации в зависимости от содержания сведений, которые не подлежат огласке, предназначены ограниченному кругу лиц, являются секретом. Естественно, установленная степень конфиденциальности информации должна сохраняться при ее обработке в информационных системах и при передаче по телекоммуникационным сетям. Другим важным свойством информации является ее целостность (integrity). Информация целостна, если она в любой момент времени правильно (адекватно) отражает свою предметную область. Целостность информации в информационных системах обеспечивается своевременным вводом в нее достоверной (верной) информации, подтверждением истинности информации, защитой от искажений и разрушения (стирания). Несанкционированный доступ к информации лиц, не допущенных к ней, умышленные или неумышленные ошибки операторов, пользователей или программ, неверные изменения информации вследствие сбоев оборудования приводят к нарушению этих важнейших свойств информации и делают ее

непригодной и даже опасной. Ее использование может привести к материальному и/или моральному ущербу, поэтому создание системы защиты информации, становится актуальной задачей. Безопасность информации в информационной системе или телекоммуникационной сети обеспечивается способностью этой системы сохранять конфиденциальность информации при ее вводе, выводе, передаче, обработке и хранении, а также противостоять ее разрушению, хищению или искажению, а также путем организации допуска к ней, защиты ее от перехвата, искажения и введения ложной информации. С этой целью применяются физические, технические, аппаратные, программно-аппаратные и программные средства защиты. Последние занимают центральное место в системе обеспечения безопасности информации в информационных системах и телекоммуникационных сетях.

Комьютерные сети и обеспечение безопасности при работе с ними

Система безопасности компьютерной сети защищает целостность информации, содержащейся в сети, и контролирует, кто получает доступ к этой информации. Политики сетевой безопасности уравновешивают необходимость предоставления услуг пользователям и необходимость контроля доступа к информации.

Существует множество точек входа в сеть. Эти точки входа включают аппаратное и программное обеспечение, которые составляют саму сеть, а также устройства, используемые для доступа к сети, такие как стационарные и портативные устройства. Из-за этих точек входа сетевая безопасность требует использования нескольких методов защиты. Средства защиты могут включать брандмауэры — устройства, которые отслеживают сетевой трафик и предотвращают доступ к частям сети на основе правил безопасности.

Процессы аутентификации пользователей с помощью идентификаторов пользователей и паролей обеспечивают еще один уровень безопасности. Сетевая безопасность включает в себя изоляцию сетевых данных, чтобы доступ к частной или личной информации был сложнее, чем к менее важной

информации. Другие меры сетевой безопасности включают в себя регулярное обновление аппаратного и программного обеспечения, информирование пользователей сети об их роли в процессах безопасности и информирование о внешних угрозах, создаваемых хакерами и другими злоумышленниками. Сетевые угрозы постоянно развиваются, что делает сетевую безопасность бесконечным процессом.

Использование общедоступного облака также требует обновления процедур безопасности для обеспечения постоянной безопасности и доступа. Безопасное облако требует безопасной базовой сети. В ячеистой сети, узлы взаимодействуют, чтобы эффективно направлять данные к месту назначения. Такая сеть обеспечивает большую отказоустойчивость, поскольку при выходе из строя одного узла существует множество других узлов, которые могут передавать данные. Ячеистые сети самонастраиваются и самоорганизуются в поисках самого быстрого и надежного пути для передачи информации.

Существует два типа ячеистых сетей - полносвязанная и частично связанная: В полносвязанной топологии каждый сетевой узел соединяется с любым другим сетевым узлом, обеспечивая высочайший уровень отказоустойчивости. Тем не менее, это стоит дороже. В частично связанной топологии соединяются только некоторые узлы, обычно те, которые обмениваются данными чаще всего.

Беспроводная ячеистая сеть может состоять из десятков или сотен узлов. Этот тип сети подключается к пользователям через точки доступа, расположенные на большой территории.

Балансировщики нагрузки эффективно распределяют задачи, рабочие нагрузки и сетевой трафик между доступными серверами. Балансировщик нагрузки отслеживает весь трафик, поступающий в сеть, и направляет его к маршрутизатору или серверу, лучше всего оборудованному для управления им. Цели балансировки нагрузки - избежать перегрузки ресурсов, оптимизировать доступные ресурсы, улучшить время отклика и максимизировать пропускную способность.

Решения для компьютерных сетей помогают увеличить трафик, увеличить положительный отклик пользователей, защитить сеть и легко предоставлять услуги. Лучшее решение для компьютерных сетей - это, как правило, уникальная конфигурация, основанная на конкретных задачах и потребностях.

Основы сохранения безопасности информации в сети

Сетевая безопасность защищает сеть и данные от взломов, вторжений и других угроз. Это обширный и всеобъемлющий термин, который описывает аппаратные и программные решения, а также процессы или правила и конфигурации, относящиеся к использованию сети, доступности и общей защите от угроз. Сетевая безопасность имеет жизненно важное значение для защиты клиентских данных и информации, обеспечения безопасности общих данных и обеспечения надежного доступа и производительности сети, а также защиты от киберугроз. Хорошо продуманное решение сетевой безопасности снижает накладные расходы и защищает потерь, возникающих в результате утечки данных или другого инцидента безопасности. Обеспечение законного доступа к системам, приложениям и данным позволяет осуществлять бизнес-операции и предоставлять услуги и продукты клиентам. Брандмауэры контролируют входящий и исходящий трафик в сетях с заранее определенными правилами безопасности. Брандмауэры защищают от недружественного трафика и являются необходимой частью ежедневных вычислений. Сетевая безопасность в значительной степени зависит от брандмауэров, и особенно брандмауэров следующего поколения, которые фокусируются на блокировании вредоносных программ и атак прикладного уровня. Сегментация сети определяет границы между сегментами сети, где активы внутри группы имеют общую функцию, риск или роль в организации. Например, шлюз периметра сегментирует сеть подразделения. Предотвращаются потенциальные угрозы за пределами сети, гарантируя, что конфиденциальные данные подразделения остаются внутри. Можно пойти дальше, определив дополнительные внутренние

границы внутри своей сети, которые могут обеспечить улучшенную безопасность и контроль доступа. Контроль доступа определяет людей или группы и устройства, которые имеют доступ к сетевым приложениям и системам, тем самым отрицая несанкционированный доступ и, возможно, угрозы.

Удаленный доступ VPN обеспечивает удаленный и безопасный доступ к корпоративной сети отдельным хостам или клиентам, таким как удаленные компьютеры, мобильные пользователи и внешние потребители. Каждый хост обычно имеет загруженное программное обеспечение VPN-клиента или использует веб-клиент. Конфиденциальность и целостность конфиденциальной информации обеспечивается благодаря многофакторной аутентификации, сканированию соответствия конечных точек и шифрованию всех передаваемых данных. Модель безопасности с нулевым доверием гласит, что пользователь должен иметь только доступ и разрешения, необходимые ему для выполнения своей роли. Это совсем другой подход, чем традиционные решения безопасности, такие как VPN, которые предоставляют пользователю полный доступ к целевой сети. Zero trust network access (ZTNA), также известный как software-defined perimeter (SDP) solutions, разрешает гранулированный доступ к приложениям организации от пользователей, которым требуется этот доступ для выполнения своих обязанностей. Системы предотвращения вторжений (IPS) могут обнаруживать или предотвращать атаки сетевой безопасности, такие как атаки методом перебора, атаки типа "Отказ в обслуживании" (DoS) и эксплойты известных уязвимостей. Когда объявляется эксплойт, у злоумышленников часто появляется возможность использовать эту уязвимость до применения исправления безопасности. В этих случаях можно использовать систему предотвращения вторжений для быстрого блокирования этих атак.

СПИСОК ИСТОЧНИКОВ

1. Иванов Д.А., Коцыняк М.А., Мамай А.В., Карасев И.В. Оценка качества роботизированных систем в условиях деструктивных информационных воздействий // Информационные технологии и системы: управление, экономика, транспорт, право – 2019: № 1 (33). С. 192-194.

2. Иванов Д.А., Мамай А.В., Спицын О.Л., Карасев И.В. Подход к обоснованию структуры воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // Информационные технологии и системы: управление, экономика, транспорт, право – 2019: № 2 (34). С. 107-110.

3. Багрецов С.А., Лаута О.С., Иванов Д.А., Михаил И.И. Методика обоснования рационального количества резервных каналов связи в информационно-телекоммуникационной сети // Электросвязь – 2020: № 8. С. 31-38.

4. Гудков М.А., Лаута О.С., Иванов Д.А., Соловьев Д.В. Применение методов искусственного интеллекта в задачах обеспечения информационной безопасности // Современные информационные технологии – 2018: С. 162.

5. Одоевский С.М., Багрецев С.А., Лебедев П.В., Иванов Д.А. Модель функционирования системы технологического управления инфокоммуникационной сетью специального назначения в условиях воздействия дестабилизирующих факторов // Известия Тульского государственного университета. Технические науки – 2021: № 2. С. 324-334.

6. Коцыняк М.А., Бударин Э.А., Карпов М.А., Муртазин И.Р., Иванов Д.А. Воздействие нарушителя на беспроводные сети передачи данных по уровням эталонной модели взимодействия открытых систем // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». II Всероссийская научно-техническая конференция – 2020: С.139-146.

7. Лаута О.С., Федоров В.Х., Баленко Е.Г., Васюков Д.Ю., Иванов Д.А. Подход к работе системы защиты сети передачи данных от компьютерных атак

на основе гибридной нейронной сети // Инженерный вестник Дона – 2023: № 1 (97). С. 237-250.

8. Башлаков П.В., Мелехов К.В., Иванов Д.А., Ярош А.А. Распределение хранения информации на объектах электронного документооборота // Технологии. Инновации. Связь. СПб. – 2023: С. 233-238.

Пономарёв К.Г.
Дальневосточный федеральный университет, аспирант 2 курса
Института математики и компьютерных технологий
ponomarev.kg@dvfu.ru
Верещагина Е. А.,
everesh@mail.ru
Департамент программной инженерии и искусственного интеллекта
Дальневосточного федерального университета, научный руководитель,
кандидат технических наук

ПРИНЦИПЫ КОНТРОЛЯ РЕЧЕВОГО ПОТОКА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ С ПРИМЕНЕНИЕМ СИСТЕМЫ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сбор и управление информации является базовым принципом работы системы управления событиями информационной безопасности, что позволяет вести автоматический поиск подозрительной активности или явных инцидентов информационной безопасности. Классическим подходом систем такого вида является сбор сетевой активности хостов, маршрутизаторов и иного сетевого оборудования организации. На основании получаемых данных происходит классификация и корреляция событий. Однако существует потребность в защите телефонных коммуникаций в организациях от нового вида кибератак на голосовые биометрические системы по методу спуфинг атак [1]. В первую очередь угрозу информационной безопасности может представлять для банковских организаций, активно внедряющие цифровые сервисы биометрической авторизации и взаимодействия с клиентами. Спуфинг атаки основаны на подмене реальной речи имитирующей модели. Таким образом, необходимо развивать механизмы защиты информации с применением

технологий высокоточных математических моделей сбора звуковой информации и развития анализа с применением нейронных сетей [2].

Звуковой поток информации может стать предметной областью для исследований в сфере информационной безопасности, что позволит определить инциденты безопасности, на которые должен обратить внимание аналитик безопасности. В данной статье излагаются основные принципы категоризации и корреляции речевой информации и практические примеры их использования.

Обычно в системах управления событиями информационной безопасности реализован специализированный модуль sniffer (перевод с английского анализатор, перехватчик, нюхач) для записи разговоров с микрофона при проведении корпоративных разговоров или совещаний. В некоторых программных решениях указанный модуль может иметь название microphone controller, однако в любом случае использует единый алгоритм распознавание звуков человеческой речи и шума Voice Activity Detection (VAD). Стоит отметить, что указанный алгоритм нашел практическое применение в звуковой аппаратуре для формирования чистоты сигнала, корректировки диктора и создания стенограмм с помощью вычислительной техники. Рассмотрим подробнее структуру алгоритма VAD.

Основной задачей VAD является выделение речи из шума и тишины. Входной переменной соответственно является часть аудиозаписи, выходным параметром будет вероятность появления речи в исследуемой аудиозаписи. Для правильной работоспособности алгоритма VAD необходимо выполнить следующие ключевые условия: задержка или длина аудио, точность или минимизация ложных срабатываний алгоритма, генерализируемость или возможность работы из различных источников, с разным уровнем шума и разной громкостью голоса.

В настоящее время также существуют готовые модели анализа потока WEBRTCVAD, Picovoice VAD, OLD Silero VAD, которые могут взять разработчики за основу реализации собственного программного решения.

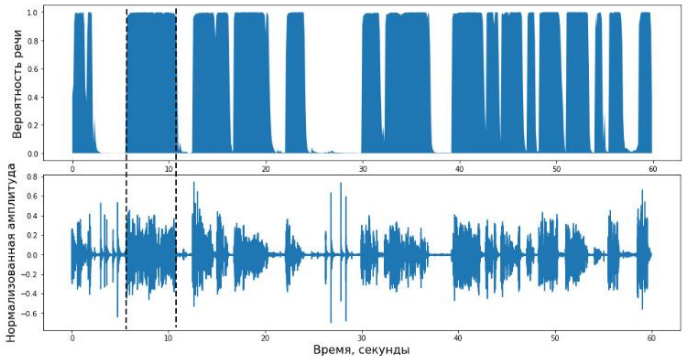

Рис. 1. Пример преобразованного аудиосигнала алгоритмом VAD

Разнообразие моделей анализа потока и математических подходов преобразования аудиосигналов обусловлено сложностью разделения речевой информации и шума. Любой аудиопоток предварительно делится на фреймы длиной 20-30 мс. Для каждого фрейма проводятся вычисления, в соответствии с которыми принимается решение о наличии речевой информации (Рис. 1).

Одним из признаков выявления речи является частота пересечения нуля Zero Crossing Rate (ZCR) или иными словами скорость изменения знака сигнала в течение кадра [3]. Частота пересечения нуля интерпретируется как мера шума сигнала. ZCR измеряется следующей формулой:

$$Z(i) = \frac{1}{2W_L}\sum_{n=1}^{W_L}|sgn[x_i(n)] - sgn[x_i(n-1)]|, 6$$

где sgn – знаковая функция, принцип работы которой описывается следующей функцией

$$sgn[x_i(n)] = f(x) = \begin{cases} -1, x_i(n) < 0 \\ 1, x_i(n) \geq 0 \end{cases}$$

Другим отличительным признаком для выявления речи является энтропия энергии аудиосигнала, характеризующая всплеск изменения энергии. Для преобразования аудиосигнала потребуется поделить каждый кадр на K подкадров равной величины. Таким образом, для каждого подкадра j вычисляется энергия кадра по следующей формуле [4]

$$e_j = \frac{E_{подкадра\ j}}{E_{кадра\ i}} = \frac{E_{подкадра\ j}}{\sum_{k=1}^{K} E_{подкадра\ k}}$$

Энтропия H(i) последовательности e_j описывается формулой

$$H(i) = -\sum_{j=1}^{K} e_j * \log_2(e_j)$$

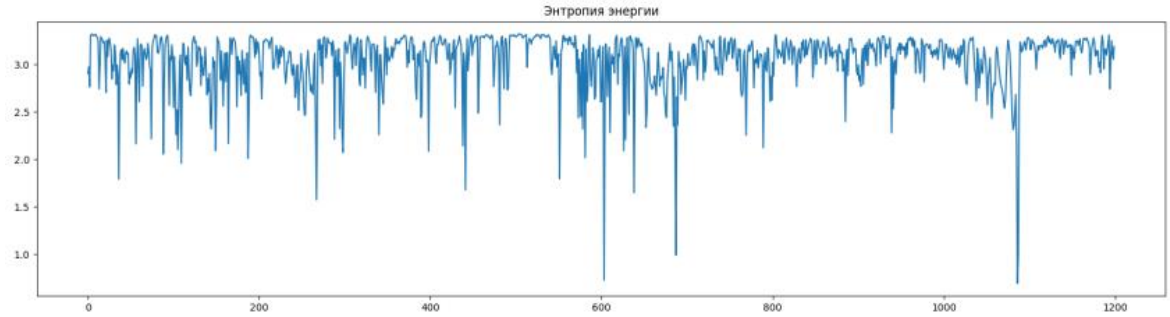

Рис. 2 Пример визуального представления энтропии энергии аудиосигнала

Данный признак использует аномальные всплески и выбросы энергии, что позволяет определить, к примеру, жанр музыки (Рис 2).

Также существует признак частотной области, использующий преобразование Фурье [5]. Такой подход в удобной форме предоставляет спектр звука и распределяет содержание частоты звуков. Используется мера спектрального центройда, указывающего центр масс спектра аудиозвука. Данный признак представляется формулой [5]

$$C_i = \frac{\sum_{k=1}^{WfL} kX_i(k)}{\sum_{k=1}^{WfL} X_i(k)}$$

где $X_i(k)$ – амплитуда спектра для k-го значению частоты в спектре дискретного преобразования Фурье.

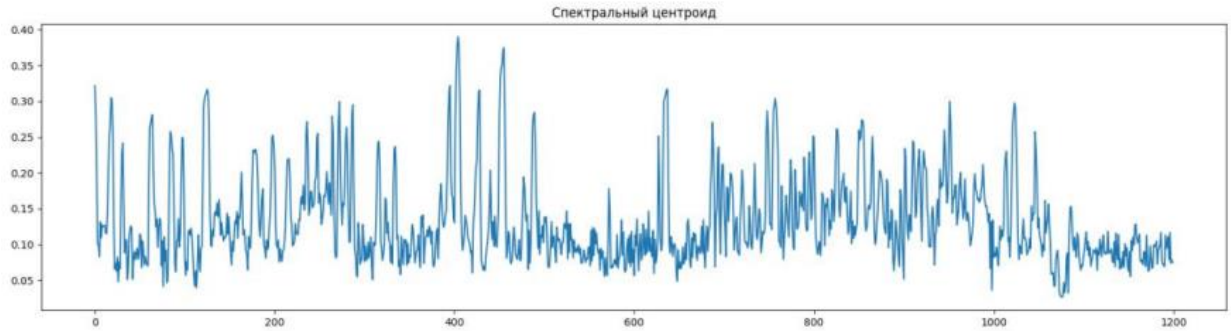

Рис 3. Пример визуального отображения реализации спектрального центроида

Следующий признак, характеризующий аудиосигнал, может использовать спектральный разброс [6]. Суть метода заключается в распределении вокруг центра масс аудиосигнала и описывается следующей формулой:

$$S_i = \sqrt{\frac{\sum_{k=1}^{W\,fL}(k - C_i)^2 * X_i(k)}{\sum_{k=1}^{W\,fL} X_i(k)}}$$

где k – значение частот дискретного преобразования Фурье, $X_i(k)$ – значения амплитуд, а C_i – значение спектрального центроида.

Стоит отметить, что в теории информации энтропия характеризуется мерой неопределенности источника сообщений и определяется как математическое ожидание количества информации в отдельных элементарных сообщениях по следующей формуле [7]

$$H = -\sum_{i=0}^{n} p_i * \log(p_i)$$

где p_i – вероятность появления i-го элементарного сообщения.

Следовательно, разработанный на математических подходах алгоритм VAD получает результат вне зависимости от громкости записи, что особенно важно при записи разговора через микрофон. Позволяет избегать сильных погрешностей, которые могут возникнуть из-за влияния выбросов, так как проводится расчет энтропии по средним значениям минимума и максимума [8]. Кроме того, с помощью математических вычислений можно определить эмоции человека на основании показателей энтропии, и с каким значением была произведена речь [9].

Обратимся к программным решениям в сфере информационной безопасности, а именно, к примеру реализации российским разработчиком «SearchInfrorm» специализированного модуля Microphone Controller.

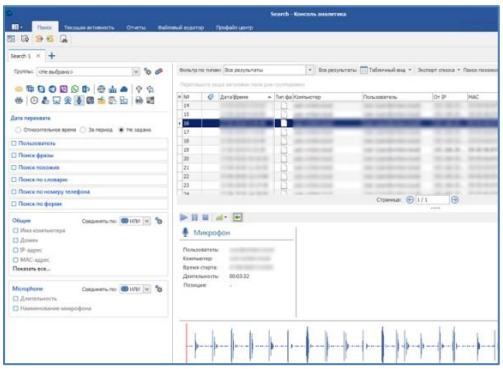

Рис 4. Пример реализации контроля за аудиопотоком в организации при проведении совещаний и выездных встреч на основе алгоритма VAD

Из примера работы специализированного модуля, опубликованного на официальном сайте компании разработчика «SearchInform» (Рис.4), мы видим сбор и корреляцию звуковой информации, а также хранение звуковых записей в отдельном файловом хранилище. По заявленным возможностям система защиты от утечек информации может автоматически анализировать аудиопоток, и используя атрибутивный поиск находить инциденты информационной безопасности. Непосредственно сам модуль устанавливается в качестве агента и может незаметно для пользователя вести запись разговора. Однако все эти действия не могут быть реализованы без базового внедрения алгоритма VAD по выявлению речевой информации, в том числе принимая во внимание эмоции человека и иные ключевые фразы, позволяющие выявить ключевые инциденты в ходе служебных разбирательств [10].

СПИСОК ИСТОЧНИКОВ

1. Лаврентьева Г.М., Новосёлов С.А., Козлов А.В., Кудашев О.Ю., Щемелинин В.Л., Матвеев Ю.Н., Де Марсико М. Методы детектирования спуфинг-атак повторного воспроизведения на голосовые биометрические системы // Научно-технический вестник информационных технологий, механики и оптики. - 2018. - №3.

2. Саенко Максим Андреевич, Мельников Денис Александрович, Данилов Михаил Алексеевич Анализ уязвимостей беспроводных каналов передачи информации // Образовательные ресурсы и технологии. - 2023. - №1 (42).
3. Савенков И. Н., Ермоленко Т. В., Цыбик А. В. РАЗРАБОТКА VAD-АЛГОРИТМА НА ОСНОВЕ ГЛУБОКОГО ОБУЧЕНИЯ // Проблемы искусственного интеллекта. - 2022. - №1 (24).
4. Макаров Ярослав Владленович Исследование возможности выделения признаков в процессе аудиоанализа // Глобус: технические науки. - 2019. - №6 (30).
5. Сайгин Андрей Александрович, Плотникова Наталья Павловна Подготовка данных для обучения нейронных сетей, решающих задачу разделения источников сигнала // E-Scio. - 2023. - №3 (78).
6. Шарий Т.В. Автоматическая идентификация языков в зашумленных аудиосигналах // проблемы искусственного интеллекта. - 2020. - №1 (16).
7. Бочаров П.П., Печинкин А.В. Теория вероятностей и математическая статистика: учебное пособие для студ. вузов, обучающихся по напр. "Физика", "Прикладная математика и информатика". 2-е изд. М.: ФИЗМАТЛИТ, - 2005. - 296 с.
8. Тутубалин В.Н. Теория вероятностей: учеб. пособие для студ. вузов. М.: Академия, - 2008. - 358 с.
9. Первушин Е.А. Обзор основных методов распознавания дикторов // Математические структуры и моделирование / Омский гос. ун-т. Омск, - 2011. Вып. - 24. - с.41–54
10. Кисилёв В.В. Автоматическое определение эмоций по речи // Образовательные технологии. М., - 2012. - № 3. - с. 85–89.

Лобов Б.Н.
Южно-Российский государственный политехнический университет имени М.И. Платова (ЮРГПУ (НПИ)), доктор технических наук, профессор
blobov@yandex.ru
Загорулько А.Ф.
Южно-Российский государственный политехнический университет имени М.И. Платова (ЮРГПУ (НПИ)), магистр
Игнатьев Д.Р.
Южно-Российский государственный политехнический университет имени М.И. Платова (ЮРГПУ (НПИ)), студент
ignatev_daniil61@mail.ru

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ И ЧАСТНЫХ УЧРЕЖДЕНИЯХ И ОРГАНИЗАЦИЯХ ПОСРЕДСТВОМ АНАЛИЗА ЗАРУБЕЖНОГО И ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО-ОБЕСПЕЧЕНИЯ И ПРОГРАММ

Суть проблемы данного доклада сводится к замене иностранного ПО и программ на отечественные аналоги для исключения нарушения законодательства Российской Федерации, заранее встроенных уязвимостей в них, а также незаконного сбора и использования данных пользователей иностранными организациями. В настоящий момент необходимо поддерживать отечественных производителей программ и программного обеспечения, поскольку спрос и необходимость в нем с каждым днем растут все больше и больше.

Импортозамещение - процесс замены зарубежных продуктов и товаров на аналогичные, произведенные внутри страны [1]. В контексте информационной безопасности речь идет прежде всего об обеспечении контролируемости,

надежности и независимости программного и аппаратного обеспечения, всех предприятий на территории Российской Федерации.

Существенным толчком для развитя процесса имортозамещения в России, является введение санкций против нее со стороны западных стран в IT-сфере. В первую очередь это массовый уход крупных IT-компаний с российского рынка, таких как: Microsoft, TeamViewer, Cisco, Intel, IBM и др. С учетом такой позиции на западе по отношению к Российской Федерации, Указом Президента от 30.03.2022 № 166, установлен запрет на закупку Юридическими лицами иностранного ПО и программ в целях его использования на объектах критической информационной инфраструктуры с 31 марта 2022 года. А также с 1 января 2025 года, запрещается органам государственной власти использовать иностранное ПО.

Итак, зарубежные программы и программное обеспечение, которые активно используются в России, включают в себя широкий спектр продуктов различных компаний. Некоторые из них весьма популярны и широко применяются в различных сферах.

Одной из самых известных зарубежных программ является операционная система Windows [9], разработанная компанией Microsoft. Windows широко используется в России как на персональных компьютерах, так и на серверах. Еще одна популярная программа от Microsoft - офисный пакет Microsoft Office, который включает в себя программы для работы с текстовыми документами, электронными таблицами, презентациями и электронной почтой.

Среди других зарубежных программ, активно используемых в России, можно отметить:

1. Adobe Creative Cloud.

Adobe Creative Cloud представляет собой комплексное программное обеспечение для работы с графикой, дизайном и мультимедиа. В его состав входят приложения, такие как Adobe Photoshop, Illustrator, InDesign, Premiere Pro и многие другие. Adobe Creative Cloud используется профессионалами в области дизайна, маркетинга и мультимедиа для создания и редактирования

изображений, векторной графики, макетов, видео и аудиоматериалов. Он предлагает широкий набор инструментов и функций, позволяющих создавать высококачественный контент.

2. AutoCAD - программное обеспечение для создания и редактирования 2D и 3D чертежей, широко применяемое в области архитектуры и инженерии.

3. SAP - система управления предприятием, которая используется для автоматизации бизнес-процессов и управления ресурсами компании.

4. Oracle - база данных и программное обеспечение для управления базами данных, широко применяемое в корпоративной среде.

5. Google Workspace.

Google Workspace (ранее известный как G Suite) представляет собой набор облачных приложений и сервисов, разработанных Google. Он включает в себя приложения, такие как Gmail, Google Drive, Google Docs, Google Sheets и Google Slides. Google Workspace позволяет пользователям работать с документами, электронными таблицами, презентациями и электронной почтой в режиме реального времени, обмениваться файлами и совместно редактировать документы. Он отличается высокой доступностью, удобством использования и возможностью работы в режиме онлайн.

6. Slack.

Slack представляет собой коммуникационную платформу для командной работы и обмена сообщениями. Он предоставляет возможность создания различных каналов для общения, обмена файлами и интеграции с другими инструментами и сервисами. Slack удобен для командной работы, особенно для удаленных или распределенных команд, и позволяет эффективно совместно работать над проектамии обсуждать задачи. Он также поддерживает интеграцию с различными инструментами разработки, управления проектами и сервисами уведомлений.

Однако в России также разработано и используется множество отечественного программного обеспечения [5]. Некоторые из популярных отечественных программ включают в себя:

1. 1С:Предприятие - платформа для автоматизации учета и управления предприятием, широко применяемая в малом и среднем бизнесе. Он предлагает широкий спектр решений, включающих системы учета, управления персоналом, управления складом, финансовый учет и другие функциональные модули. 1С:Предприятие отличается гибкостью и настраиваемостью, позволяя организациям адаптировать программу к своим уникальным потребностям. Он также широко используется в государственном секторе и образовании;

2. Лаборатория Касперского - комплексное программное обеспечение для информационной безопасности, включающее в себя антивирусную защиту, защиту от вредоносных программ и другие инструменты. Программное обеспечение Kaspersky Lab широко используется как в корпоративном, так и в домашнем секторе, и известно своей надежностью и эффективностью в борьбе с различными видами киберугроз.

3. ALT Linux - российская операционная система, основанная на Linux, которая используется в различных сферах, включая государственные учреждения и предприятия.

4. SPARK.

SPARK - это бухгалтерская программа, разработанная российской компанией "Новая Система". Она предлагает инструменты для ведения учета, формирования отчетности и автоматизации финансовых процессов. SPARK широко используется в бухгалтерии и финансовом управлении различных организаций и отличается простотой использования и соответствием требованиям российского законодательства.

Конечно, это только небольшой обзор зарубежных и отечественных программ, активно используемых в России. В зависимости от конкретных потребностей и сферы деятельности, выбор программного обеспечения может быть очень широким и разнообразным.

Импортозамещение в контексте программного обеспечения и программ относится к стратегии, направленной на сокращение импорта и поддержку отечественного производства программных продуктов. Основная идея

заключается в замещении импортных программ российскими аналогами для укрепления местного рынка программного обеспечения и развития отечественной индустрии.

Цели проведения импортозамещения в сфере программного обеспечения могут включать [2]:

- Развитие отечественной IT-индустрии
- Снижение зависимости от иностранных поставщиков
- Безопасность и контроль данных
- Технологический прогресс и инновации

В целом, импортозамещение в сфере программного обеспечения и программ направлено на развитие отечественной IT-индустрии, снижение зависимости от иностранных поставщиков, обеспечение безопасности данных и стимулирование технологического прогресса в России.

В нынешней ситуации, российские операционные системы и программы имеют несколько основных преимуществ перед зарубежными:

Во-первых, безопасность. Прежде всего это заключается в том, что они разрабатываются с учетом особенностей российского законодательства и требований безопасности, но также они ничем не хуже в области защиты от вредоносного ПО и хакерских атак, поскольку более закрыты и не сильно актуальны среди обычных пользователей;

Во-вторых, национальные потребности. Только отечественные производители могут четко понимать, что нужно российским пользователям [3]. Такие программы поддерживают русский язык, имеют встроенную поддержку пользователей, а также соответствуют российским стандартам и сертификации, что в свою очередь отвечает требованиям нашего рынка;

И, в-третьих, легальность. На данный момент в связи с последними событиями, большинство зарубежных программ не соответствуют требованиям нашего законодательства, и, соответственно, их использование может быть противоправным, чего не может быть в случае с нашими, отечественными программами и программным обеспечением.

Анализ и определение зарубежного ПО и программ, используемых в отдельно взятых юридических, а также и в государственных учреждениях показывает нам, что для полной независимости, а также исключения возможных угроз или атак со стороны запада – замещения данного ПО и программ необходимо и максимально актуально.

СПИСОК ИСТОЧНИКОВ

1. Соловьев А.И. Импортозамещение в россии: проблемы и пути решения // Экономика. Налоги. Право. 2016. № 4. С. 66–71;
2. Муравник В.Б., Захаренков А.И., Добродеев А.Ю. Некоторые предложения по подходу и порядку реализации политики и стратегии импортозамещения в интересах национальной безопасности и укрепления обороноспособности Российской Федерации // Вопросы кибербезопасности. 2016. № 1 (14). С. 2–8;
3. Заботина Н.Н. Импортозамещение программного обеспечения в России: проблемы, планы и перспективы//Научные исследования и разработки в эпоху глобализации: сборник статей Международной научно-практической конференции в 3 ч. Ч. 2. Уфа: АЭТЕРНА, 2016. 198 с.;
4. Преимущества замещения иностранных ИТ-решений отечественными// TADVISER. – [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Преимущества_замещения_иностранных_ИТ-решений_отечественными;
5. Российское программное обеспечение. Отечественное ПО// TADVISER. – [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Российское_программное_обеспечение_(Отечественное_ПО);
6. Д. Волкова Успех импортозамещения: мощные графические процессоры на рынке РФ// Д.Волкова. – TADVISER.– [Электронный ресурс]. – Режим доступа:

https://www.tadviser.ru/index.php/Статья:Успех_импортозамещения:_мощные_графические_процессоры_на_рынке_РФ?erid=LjN8JyKYW;

7. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента от 30.03.2022 № 166 // КонсультантПлюс. – [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_413177/ (дата обращения: 30.05.2023).

8. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента от 01.05.2022 № 250 // КонсультантПлюс. – [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_416198/ (дата обращения: 30.05.2023);

9. Депутаты Госдумы переходят с продуктов Microsoft на Astra Linux и «МойОфис»// – TADVISER. – [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Проект:Astra_Linux_и_МойОфис_в_Госдуме;

10. Российские программно-аппаратные комплексы: новый виток развития// – TADVISER. – [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Российские_программно-аппаратные_комплексы:_новый_виток_развития.

Потапова Д.А.
Аспирант 3 курса кафедры «Прикладные информационные технологии»
Институт кибербезопасности и цифровых технологий РТУ МИРЭА
Potapova.daria1998@yandex.ru
Лавров П.В.
Студент 4 курса кафедры «Защита информации»
Институт кибербезопасности и цифровых технологий РТУ МИРЭА
Ильменёв П.А.
Студент 4 курса кафедры «Защита информации»
Институт кибербезопасности и цифровых технологий РТУ МИРЭА
Ларичева М.С.
Студент 4 курса кафедры «Информационные технологии»
Институт кибербезопасности и цифровых технологий РТУ МИРЭА
larichevams@gmail.com

АКТУАЛЬНЫЕ СПОСОБЫ ПРОТИВОДЕЙСТВИЯ И ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ ОТЕЧЕСТВЕННЫХ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ

В современном цифровом мире, где информация является одним из самых ценных ресурсов, сетевые атаки стали неотъемлемой угрозой для организаций и частных лиц. Нарушители используют все более совершенные методы для эксплуатации уязвимостей современных систем. В связи с этим одной из приоритетных задач перед ИБ сообществом стоит актуализация средств по обнаружения и противодействиям сетевым атакам.

Цель данной статьи заключается в исследовании актуальных способов борьбы с этой угрозой с использованием отечественных программно-аппаратных комплексов. На примере реальных инцидентов, мы стремимся проанализировать эффективность таких решений, а также выявить их сильные и слабые стороны.

В работе проанализированы несколько событий информационной безопасности, классифицированные как инциденты, с целью выявления сильных и слабых сторон рассмотренных средств защиты. Наш анализ поможет оценить важность использования отечественных решений и их роль в обеспечении безопасности сетей и данных.

В рамках данного исследования проводится обзор различных видов сетевых атак, среди которых особое внимание уделяется атакам типа отказа в обслуживании (DDoS) и атакам, связанным с нецелевым сканированием инфраструктуры.

Атаки DDoS, представляющие собой координированные попытки перегрузить сетевые ресурсы, остаются одной из наиболее распространенных и разрушительных угроз. Мы рассмотрим разнообразные типы атак, используемые злоумышленниками, и потенциальный объем причиняемого ущерба информационным системам.

Также в статье будет рассмотрено нецелевое сканирование инфраструктуры, включая цели и способы реализации атак. Исследование поможет выявить эффективные методы защиты от данных угроз, акцентируя внимание на использовании отечественных программно-аппаратных комплексов.

В рамках данного исследования представлен обзор двух ключевых средств защиты отечественного производства, используемых для противодействия различным видам сетевых атак:

Средство защиты Mitigator является мощным инструментом для предотвращения атак типа DDoS. Mitigator обладает способностью выявления и блокирования атак, которые пытаются перегрузить сетевые ресурсы, что позволяет поддерживать стабильную работу сети и сервисов даже в условиях продолжительных и площадных атак. Подробная схема работы данного продукта изображена на Рис. 1.

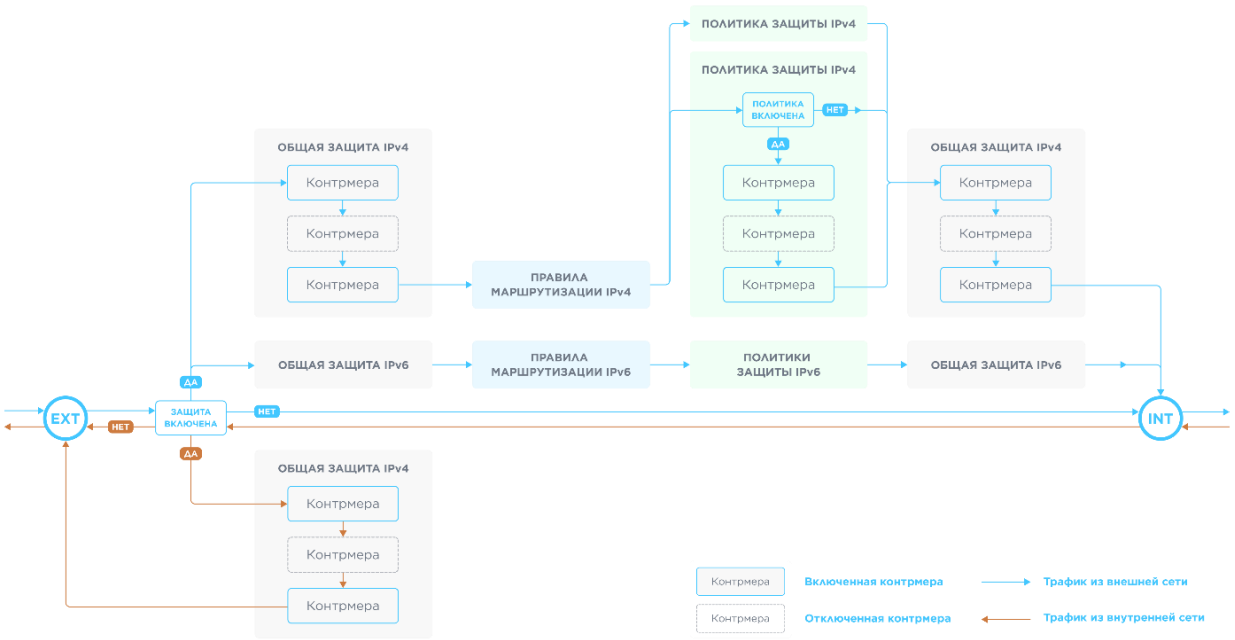

Рис. 1. Механизм работы продукта Mitigator

Средство защиты Positive Techhnologies Network Attack Discovery (PT NAD) - система поведенческого анализа сетевого трафика для расследований, который обнаруживает вредоносную активность злоумышленников на периметре и внутри сети, в том числе в зашифрованном трафике. Это важное средство для выявления потенциальных угроз и несанкционированных попыток доступа к сетевым ресурсам.

Оба этих средства представляют собой важные компоненты в обеспечении безопасности сетевых ресурсов и данных, и их использование имеет решающее значение в современной цифровой среде. Подробная схема работы PT NAD на Рис. 2.

После рассмотрения работы средств защиты перейдем к анализу реальных инцидентов, чтобы более детально изучить, как эти средства проявляют себя в реальных сценариях.

В первом примере рассмотрим типы атак UDP и TPC SYN Flood, которые являются самыми распространенными типами DDoS-атак. Атаки такого типа могут привести к отказу в обслуживании, например, Web-ресурсов, серверов.

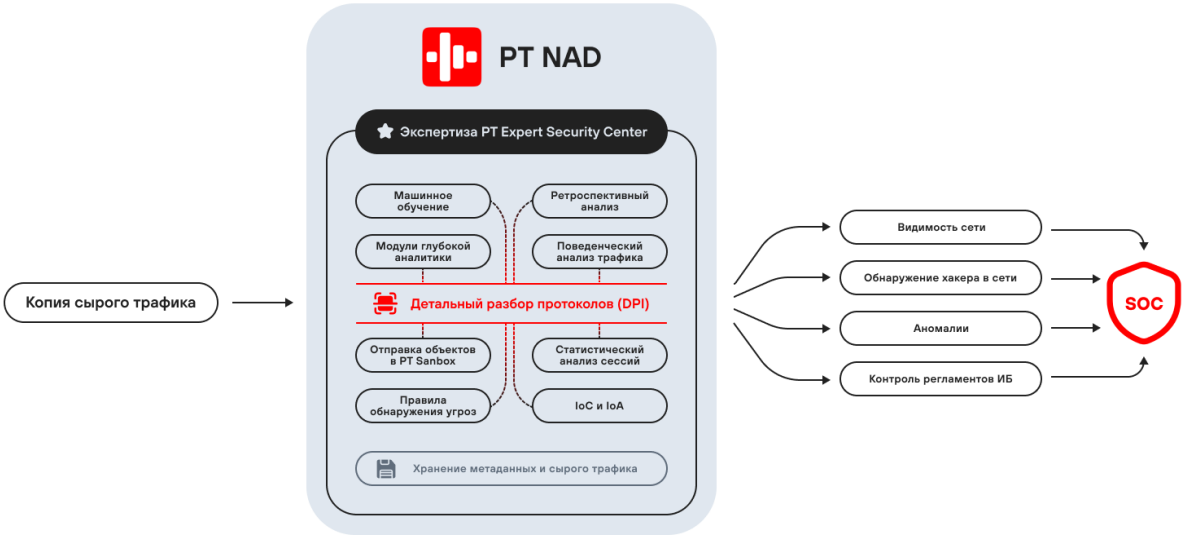

Рис. 2. Принцип работы PT NAD

Принцип работы UDP-flood. На этапе инициации атаки злоумышленники отправляют большое количество UDP-пакетов на целевой сервер. Эти пакеты могут иметь разные источники, но обычно они фальсифицированы так, чтобы скрыть настоящий источник атаки.

Отличительной чертой UDP-атак является то, что UDP не устанавливает соединение как TCP. Поэтому сервер не ожидает подтверждения доставки и начинает обрабатывать пакеты независимо от того, действительны они или нет.

Поскольку целевой сервер начинает обрабатывать большое количество входящих UDP-пакетов, это может привести к перегрузке сетевых ресурсов, включая процессор, память и пропускную способность сети.

Принцип работы TCP SYN-flood. Злоумышленники отправляют большое количество TCP-пакетов с флагом SYN (запрос на установление соединения) на целевой сервер.

Сервер начинает обрабатывать каждый запрос на установление соединения. Он создает запись для каждого запроса и ожидает завершения установления соединения. Злоумышленники не завершают установление соединения, поэтому на сервере остаются множество незавершенных

соединений, которые занимают ресурсы, включая память и место в таблицах управления соединениями.

По мере накопления незавершенных соединений сервер может исчерпать свои ресурсы, что приводит к отказу в обслуживании для легитимных клиентов.

Пример защиты от данных типов атак с использованием Mitigator (рис. 3).

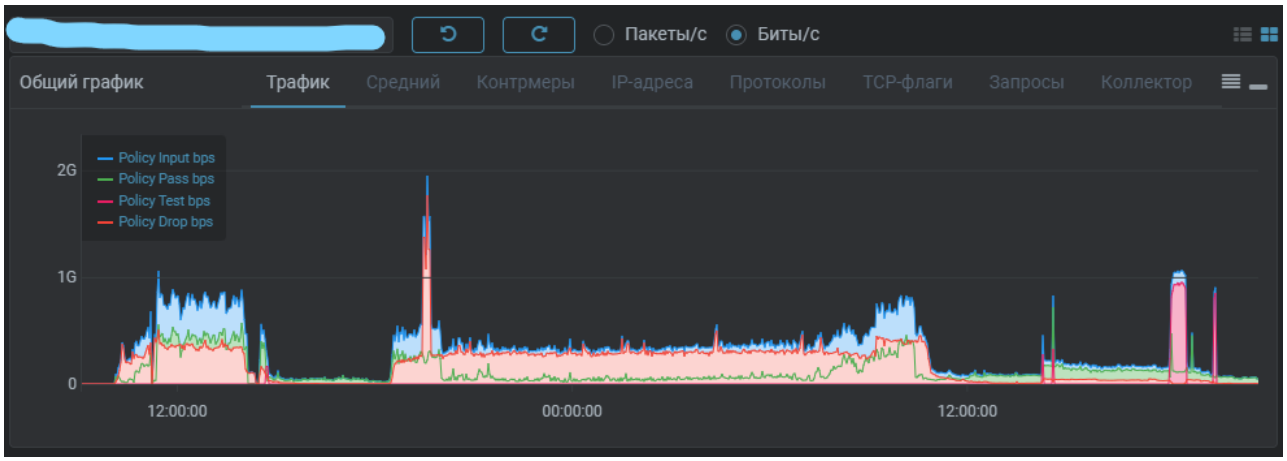

Рис. 3. Трафик атаки в системе Mitigator

Данная атака длилась с 10 часов одного дня до 20 часов следующего дня (34 часа). Максимальный объем трафика составил 3.85 Gbps, 1.17 Mpps. Атака подавлена полностью.

На графике показан входящий на защищаемый ресурс трафик (синий цвет), заблокированный системой защиты трафик (красный цвет) и пропущенный трафик легитимных пользователей (зеленый цвет). Mitigator может отличать трафик реальных клиентов от трафика злоумышленников, которые организуют атаку. Таким образом, пользователи не теряют доступ к защищаемому ресурсу во время проведения атаки.

В системе есть возможность посмотреть, какие контрмеры блокировали трафик и в каком объеме (рис. 4). Также можно смотреть количество уникальных IP-адресов в трафике, распределение используемых протоколов и TCP-флагов. Кроме того, в каждой контрмере есть график заблокированного трафика. Для минимального влияния на легитимный трафик предусмотрена

опция «мягкий старт» у некоторых контрмер, чтобы не сбрасывать установленные на момент включения фильтрации сессии.

Рис. 4. Распределение заблокированного трафика контрмерами

Этот функционал дает возможность проанализировать специфику атаки, смягчить политику защиты в случае попадания легитимного трафика в блокировку, или наоборот, ужесточить политику защиты, если трафик злоумышленника пропускается системой как доверенный.

Перейдем к анализу реальных инцидентов с использованием средства защиты PT NAD для обнаружения атак, связанных с нецелевым сканированием инфраструктуры. Данные атаки получили довольно-таки большое распространение в связи с тем, что многие web-сервисы стали уязвимы. Данная атака начинается со сбора злоумышленниками информации о целевой системе или сети. Это может включать в себя сбор информации о домене, IP-адресах, сервисах, портах и конфигурации системы.

Происходит это посредством сканирования портов, то есть злоумышленники выполняют сканирование портов, чтобы определить, какие порты открыты и какие службы работают на них. Это позволяет им выявить потенциальные уязвимости и целевые объекты для атаки.

После этого происходит идентификация слабых мест. Злоумышленники ищут уязвимые места, такие как устаревшие версии программного обеспечения, слабые пароли, недостатки в конфигурации, недооцененные службы и другие слабые точки в системе.

В конечном итоге злоумышленники стараются проэксплуатировать уязвимость найденную раннее. Поэтому важно регулярно мониторить системы и службы. Вовремя обновлять их, чтобы защититься от данных атак.

Одним из инструментов, помогающих выявлять данную активность, является PT NAD. Разберем это на примере реального инцидента (рис. 5).

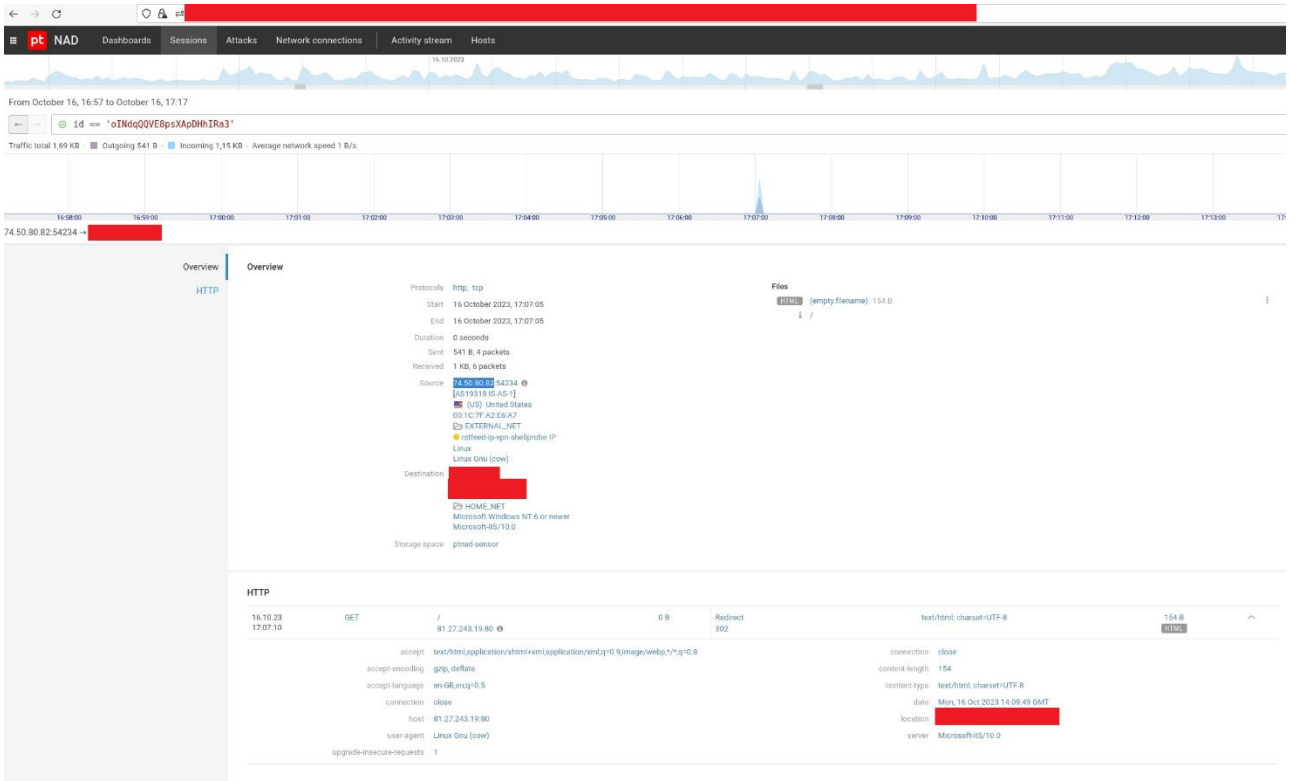

Рис. 5. Карточка инцидента в PT NAD

В данном кейсе мы видим попытку сканирования почтового сервера с IP-адреса 74.50.80.82 и региона США. В данной карточке мы можем заметить, какой метод сканирования использовался, в данном случае GET-запрос. Также можно увидеть с какого фаервола компании пришел данный трафик. Заметим, что соединение было отброшено, а пользователю пришел код ответа с

перенаправлением (302). Когда сервер отправляет код состояния 302 в ответ на запрос, он также обычно включает заголовок "Location", который указывает на новый URL, куда должен перейти клиент. Это перенаправление может быть использовано, например, для перенаправления пользователя на страницу входа или на другую версию ресурса, доступную по другому URL. Исходя из этого атака была неуспешной.

Используя подобные системы глубокого анализа сетевого трафика, мы можем автоматически обнаруживать попытки вторжения или сканирования по ряду признаков, которые смогут помочь в расследовании и восстановлении хронологии инцидента. Таким образом, мы можем мониторить состояние критических активов и своевременно реализовать необходимые меры защиты при угрозе.

Переходя к заключению статьи, важно подчеркнуть, что анализ атак, включая атаки связанные с нецелевым сканированием и атаки DDoS, является ключевым шагом в обеспечении безопасности сетевых ресурсов, в связи с тем, что данные типы атак являются самыми распространенными и наиболее простыми в реализации.

Такие атаки могут иметь серьезные последствия для организаций и отдельных пользователей, и защита от них становится все более важной.

Комбинирование двух типов решений для защиты, а именно средств для противодействия (например, Mitigator для предотвращения DDoS-атак) и средств для обнаружения (например, PT NAD для обнаружения нецелевого сканирования инфраструктуры), позволяет создать комплексную систему безопасности, которая обеспечивает как предотвращение атак, так и способность быстро обнаруживать и реагировать на них.

Средства для противодействия помогают предотвращать атаки на ранних стадиях, прежде чем они могут нанести вред. Средства для обнаружения, с другой стороны, позволяют быстро выявлять атаки, которые могли пройти через первую линию защиты, и немедленно реагировать на них.

Также комбинирование решений для обнаружения и противодействия способствует сбору большего объема данных о сетевой активности. Это улучшает аналитику и позволяет более точно настраивать систему обнаружения.

Всесторонний подход к защите помогает реализовать принцип эшелонированной защиты, который означает, что даже если одно средство защиты уязвимо или обмануто, другие уровни защиты остаются активными.

СПИСОК ИСТОЧНИКОВ

1. What is a UDP flood DDoS attack [Электронный ресурс] – Режим доступа: https://www.educative.io/answers/what-is-a-udp-flood-ddos-attack, свободный. – Загл. с экрана.
2. Укрепление стека TCP/IP для защиты от SYN атак [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/analytics/216320.php, свободный. – Загл. с экрана.
3. Защита от DDoS. DNS Amplification [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/blog/personal/aodugin/310503.php, свободный. – Загл. с экрана.
4. Защита от DDoS. NTP Amplification [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/blog/personal/aodugin/310785.php, свободный. – Загл. с экрана.
5. SYN flood attack [Электронный ресурс] – Режим доступа: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/, свободный. – Загл. с экрана.
6. Документация Mitigator [Электронный ресурс] – Режим доступа: https://docs.mitigator.ru/v23.08/kb/quick-setup/, свободный. – Загл. с экрана.

7. Документация PT NAD [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/, свободный.
8. Нецелевое сканирование [Электронный ресурс] – Режим доступа: https://gardatech.ru/articles/smi/zashchita-ot-setevykh-atak/, свободный.
9. Как защититься от сканирования портов? [Электронный ресурс] – Режим доступа: https://habr.com/ru/articles/686120/, свободный.
10. Оценка возможностей NAD [Электронный ресурс] – Режим доступа: https://habr.com/ru/companies/tssolution/articles/552752/, свободный.

Потапова Д.А.
Аспирант 3 курса кафедры «Прикладные информационные технологии»
Институт кибербезопасности и цифровых технологий РТУ МИРЭА
Potapova.daria1998@yandex.ru
Ушаков Д.А.
Студент 4 курса кафедры «Защита информации»
Институт кибербезопасности и цифровых технологий РТУ МИРЭА
ushakov.d.a1@edu.mirea.ru
Ватутин И.Г.
Студент 4 курса кафедры «Защита информации»
Институт кибербезопасности и цифровых технологий РТУ МИРЭА
ivanvaiutin860@gmail.com

АНАЛИЗ УГРОЗ KERBEROS: УЧИМСЯ ДУМАТЬ, КАК ЗЛОУМЫШЛЕННИКИ

В мире кибербезопасности, знание противника и понимание его тактик - ключ к эффективной защите. Наши собственные системы и данные никогда не были более ценными, и, следовательно, необходимость понимания потенциальных угроз никогда не была более критичной.

Данная статья позволит углубиться в мир кибербезопасности, проанализировать угрозы Kerberos и приобрести навыки "мышления как злоумышленник". Мы изучим разнообразные атаки, как стандартные, так и менее известные, чтобы быть лучше подготовленными к защите наших сетей и ресурсов.

Системы Kerberos, используемые для аутентификации и авторизации в сетях, являются важным элементом обеспечения безопасности информации и ресурсов. Однако в мире кибербезопасности не существует непреодолимых барьеров, и злоумышленники постоянно разрабатывают новые способы атаки.

Важно понимать, как они действуют и какие методы они используют, чтобы более эффективно защищать наши сети и данные.

В нашей статье, мы проведём исследование особенностей протокола Kerberos, как их видят злоумышленники. Постараемся взглянуть на этот протокол глазами тех, кто стремится обойти его защиту, чтобы получить доступ к чужим данным и ресурсам.

Цель данной статьи - обратить внимание на уязвимости и редкие угрозы, которые могли бы выйти за пределы стандартных тестов на проникновение.

Задачей данного исследования состоит в проведении качественного анализа среди атак на упомянутый протокол.

Для начала рассмотрим что такое Kerberos и по какому принципу он работает.

Kerberos - это протокол аутентификации и системы управления доступом, разработанные для обеспечения безопасности в компьютерных сетях. Основной принцип работы Kerberos можно описать следующим образом:

1. Аутентификация: Пользователь (клиент) отправляет запрос на аутентификацию Key Distribution Center (KDC). KDC выдает пользователю билет Ticket Granting Ticket (TGT), используемый для получения временных сессионных ключей.

2. Запрос билета: Когда пользователь хочет получить доступ к определенному ресурсу в сети, он отправляет KDC запрос на билет сессии (серверного). Этот запрос включает в себя TGT и запрос на ресурс.

3. Получение билета сессии: KDC проверяет TGT и, если пользователь имеет право доступа, выдает билет сессии, который содержит сессионный ключ.

4. Доступ к ресурсу: Пользователь использует билет сессии для доступа к запрошенному ресурсу. Сервер ресурса проверяет билет сессии с использованием сессионного ключа, обеспечивая безопасный доступ.

5. Завершение сессии: По завершении сессии, сессионный ключ уничтожается, что делает его непригодным для повторного использования.

Подобная схема представлена на рисунке 1.

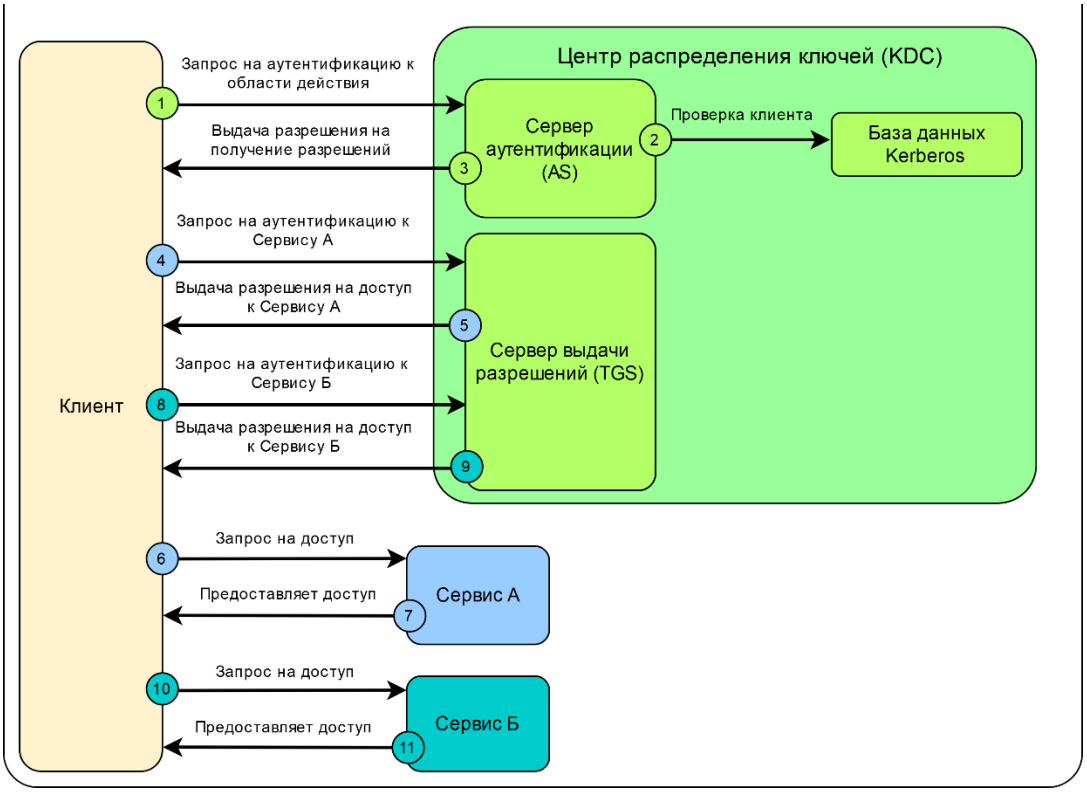

Рис. 1 – Аутентификации в протоколе Kerberos.

Kerberos обеспечивает высокий уровень безопасности, так как все билеты и ключи шифруются и имеют ограниченное время действия, что уменьшает риски атак и утечек данных. Этот протокол обеспечивает сильную аутентификацию и авторизацию пользователей в сетях и остается популярным инструментом для обеспечения безопасности в корпоративных средах.

В контексте данной статьи были проанализированы различные атаки на протокол Kerberos. Результатом проведённой работы является нижеприведенная таблица 1.

Табл. 1. – Результат анализ атак на протокол Kerberos

Наименование атаки	Pass-the-Ticket (PtT)	Skeleton Key
Сложность проведения	Средняя	Средняя
Tactic MITRE	Credential Access	Credential Access
Краткое описание атаки	Атака Pass-the-Ticket позволяет использовать билеты Kerberos, полученные извне, для аутентификации в системе.	обойти аутентификацию Kerberos, получив доступ к системе как любой пользователь.
Меры противодействия	Внедрение механизмов защиты, мониторинг событий для выявления подозрительной активности, регулярное обновление ключей аутентификации.	Усиление мониторинга и аудита Kerberos, регулярное обновление паролей, использование двухфакторной аутентификации.

Продолжение Таблицы 1

Kerberoasting	Средняя	Credential Access	хеш-значений паролей пользователей из системы для последующей попытки подбора паролей.	Регулярное обновление ключей аутентификации, мониторинг событий, усиление политик паролей, внедрение механизмов защиты.
Silver Ticket Attack	Средняя	Credential Access	атакующему создать собственные билеты Kerberos (Silver Ticket) для аутентификации в системе.	Ограничение привилегий доступа к контроллеру домена, мониторинг событий, регулярное обновление ключей аутентификации.
Golden Ticket Attack	Средняя	Persistence	Kerberos (Golden Ticket), что позволяет злоумышленнику продолжать доступ и аутентификацию.	Усиление мониторинга событий, ограничение привилегий доступа к контроллеру домена, регулярное обновление ключей аутентификации.

Продолжение Таблицы 1

DCShadow Attack	Pass-the-Cache (PtC)	Pass-the-Key (PtK)	
Сложная	Средняя	Сложная	
Defense Evasion	Credential Access	Credential Access	
внедрить изменения в контроллерах домена и реплицировать их на другие контроллеры. Усиление механизмов защиты, ограничение привилегий доступа к контроллеру, регулярное обновление ключей аутентификации.	атакующему получить доступ к кэшу билетов Kerberos и использовать их для аутентификации. Внедрение механизмов защиты, мониторинг событий для выявления подозрительной активности, регулярное обновление ключей аутентификации.	наличия административных привилегий в сети и позволяет имитировать ключи аутентификации. Усиление мониторинга и аудита системы, установка механизмов защиты, ограничение доступа к ключам аутентификации.	

Продолжение Таблицы 1

Diamond Ticket	Сложная	Persistence	который обладает долгосрочной жизнью и может использоваться для аутентификации.	Усиление мониторинга событий, ограничение привилегий доступа к контроллеру домена, регулярное обновление ключей аутентификации.

Разберем подробнее некоторые из наименее распространенных и до сих пор актуальных атак.

Первой из рассматриваемых атак является атака «Diamond ticket». Как и Golden Ticket, Diamond ticket - это TGT, который может быть использован для доступа к любой услуге в качестве любого пользователя. Golden Ticket подделывается полностью автономно, шифруется с помощью хэша krbtgt этого домена, а затем передается в сеанс входа для использования. Поскольку контроллеры домена не отслеживают TGT, которые он (или они сами) выдал на законных основаниях, они примут TGT, зашифрованные с помощью его собственного хэша krbtgt.

Существует два распространенных метода обнаружения использования Golden Ticket:

1. Поиск TGS- REQ, не имеющих соответствующего AS- REQ.
2. Поиск TGT, которые имеют неправдоподобные значения, такие как 10-летний срок действия Mimikatz по умолчанию.

Diamond ticket создается путем изменения полей легитимного TGT, который был выдан DC. Это достигается с помощью запроса TGT, расшифровки его с помощью хэша krbtgt домена, изменения нужных полей

билета, затем повторного шифрования. Это устраняет два вышеупомянутых недостатка Golden Ticket, потому что:

1. TGS-REQ будет иметь предшествующее AS-REQ.
2. TGT был выдан KDC, что означает, что в нем будут указаны правильные данные согласно политикам Kerberos домена.

В качестве второй не столь известной, но всё еще эффективной атаки рассмотрим атаку "Skeleton Key". Вышеупомянутая атака работает по следующему принципу:

1. Внедрение "Skeleton Key": Злоумышленники, обладая административными правами на контроллере домена, внедряют "Skeleton Key" - поддельный пароль (мастер-ключ), который работает до перезагрузки устройства.
2. Использование "Skeleton Key": После внедрения "Skeleton Key" злоумышленники могут использовать его для авторизации на любых аккаунтах в системе, включая административные учетные записи. Это означает, что они могут получить полный контроль над аккаунтами без необходимости знания изначальных паролей.
3. Бесследное сокрытие: "Skeleton Key" не меняет фактические пароли пользователей и работает одновременно с ними, что делает задачу обнаружения сложной.
4. Персистентность: "Skeleton Key" может оставаться активным в системе на протяжении продолжительного времени.

Для защиты от данной атаки важно поддерживать высокий уровень безопасности контроллера домена: проводить мониторинг событий на наличие подозрительной активности и осуществлять регулярную проверку систем на наличие несанкционированных изменений.

Узнав об основных принципах работы распространенного протокола аутентификации и авторизации Kerberos, а также познакомившись с множеством как стандартных, так и малоизвестных атак, мы подчеркнули

необходимость защиты даже самых продвинутых и надежных систем, так как даже в них существуют уязвимости, продиктованные самой архитектурой.

СПИСОК ИСТОЧНИКОВ

1. MITRE ATT&CK для Kerberos: Официальный ресурс MITRE Corporation, предоставляющий информацию о тактиках и техниках, связанных с Kerberos: MITRE ATT&CK Kerberos. URL: https://attack.mitre.org/techniques/T1558/002/ (дата обращения: 10.10.2023).
2. NIST Special Publication 800-63B: Документ National Institute of Standards and Technology о цифровой аутентификации, включая Kerberos: NIST SP 800-63B. URL: https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview (дата обращения: 10.10.2023).
3. Справочник Microsoft по Kerberos: Официальная документация Microsoft. URL: https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview (дата обращения: 13.10.2023).
4. RFC4120 — The Kerberos Network Authentication Service (V5) // IETF | Internet Engineering Task Force URL: https://tools.ietf.org/html/rfc4120 (дата обращения:13.10.2023).
5. Бэкдоры в Active Directory. Используем групповые политики, чтобы сохранить доступ к домену. URL: https://xakep.ru/2020/05/15/windows-ad-backdoor/ (дата обращения: 13.10.2023).
6. MIT Kerberos Documentation. MIT Kerberos Consortium URL: https://web.mit.edu/kerberos/krb5-devel/doc/ (дата обращения: 10.10.2023).

7. A Diamond (Ticket) in the Ruff. URL: https://www.semperis.com/blog/a-diamond-ticket-in-the-ruff/ (дата обращения: 13.10.2023).
8. Kerberos Protocol Tutorial (Fulvio Ricciardi). URL: https://www.kerberos.org/software/tutorial.html (дата обращения: 13.10.2023).
9. Kerberos API // OpenNet URL: https://www.opennet.ru/man.shtml?topic=gss_init_sec_context&category=3&russian=4 (дата обращения: 15.10.2023).
10. Basic Concepts for the Kerberos Protocol // MSDN URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961976(v=technet.10)?redirectedfrom=MSDN (дата обращения: 10.10.2023).

Чекунов Н.Д.,
студент МТУСИ, Москва, Россия,
nikita271002@yandex.ru
Большаков А.С.,
доцент кафедры ИБ, кандидат технических наук.,
МТУСИ, Москва, Россия,
alexbol57@mail.ru

РАЗРАБОТКА ЛАБОРАТОРНОГО СТЕНДА ОЦЕНКИ ЗАЩИЩЕННОСТИ ИС НА ПЛАТФОРМЕ EVE-NG

Введение

Последние мировые события показали, насколько сильно важна безопасность информационных систем. Лабораторные стенды предоставляют идеальную среду для тренировки и обучения специалистов по информационной безопасности.

Раньше для определения актуальных угроз использовались две отдельные методики: методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (2008 года); методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (2007 года). 5 февраля 2021 года ФСТЭК утвердил новый документ «Методика оценки угроз безопасности информации» который заменил предыдущие документы.

Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации и т.д

В методике 2021 года описывается:

- Порядок оценки угроз безопасности информации;
- Определение негативных последствий от реализации угроз безопасности информации;
- Определение возможных объектов воздействия угроз безопасности информации;
- Оценка возможности реализации угроз безопасности информации и определение их актуальности;
    - Определение источников угроз безопасности информации;
    - Оценка способов реализации угроз безопасности информации;
    - Оценка актуальности угроз безопасности информации;

По заявлению с 2021 по 2022 год ФСТЭК рассмотрел 695 документов моделей угроз безопасности информации, сделанных по новой методике. Из них было возвращено на доработку 67% (рис. 1).

Рис. 1. Процент возвращенных документов

В данном контексте становится ещё более актуальным разработка лабораторного стенда, благодаря которому студент получит опыт как в пентестировании, так и оценки защищенности ИС.

План выполнения

План выполнения работы состоит из:

1. выбор платформы для создания киберполигона;
2. проектирование информационной системы;
3. создание матрицы атак и сценариев атак;
4. проведение пентестирования;
5. автоматизация установки и настройки программного обеспечения с целью “перезапуска” полигона, используя Ansible playbook;
6. написание методического пособия для работы на лабораторном стенде;

Выбор платформы

Для создания киберполигона выбрана платформа EVE-NG, так как предназначена для эмуляции сетевых инфраструктур со сложными топологиями и оборудованием различных вендеров: Cisco (QEMU, Dynamips, IOL), Mikrotik, Juniper, Linux, Windows, Docker, ESXi.

Проектирование информационной системы

Топология информационной системы полигона включает в себя различные программные и аппаратные средства для увеличения количества сценариев атак. В EVE-NG можно легко расширить и изменить топологию, чтобы лабораторный стенд соответствовал актуальным угрозам БДУ ФСТЭК.

Текущая версия топологии киберполигона изображена на рисунке 2:

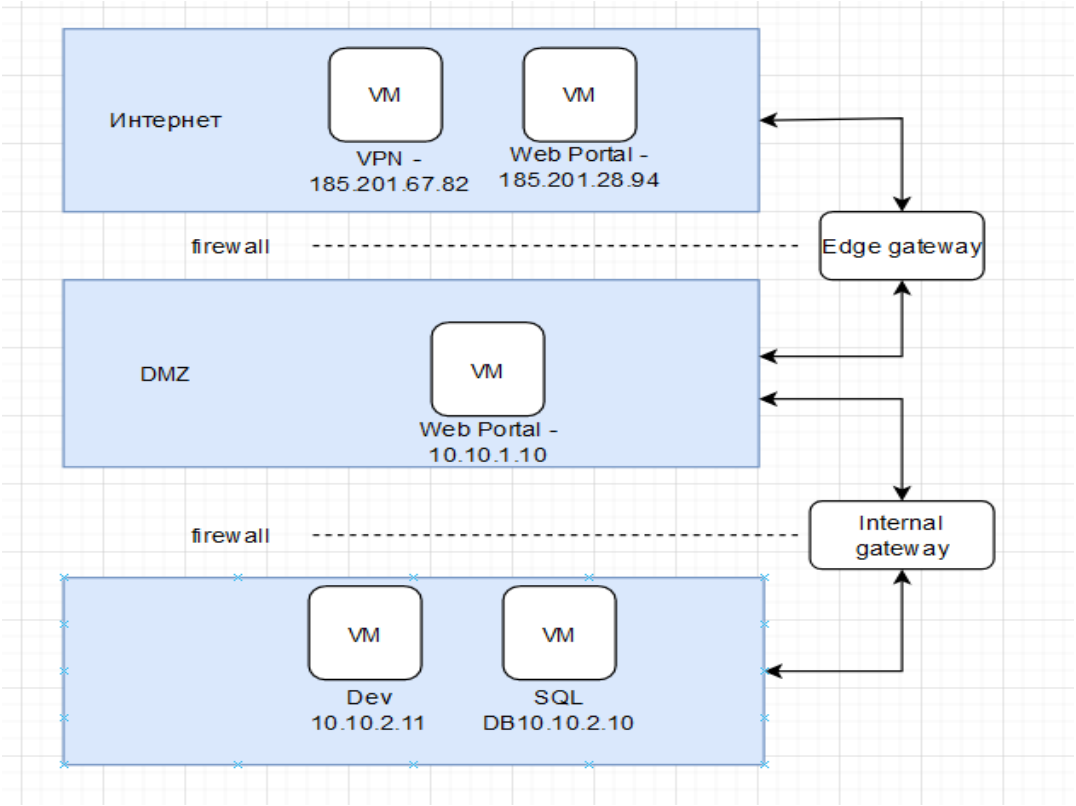

Рис. 2. Текущая версия топологии.

Создание матрицы атак и сценариев атак

Матрица атак (или матрица угроз) - это инструмент, используемый в области информационной безопасности для идентификации потенциальных угроз и атак на информационные системы. Она помогает оценить вероятность возникновения различных видов атак и их влияние на систему.

Чтобы составить матрицу атак, необходимо выполнить следующие действия:

1. определить список возможных угроз и типы атак, которые могут быть совершены.
2. изучить систему или сеть, которую необходимо защитить, и выявить потенциальные уязвимости.
3. идентифицировать уязвимые места, которые могут быть использованы для атаки.
4. определить вероятность и возможные последствия каждой атаки.
5. оценить уровень риска для каждой уязвимости или атаки.

6. заполнить матрицу атак, разместив угрозы по строкам и уязвимости по столбцам, и указать оценку риска для каждой комбинации.

Составление матрицы атак является важным шагом в разработке стратегии информационной безопасности и позволяет организации грамотно управлять рисками и обеспечивать защиту информации.

Текущая версия информационной системы полностью соответствует матрице атак приведенной в «Методики оценки угроз безопасности информации» ФСТЭК (рис. 3). По мере изменения киберполигона, будет изменяться и матрица атак.

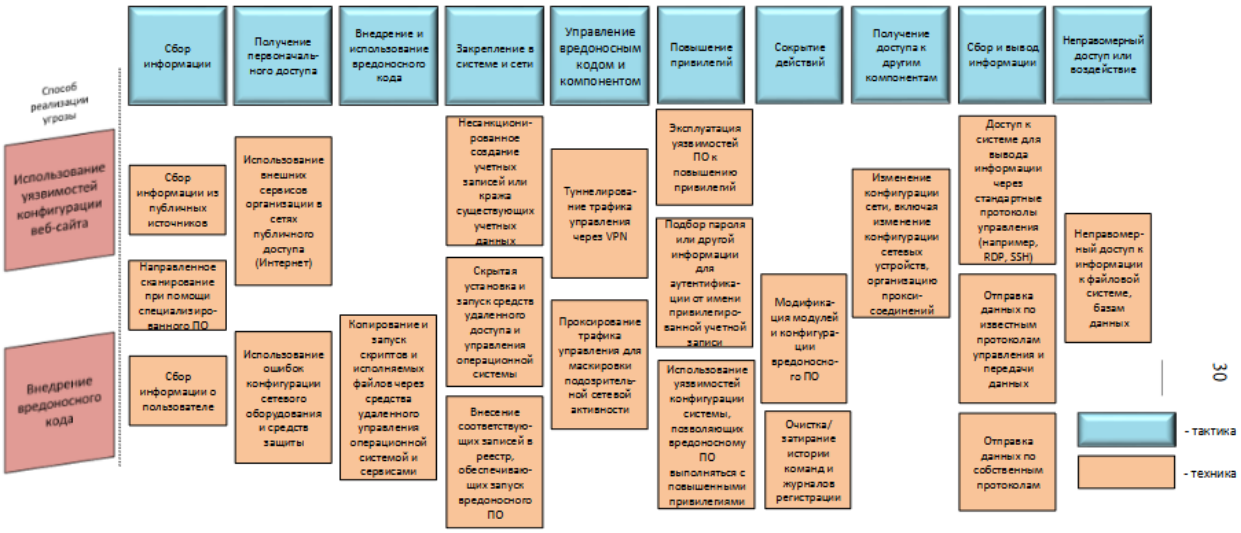

Рисунок 3. Матрица атак.

Существует 2 подхода к пентестированию информационных систем: «белый ящик» и «чёрный ящик».

В методике «белый ящик» пентестер может находится снаружи или внутри тестируемой системы. Он изучает информации предоставленную информацию: анализирует документацию, архитектуру, сетевые и системные настройки, исходный код и другие доступные ресурсы для ознакомления с системой. Затем проводит исследование и анализ исходного кода, идентифицирует потенциальные уязвимости и проблемы безопасности, которые могут быть использованы злоумышленниками. В конце пентестер

использует знания о системе и найденные уязвимости для попытки эксплуатации их с целью проверки, насколько система защищена и составляет отчёт по проделанной работе.

«Черный ящик» отличается от белого тем, что пентестер не знает ничего об анализируемой системе. Ему нужно самому собрать информацию используя публичные домены, поисковые системы, социальные сети и т.д. Это позволяет получить представление о системе, ее архитектуре и возможностях.

На созданном лабораторном стенде можно проводить пентестирование по обеим методикам.

Автоматизация стенда

За автоматизацию настройки виртуальных машин будет отвечать Ansible. Ansible - это система автоматизации IT-процессов, которая позволяет управлять и настраивать компьютерные системы, сети и инфраструктуру через скрипты, называемые "плейбуками". Она является открытым программным обеспечением и использует простой и понятный для разработчиков язык YAML для описания конфигураций и задач.

Ansible позволяет администраторам выполнить повторяющиеся задачи на большом количестве систем одновременно, обеспечивая единообразную конфигурацию и управление. Он основан на модели "последовательного выполнения команд", что позволяет обновлять и настраивать системы без необходимости в прерывании работы или влиянии на работу пользователей.

Вывод:

Лабораторный стенд оценки защищенности ИС на платформе EVE-NG может быть успешно использован в образовательных учреждениях, а также в компаниях и организациях, занимающихся обеспечением информационной безопасности, для обучения и тренировки специалистов, а также для проведения практических тестов и анализа уровня защищенности системы.

СПИСОК ИСТОЧНИКОВ

1. «Базовая модель угроз персональных данных при их обработке в информационных системах персональных данных» – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/bazovaya-model-ot-15-fevralya-2008-g

2. «Методика оценки угроз безопасности информации» – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

3. «База данных угроз безопасности информации» – URL: https://bdu.fstec.ru/threat

4. «Методика оценки угроз ФСТЭК: что нового» [Интернет-ресурс] – URL: https://www.securitylab.ru/blog/personal/Business_without_danger/351896.php

5. «Пособие по Ansible» [Интернет-ресурс] – URL: https://habr.com/ru/articles/305400/

6. «Официальный сайт EVE-NG» - https://eve-ng.ru/

7. «Строим киберполигон» [Интернет-ресурс] - URL: https://xakep.ru/2021/08/09/eve-ng/

8. «Сценарии для взлома» [Интернет-ресурс] - URL: - https://xakep.ru/2017/04/10/hacking-attack-types/

9. «Официальный сайт Ansible» – URL: https://www.ansible.com/

10. «Что такое пентест и для чего он нужен» [Интернет-ресурс] – URL: https://skillbox.ru/media/code/chto-takoe-pentesty-i-dlya-chego-oni-nuzhny/

Е. В. Завадский,
Санкт-Петербургский политехнический университет
Петра Великого
М. О. Калинин,
Санкт-Петербургский политехнический университет
Петра Великого

АДАПТИВНАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ КИБЕРЗАЩИЩЕНОСТЬ НА БАЗЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗ ГРАФОВ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ ЦИФРОВОГО ДВОЙНИКА

Цифровизация, гибкость и автономность технологических процессов повышают восприимчивость киберфизических систем (КФС) к возникающим угрозам кибербезопасности. Несмотря на развитие передовых средств защиты, методы, применяемые группировками для проникновения, закрепления и дальнейшего распространения во внутренней сети организации, постоянно модифицируются. С целевыми кибератаками (APT) сталкивается 65% компаний, расположенных по всему миру [1]. При этом работа 40% организаций была нарушена не менее чем на 8 часов [2, 3].

В рамках данной работы предложена система выявления и динамическое противодействия атакам программ-вымогателей (WannaCry) и APT-группировок, которая базируется на интеллектуальном анализе графов функциональных зависимостей и потенциальных атак, а также применении цифровых двойников защищаемой КФС.

Анализ существующих решений обеспечения киберзащищенности КФС

Системы honeypot, основной задачей которых является отвлечение злоумышленника от критических ресурсов, являются одним из традиционных методов защиты СИ [4]. Узлы honeypot должны быть неотличимы от узлов в

реальной сети. Большинство систем honeypot для КФС являются малоинтерактивными [5-11], что позволяет злоумышленникам легко идентифицировать данные узлы и обойти их.

В отличие от honeypot, технология deception работает согласно стандартному алгоритму проведения атаки, который включает сбор и анализ данных, выделение перспективных для развития атаки узлов и выполнение распространения [12]. Для отвлечения злоумышленников в СИ внедряются узлы-приманки с ложными параметрами. При обнаружении таких узлов, атакующий может использовать их для доступа к специальным узлам-ловушкам. Для управления deception-системой обычно применяются методы теории игр [13, 14]. Однако, не все проблемы могут быть полностью проанализированы с её помощью, и каждый игрок должен знать функцию затрат другого игрока.

В статьях [15-18] исследователи применяют методы машинного обучения для обнаружения вторжений и аномалий в поведении КФС, и демонстрируют высокую точность предлагаемых решений. Применение роевых алгоритмов в системах обнаружения вторжений (IDS) может еще более повысить качество обнаружения атак путем использования распределенного анализа межузловой сети, основанного на знаниях. В статье [19] описывается интеллектуальная система обеспечения безопасности, основанная на агентах, а в [20-25] предлагаются методы оптимизации извлечения признаков с использованием сверточных нейронных сетей и генетических алгоритмов. Эти методы достигают высокой точности обнаружения кибератак на тестовых наборах данных. Однако, в случае проведения атак, которые не были предусмотрены при обучении моделей, и при отсутствии корреляции значений признаков, скомпрометированные узлы могут остаться незамеченными алгоритмами машинного обучения.

Кроме того, методы Honeypot / Deception и интеллектуальные методы предупреждают о вредоносной активности, но не противодействуют ей. В работах [26-30] исследователи предложили ряд методов, основанных на

биоинспирированных методах и теории управления, чтобы минимизировать последствия действий злоумышленников. Правильная реакция таких систем имеет вероятностный характер. Кроме того, для решения этой задачи была разработана концепция системы иммунизации. Например, в работе [31] система иммунизации обнаруживает вторжение в контролируемую СИ и противодействует определенному перечню атак на её критические узлы. Все эти решения действительно применяются для «апостериорной» защиты КФС, но они не идентифицируют источник атаки – скомпрометированный узел, который продолжает наносить ущерб в атакованной инфраструктуре.

Таким образом, необходимо новое решение, которое обеспечивает выявление злонамеренного поведения узлов СИ и противодействие атакам для минимизации последствий деструктивных воздействий.

Комплексное решение для обеспечения безопасности КФС

В рамках решения задачи обеспечения кибербезопасности сетевой инфраструктуры (СИ) КФС требуется выполнить следующие операции:

Выявить наличия вредоносного воздействия.

Определить скомпрометированные злоумышленником узлы.

Исключить обнаруженные узлы из СИ.

Перестроить функциональные цепочки для сохранения корректности протекания технологических процессов.

В условиях постоянного совершенствования техник атакующими необходимы выполнять ситуационный контроль состояния системы на базе интеллектуального анализа графа функциональных зависимостей. Узлы СИ КФС $V = \{v_1, v_2, \dots, v_n\}$ поддерживают выполнения набора функций $F_{v_i} = \left\{ f_1^{(i)}, f_2^{(i)}, \dots \right\}$, где $f_k^{(i)} -$ функции поддерживаемые узлом v_i, для обеспечения корректного протекания технологических процессов $P_{process}^{(j)} = \left\{ f_1^{(j)}, f_2^{(j)}, \dots, f_n^{(j)} \right\}$, где $f_k^{(j)}$ – функция, поддерживаемая узлом v_i и используемая в технологическом процессе j. Таким образом, узлы объединены в цепочку и

взаимодействуют между собой в рамках определенного технологического процесса $R_{process_j} = \left\{v_1^{(j)}, v_2^{(j)}, \dots, v_n^{(j)} \mid f_{j_1} \in F_{v_1^{(j)}} \,\&\, \dots \,\&\, f_{j_n} \in F_{v_n^{(j)}}\right\}$. Данная сеть связанных функциональных узлов называется графом функциональных зависимостей.

Для выявления вредоносных воздействий на защищаемую СИ в граф функциональных зависимостей внедряются узлы-индикаторы ($v_{indicator}$). Они обладают следующими свойствами:

Виртуальность: узлы-индикаторы представляют собой виртуальные машины.

Неотличимость: узлы-индикаторы должны быть схожи с реальными узлами защищаемой СИ с точки зрения злоумышленника.

Поддержка набора функций: узлы-индикаторы должны поддерживать ряд функций, необходимых в данной КФС.

Команда защиты обладает полным внешним контролем над ОС узла-индикатора для обнаружения и реагирования на вредоносные действия.

Отсутствие штатного сетевого взаимодействия с узлами-индикаторами не является обнаруживающим фактором, так как они могут быть задействованы в других технологических процессах, не затронутых атакующим.

Для определения множества скомпрометированных узлов необходимо задать условие отнесения узла v_i к множеству скомпрометированных $V_{compromised}$.

Определение 1. Скомпрометированным считается каждый узел, который включен в граф $G_{interaction}$, построенный при помощи способа обратного распространения от узла-индикатора по цепочке сетевых взаимодействий: $v_i \in V_{compromised}$, если $v \in V(G_{interaction})$.

Набор узлов, выполняющих определенные функции, ограничен. Поэтому требуется обеспечить максимальную точность определения скомпрометированных узлов. Это можно сделать с помощью графов потенциальных атак. Каждому узлу-индикатору должен быть присвоен граф

потенциальных атак, который показывает путь от входной атаки точки до данного узла.

Определение 2. Если узел включен в граф, полученный в результате пересечения графа, являющегося объединением графов потенциальных атак G_{attack} затронутых узлов-индикаторов, и графа $G_{interaction}$, построенного согласно первому утверждению $v_i \in \{V_{compromised}\}$, если $v \in V(G_{interaction} \cap (G_{attack}^{(1)} \cup G_{attack}^{(2)} \cup \dots))$, то он считается скомпрометированным.

В ходе тестирования корректности работы системы выявления вредоносного воздействия, базирующийся на приведенных ранее определениях, выявлены ложноположительные срабатывания. Для решения данной проблемы сформулируем третье утверждение.

Определение 3. Если узлы-индикаторы не сигнализируют о вредоносном воздействии со стороны рассматриваемого узла, и он не входит в граф, состоящий из затронутых в ходе атаки узлов-индикаторов: $v_i \notin \{V_{compromised}\}$, если $\left(\forall v_{indicator}^{(j)}: \text{is\_signal}\left(v_{indicator}^{(j)}\right) = \text{false}\right)$ & $(v_i \notin s_{km} =< v_{indicator}^{(k)}, \dots, v_{indicator}^{(m)} >, \forall v_{indicator}^{(k)}, v_{indicator}^{(m)} \text{is\_signal}\left(v_{indicator}^{(k)}\right) = \text{true}, \text{is\_signal}\left(v_{indicator}^{(m)}\right) = \text{true})$, где is_signal – функция, возвращающая статус узла-индикатора, то данный узел является нескомпрометированным.

В случае не удаления всех скомпрометированных узлов из СИ необходимо использовать сигнатурный метод детектирования вредоносного воздействия. Для определения паттернов поведения необходимо выделить все определенные как скомпрометированные узлы в изолированный цифровой двойник, аналогичный защищаемой СИ. На рисунке 1 приведена результирующая схема алгоритма работы системы выявления и противодействия вторжению.

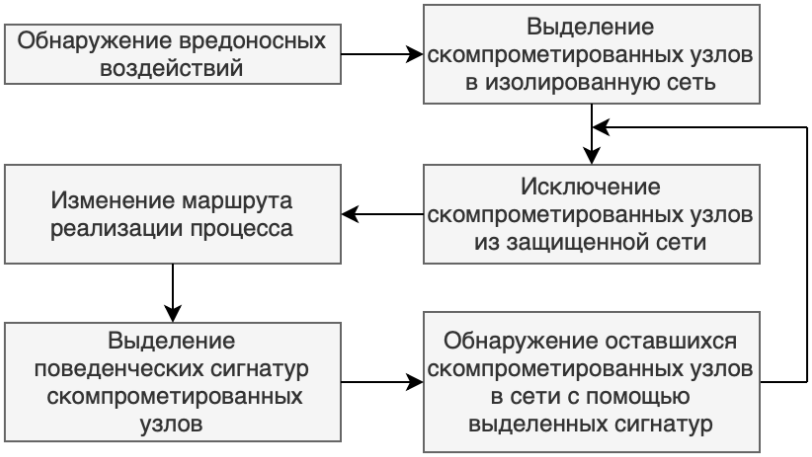

Рисунок 1 – Алгоритм выявления и исключения скомпрометированных узлов

Для тестирования предложенной системы выявления и противодействия атакам программ-вымогателей (WannaCry) и APT-группировок был разработан симулятор, который моделирует атаку и формирует график зависимости числа скомпрометированных злоумышленником узлов сети от времени на основе заданной конфигурации КФС. Эффективность защиты – оценка количества корректно обнаруженных и исключённых из СИ КФС скомпрометированных узлов.

Согласно полученным результатам оценки эффективности защиты предложенная система обеспечения киберзащищенности КФС позволяет выявить 100% скомпрометированных узлов при различных сценариях распространения программы-вымогателя и APT-атаки, что подтверждает корректную работу защитника на угрозы кибербезопасности различного рода и вариативности.

Отметим, что ряд сценариев тестирования завершился ошибкой восстановления технологического процесса $R_{process}$, что связано с исключением из СИ КФС всех узлов, выполняющих требуемую функцию.

В таблице 1 приведено сравнение предложенного решения с рассмотренными при проведении анализа области.

Таблица 1 – Сравнение подходов к обеспечению безопасности КФС

Название	**Выявление непредусмотренных конфигурацией атак**	**Автономное противодействие атакам**	**Автоматическое обновление базы сигнатур компрометации**	**Высокие требования к вычислительным ресурсам**
Honeypot / Deception [4-14]	+	-	-	-
IDS / ML [15-25]	-	-	-	-
Биоинспирированный / иммунный [26-31]	+	+	-	-
Предложенный	+	+	+	+

Существующие решения не предоставляют полного подхода к обнаружению и минимизации вредоносного воздействия. Предлагаемое решение позволяет точно определить скомпрометированные узлы, используя введенные определения и механизм сбора поведенческих сигнатур в изолированной виртуальной сети для детектирования ранее не выявленных скомпрометированных узлов.

Для эффективной работы предложенного метода необходимо быстро и бесшовно (с точки зрения злоумышленника) подключать скомпрометированные узлы в виртуальную изолированную сеть. Создание виртуальной СИ требует значительных вычислительных ресурсов. Однако это позволяет формировать паттерны поведения скомпрометированных узлов и дополнять ими базы, которые могут быть использованы в том числе IDS.

Стоит учитывать, что для работы предложенного решения также необходим механизмы резервирования наиболее критичных узлов и восстановления скомпрометированных узлов, так как при исключении из СИ некоторых узлов, выполняющих определенный набор функций, технологический процесс может быть не восстановим. Выявление критичных узлов может быть выполнено при помощи метода на базе графовой нейронной сети, предложенного в статье [32].

Реализация второго механизма подразумевает восстановление скомпрометированного узла из резервной копии и его встраивание в СИ КФС.

Заключение

Успешные атаки на компоненты критической инфраструктуры могут привести к нарушению промышленных процессов, уничтожению дорогостоящих устройств и нарушению социальной и экономической жизни. Поэтому обеспечение кибербезопасности КФС является важнейшей задачей.

В рамках данного исследования было предложено комплексное решение для активного обнаружения и противодействия кибератакам, целью создания которого является усиление защиты функциональной инфраструктуры критических КФС.

СПИСОК ИСТОЧНИКОВ

1. ISTR Internet Security Threat Report Volume 24. URL: https://docs.broadcom.com/doc/istr-24-2019-en

2. Cisco Cybersecurity Report 2018. URL: https://www.cisco.com/c/dam/global/hr_hr/solutions/small-business/pdf/small-mighty-threat.pdf

3. Cybersecurity threat trends: phishing, crypto top the list. URL: https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

4. Franco J. et al. A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems //IEEE Communications Surveys & Tutorials. – 2021. – Т. 23. – №. 4. – С. 2351-2383.

5. Shi L. et al. Dynamic distributed honeypot based on blockchain //IEEE Access. – 2019. – Т. 7. – С. 72234-72246.

6. Vasilomanolakis E. et al. Multi-stage attack detection and signature generation with ICS honeypots //NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. – IEEE, 2016. – С. 1227-1232.

7. Gallenstein J. K. Integration of the network and application layers of automatically-configured programmable logic controller honeypots. – Air Force Institute of Technology, 2017.

8. Abe S. et al. Developing deception network system with traceback honeypot in ICS network //SICE Journal of Control, Measurement, and System Integration. – 2018. – Т. 11. – №. 4. – С. 372-379.

9. Kołtyś K., Gajewski R. Shape: A honeypot for electric power substation //Journal of Telecommunications and Information Technology. – 2015. – №. 4. – С. 37-43.

10. Buza D. I. et al. CryPLH: Protecting smart energy systems from targeted attacks with a PLC honeypot //International Workshop on Smart Grid Security. – Springer, Cham, 2014. – С. 181-192.

11. Serbanescu A. V., Obermeier S., Yu D. Y. ICS threat analysis using a large-scale honeynet //3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3. – 2015. – С. 20-30.

12. Fraunholz D. et al. Demystifying deception technology: A survey //arXiv preprint arXiv:1804.06196. – 2018.

13. Pawlick J., Colbert E., Zhu Q. A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. *ACM Computing Surveys*, 2017.

14. Fraunholz D., Schotten H. Strategic defense and attack in deception-based network security. *International Conference on Information Networking*, 32, 2018.

15. Korzhuk V. et al. Identification of Attacks against Wireless Sensor Networks Based on Behaviour Analysis //J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. – 2019. – Т. 10. – №. 2. – С. 1-21.

16. Junejo K. N., Goh J. Behaviour-based attack detection and classification in cyber physical systems using machine learning //Proceedings of the 2nd ACM international workshop on cyber-physical system security. – 2016. – С. 34-43.

17. Moon D. et al. DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks //The Journal of supercomputing. – 2017. – Т. 73. – №. 7. – С. 2881-2895.

18. Ovasapyan T., Moskvin D., Tsvetkov A. Detection of attacks on the Internet of Things based on intelligent analysis of devices functioning indicators //13th International Conference on Security of Information and Networks. – 2020. – С. 1-7.

19. Fatani A. et al. Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system //Sensors. – 2021. – Т. 22. – №. 1. – С. 140.

20. Nandy S. et al. An intrusion detection mechanism for secured IoMT framework based on swarm-neural network //IEEE Journal of Biomedical and Health Informatics. – 2021. – Т. 26. – №. 5. – С. 1969-1976.

21. Zivkovic M. et al. Novel hybrid firefly algorithm: an application to enhance XGBoost tuning for intrusion detection classification //PeerJ Computer Science. – 2022. – Т. 8. – С. e956.

22. Kunhare N., Tiwari R., Dhar J. Intrusion detection system using hybrid classifiers with meta-heuristic algorithms for the optimization and feature selection by genetic algorithm //Computers and Electrical Engineering. – 2022. – Т. 103. – С. 108383.

23. Liu H., Lang B. Machine learning and deep learning methods for intrusion detection systems: A survey //Applied sciences. – 2019. – Т. 9. – №. 20. – С. 4396.

24. Sarnovsky M., Paralic J. Hierarchical intrusion detection using machine learning and knowledge model //Symmetry. – 2020. – Т. 12. – №. 2. – С. 203.

25. Abdulhammed R. Features dimensionality reduction approaches for machine learning based network intrusion detection 397 //Electronics. – 2019. – Т. 8. – №. 3. – С. 322.

26. Zang T. et al. Current Status and Perspective of Vulnerability Assessment of Cyber-Physical Power Systems Based on Complex Network Theory //Energies. – 2023. – Т. 16. – №. 18. – С. 6509.

27. Farraj A. K. et al. A game-theoretic control approach to mitigate cyber switching attacks in smart grid systems //2014 IEEE International Conference on Smart Grid Communications (SmartGridComm). – IEEE, 2014. – С. 958-963.

28. Barreto C., Cárdenas A. A., Quijano N. Controllability of dynamical systems: Threat models and reactive security //International Conference on Decision and Game Theory for Security. – Springer, Cham, 2013. – С. 45-64.

29. Hu P. et al. Dynamic defense strategy against advanced persistent threat with insiders //2015 IEEE Conference on Computer Communications (INFOCOM). – IEEE, 2015. – С. 747-755.

30. Zhu Q., Basar T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems //IEEE Control Systems Magazine. – 2015. – Т. 35. – №. 1. – С. 46-65.

31. Yuan Y., Sun F., Liu H. Resilient control of cyber-physical systems against intelligent attacker: a hierarchal stackelberg game approach //International Journal of Systems Science. – 2016. – Т. 47. – №. 9. – С. 2067-2077.

32. Zegzhda D., Pavlenko E., Aleksandrova E. Modelling Artificial Immunization Processes to Counter Cyberthreats //Symmetry. – 2021. – Т. 13. – №. 12. – С. 2453.

Балеев М. А.
ЮФУ, ИКТИБ, кафедра БИТ им О.Б. Макаревича, студент,
baleev@sfedu.ru
Пескова О.Ю.
ЮФУ, ИКТИБ, кафедра БИТ им О.Б. Макаревича, к.т.н., доцент,
oyupeskova@sfedu.ru

OSINT-ИНСТРУМЕНТАРИЙ - ОПРЕДЕЛЕНИЕ ГЕОГРАФИЧЕСКОГО ПОЛОЖЕНИЯ ОБЪЕКТА ПО IP-АДРЕСУ

Данная работа описывает методику определения местоположения объекта, как юридического лица, по данному IP-адресу.

Задачи работы:

- формирование списка признаков, позволяющих определить расположение объекта;
- обзор сервисов, представляющих подобные услуги;
- разработка методики нахождения георасположения объекта по известному IP-адресу;
- разработке инструмента, основанного на сильных и слабых сторонах прямых аналогов, выполняющего данного рода задачи.

Введение

Большинство пользователей сети Интернет знают о существовании их уникального идентификатора в сети - IP-адресе. Кроме обычного применения, по IP-адресу в различных базах данных можно найти интересующую исследователя информацию, например, информацию об используемом провайдере или широте и долготе устройства [1, 2].

Подобными задачами занимается OSINT (open-source intelligence) – разведка по открытым источникам. Ее технологию можно применять как для физических, так и для юридических лиц.

Определить точное местоположение физического лица по IP-адресу проблематично, так как IP-адрес физического лица закреплен не конкретно за объектом, а за организацией-провайдером, которая предоставляет услуги объекту [3, 4].

В свою очередь организация может пользоваться как арендованным хостингом, так и своим личным. В первом случае определение местоположения по IP-адресу затруднительно, однако во втором случае данный поиск даст достаточное количество правильных результатов, именно поэтому в данной статье описывается методика определения местоположения организации, как юридического лица, по IP-адресу.

Получение IP-адреса

Способы получения IP-адреса:

- анализ заголовка электронного письма, отправленного исследуемым объектом [5, 6].
- анализ доменного имени, используя специальные инструменты, определяющие IP-адрес при помощи протокола DNS [7];
- анализ утечек различных баз данных, в которых фигурируют пользовательские адреса.

Сравнительный анализ инструментов

Был проведен анализ OSINT-инструментов как с точки зрения удобства использования, так и с точки зрения наличия тех или иных функциональных возможностей.

Критерии оценивания инструмента предполагают оценку от 0 до 10, однако в пунктах, в которых промежуточная оценка невозможна, используется та же система оценивания, однако вместо 10 возможных значений, предполагается только 2: 0 - нет в наличии, 10 - в наличии. Лучший инструмент выбирается по сумме очков за все критерии.

Были проанализированы следующие инструменты-сервисы: 2ip.ua, Калькулятор. Справочный портал, Web-технологии, XSEO, InfoBylp, Деанонимайзер, Whois Domain Bot, IPVOID, IPAddress.com, IPFingerPrints.

Критерии оценивания:

1) Русскоязычный интерфейс;
2) Автоопределение IP-адреса;
3) Полнота информации о геолокации;
4) Полнота дополнительной информации;
5) Наличие дополнительных функций;
6) Корректность информации.

Табл. 1. Сравнительный анализ инструментов OSINT-разведки

№	Критерий / Сервис	№ 1	№ 2	№ 3	№ 4	№ 5	№ 6	Итого
1	2ip.ua [8]	8	10	6	7	10	10	51
2	Калькулятор. Справочный портал [9]	2	0	2	3	0	10	17
3	Web-технологии [10]	10	10	10	7	10	10	57
4	XSEO [11]	5	10	10	8	0	10	43
5	InfoBylp [12]	2	10	10	10	10	10	52
6	Деанонимайзер [13]	10	0	7	5	0	10	32
7	Whois Domain Bot [14]	0	0	2	6	0	10	18
8	IPVOID [15]	0	0	10	3	10	10	33
9	IPAddress.com [16]	0	10	7	3	0	10	30
10	IPFingerPrints [17]	0	10	10	6	0	0	26

Результат сравнительного анализа: лучший инструмент - сервис «Web технологии», так как он является наиболее удобными для использования, а также предлагает пользователю достаточно обширные функциональные возможности.

Разработанная методика поиска и анализа информации о расположении объектов по IP-адресу

Разработанная авторами методика нахождения местоположения предполагает анализ IP-адреса при помощи нескольких инструментов (не менее 3), и дальнейший анализ предоставленных данных.

Разработанная методика определения местоположения организации по IP-адресу:

1. ввод исследуемого IP-адреса в поисковую строку сервиса;
2. поиск информации о географическом положении (широта и долгота, адрес) в предоставленной сервисом информации;
3. ввод полученной информации о географическом положении в картографический сервис;
4. сбор общедоступной информации об объекте, расположенном по данным координатам;
5. повторение пунктов 1–3 не менее 3 раз;
6. анализ полученных результатов после пункта 4 для выбора наиболее точного результата.

Разработанное программное обеспечение поиска и анализа информации о расположении объектов по IP-адресу

После разработки методики был разработан telegram-бот, предоставляющий информацию об IP-адресе сразу по 2 источникам (IP-API, IpInfo).

Инструмент использует 2 источника, так как только эти интерфейсы (API) являются бесплатными в использовании - подавляющее большинство интерфейсов, работающих с данного рода информацией, предоставляются по подписке. Демонстрация работы бота по поиску информации по IP-адресу представлена на рисунке 1.

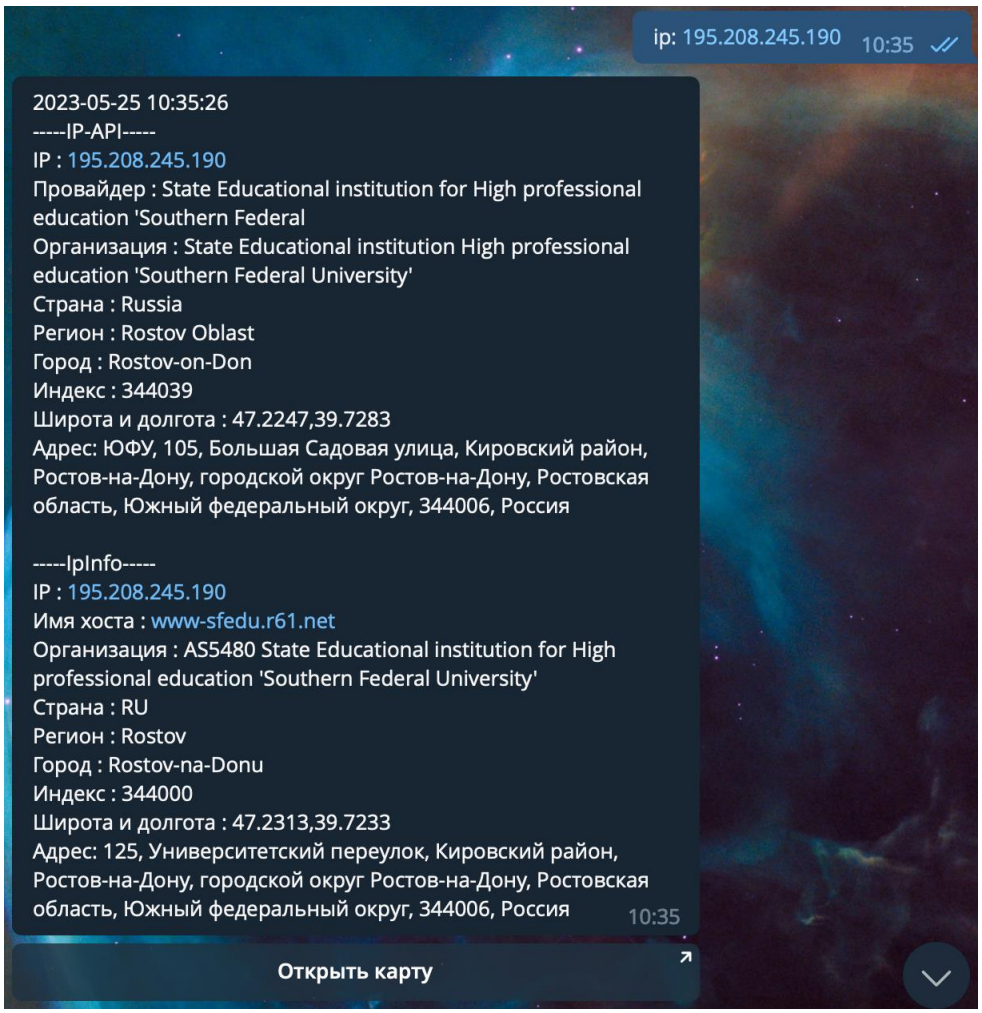

Рисунок 1 - Пример поиска по IP-адресу

В сгенерированном сообщение предоставляется:

- наименование провайдера;
- наименование организации, которой принадлежит IP-адрес;
- страна, регион и город, в котором зарегистрирован IP-адрес;
- Индекс, а также широта и долгота объекта;
- полный адрес объекта.

Бот написан на ЯП “Python”, связь между программным кодом и сервисом Telegram реализована при помощи библиотеки “telebot”.

На данный момент бот не имеет постоянного хостинга, следовательно, запускается с рабочего ПК.

Кроме определения информации по IP-адресу бот также обладает дополнительными функциональными возможностями, например, упомянутый

ранее способ получения IP-адреса - инструмент анализа доменного имени по DNS протоколу (рис. 2).

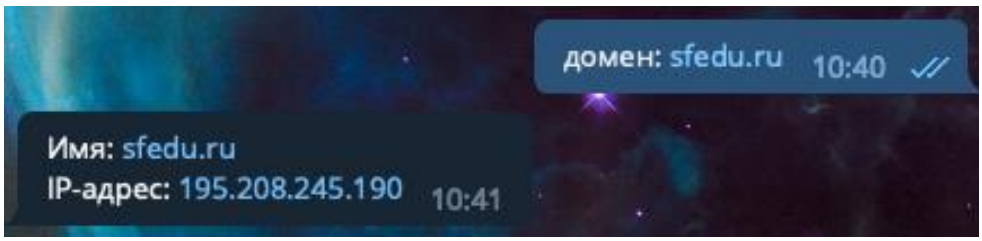

Рисунок 2 - Пример определения IP-адреса по доменному имени

В сгенерированном сообщении о доменном имени предоставляется информация об IP-адресе, принадлежащему домену.

Как уже говорилось ранее, результаты, предоставляемые данного рода сервисами, могут отличаться из-за разных используемых источников, однако это не значит, что выбранные API дают некорректные результаты.

Созданный инструмент является конкурентноспособным, опережая конкурентов по количеству одновременно используемых источников и по наличию дополнительных функциональных возможностей.

Также в процессе разработки находится веб-версия инструмента, обладающие еще большими функциональными возможностями. Помимо описанных функций веб-версия на данный момент предоставляет пользователю возможность отображения полученной информации на интерактивной карте, возможность ведения истории поиска, а также предоставляет расширенный пакет информации о доменном имени.

Заключение

В ходе выполнения данной работы был произведен сравнительный анализ существующих OSINT-инструментов данной сферы, разработана и продемонстрирована методика определения геолокации по IP-адресу, создан собственный OSINT-инструмент, обладающий преимуществами перед своими аналогами.

Также кратко был описан создаваемое в данный момент веб-приложение, которое в совокупности с telegram-ботом впоследствии образует одну систему поиска данного рода информации.

СПИСОК ИСТОЧНИКОВ

1. Минченко, В. Разведка на основе открытых источников (OSINT) и ее методология в современных реалиях / В. Минченко, Г. Ф. Вильдяйкин // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований : Материалы III Всероссийской национальной научной конференции студентов, аспирантов и молодых ученых. В 3-х частях, Комсомольск-на-Амуре, 06–10 апреля 2020 года / Редколлегия: Э.А. Дмитриев (отв. ред.) [и др.]. Том Часть 2. – Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный университет, 2020.
2. Кутурга, В. В. Методы интеллектуального анализа данных при поиске устройства по ip адресу / В. В. Кутурга // Аллея науки. – 2018. – Т. 3, № 11(27).
3. Альтерман, А. Д. Понятие IP-адреса компьютера и его модификация / А. Д. Альтерман, А. С. Парфенова // Современные научные исследования и разработки. – 2018. – № 12(29).
4. Лемайкина С. В. Новый арсенал OSINT в цифровом мире. Разведка по открытым источникам //информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности. – 2021. – С. 27-31.
5. Янгаева, М. О. OSINT. Получение криминалистически значимой информации из сети Интернет / М. О. Янгаева, Н. О. Павленко // Алтайский юридический вестник.
6. Электронная библиотека. Информационные технологии. Структура электронного письма [электронный ресурс] // e-biblio.ru. URL: https://e-biblio.ru/book/bib/01_informatika/infteh/book/docs/piece170.htm.

7. Быстров А. К. Доменное имя и связанные с ним объекты //Современное право. – 2014. – №. 5. – С. 58-61.

8. Сервис “2ip.ua” – URL: https://2ip.ua/ru/ (дата обращения: 18.10.2023).

9. Сервис “Калькулятор. Справочный портал” – URL: https://www.calc.ru/informatsiya_ob_ip.html (дата обращения: 18.10.2023).

10. Сервис “Web-технологии” – URL: https://htmlweb.ru/analiz/whois_ip.php?ip= (дата обращения: 18.10.2023).

11. Сервис “XSEO” – URL: https://xseo.in/ipinfo (дата обращения: 18.10.2023).

12. Сервис “InfoByIp” – URL: https://www.infobyip.com/ (дата обращения: 18.10.2023).

13. Сервис “Деанонимайзер” – URL: https://t.me/deanonym_6_bot (дата обращения: 18.10.2023).

14. Сервис “Whois Domain Bot” – URL: https://t.me/WhoisDomBot (дата обращения: 18.10.2023).

15. Сервис “IPVOID” – URL: https://www.ipvoid.com/ (дата обращения: 18.10.2023).

16. Сервис “IPAddress.com” – URL: https://ipaddress.com.ng/ (дата обращения: 18.10.2023).

17. Сервис “IPFingerPrints” – URL: https://www.ipfingerprints.com/ (дата обращения: 18.10.2023).

Полтавцева М.А.
ФГАОУ ВПО СПбПУ Петра Великого
Институт компьютерных наук и кибербезопасности
Высшая школа кибербезопасности, профессор
д. т. н, доцент
poltavtseva@ibks.spbstu.ru
Калинин М.О.
ФГАОУ ВПО СПбПУ Петра Великого
Институт компьютерных наук и кибербезопасности
Высшая школа кибербезопасности, профессор
д. т. н, профессор
max@ibks.spbstu.ru

МОДЕЛИРОВАНИЕ ДАННЫХ И ПРОЦЕССОВ В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ БОЛЬШИХ ДАННЫХ

Современная экосистема больших данных включает несколько уровней рассмотрения объектов, процессов и целей обработки информации. Это в первую очередь физическая инфраструктура, включающая центры обработки данных, облачные и граничные (fog) решения. Следующий уровень – это инфраструктура управления информацией или системы управления большими данными. Сегодня это совокупность различных СУБД[1] объединенных в рамках процесса управления данными [1]. Третий уровень – уровень экономики данных и знаний, или организационное управление информацией в рамках организации, передача на аутсорсинг. С точки зрения кибербезопасности основную проблему сегодня, в первую очередь, представляет задача построения защищенных систем управления данными и обеспечение безопасности данных на втором уровне рассмотрения. Безопасность технологий нижнего уровня является общей задачей безопасности распределенных систем

[1] Системы управления базами данных

вне зависимости от класса, а безопасность верхнего – во многом организационной задачей, за исключением ряда решений, основанных на технологиях управления данными (например, обезличивания данных).

Сложность в обеспечении безопасности систем управления большими данными заключается в нескольких ключевых отличиях решений этого класса от традиционных СУБД:

1. Сложность жизненного цикла данных;
2. Различная структуризация и грануляция данных на протяжении всего жизненного цикла;
3. Не доверенная распределенная среда обработки.

Многовариантность источников данных и широкий спектр применения самой информации (как во времени, так и в отношении областей и целей применения), свойственные большим данным, обуславливают усложнение жизненного цикла данных. В свою очередь на различны этапах этого жизненного цикла используются различные инструменты обработки информации с различной грануляцией данных. Это значительно усложняет решение задач обеспечения безопасности над данными, в частности задач разграничения и контроля доступа, аудита, анализа защищенности. Использование распределенной среды при обработке больших данных усугубляется принадлежностью различных задействованных узлов и решений не только различным, часто – географически распределенным подразделениям организации, но и юридическим лицам. В этом случае нарушителями могут быть сотрудники, обслуживающие или имеющие иной доступ к любому звену распределенной инфраструктуры.

Консистентный подход к обеспечению безопасности систем управления большими данными определяет как необходимое условие согласованное представление данных и процессов их обработки на всех уровнях рассмотрения. Что, в свою очередь, требует разработки такого представления (модели системы управления большими данными) и построения ее взаимных отображений с моделями данных каждого задействованного инструмента.

Также, как для традиционных СУБД решение задач безопасности базируется на модели данных конкретной системы управления базами данных, так и для систем больших данных необходима разработка общей модели представления.

Надо отметить, что решение подобной задачи актуально не только для решения задач кибербезопасности, но и, например, для задач проектирования таких систем на уровне управления данными. И если для кибербезопасности сегодня практически не предлагается комплексных подходов к безопасности больших данных и рассматриваются только отдельные решения в рамках инструментов и экосистем, для решения задачи согласованного управления информацией в инженерии данных представлен ряд подходов. Сначала исследователями и практиками было предложено использование языковых средств для трансформации запросов и операций [2,3] включая использование общих языковых средств с неявно заданной моделью обработки [4]. Однако такой подход оказался неэффективным и сегодня работы сосредоточены в области построения высокоуровневого представления данных на основе теории категорий для реляционных [5] и не реляционных [6] систем, расширении в рамках этого подхода модели сущность связь (Entity-Relation) [7]. Основной проблемой использования этого подхода остается проблема соответствия, возникшая при попытке совмещения объектного описания предметной области и плоских реляционных таблиц (см. например [8]). Даже однозначное реляицонно – объектное отображение на сегодня (за тридцать лет исследований) не имеет эффективной методологии, не говоря уже о не реляционных решениях с более слабой структуризацией.

Отсутствие такого отображения обуславливает автоматизированный, а не автоматический процесс проектирования схем данных и инженерии данных в СУБД, с высокой зависимостью от реализующего специалиста. Что в условиях сложности систем управления большими данными не является преимуществом. Таким образом, возникает необходимость поиска новых моделей, достаточных по выразительной мощности для решения задач кибербезопасности и обладающих высокой степенью автоматизации.

Одним из критериев, обуславливающих возможность эффективного построения взаимного отображения между моделями данных является использование общего математического базиса. Систематизация математических основ моделей данных в СУБД приведена на рисунке 1. Опираясь на нее, можно сказать о наибольшей эффективности теоретико-множественного подхода для решения поставленной задачи, так как в силу общего математического базиса он будет наилучшим образом коррелировать с моделями уровня инженерии данных. Общая математическая основа позволит также построить однозначные отображения между моделями и операциями в них.

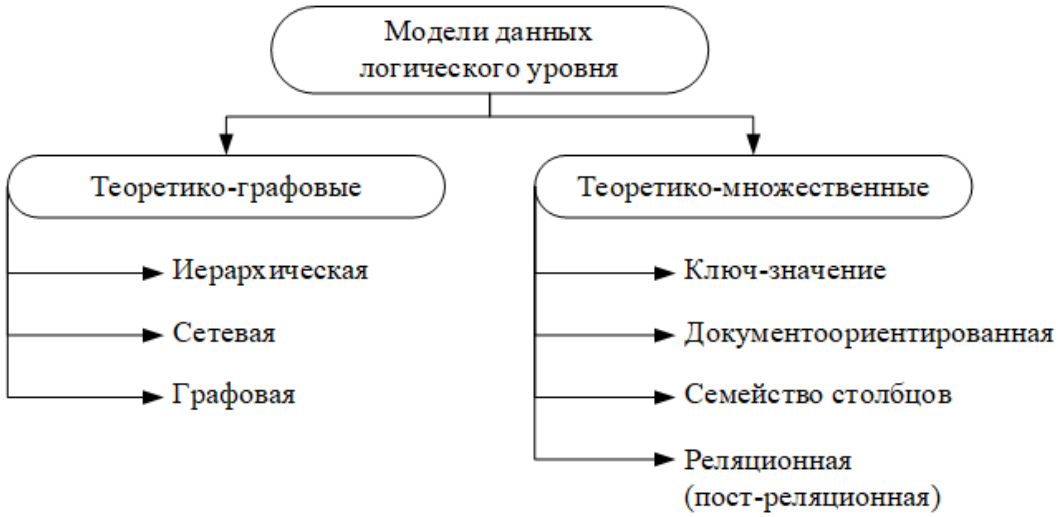

Рис. 1. Математические основы моделей данных логического уровня в СУБД

Основной структурой данных а такой модели будет $f=<Id, Value>$ – единица данных, где *Id* – уникальный идентификатор в рамках системы в целом (в общем случае составной), а $Value=data \cup \{ f \}$ – то есть, либо иметь некоторое конкретное значение данных, либо представлять собой объединение других фрагментов с их собственными идентификаторами. Операциями над фрагментами будут *E – extract* или выделение фрагмента (включая разделение фрагмента на два и более), *U – union* или объединение фрагментов (включение одного или более фрагмента в другой) и *T – transform*, или трансформация

фрагмента с изменением его семантики. Последняя операция также включает в себя действия по созданию новых фрагментов данных. Ограничением является требование уникальности идентификатора фрагмента а связи между фрагментами определяются порождением новых фрагментов на основе других и формализуются как $f_i \rightarrow f_j$, когда f_j был порожден на основе f_i или, говоря иначе, $f_j = T(f_i)$.

Так как модель данных подразумевает не только согласованные структуры данных и ограничения, но и операции над данными в рамках математического базиса и его расширений, возникает возможность построения с использованием концептуальной модели верхнего уровня, как инструмента моделирования, процесса обработки данных в системе больших данных, по аналогии с планами выполнения запросов в СУБД. Формирование такой модели над действующими системами и поддержание ее адекватности возможно на основе технологий распределенного реестра, интегрированных с системами аудита и журналами транзакций (операций) в системах управления базами данных.

Узкая семантика модели ограничивает ее применение для проектирования схем баз данных, однако ее близость к фактическим структурам данных операциям в СУБД позволяет использовать предложенное представление для аудита систем больших данных; анализа систем разграничения доступа; проектирования, оценки и итерационной корректировки политик безопасности, а также оценки защищенности решений данного класса.

СПИСОК ИСТОЧНИКОВ

1. Özsu, M.T. Distributed and Parallel Database Design. / M.T. Özsu, P. Valduriez // Principles of Distributed Database Systems Springer, Cham. – 2020. – 674 p. – doi: 10.1007/978-3-030-26253-2.

2. Krishnapriya V.M A Study for Integrating SQL and NoSQL Databases / V.M. Krishnapriya, S. Libin , G. Gibin // International Conference on Interllectual

Property Rights. – 2021. – URL: https://www.ijsr.net/conf/ICIPR2021/ICIPR2021_16.pdf (access date 19.09.2023)

3. Lu J. Multi-model Databases: A New Journey to Handle the Variety of Data. / J. Lu, I. Holubová // ACM Comput. Surv. – 2019. – vol. 52. – №. 3. – pp. 1-38. – doi: 10.1145/3323214.

4. Koupil P. MM-cat: A Tool for Modeling and Transformation of Multi-Model Data using Category Theory / P. Koupil, M. Svoboda, I. Holubová // 2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C), Fukuoka, Japan. – 2021. – pp. 635-639. – doi: 10.1109/MODELS-C53483.2021.00098.

5. Shinavier J. Algebraic Property Graphs. / J. Shinavier, R. Wisnesky, J. G. Meyers // arXiv preprint arXiv:1909.04881. – 2019. – doi: 10.48550/ARXIV.1909.0488

6. Uotila V. A formal category theoretical framework for multi-model data transformations / V. Uotila, J. Lu //Heterogeneous Data Management, Polystores, and Analytics for Healthcare: VLDB Workshops, Poly 2021 and DMAH 2021, Virtual Event, August 20, 2021, Revised Selected Papers 7. Springer International Publishing. – 2021. – pp. 14-28. – doi: 10.1007/978-3-030-93663-1_2

7. Gobert M. Conceptual modeling of hybrid polystores / M. Gobert, L. Meurice, A. Cleve //Conceptual Modeling: 40th International Conference, ER 2021, Virtual Event, October 18–21, 2021, Proceedings 40. – Springer International Publishing. – 2021. – pp. 113-122. – doi: 10.1007/978-3-030-89022-3_10.

8. Полтавцев, А. А. Сервер объектного представления как связующее звено между объектной логикой и реляционным хранением / А. А. Полтавцев // Информационные ресурсы и системы в экономике, науке и образовании : Сборник статей VII Международной научно-практической конференции, Пенза, 27–28 апреля 2017 года. – Пенза: Автономная некоммерческая научно-образовательная организация «Приволжский Дом знаний», 2017. – С. 98-101. – EDN ZHMNUR.

Богдалов Р.Р.
МТУСИ, Москва, Россия,
ruslanchik_bog@mail.ru

РАЗРАБОТКА ПРОГРАММНОГО ПРОДУКТА КЛАССИФИКАЦИИ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ В АРМ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Введение

В современном высокотехнологичном мире, где цифровые технологии проникают во все сферы жизни, вопросы кибербезопасности становятся более актуальными, чем когда-либо. Постоянное развитие технологических возможностей сопровождается возрастанием угроз со стороны киберпреступников, чьи атаки становятся все более изощренными. В этом контексте разработка программного обеспечения для обнаружения нелегитимных вычислительных процессов с использованием методов машинного обучения представляет собой важный этап в обеспечении кибербезопасности.

Актуальность работы

Данная работа направлена на реализацию требований приказов ФСТЭК России [1, 2, 3, 4] «Обнаружение вторжений». Киберпреступники применяют новейшие методы маскировки и скрытия вредоносных действий, что усложняет их обнаружение и предотвращение и поэтому возникает потребность развивать способы их обнаружения.

Из чего следует, что автоматизация процесса выявления несанкционированных вычислительных процессов становится неотъемлемой частью стратегии обеспечения кибербезопасности. Традиционные методы анализа и мониторинга зачастую оказываются недостаточно эффективными и время затратными в условиях современной киберугрозы. Автоматизированные системы, основанные на методах машинного обучения, позволяют оперативно

выявлять подозрительные и потенциально вредоносные действия, что увеличивает шансы на своевременное реагирование и минимизацию ущерба.

Таким образом, в контексте современной кибербезопасности, актуализация и развитие автоматизированных систем выявления несанкционированных вычислительных процессов является стратегически важным шагом в защите информационных ресурсов и данных. Она позволяет не только обнаруживать атаки на ранних этапах, но и эффективно адаптироваться к постоянно меняющимся угрозам киберпреступности.

Цель работы

Цель данной исследовательской работы заключается в разработке программного продукта, способного автоматически выявлять несанкционированные вычислительные процессы с использованием методов машинного обучения. Предполагается создание базы данных процессов, анализ которой позволит обучить модель распознавания подозрительных активностей. Эта модель будет впоследствии интегрирована с высокоэффективным сканером, обеспечивая непрерывную круглосуточную защиту компьютерной системы.

Таким образом, цель данного исследования заключается в создании средства киберзащиты, способного оперативно и надежно выявлять несанкционированные вычислительные процессы, что в конечном итоге содействует повышению общей кибербезопасности в условиях современного цифрового пространства.

Принцип работы программы

В процессе создания программного продукта для выявления несанкционированных вычислительных процессов, первым этапом является формирование базы данных, содержащей информацию о различных процессах, работающих на компьютере (Рисунок 1).

В эту базу вносятся следующие параметры:

- название процесса;
- процент нагрузки на графический процессор (GPU);
- процент использования оперативной памяти, тип процесса;
- процент нагрузки на центральный процессор (ЦП).
- наличие сетевой активности

	pid double precision	process_name character varying (255)	cpu_usage double precision	memory_usage double precision	process_type character varying (255)	network_activity boolean
1	0	System Idle Process	0	4.8387533822886146e-05	running	false
2	4	System	0	0.09462182239065385	running	false
3	184	Registry	0	0.2408731433703272	running	false
4	208	RuntimeBroker.exe	0	0.08951693757233936	running	false
5	324	opera.exe	0	0.7102322214523228	running	false
6	760	smss.exe	0	0.007064579938141377	running	false
7	800	svchost.exe	0	0.1854694171431226	running	true
8	1084	svchost.exe	0	0.0370164633745079	running	false
9	1100	svchost.exe	0	0.0675248034498376	running	false
10	1160	csrss.exe	0	0.04323426147074877	running	false
11	1260	wininit.exe	0	0.04492782515454978	running	false
12	1332	services.exe	0	0.06691995927705154	running	false
13	1356	lsass.exe	0	0.1640821271934069	running	false
14	1428	svchost.exe	0	0.0753877776960566	running	false
15	1480	svchost.exe	0	0.2056470187472661	running	false
16	1508	fontdrvhost.exe	0	0.021096964746778357	running	false
17	1564	WUDFHost.exe	0	0.12679953238287311	running	false
18	1624	svchost.exe	0	0.10884775733458238	running	false
19	1672	svchost.exe	0	0.06636350263808835	running	false
20	1740	WUDFHost.exe	0	0.05617792676837081	running	false
21	2012	Monitor.exe	0	0.13035601611885525	running	false

Рисунок 1 – Создание базы данных

Исходные данные для формирования базы получаются из анализа процессов, работающих на компьютере. Это включает в себя процессы, запущенные как операционной системой, так и установленными программами. После этого формируется "белый список" процессов, являющихся допустимыми и безопасными. Эти данные собираются в результате парсинга и анализа системной активности. Принцип реализации представлен на рисунке 2.

Рисунок 2 – Принцип записи данных в базу данных

Следующим этапом является создание базы данных "черного списка", включающей в себя известные вредоносные процессы и программы. Это позволяет системе отличать потенциально опасные процессы от безопасных. Принцип реализации представлен на рисунке 3.

Рисунок 1.3 - Принцип записи данных в базу данных

С учетом подготовленных баз данных "хороших" и "плохих" процессов возможно перейти к обучению модели с учителем. Применяются методы машинного обучения, которые позволяют модели выявлять аномалии в работе процессов и классифицировать их на основе предоставленных признаков.

Таким образом, описанный процесс представляет собой комплексную методологию, направленную на разработку высокоэффективного средства киберзащиты. Включая этапы от сбора данных до интеграции модели в код, он обеспечивает надежную защиту компьютерной системы от современных киберугроз.

СПИСОК ИСТОЧНИКОВ

1. Шелухин О.И. Методы машинного обучения в информационной безопасности: учебное пособие Москва: Московский технический университет связи и информатики, Текст: электронный
2. "Требования по безопасности" Официальный веб-сайт ФСТЭК (fstec.ru). [Интернет-ресурс]. - https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-14-aprelya-2023-g-n-64?ysclid=lnpvn3b5xq967850296
3. Материал о процессах в Windows. URL: https://sysadminium.ru/kak_ustroen_windows-processy_windows/
4. 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 Текст: электронный
5. Документация PostgreSQL URL: https://www.postgresql.org/docs/
6. Приказ ФСТЭК №17 URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17
7. Psutil - документация URL: https://psutil.readthedocs.io/en/latest/
8. Psycopg2 – документация URL: https://pythonru.com/biblioteki/vvedenie-v-postgresql-s-python-psycopg2

9. Time – документация. URL: https://docs.python.org/3/library/time.html

10. Шелухин О.И., Раковский Д.И. Многозначная классификация меток классов системных журналов компьютерных сетей. Сравнительный анализ эффективности классификаторов // Вопросы кибербезопасности. 2023. Т. 55, № 3. С. 62–77.

Листинг 1

Код парсера.

```
import psycopg2
import psutil
import time

connection = psycopg2.connect(
    host="127.0.0.1",  # IP адрес
    database="postgres",  # Название базы данных
    user="postgres",  # Имя пользователя
    password="zgthdsqdctulf5")

create_table_query = '''
CREATE TABLE computer_activity (
    pid FLOAT,
    process_name VARCHAR(255),
    cpu_usage FLOAT,
    memory_usage FLOAT,
    process_type VARCHAR(255),
    network_activity BOOLEAN,
    network_usage_percent FLOAT
);
'''
cursor = connection.cursor()
#cursor.execute(create_table_query)

clear_table_query ='''
ALTER TABLE computer_activity
DROP COLUMN network_usage_percent;
'''
```

```
        cursor.execute(clear_table_query)

        connection.commit()

        def write_data():
            for proc in psutil.process_iter(['pid', 'name', 'cpu_percent', 'memory_percent',
'memory_info', 'connections']):
                pid = proc.info['pid']
                process_name = proc.info['name']
                cpu_usage = proc.info['cpu_percent']
                memory_usage = proc.info['memory_percent']
                connections = proc.info['connections']

                total_io_counters = psutil.net_io_counters()
                total_bytes = total_io_counters.bytes_sent + total_io_counters.bytes_recv

                process_type = psutil.Process(pid).status()

                network_activity = False
                for conn in connections:
                    if conn.status == psutil.CONN_ESTABLISHED:
                        network_activity = True
                        break

                #network_usage_percent = psutil.net_io_counters().bytes_sent +
psutil.net_io_counters().bytes_recv

                cursor.execute(
```

```
            "INSERT INTO computer_activity (pid, process_name, cpu_usage, memory_usage, process_type, network_activity, network_usage_percent) VALUES (%s, %s, %s, %s, %s, %s, %s)",
            (pid, process_name, cpu_usage, memory_usage, process_type, network_activity, network_usage_percent))

    write_data()

    connection.commit()
    cursor.close()
```

Епифанцев С.В.,
магистрант, Московский технический
университет связи и информатики;
Верба В.А.,
к.т.н., доцент, Московский технический
университет связи и информатики,
ЧУ ВО «Институт государственного
администрирования» (г. Москва);
Корабельников Д.А.,
ГБОУ Школа 1770 города Москвы

СОРЕВНОВАНИЯ В ФОРМАТЕ CTF КАК ВАЖНЫЙ ИНСТРУМЕНТ ПРОФОРИЕНТАЦИОННОЙ ПОДГОТОВКИ ШКОЛЬНИКОВ ДЛЯ ПОСТУПЛЕНИЯ В ТЕХНИЧЕСКИЕ ВУЗЫ НА НАПРАВЛЕНИЯ, СВЯЗАННЫЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Ключевые слова: ctf, capture the flag, информационная безопасность, ВУЗ, школа, обучение, профориентация.

С каждым днем информационные технологии входят в жизнь людей все больше и больше. Связано это с тем, что информационные технологии позволяют существенно упростить жизнь человека. Однако, информационные технологии несут не только пользу, но и создают новые угрозы, с которыми необходимо бороться. Для борьбы с появляющимися угрозами, в свою очередь, нужны специалисты в области информационной безопасности.

Подготовку будущего специалиста в области информационной безопасности необходимо начинать со школы. Это необходимо для того, чтобы после выпуска школьник целенаправленно поступал в технические вузы на направления, связанные с информационной безопасностью. Осознанный выбор направления обучения приведет к тому, что будущий студент будет более ответственно подходить к учебе, что приведет к получению более

качественных кадров по выпуску из высшего учебного заведения. Также подготовка специалистов со школы позволит им получить базовые знания в области информационной безопасности, что упростит для школьника процесс обучения в высшем учебном заведении.

Однако, для того, чтобы школьник смог определиться с тем, что ему интересна тематика, связанная с информационной безопасностью, необходимо объяснить школьнику что такое информационная безопасность и с какими задачами сталкиваются специалисты, работающие в области информационной безопасности. И, как правило, школьный курс не затрагивает данную тематику. Поэтому школьник при поступлении в высшее учебное заведение не может совершить осознанный выбор направления, связанного с информационной безопасностью. Для устранения пробела в данной области могут использоваться соревнования по информационной безопасности в формате CTF. Также данные соревнования могут использоваться для выявления школьников, которым интересна тематика информационной безопасности, а также соревнования формата CTF могут использоваться для их последующей подготовки.

CTF – соревнования по информационной безопасности, которые проходят в игровой форме. Участники должны находить флаги, которые организаторы прячут в различных уязвимых программах или веб-сайтах. За каждый найденный флаг игрок или команда получает некоторое количество баллов. Победителем становится команда, которая набрала больше баллов, чем остальные команды.

Соревнования формата CTF бывают двух видов: task-based и attack-defence. В первом виде соревнования участники должны решать задачи из различных категорий. Как правило, категории задач следующие: web, reverse, forensic, crypto, ppc, OSINT.

В задачах категории web необходимо найти уязвимости в веб-приложении и проэксплуатировать их. Данная категория задний позволяет изучить такие виды атак, как SQL-инъекции, XSS-инъекции, уязвимости в

аутентификации и авторизации, уязвимости в обработке файлов, уязвимости в сетевых протоколах.

В задачах категории reverse участники отрабатывают навыки обратной разработки программного обеспечения, а также навыки анализа исполняемых файлов. При решении задач данной категории участники получают код программы или исполняемый файл. После чего участники должны выявить уязвимости или слабые места программы и использовать найденные слабые места для получения флага.

Задачи категории forensic позволяют участникам соревнований познакомиться с направлением расследования инцидентов (например, взлом веб-сервера или утечка конфиденциальной информации). При решении заданий из данной категории участникам выдаются файлы или образы, из которых необходимо извлечь какую-либо информацию. Примерами направлений заданий из данной категории являются: анализ файловой системы, анализ сетевого трафика.

В задачах категории crypto участникам предлагается ознакомиться с еще одним разделом, связанным с информационной безопасностью, – криптография. В задачах данной категории участникам необходимо используя различные уязвимости в шифрах расшифровывать данные. В расшифрованных данных находится флаг. Данная категории позволяет участникам соревнований ознакомиться с различными видами шифров и с различными видами уязвимостей, которые присутствуют в тех или иных шифрах.

В задачах категории ppc участникам необходимо разрабатывать программы или автоматизировать обработку большого количества данных. Решая задачи данной категории, участники соревнований смогут отработать навык разработки программного обеспечения.

В задачах категории OSINT участникам предстоит решать задачи, связанные с конкурентной разведкой. В данной категории участникам необходимо собирать и анализировать информацию из открытых источников, например, веб-сайты, социальные сети, форумы и т.д. Примерами заданий из

данной категории являются: поиск информации о человеке по имени, номеру, почте, анализ связи между пользователями социальных сетей, анализ изображений и аудио-файлов для поиска сокрытой информации.

Описанные выше категории являются основными категориями, но организаторы различных соревнований могут добавлять или убирать какие-либо из категорий. Также, часто для решения заданий необходимо использовать знания из различных категорий. Например, при решении задачи категории web может потребоваться знание категории crypto.

В соревнованиях вида attack-defence участники должны защищать собственную инфраструктуру, а также атаковать инфраструктуру противника для получения флагов. Защита собственной инфраструктуры заключается в правильной настройке системы, поиске уязвимостей собственной системы и их устранения. Атака инфраструктуры противника заключается в поиске уязвимостей в сервисах противника и последующей эксплуатации уязвимостей для проникновения в инфраструктура противника и получения флага, хранящегося в сервисах противника. Однако, для участия в соревнованиях данного вида, необходимо обладать знаниями в области администрирования, а также иметь знания в области информационной безопасности. В связи с этим данные соревнования не подходят для начинающих специалистов, т.к. у них не достаточно знаний для развертывания и администрирования инфраструктуры.

Для профориентации и первоначального обучения школьников информационной безопасности больший интерес представляет CTF вида task-based. Связано это с тем, что данный вид соревнований разрабатывался для тех, кто еще не имеет достаточных знаний в администрировании и информационной безопасности. Соревнования вида task-based позволят школьникам ознакомиться с различными направлениями в информационной безопасности (например, криптография, OSINT, реверс-инженеринг, программирование) и выбрать одно или несколько направлений, которые будут наиболее интересны школьнику. Когда школьник определится с направлением, в котором ему интересно развиваться, он сможет уделять большее количество времени

задачам данной категории, тем самым больше погружаясь в выбранное направление.

Преимуществом использования соревнований формата CTF при работе со школьниками является то, что обучение происходит в игровой форме. Игровая форма привлекает внимание школьников, благодаря чему обучение проходит с большим интересом.

Однако, при использовании соревнований формата CTF для выявления школьников, которым интересна тема информационной безопасности, а также при их обучении, важным является наличие простых заданий, которые могут быть выполнены большинством школьников, так как в случае, если у школьника не получится решить ни одну задачу, то у него может пропасть интерес.

Еще одним преимуществом соревнований формата CTF является то, что школьник может попробовать различные категории заданий и исходя из этого понять какое направление в информационной безопасности его больше привлекает. После того, как школьник выяснит направление, которое для него наиболее интересно, он сможет больше углубиться в данное направление.

Также, важно отметить, что решение задач в соревнованиях формата CTF позволяет развить у школьников навык поиска и обработки информацией, а также навык решения нестандартных задач. Данные навыки являются важными не только для специалиста в области информационной безопасности, но и для любого специалиста работающего в сфере информационных технологий.

Таким образом, соревнования в формате CTF являются инструментом, который может быть использован для устранения пробела в знаниях школьников об информационной безопасности, а также о задачах, которые решают специалисты по информационной безопасности. Кроме того, данные соревнования позволяют выявлять школьников, которым интересна информационная безопасность, а также обучать школьников основам информационной безопасности.

СПИСОК ИСТОЧНИКОВ

1. Мансуров А.В. Ctf-ориентированная парадигма изучения практических вопросов информационной безопасности // Символ науки. 2016. №8-2.
2. Колегов Денис Николаевич, Чернушенко Юрий Николаевич О соревнованиях ctf по компьютерной безопасности // ПДМ. 2008. №2 (2).
3. Варенина Людмила Петровна Геймификация в образовании // ИСОМ. 2014. №6-2.
4. Jan Vykopal, Valdemar Švábenský, Ee-Chien Chang Benefits and Pitfalls of Using Capture the Flag Games in University Courses //SIGCSE '20: The 51st ACM Technical Symposium on Computer Science Education
5. Гимельштейн Евгения Александровна, Годван Дмитрий Федорович, Стецкая Диана Валерьевна ПРИМЕНЕНИЕ ИНСТРУМЕНТОВ ГЕЙМИФИКАЦИИ В ОБРАЗОВАНИИ // Бизнес-образование в экономике знаний. 2020. №3 (17).
6. CTF News [электронный ресурс] // Что такое CTF. URL: https://ctfnews.ru/what-is-ctf/.
7. Xakep [Электронный ресурс] // CTF: Capture the Flag. Как взлом стал спортивным состязанием. URL: https://xakep.ru/2016/06/14/ctf/.
8. МГУ – Школе [электронный ресурс] // Гамаюнов Д.Ю. CTF-движение как новый формат обучения информационным технологиям. URL: http://teacher.msu.ru/sites/default/files/resursy/Гамаюнов%20Д.Ю.%20CTF-движение%20как%20новый%20формат%20обучения%20информационным%20технологиям_0.pdf
9. Белопахов А.С. ИСПОЛЬЗОВАНИЕ ИГРЫ «CAPTURE THE FLAG» КАК ИНСТРУМЕНТА ФОРМИРОВАНИЯ НАВЫКА ОТРАЖЕНИЯ КИБЕРАТАК У ПРОФЕССИОНАЛЬНЫХ ПРОГРАММИСТОВ // Вестник науки. 2023. №5 (62).
10. Хабр [электронный ресурс] // Соревнования Capture The Flag (CTF) и все, что вы о них еще не знали. URL: https://habr.com/ru/companies/swordfish_security/articles/734324/.

Сиротский А.А.
Национальный Исследовательский
Московский Государственный
Строительный Университет, доцент,
к.т.н., доцент,
hotwater2009@yandex.ru

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ РЕСУРСЫ ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Одной из ключевых задач в работе специалиста по информационной безопасности является задача разработки и поддержания в актуальном состоянии модели угроз безопасности обрабатываемой конфиденциальной информации.

Как известно, с 2021 года вступила в силу новая методика оценки угроз безопасности информации [1], которая заменила собой ряд ранее действовавших документов, и которая представляет собой универсальный подход к формированию моделей угроз безопасности информации применительно к различным видам конфиденциальной информации и различным информационным объектам. Как частный случай, данная методика применяется теперь и для моделирования угроз безопасности персональным данным в информационных системах персональных данных. Задача обеспечения безопасности персональных данных и выявление соответствующих им угроз безопасности, является одной из самых актуальных задач в связи с имевшими место инцидентами и введением новых законодательных норм и требований [2, 3].

Принципиально важным нововведением названной выше методики является то, что она для формирования перечня угроз указывает на использование информационных ресурсов, содержащих перечни и описания угроз, виды и шаблоны компьютерных атак, сведения об уязвимостях

программного обеспечения, типичные действия злоумышленников, и другую полезную для специалиста по информационной безопасности информацию.

Ресурсы данного типа, содержащие справочную, и можно сказать, опорную информацию, разрабатываются и поддерживаются как в нашей стране, так и в иностранных источниках. Все эти данные и сведения могут оказать неоценимую помощь при актуализации моделей угроз безопасности и выработке решений по противодействию выявленным угрозам. Кроме того, базы знаний об угрозах и уязвимостях могут оказаться весьма полезными на этапах проведения внутренних и внешних аудитов безопасности на предмет соответствия требованиям по защите информации [4].

Целью данного исследования является анализ и систематизация доступных информационных ресурсов, содержащих обобщающие, справочные и описательные сведения для формирования моделей угроз безопасности.

Первым информационным ресурсом, безусловно, является пополняемый банк данных угроз безопасности информации ФСТЭК России [5]. На текущий момент в нём представлено 222 угрозы, которые классифицируются по следующим признакам:

- объект воздействия (система, оборудование, программный код, и т.п.);
- тип нарушителя (внутренний или внешний);
- потенциал нарушителя (низкий, средний или высокий);
- последствия реализации угрозы (нарушение целостности, нарушение конфиденциальности, нарушение доступности).

Вторым информационным ресурсом является пополняемый банк данных обнаруженных уязвимостей программного обеспечения, который также представлен в открытом доступе на сайте ФСТЭК России [6]. На текущий момент в нём представлено 50952 записи об уязвимостях программного обеспечения, которые содержат следующую информацию:

- наименование программного продукта;
- название компании-разработчика программного продукта (вендор);
- версии, в которых выявлены уязвимости;

- тип программного продукта;

- операционная система функционирования программного продукта;

- тип и идентификатор ошибки соответствии с общим перечнем ошибок Common Weakness Enumeration (CWE);

- класс уязвимости (уязвимость кода, уязвимость архитектуры, многофакторная уязвимость);

- базовый вектор уязвимости по общей системе оценки уязвимостей CVSS (Common Vulnerability Scoring System);

- уровень опасности (низкий, средний, высокий, критический);

- возможные меры по устранению уязвимости, как правило, в виде ссылки на страницу разработчика программного продукта, содержащую соответствующие указания;

- сведения об устранении уязвимости разработчиком (устранена, либо не устранена);

- иная полезная информация.

Третьим информационным ресурсом можно назвать калькулятор-справочник системы оценки уязвимостей CVSS, также представленный на сайте ФСТЭК России [7]. Он позволяет осуществить сравнительный анализ уязвимостей по уровню той потенциальной опасности, которую они могут представлять в случае их эксплуатации со стороны злоумышленников.

Четвёртым информационным ресурсом можно назвать глобальный форум групп реагирования на инциденты безопасности FIRST, на сайте которого в том числе представлено и полное руководство по CVSS [8].

Пятым информационным ресурсом отметим каталог распространённых недостатков программного обеспечения CWE [9], на текущий момент актуальной является версия 4.12, содержащая 933 записи.

Шестым, и весьма полезным информационным ресурсом назовём отечественный портал «Безопасность пользователей в сети Интернет», находящийся под эгидой Национального координационного центра по компьютерным инцидентам (НКЦКИ) [10], и содержащий свою базу

уязвимостей программного обеспечения [11] и Бюллетени НКЦКИ по новым обнаруженным уязвимостям программного обеспечения [12], причём последние можно скачать либо в виде файлов в формате pdf, либо в формате json, что может быть полезно при создании собственных средств аналитики.

Из иностранных информационных ресурсов, седьмым по счёту, отметим национальную базу данных уязвимостей NIST [13], также содержащую описание уязвимостей программного обеспечения, и на которую зачастую ссылаются другие информационные ресурсы.

В качестве восьмого ресурса рассмотрим Common Attack Pattern Enumerations and Classifications (CAPEC) [14], который рекомендован методикой ФСТЭК. Данный сервис представляет собой перечень и описание распространённых шаблонов компьютерных атак, который может быть использован для анализа возможных действий в отношении компонентов информационной системы с позиций злоумышленника. Всего ресурс описывает 559 шаблонов атак, классифицируя их по механизмам и доменам.

Новая методика оценки угроз безопасности информации отличается ещё одним важным нововведением: представлением возможностей реализации угроз безопасности в виде сценариев, базирующихся на совокупности тактик и техник, которыми может владеть и пользоваться потенциальный злоумышленник. В этом контексте важным информационно-аналитическим ресурсом, позволяющим провести анализ тактик и техник злоумышленников является (девятый по счёту) ресурс - глобально доступная база знаний о тактике и приемах противника, основанная на реальных наблюдениях (ATT&CK) [15]. Интересно заметить, что тактики и техники представлены в виде трёх матриц, в зависимости от группы объектов, к которым они могут быть применены:

- матрицы тактик и техник для корпораций;
- матрицы тактик и техник для мобильных устройств;
- матрицы тактик и техник для компьютерных сетей (Интернета).

Такое представление матриц значительно расширяет перспективы моделирования сценарных действий злоумышленников, по сравнению с

перечнем тактик и техник, представленных в качестве базовой основы в Методике оценки угроз безопасности информации ФСТЭК.

Десятым ресурсом выделим онлайн-проект ATT&CK Navigator [16] практической реализации матрицы ATT&CK, который позволяет интерактивно посредством веб-интерфейса осуществлять работу с матрицей, делать на матрице множественные слои, каждый из которых будет отражать техники конкретной категории нарушителей.

Одиннадцатый из рассматриваемых в данном исследовании ресурсов – это открытый проект обеспечения безопасности веб-приложений OWASP [17]. Он в отличие от рассмотренных выше ресурсов не является ни каталогом, ни справочником, а представляет собой интернет-сообщество заинтересованных специалистов, развивающих в рамках данного ресурса ряд проектов, направленных на создание безопасного программного обеспечения. Проблема создания безопасного программного обеспечения с течением времени только обостряется и нуждается в развитии технологий безопасного программирования, которые в свою очередь в ближайшем будущем могут стать одной из востребованных специальностей, что отражено в ряде работ [18, 19, 20, 21, 22]. OWASP предлагает пользователям руководство по тестированию веб-приложений, тренировочную среду, руководство по разработке безопасного программного кода, и другие проекты.

Двенадцатый ресурс - Common Vulnerabilities and Exposures (CVE) [23] – способен осуществить органичную поддержку разработчикам программного обеспечения и представляет собой базу данных публично раскрытых уязвимостей кибербезопасности. На текущий момент – это одна из самых ёмких баз, содержащая 214106 записей. Пополнение базы осуществляется при участии большого количества партнёров.

Помимо угроз безопасности, возникающих по намеренным действиям злоумышленников, существует группа угроз безопасности, обусловленных распространением вредоносного программного обеспечения. Причём пути его проникновения могут быть обусловлены как недостатками сетевой защиты, так

и организационным несовершенством регламентов использования съёмных машинных носителей информации [24]. Оценка потенциального ущерба от несанкционированно распространившего вредоносного программного обеспечения может быть проанализирован на основе описаний действия известных вредоносных программ. Такие каталоги существуют у разработчиков и производителей антивирусного программного обеспечения. К сожалению, единой классификации компьютерных вирусов не существует, и каждый разработчик антивирусных программ ведёт свои базы знаний и применяет свои системы именования вредоносных программ.

Тринадцатым ресурсом обозначим онлайн-справочник компьютерных вирусов разработчика антивирусных программных продуктов Dr.WEB [25]. По имеющимся в справочнике вирусам, представлены описания по:

- выполняемым вредоносным функциям;
- запускаемым процессам;
- модифицируемым, подменяемым или удаляемым файлам и каталогам;
- сетевой активности;
- программным и сетевым запросам;
- загружаемым модулям;
- методам удаления и лечения.

Четырнадцатым ресурсом обозначим аналогичный онлайн-справочник компьютерных вирусов разработчика антивирусных программных продуктов «Лаборатория Касперского» [26]. Вирусные модули здесь называются угрозами. Структура описания вирусных модулей аналогичная. Полезной функцией является отображение иерархического дерева угроз.

Пятнадцатым ресурсом назовём каталог уязвимостей программного обеспечения от той же компании - «Лаборатория Касперского» [27]. В каталог вносятся уязвимости, выявленные в программных продуктах различных разработчиков, доступна сортировка по вендорам. Данный ресурс для более предметного и детального анализа безопасности обслуживаемой системы может быть использован совместно с перечнем уязвимостей ФСТЭК.

Подводя итоги, отметим, что в данном исследовании приведены и охарактеризованы 15 информационно-аналитических ресурсов, которые можно считать необходимым минимумом в практике специалиста по информационной безопасности при выполнении и планировании работ, организационных и программно-технических процедур по предупреждению нарушений безопасности информационных систем и противодействию внешним сетевым воздействиям.

СПИСОК ИСТОЧНИКОВ

1. Методический документ «Методика оценки угроз безопасности информации». Утв. ФСТЭК России 5 февраля 2021 г. – 93 с. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g. [Проверено 12.10.2023].
2. Сиротский, А.А. Анализ изменений законодательства о персональных данных, вступающих в силу с 1 сентября 2022 г / А.А. Сиротский // Безопасность информационных технологий. – 2022. – Т. 29, № 4. – С. 67-81. – DOI 10.26583/bit.2022.4.06. – EDN MFRYWU.
3. Сиротский, А.А. Организационно-правовые изменения в процессах обработки персональных данных в связи с изменениями законодательства, вступающими в силу с 1 сентября 2022 года / А.А. Сиротский // Теория и практика обеспечения информационной безопасности: сборник трудов II Всероссийской научно-практической конференции, Москва, 02 ноября 2022 года. – Москва: Без Издательства, 2022. – С. 105-113. – EDN GPCUGH.
4. Сиротский, А.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов / А.А. Сиротский, С.А. Резниченко // Безопасность информационных технологий. – 2021. – Т. 28, № 3. – С. 103-117. – DOI 10.26583/bit.2021.3.09. – EDN LSDPLE.

5. Банк данных угроз безопасности информации ФСТЭК России. Режим доступа: https://bdu.fstec.ru/threat. [Проверено 12.10.2023].
6. Банк данных уязвимостей программного обеспечения ФСТЭК России. Режим доступа: https://bdu.fstec.ru/vul. [Проверено 12.10.2023].
7. Справочник-калькулятор CVSS. Режим доступа: https://bdu.fstec.ru/calc?bs=AV%3AN%2FAC%3AH%2FAu%3AN%2FC%3AC%2FI%3AC%2FA%3AC. [Проверено 12.10.2023].
8. Глобальный форум групп реагирования на инциденты безопасности FIRST. Полное руководство по CVSS. Режим доступа: https://www.first.org/cvss/v2/guide. [Проверено 12.10.2023].
9. Каталог распространённых недостатков программного обеспечения CWE. Режим доступа: https://cwe.mitre.org/index.html. [Проверено 12.10.2023].
10. Национальный координационный центр по компьютерным инцидентам. Режим доступа: https://www.cert.gov.ru/incident.html. [Проверено 12.10.2023].
11. Портал «Безопасность пользователей в сети Интернет». База уязвимостей программного обеспечения. Режим доступа: https://safe-surf.ru/specialists/base-vulnerabilities/. [Проверено 12.10.2023].
12. Портал «Безопасность пользователей в сети Интернет». Бюллетени НКЦКИ: новые уязвимости ПО. Режим доступа: https://safe-surf.ru/specialists/bulletins-nkcki/. [Проверено 12.10.2023].
13. NIST. National vulnerability database. Режим доступа: https://nvd.nist.gov/. [Проверено 12.10.2023].
14. Common Attack Pattern Enumerations and Classifications (CAPEC). Режим доступа: https://capec.mitre.org/. [Проверено 12.10.2023].
15. MITRE ATT&CK. Режим доступа: https://attack.mitre.org/. [Проверено 12.10.2023].
16. MITRE ATT&CK Navigator. Режим доступа: https://mitre-attack.github.io/attack-navigator/. [Проверено 12.10.2023].

17. Open Web Application Security Project (OWASP). Режим доступа: https://owasp.org/. [Проверено 12.10.2023].
18. Сиротский, А.А. Безопасность программного обеспечения - специальность будущего / А.А. Сиротский // Преподавание информационных технологий в Российской Федерации: Материалы Шестнадцатой открытой Всероссийской конференции, Москва, 14–15 мая 2018 года. – Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2018. – С. 51-54. – EDN XUJELZ.
19. Корнеев, А.А. Проблемы безопасности сетевой инфраструктуры многопользовательских систем проектирования, функционирующих в строительстве / А.А. Корнеев, А.А. Сиротский // Мой профессиональный стартап: Сборник статей по материалам X Всероссийской научно-практической конференции, Нижний Новгород, 30 марта 2023 года. – Нижний Новгород: федеральное государственное бюджетное образовательное учреждение высшего образования "Нижегородский государственный педагогический университет имени Козьмы Минина", 2023. – С. 318-321. – EDN IUPQXV.
20. Сиротский, А.А. Интегративные аспекты по защите информационных систем персональных данных с использованием решений 1С / А.А. Сиротский // Новые информационные технологии в образовании : Сборник научных трудов XXIII Международной научно-практической конференции, Москва, 31 января 2023 года. Том 1. – Москва: Общество с ограниченной ответственностью "1С-Паблишинг", 2023. – С. 231-235. – EDN RWYPUK.
21. Сиротский, А.А. Противодействие утечкам персональных данных из телекоммуникационных систем / А.А. Сиротский // REDS: Телекоммуникационные устройства и системы. – 2023. – Т. 13, № 3. – С. 33-40. – EDN FMEXPW.

22. Сиротский, А.А. Безопасность в Java / А.А. Сиротский, П.И. Кулешов // Современные проблемы информационной безопасности и программной инженерии: Сборник избранных статей научного семинара №1(6) кафедры информационной безопасности и программной инженерии, Москва, 24 января 2014 года / Российский государственный социальный университет, кафедра информационной безопасности и программной инженерии. – Москва: Общество с ограниченной ответственностью "Сам Полиграфист", 2014. – С. 50-56. – EDN UPTCHB.
23. Программа CVE. Режим доступа: https://www.cve.org/. [Проверено 12.10.2023].
24. Сиротский, А.А. Защита от распространения компьютерных вирусов через USB-Flash накопители / А.А. Сиротский // Машиностроитель. – 2012. – № 6. – С. 29-31. – EDN SDKMFL.
25. Dr.WEB. Вирусная библиотека. Режим доступа: https://vms.drweb.ru/search/. [Проверено 12.10.2023].
26. Лаборатория Касперского. Угрозы. Режим доступа: https://threats.kaspersky.com/ru/threat/. [Проверено 12.10.2023].
27. Лаборатория Касперского. Уязвимости. Режим доступа: https://threats.kaspersky.com/ru/vulnerability/. [Проверено 12.10.2023].

Крундышев В.М.
Санкт-Петербургский политехнический университет Петра Великого, доцент,
кандидат технических наук,
vmk@ibks.spbstu.ru
Калинин М.О.
Санкт-Петербургский политехнический университет Петра Великого,
профессор,
доктор технических наук, профессор,
max@ibks.spbstu.ru

МЕТОД ОБНАРУЖЕНИЯ АТАК ИСКАЖЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В последнее десятилетие с учетом роста решений, использующих технологии искусственного интеллекта для анализа данных, все более актуальным становится вопрос защиты вычислительных моделей от целенаправленных атак. Одним из наиболее распространенных типов атак являются атаки искажения (англ. evasion attack), как правило, направленные на нейронные сети, так как те особенно восприимчивы к малым возмущениям [1]. Существует большое количество атак данного типа, каждая из которых нацелена на получение возмущения, позволяющего отнести образец к другому классу и обмануть вычислительную модель. Искажения строятся на оптимизационных и градиентных методах, также могут использоваться генеративные нейросети GAN для генерации вредоносных образцов [2]. В основном такой тип атак направлен на нанесение ущерба моделям типа «белого ящика» или «серого ящика», редко – на модели «черного ящика».

Анализ существующих решений по обеспечению защищенности систем искусственного интеллекта от атак искажения показал, что все известные решения сводятся к повышению устойчивости вычислительных моделей в условиях целенаправленных деструктивных воздействий [3-10]. Известные

методы не обеспечивают комплексную защиту вычислительных моделей, а лишь снижают эффект от атаки искажения. Результаты анализа существующих решений представлены в таблице 1.

Табл. 1. Сравнение методов защиты от атак искажения

Метод защиты	Механизм	Преимущества	Недостатки
Состязательное обучение	Детерминированные алгоритмы	Позволяет предотвратить искажение. Снижает вычислительную мощность. Повышает объем выборки	Один из самых сложных методов. Не всегда может охватить полный спектр возможных состязательных образцов
	Состязательное обучение на базе генеративной состязательной нейросети (GAN)	Повышает объем выборки	
Рандомизация	Случайное изменение данных	Эффективен для типа работы нарушителя с моделью как с «серым» и «черным ящиком»	Возможна неудача при атаке нарушителя на модели типа «белого ящика»
	Случайное зашумление данных	Повышает устойчивость глубокой ИНС (DNN) к случайным возмущениям. Эффективен против L_1- и L_2 -атак	Падение производительности метода на некоторых атаках
	Случайная функция обрезки	Повышает устойчивость глубокой ИНС (DNN) к случайным возмущениям	Падение производительности метода на некоторых атаках
Шумоподавление	Сжатие данных	Оборонительный метод защиты. Позволяет смягчить эффект искажения	Могут быть неэффективны против адаптивной атаки C&W
	Дистилляция входных данных с помощью GAN		
Вес-разреженная глубокая нейросеть (weight-sparse DNN)		Разреженные веса приводят к более надежным устойчивым ИНС. Эффективно работает против L_∞- и L_2-атак	Специфических недостатков не имеет
Метод ближайших соседей kNN		kNN эффективен при большой и плотной выборке. DkNN хорошо противостоит атаке C&W	При малом радиусе может давать плохие результаты
Байесовский метод		Работает лучше, чем состязательное обучение, а также метод RSE	Остается открытым вопрос о более оптимальном решении данного метода
Универсальный метод защиты на базе Perturbation Rectifying Network		Позволяет производить «очистку» входных данных	Специфических недостатков не имеет

Для обнаружения атак искажения предложен подход на основе поиска аномалий в тестовых данных. В основу разработанного метода положено, что при решении задачи классификации входных данных вычислительные модели определяют принадлежность каждого образца к тому или иному классу с определенной степенью уверенности (вероятностью). Чем качественнее обучена вычислительная модель, тем чаще на этапе тестирования степень уверенности будет стремиться к 100%. При этом очевидно, что с некоторой периодичностью в тестовых данных будут встречаться «сложные» образцы, которые нельзя будет однозначно отнести к тому или иному классу. Однако при реализации целенаправленной атаки искажения на вычислительную модель плотность распределения «сложных» образцов существенно возрастает.

Таким образом, идея метода заключается в анализе степени уверенности при решении задачи классификации последовательности входных данных определенного размера. Для обеспечения баланса между количеством ошибок первого и второго рода введена рейтинговая шкала. В случае если в анализируемой последовательности входных данных степень уверенности ниже установленного допустимого порогового значения, то рейтинг узла-отправителя данных снижается. В случае если рейтинг узла равен нулю, данный узел блокируется, происходит разрыв установленного соединения для прекращения атаки на вычислительную модель.

В зависимости от архитектуры вычислительной модели и набора данных для обеспечения высокой точности обнаружения аномалий в тестовой выборке необходимо определить значения параметров разработанного метода: n – количество тестовых образцов, анализируемых за одну итерацию; r – рейтинг узла-отправителя тестовых данных; $threshold$ – пороговое значение степени уверенности при классификации тестовых данных.

Формальное описание разработанного метода обнаружения атак искажения на основе поиска аномалий в тестовых данных представлено ниже:

1. Установка соединения между узлом, отправляющим тестовые данные, из множества узлов $node_t \in Nodes$ и системой искусственного интеллекта (инициализация).

2. Установка данному узлу начального значения рейтинга r: $Rating_{node_t} = r$.

3. На вход вычислительной модели на этапе тестирования от узла поступает множество входных данных, состоящих из отдельных векторов установленного размера n: $Input = \{v_1, \ldots, v_i, \ldots, v_n\}$.

4. Вычислительная модель с определенной вероятностью (степенью уверенности) относит каждый вектор к определенному классу: $P = \{p_1, \ldots, p_i, \ldots, p_n\}$.

5. Определяется средняя вероятность для рассматриваемого множества векторов: $p_{average_n} = \frac{p_1, \ldots, p_i, \ldots, p_n}{n}$.

6. Если средняя вероятность меньше установленного порогового значения $p_{average_n} < threshold$, то рейтинг узла, отправляющего данные тестовые данные понижается на 1: $Rating_{node_t} = Rating_{node_t} - 1$.

7. Если рейтинг данного узла равен 0: $Rating_{node_t} = 0$, то соединение с ним разрывается, и данный узел добавляется в список заблокированных узлов: $node_t \in Ban_{nodes}$.

8. Переход на шаг 3.

Значения параметров разработанной модели определяются в зависимости от защищаемой системы искусственного интеллекта, текущей модели угроз и т.д. Разработанный метод не требует формирования обучающего набора данных и применим к вычислительным моделям любой архитектуры.

На рисунке 1 представлена временная диаграмма взаимодействия злоумышленника с системой искусственного интеллекта, в основе которой лежит разработанный метод обнаружения атаки искажения.

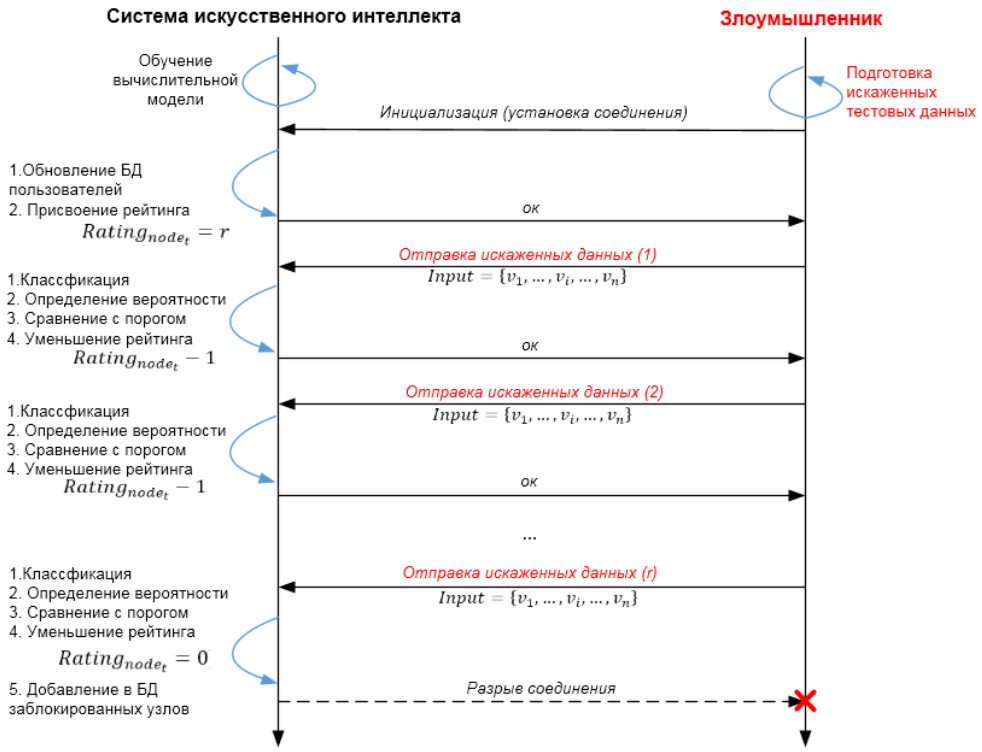

Рис. 1. Временная диаграмма обнаружения атак искажения

Для реализации системы искусственного интеллекта, моделирования деструктивных воздействий, а также разработанного метода обнаружения атак искажения были использованы следующие библиотеки: tensorflow, pytorch, numpy, keras, pandas, matplotlib и т.д. В качестве языка программирования был выбран язык Python версии 3.8.10.

В качестве вычислительной модели была выбрана сверточная нейронная сеть (CNN), реализованная с использованием библиотеки pythorch, предназначенная для классификации изображений. Для данной вычислительной модели была определена следующая архитектура:

– 2 слоя свертки (*conv1* и *conv2*), позволяющих уменьшить количество хранимой в памяти информации и выделить опорные признаки изображения, такие как ребра, контуры или грани;

– 2 слоя регуляризации (*dropout1* и *dropout2*), предназначенных для борьбы с переобучением нейронной сети за счет предотвращения сложных коадаптаций отдельных нейронов на тренировочных данных во время обучения;

– 2 слоя линейного преобразования (*fc1* и fc2), отвечающих за классификацию.

В качестве набора данных для проведения экспериментов был выбран набор данных MNIST (сокращение от «Modified National Institute of Standards and Technology»), содержащий нормализованные, сглаженные и приведенные к черно-белым полутоновые изображения рукописных цифр (0-9) разрешением 28x28 пикселей. Объем обучающего набора данных составил 60000 изображений. Для тестирования и оценки качества обучения вычислительной модели было использовано 10000 изображений.

На рисунке 2 представлена матрица согласованности, демонстрирующая высокую точность работы исходной вычислительной модели, обученной на «чистых» данных. Обученная исходная вычислительная модель на базе сверточной нейронной сети обладает точностью распознавания рукописных цифр из набора данных MNIST, близкой к 100%

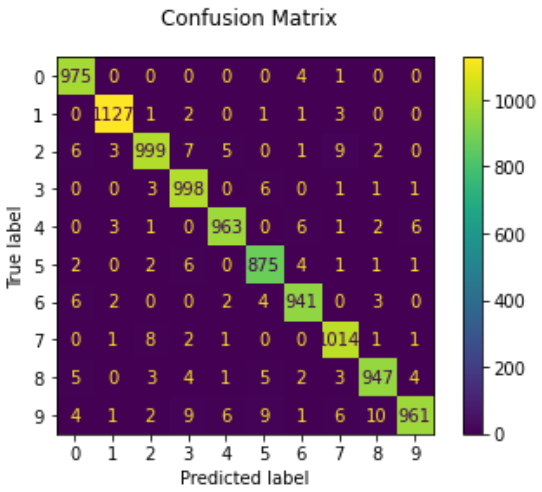

Рис. 2. Матрица согласованности вычислительной модели

Для обученной вычислительной модели была проведена серия экспериментов на «чистых» тестовых данных. В результате проведенного экспериментального исследования установлено, что вычислительная модель со степенью уверенности (вероятностью) более 50% определяет каждый образец из тестового набора данных принадлежащим одному из классов (1-9). Также

установлено, что доля тестовых изображения, для которых степень уверенности менее 75% составляет 3,77% от общего объема тестовых данных. Доля тестовых изображений, для которых степень уверенности менее 60% составляет 0,58% (Рис. 3).

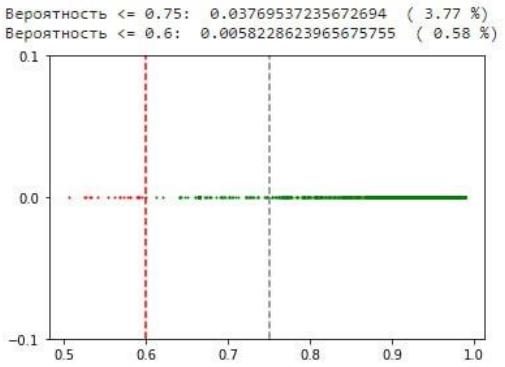

Рис. 3. Распределение степени уверенности при классификации «чистых» тестовых данных

С целью моделирования действий злоумышленника при реализации атаки искажения на вычислительную модель была выбрана часть набора данных, которая подверглась модификации. Были сгенерированы состязательные образцы путем наложения шумов на исходные изображения. Для создания искаженных изображений использовался метод быстрого градиента (FGSM). За интенсивность наложения шумов и степень искаженности исходного изображения отвечает коэффициент пертурбации. Для моделирования атаки искажения на вход вычислительной модели подается 10000 тестовых изображений в соотношении: 50% – «чистые» изображения и 50% – искаженные изображения (коэффициент пертурбации – 0,3).

На Рисунке 4 представлено распределение степеней уверенности при моделировании атаки с использованием искаженных тестовых данных. Как видно из графика, что доля точек в диапазоне $[0,5;0,6]$ существенно возросла, в данный диапазон попало 45,79% точек.

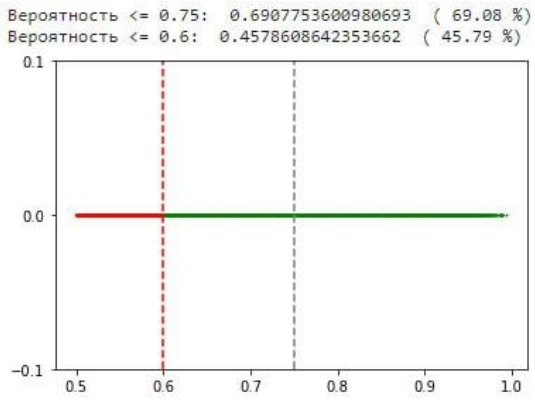

Рис. 4. Распределение степени уверенности при моделировании атаки искажения

Для определения оптимальных значений параметров разработанного метода обнаружения атак искажения вычислительной модели на основе поиска аномалий в тестовых данных была проведена серия экспериментов с использованием разработанных сценариев: «без атаки» и «с атакой». Сценарий «без атаки» подразумевает, что на выход вычислительной модели подаются только «чистые» тестовые данные – 10000 изображений. Сценарий «с атакой» подразумевает, что на вход вычислительной модели в случайном порядке подаются как чистые, так и искаженные образцы. Для усложнения задачи обнаружения атаки установлено соотношение искаженных изображений к «чистым» – 1 к 9 (1000 искаженных изображений с коэффициентом пертурбации равным 0,3 и 9000 «чистых» изображений). Тестирование проводилось при следующих значениях параметров разработанного метода обнаружения: n – длина анализируемой цепочки входных данных за 1 итерацию (3,4,5 или 6); r – начальное значение рейтинга узла (3,4,5,6 или 7); $threshold$ – порог степени уверенности (0,55, 0,60, 0,65, 0,70 или 0,75). Для каждой комбинации параметров было выполнено 50 запусков сценария «без атаки» и 50 запусков сценария «с атакой».

В результате экспериментальных исследований установлено, что разработанный метод обнаружения атак искажения вычислительной модели, основанный на поиске аномалий в тестовых данных, обеспечивает точность

обнаружения 98%. Для обнаружения атаки искажения на обученную сверточную нейронную сеть, реализующую распознавание изображений из набора данных MNIST, необходимо установить следующие значения параметров: длина анализируемой цепочки изображений – 5, порог степени уверенности – 0,60, начальный рейтинг узла – 5. При данных параметров разработанный метод не обнаруживает 1 атаку из 50 при отсутствии ложных срабатываний. Для обнаружения атаки искажения в среднем необходимо проанализировать 52 тестовых образца (при перемешанных «чистых» и искаженных изображений в соотношении 9 к 1).

СПИСОК ИСТОЧНИКОВ

1. Liu. X., Cheng, M., Zhang, H., Hsieh, C. Towards robust neural networks via random self-ensemble. In: Proceedings of the 2018 European Conference on Computer Vision; 2018 Sep 8–14; Munich, Germany; 2018. – P. 369–85.
2. Meng, D., Chen, H. MagNet: a two-pronged defense against adversarial examples. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security; 2017 Oct 30–Nov 3; New York, NY, USA; 2017. – P. 135–47.
3. Raghunathan, A., Steinhardt, J., Liang, P. Certified defenses against adversarial examples. 2018. arXiv:1801.09344.
4. Guo, Y., Zhang, C., Zhang, C., Chen, Y. Sparse DNNs with improved adversarial robustness. In: Proceedings of the 32nd Conference on Neural Information Processing Systems; 2018 Dec 3–8; Montréal, QC, Canada; 2018. – P. 242–51.
5. Wang, Y., Jha, S., Chaudhuri, K. Analyzing the robustness of nearest neighbors to adversarial examples. 2017. arXiv: 1706.03922.
6. Papernot, N., McDaniel, P. Deep k-nearest neighbors: towards confident, interpretable and robust deep learning. 2018. arXiv:1803.04765.
7. Liu, X., Li, Y., Wu, C., Hsieh, C. Adv-BNN: improved adversarial defense through robust Bayesian neural network. 2018. arXiv:1810.01279.

8. Xiao, C., Deng, R., Li, B., Yu, F., Liu, M., Song, D. Characterizing adversarial examples based on spatial consistency information for semantic segmentation. In: Proceedings of the European Conference on Computer Vision; 2018 Sep 8–14; Munich, Germany; 2018. – P. 217–34.
9. Akhtar, N., Liu, J., Mian, A. Defense Against Universal Adversarial Perturbations, – 2018.
10. Hinton, G., Vinyals, O., Dean, J. Distilling the knowledge in a neural network // arXiv preprint arXiv:1503.02531. – 2015.

Бортников М.В.
Алтайский государственный технический университет им. И. И. Ползунова,
maksim.bortnikov@inbox.ru
Якунин А.Г.
Алтайский государственный технический университет им. И. И. Ползунова,
зав. кафедрой, д.т.н., профессор
almpas@list.ru

ПРИМЕНЕНИЕ CIPHER BLOCK CHAINING ТЕХНОЛОГИИ ДЛЯ ОБМЕНА ДАННЫМИ В IOT УСТРОЙСТВАХ

В современном мире информационные технологии развиваются достаточно быстро. Современные микроконтроллеры становятся всё более функциональными, и их вычислительная мощность продолжает расти, в то время как стоимость продолжает уменьшаться. Как следствие, продолжает расти количество встраиваемых систем на базе микроконтроллеров. Одно основных применений таких систем – автоматизированные системы управления производственными процессами [1,2] и IoT – устройства [3,4], в том числе используемые в составе SCADA – систем для автоматизации как производственных процессов, так и системах типа «Умный дом» [4,5].

Для управления IoT – устройствами и системами автоматизации на их основе с выносных пультов или с персональных компьютеров, а также для коммуникации между самими устройствами используются, как правило, беспроводные каналы связи, поэтому возникает необходимость обеспечения их надёжной защиты соответствующими протоколами обмена от неавторизированного вмешательства третьих сторон [6].

Защищённые протоколы используются в условиях, где необходимо поддержание конфиденциальности, подлинности и целостности передаваемых данных, например, в банковском секторе, электронной коммерции, службах электронной почты, разных отраслях промышленности, включая SCADA –

системы [6]. Защищённый протокол, предназначенный для взаимодействия средств вычислительной техники, к которым относятся и IoT – устройства, обычно включает в себя шифрование, аутентификацию и проверку целостности для обеспечения защиты передаваемых данных от несанкционированного доступа или манипуляций. Несмотря на то, что существует множество эффективных и устоявшихся на сегодняшний день защищённых протоколов взаимодействия устройств [7], полномасштабные защищённые протоколы не совсем уместно использовать во встраиваемых системах из-за их требовательности к ресурсам, и сложности работы с их имплементацией, особенно когда речь заходит об IoT – устройствах на микроконтроллерах с ограниченной вычислительной мощностью и чрезвычайно малым объёмом памяти. Отсюда вытекает актуальность разработки более простых и нетребовательных к вычислительным ресурсам микроконтроллеров защищённых протоколов взаимодействия IoT устройств, а также иных встраиваемых устройств, чему и посвящена данная работа.

Изначально была рассмотрена возможность применения для этих целей таких протоколов, как TLS (Transport Layer Security), PGP (Pretty Good Privacy) и SSH (Secure Shell) [7].

TLS, как следует из названия, является протоколом транспортного уровня уровне модели OSI, в котором для передачи данных чаще всего применяются асимметричные алгоритмы шифрования, предполагающие на стадии установления соединения применение сертификатов, выдаваемых удостоверяющими центрами [8], что мало подходит для применения в системах автоматизации. Использование же в протоколе симметричных алгоритмов и протокола Диффи-Хеллмана для обмена ключами в беспроводных сетях, в которых в основном и работают IoT устройства может оказаться небезопасным, да и ресуроёмким.

SSH – это протокол – оболочка прикладного уровня, который может содержать внутри себя другие протоколы, а также использовать разные алгоритмы шифрования (AES, Blowfish и другие) и аутентификации данных [9].

Обычно он используется для безопасного доступа к удалённому компьютеру и мало пригоден для Mesh – сетей.

PGP – протокол, обеспечивающий наибольшую степень криптографической защиты за счёт использования при обмене симметричных и асимметричных протоколов шифрования, сжатия данных и хэширования [10] и, в силу такой «тяжеловесности» и применения асимметричных алгоритмов шифрования, тоже малопригоден для вычислительных сетей, в которых присутствуют IoT устройства.

После анализа вышеперечисленных и ряда других протоколов было решено для построений беспроводных mesh – сетей на базе IoT устройств использовать собственный защищённый протокол, включающий комбинированный алгоритм шифрования и оригинальный алгоритм деривации ключей, не использующий протокол Диффи-Хеллмана. В основу предлагаемого протокола была положена Cipher Block Chaining – технология шифрования, предполагающая для повышения криптостойкости и уменьшения вероятности совершения атаки «встреча посередине», или MitM) – атаки (man in the middle) [11] последовательное применение сразу нескольких алгоритмов шифрования [12, раздел 9.3]. В качестве таких алгоритмов были выбраны алгоритмы AES, Blowfish и Serpent. На рисунке 1 представлена блок – схема работы такого алгоритма.

Получившийся алгоритм шифрования получает на входе 10 ASCII символов (80 бит), конкатенирует к ним 6 случайных символов (48 бит) и шифрует получившиеся 128 бит тремя алгоритмами шифрования (последовательно). После каждого использования алгоритма ключ этого алгоритма инкрементируется. После шифрования всего открытого текста и завершения сеанса связи ключи возвращаются к исходному значению.

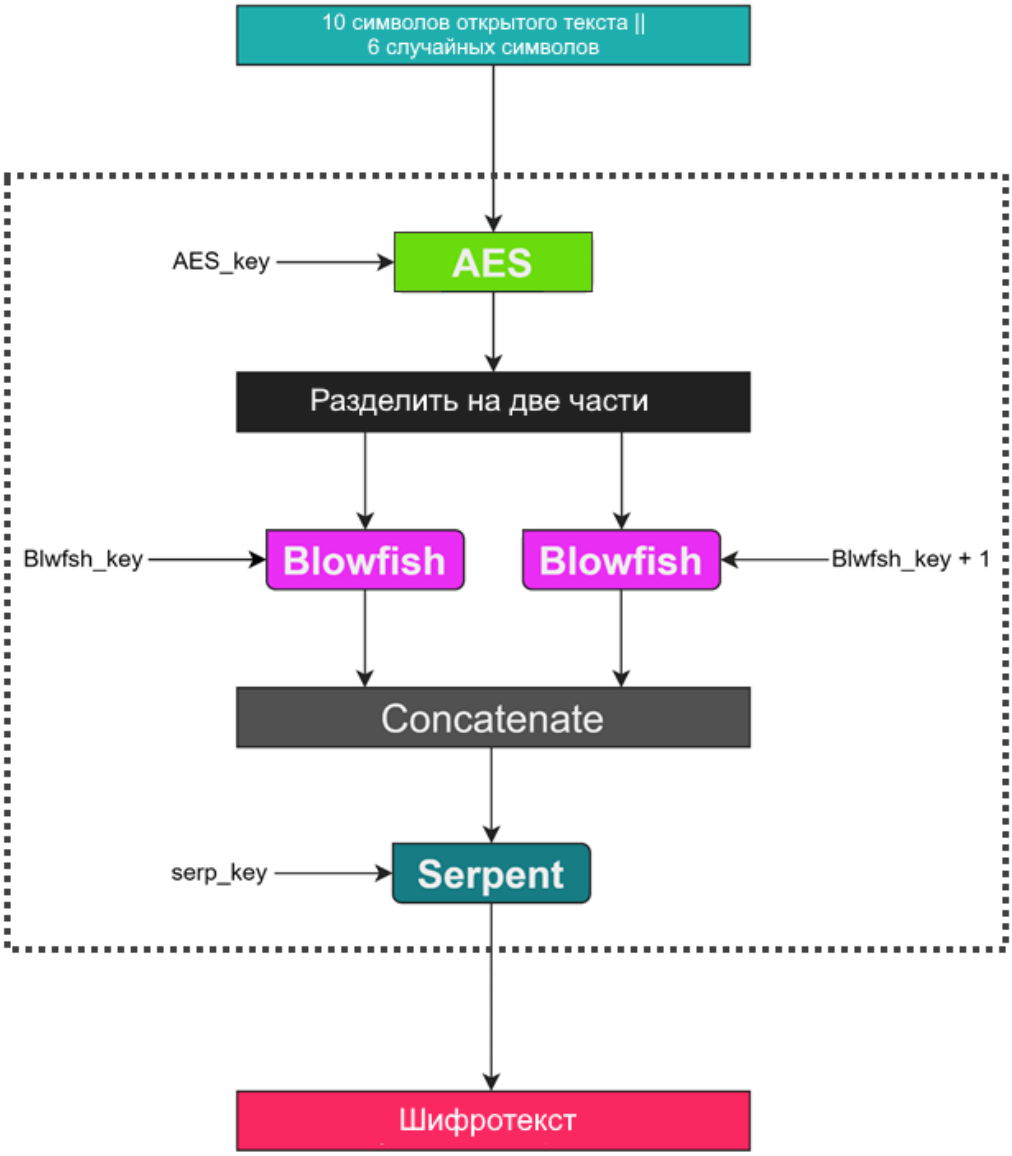

Рисунок 1 – Алгоритм шифрования AES + Blowfish + Serpent

После проведения анализа хэш функций и построенных на их основе HMAC [13], для функции деривации ключей разрабатываемого протокола была выбрана хэш функция SHA512, а в качестве алгоритма аутентификации и проверки целостности был выбран HMAC-SHA256. Таким образом, в предложенном алгоритме шифрования имеется четыре ключа. Три из них показаны на рисунке 1, а четвёртый относится к HMAC-SHA256.

Спроектированный защищённый протокол для взаимодействия IoT устройств функционирует следующим образом. В начале процедуры обмена

передатчик генерирует случайное значение четырёх ключей и с помощью изначально «зашитых» в его памяти ключей шифрует и отправляет эти значения приёмнику, а также модифицирует начальное значение своих ключей на основе только что сгенерированных случайных значений.

Получив от передатчика пакет с зашифрованными случайными значениями новых ключей, приёмник расшифровывает его (также своими начальными значениями ключей, аналогичными ключам передатчика) и модифицирует полученные ключи на основе расшифрованных значений тем же алгоритмом, что и передатчик. Далее приёмник генерирует и шифрует новые случайные значения ключей с использованием только что модифицированных значений и отправляет их передатчику, модифицируя свои только что полученные от передатчика ключи на основе сгенерированных значений.

Получив пакет с новой серией зашифрованных случайных значений ключей от приёмника, передатчик расшифровывает пакет и модифицирует ключи на только что полученных значений. В результате такого взаимного обмена и у приёмника, и у передатчика получатся дважды изменённые наборы ключей, полученные случайным образом из их исходных значений. Затем передатчиком генерируется новый набор ключей, которые аналогичным образом передаются приёмником и модифицируются до новых значений. В результате начальные значения ключей оказываются трижды модифицированы случайным образом (дважды на стороне передатчика и один раз – на стороне приёмника), что существенно снижает вероятность их перехвата. Схема обмена симметричными ключами по предложенному алгоритму приведена на рисунке 2, а изменение состояния ключей в ходе такого обмена показано на рисунке 3.

Конечно, предложенный алгоритм не защищает полностью обмен данными от MitM атаки, но в силу того, что процесс обмена протекает достаточно быстро, он сильно снижает вероятность её успешности. И при этом существенно снижается нагрузка на микроконтроллер, так как предложенный алгоритм не требует применения вычислений с числами большой размерности.

Рисунок 2 – Последовательность процедуры деривации ключей при установлении связи между устройствами

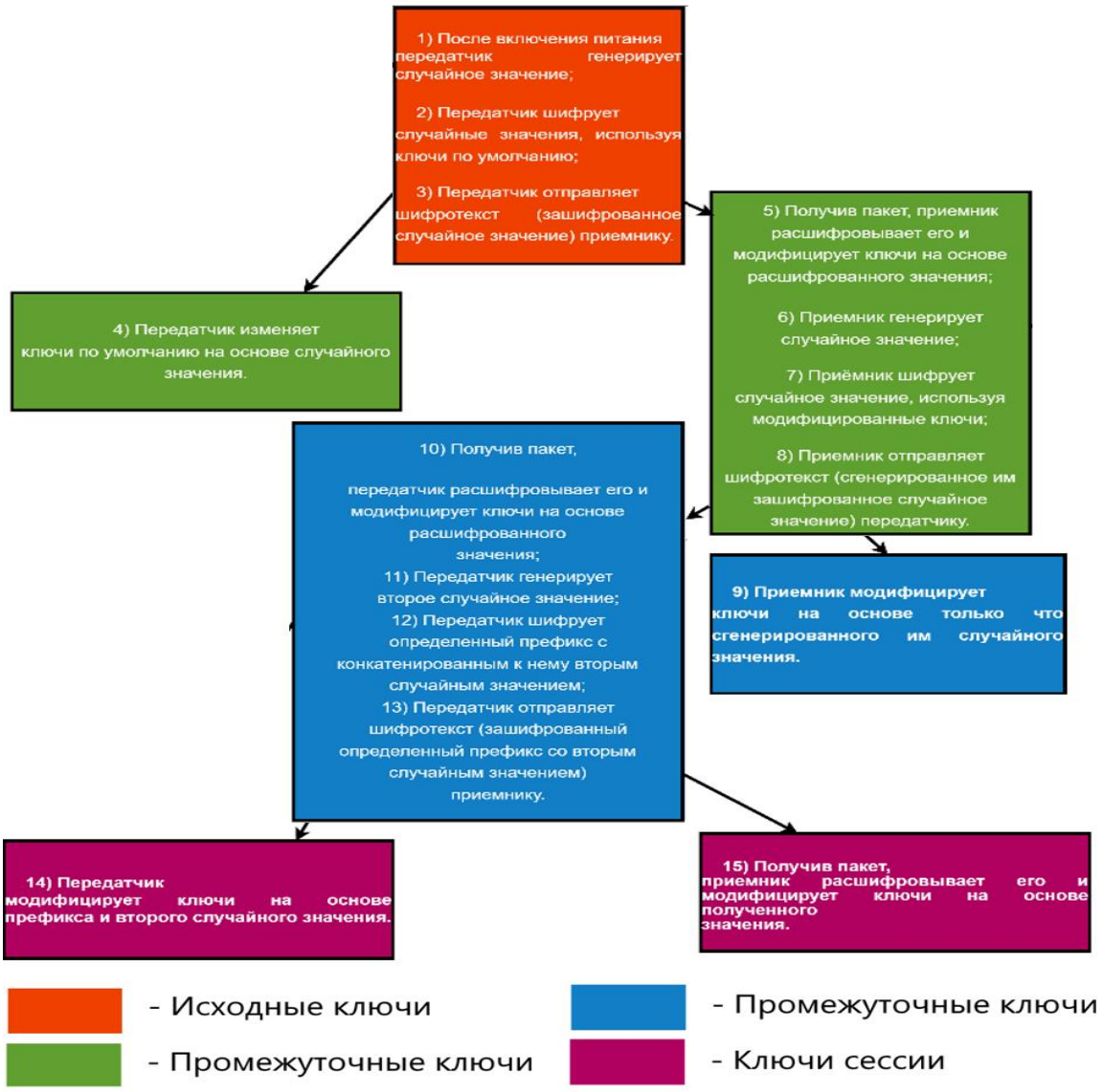

Рисунок 3 – Этапы деривации ключей

Спроектированный защищённый протокол был реализован в среде разработки Arduino IDE и использован в макете системы, состоящей из блока управления и исполнительного IoT устройства, включающего четыре реле. Фото работающего макета системы с IoT устройством и Wi-Fi защищённым каналом передачи сигналов управления представлено на рисунке 4.

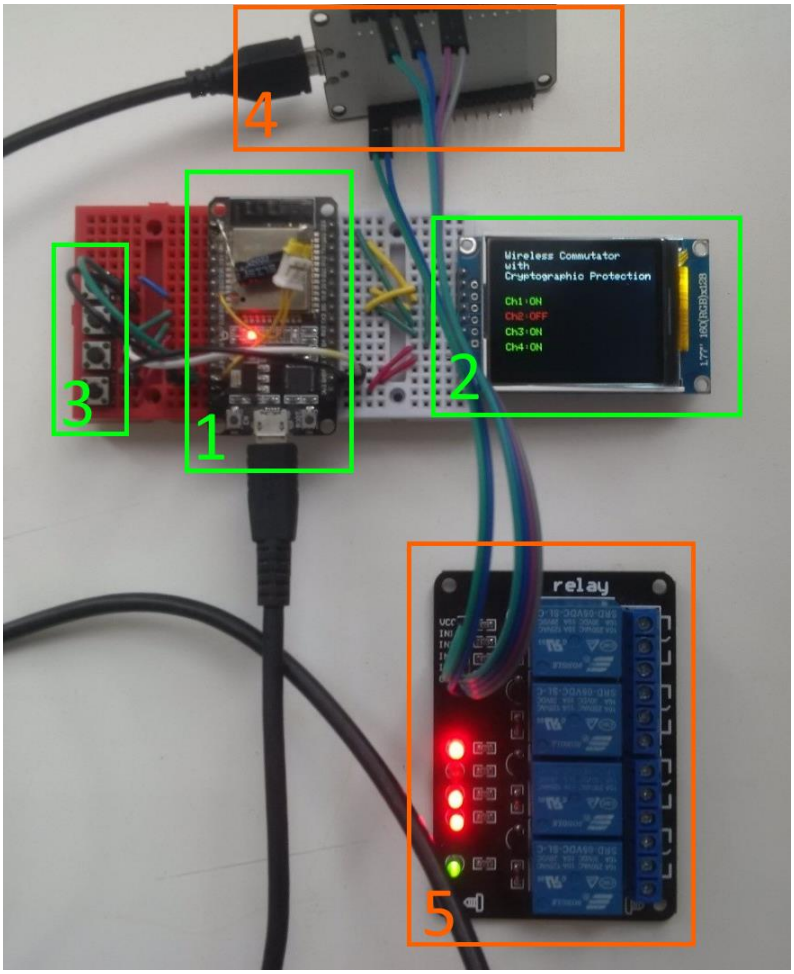

Рисунок 4 – Система дистанционного управления исполнительным устройством по защищенному каналу беспроводной связи. 1 –плата передатчика, 2 – дисплей передатчика, 3 – блок подключенных к передатчику кнопок для управления исполнительным устройством, 4 – плата приёмника, 5 – блок из четырёх реле, подключённых к плате плате приёмника.

Модули как передатчика, так и приёмника были выполнены на базе микроконтроллера ESP32 [14], а в блоке управления имелся также TFT дисплей

на базе контроллера ST7789. Нажатие на любую из кнопок включало или выключало соответствующее этой кнопке реле, а состояние всех реле (включено или выключено) отображалось на дисплее.

СПИСОК ИСТОЧНИКОВ

1. Шишов, О. Современные средства АСУ ТП / Шишов О. — М.: Инфра-Инженерия, 2021. — 532с. —URL: https://znanium.com/read?id=382258 (дата обращения: 20.10.2023)
2. Шишов, О. Технические средства автоматизации и управления/ Шишов О. — М.: ИНФРА-М, 2019 г. 396с
3. Зайнал Альнамер Интернет вещей (IoT): проблемы и будущие направления // Информационные технологии. – 2018. – № 2. – С. 24-26 http://www.logistika-prim.ru/sites/default/files/24-26_internetzainal.pdf (дата обращения: 20.10.2023)
4. Довгаль В.А. Интернет Вещей: концепция, приложения и задачи/ В. А. Довгаль, Д. В. Довгаль // Вестник АГУ. — 2018. — №1 (216) . — С. 129-135. — http://vestnik.adygnet.ru/files/2018.1/5228/129-135.pdf (дата обращения: 20.10.2023)
5. Юрий Широков, Ю. SCADA и автоматизация зданий в эпоху IoT / Ю. Широков// Системная интеграция. — 2020. — № 1. — С. 60-66. https://303421.selcdn.ru/soel-upload/iblock/699/699d80a2a79f92b76df4ce9aa6f23333/20201060.pdf (дата обращения: 20.10.2023)
6. Almalawi, A. SCADA Security: Machine Learning Concepts for Intrusion Detection and Prevention/ Abdulmohsen Almalawi, Zahir Tari, Adil Fahad, XUN YI. — Wiley, E-Book. — 2020. — 224 p. — URL: https://www.wiley.com/en-us/SCADA+Security%3A+Machine+Learning+Concepts+for+Intrusion+Detection+and+Prevention-p-9781119606352 (дата обращения: 20.10.2023)
7. Verma, O. P. Design and Analysis of Security Protocol for Communication / O. P. Verma, S. Balamurugan, Sheng-Lung Peng, Dinesh Goyal. — Wiley. —

2020. —368 p. — URL: https://www.wiley.com/en-us/Design+and+Analysis+of+Security+Protocol+for+Communication-p-9781119555742 (дата обращения 15.10.2023)

8. Boyd, C. Protocols for Authentication and Key Establishment / Colin Boyd, Anish Mathuria. — Springer Berlin Heidelberg. —2013. — 321 p. — URL: https://link.springer.com/book/10.1007/978-3-662-58146-9 (дата обращения: 15.10.2023)
9. Daniel, J. SSH, The Secure Shell / Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes. — O'Reilly Media, Incorporated. — 2005. —645 p. — URL: https://www.google.com/books/edition/SSH_The_Secure_Shell/3XzIFG3w8-YC?hl=fr&gbpv=1&dq=SSH&printsec=frontcover (дата обращения: 20.10.2023)
10. Angstmann, P. Bedeutung von PGP (Pretty Good Privacy) / Philipp Angstmann. —GRIN Verlag. — 2008. —60 p. — URL: https://www.google.de/books/edition/Bedeutung_von_PGP_Pretty_Good_Privacy/Bf_XI0xtCEQC?hl=de&gbpv=1&dq=PGP&pg=PT23&printsec=frontcover (дата обращения: 20.10.2023)
11. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C / Bruce Schneier. — Willey. —1996. —784 p. —URL: https://books.google.is/books?id=Ok0nDwAAQBAJ&pg=PT83&hl=is&source=gbs_toc_r&cad=3#v=onepage&q&f=false (дата обращения: 20.10.2023)
12. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Шнайер, Б. — М.: Триумф, 2002. — 816 с. ISBN 5-89392-055-4.
13. Mittelbach. The Theory of Hash Functions and Random Oracles / Arno Mittelbach, Marc Fischlin. — Springer International Publishing. — 2021. — 788 p. — URL: https://www.google.is/books/edition/The_Theory_of_Hash_Functions_and_Random/Ly8WEAAAQBAJ?hl=is&gbpv=1&dq=hash+functions&printsec=frontcover (дата обращения: 20.10.2023)

14. Описание микроконтроллера ESP32. URL: http://micpic.ru/home/proekty-na-esp32/194-opisanie-mikrokontrollera-esp32.html (дата обращения: 20.10.2023).

ISBN 978-5-6050465-7-8

ТИПОИБ-2023