ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(51) / 2024

УЧРЕДИТЕЛИ

ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИУ)»

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76. ЮУрГУ, Издательский центр
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 1(51) / 2024

FOUNDER

SOUTH URAL STATE UNIVERSITY (NIU)

CHAIRMAN OF THE EDITORIAL BOARD

CHUVARDIN O. P.,
Head of Department Federal Service for Technical and Export Control of Russia for the Urals Federal District

CHIEF EDITOR

SOKOLOV A.N.,
Ph.D., Associate Professor, Head of Department "Information Protection", South Ural State University (National Research University) (Chelyabinsk city)

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SCHREIBER A. E.

PROOFREADING

FEDOROV V. S.

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76 SUSU, Publishing Center
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

УДК 004.056.53 Вестник УрФО № 1(51) / 2024, с. 5–13

Баранкова И.И., Кузьмина У.В., Федорова А.Р., Кульевич Ю.Я., Казаков О.А.

DOI: 10.14529/secur240101

ЭФФЕКТИВНЫЕ МЕТОДЫ ДЛЯ ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ

В данной статье приводится анализ технологии радиозакладного устройства, представляющей устройство, эмулирующее их деятельность. Это устройство работает в диапазоне частот от 88 до 108 МГц, используя биполярный транзистор и электретный микрофон для амплитудной и частотной модуляции звуковых сигналов. Также производится разбор радиоподавляющего устройства, блокирующего радиосигналы и делающего радиозакладные устройства недоступными для прослушивания. Дополнительно в контексте современных требований безопасности рассмотрено устройство «индикатор поля» для обнаружения радиозакладных устройств в помещениях с оперативностью, высокой чувствительностью и способностью предупреждать о потенциальных угрозах. Данные устройства были созданы и испытаны в реальных условиях. Приведенные графики и технические детали визуализируют разницу в мощности между сигналами радиоподавляющего и радиозакладного устройств, делая последнее недоступным для прослушивания.

Ключевые слова: *индикатор поля, обнаружение радиозакладного устройства, подавление радиосигналов, радиоподавляющее устройство, радиопомехи, электромагнитное поле, эмуляция радиозакладного устройства.*

Barankova I.I., Kuzmina U.V., Fedorova A.R., Kulevich Yu.Ya., Kazakov O.A.

EFFECTIVE METHODS FOR DETECTING AND SUPPRESSING RADIO-LAYING DEVICES

This article provides an analysis of the technology of a radio-laying device, representing a device that emulates their activities. This device operates in the frequency range from 88 to 108 MHz, using a bipolar transistor and an electret microphone for amplitude and frequency modu-

lation of audio signals. A radio suppression device is also being disassembled, blocking radio signals and making radio billboards inaccessible to listening. Additionally, in the context of modern security requirements, the device «field indicator» for detecting radio-laying devices in rooms with operability, high sensitivity and the ability to warn of potential threats is considered. These devices were created and tested in real conditions. The graphs and technical details below visualize the difference in power between the signals of a radio suppression and a radio alarm device, making the latter inaccessible to listening.

Keywords: *field indicator, detection of a radio laying device, suppression of radio signals, radio suppressing device, radio interference, electromagnetic field, emulation of a radio laying device.*

Введение

Радиосигналы представляют собой фундаментальный элемент для развертывания беспроводных коммуникаций, радиовещания и различных приложений в области связи. Однако, возникает также значимость их блокирования в ситуациях, требующих ограничения или прекращения их распространения. В данной статье рассматриваются три аспекта для повышения уровень безопасности в использовании беспроводных технологий: создание устройства, эмулирующего деятельность радиозакладного устройства (далее – ЭДРЗУ), радиоподавляющего устройства (далее – РПУ), а также устройства «индикатор поля».

Основной целью разработки ЭДРЗУ, является изучение способов эффективной защиты от подобного рода технических устройств. Для этого часто применяются два основных метода: подавление сигнала и обнаружение источника сигнала. Ниже описаны преимущества и недостатки каждого из этих методов.

Подавление сигнала представляет собой эффективный метод борьбы с РЗУ, так как он способен мгновенно мешать их работе, предотвращая передачу информации. Быстрая реакция делает этот метод подходящим для ситуаций, требующих моментального противодействия угрозе. Однако, использование средств подавления может нарушать законодательство о связи, а также вызывать коллатеральные повреждения, воздействуя на другие беспроводные устройства в районе применения.

С другой стороны, обнаружение источника сигнала обладает преимуществами точности и пассивности. Такие системы способны точно локализовывать и идентифицировать источники радиосигналов, а пассивный режим работы позволяет избежать создания дополнительных помех. Однако, этот метод имеет свои недостатки, такие как сложность обнаружения, особенно если РЗУ скрыты или используют технические средства для избегания обнаружения. Кроме того, обнаружение может потребовать времени, что создает риск того, что злоумышленники успеют выполнить свои задачи до выявления [1].

Выбор между представленными методами зависит от конкретных условий и требований безопасности. В ряде случаев может быть эффективным использование комбинации обоих методов для обеспечения комплексной защиты от РЗУ.

Устройство, эмулирующее деятельность РЗУ

Для создания устройства, способного генерировать радиосигналы в середине УКВ ЧМ диапазона был выбран диапазон частот равный 88-108 МГц, так как сигналы данного диапазона можно поймать обычным радиоприемником, что в свою очередь облегчит этап тестирования устройств.

Принципиальная схема ЭДРЗУ на одном транзисторе представлена на рис. 1.

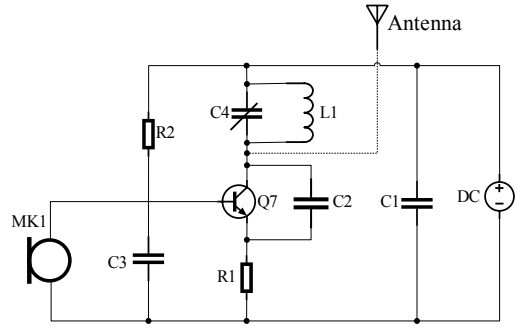


Рис. 1. Принципиальная схема ЭДРЗУ на одном транзисторе

Учитывая компоненты схемы, были использованы LC-генератор (L1, C4), построенный на основе биполярного транзистора Q7 типа 2N3904 и схема «ёмкостной, трёхточки». Данный генератор имеет возможность точечной настройки частоты вещания ЭДРЗУ с помощью переменной ёмкости конденсатора. В

то время как транзистор Q7 генерирует сигнал с заданной частотой.

Для достижения амплитудной и частотной модуляции сигнала звуковой информацией в создаваемом сигнале, использовался электретный микрофон MK1.

Резистор R2 и конденсатор C3, соединенные последовательно, выполняют роль RC-фильтра, который позволяет снизить уровень шума, поступающего с микрофона. Резистор R1 ограничивает ток, поступающий на транзистор Q7, обеспечивая его стабильную работу. Конденсатор C1, подключенный параллельно, способствует сглаживанию импульсов от источника питания, что также способствует повышению качества сигнала [2-3].

Перед сборкой схемы необходимо рассчитать мощность РЗУ, чтобы понимать эффективную дальность передачи, а также, чтобы оценить, насколько долго устройство может работать от автономного источника питания.

Номиналы компонентов выбираются таким образом, чтобы частота генерации составила около 90-100 МГц. Ниже представлены формулы для подбора номиналов компонентов.

Мощность рассчитывается по закону Ома для цепи постоянного тока:

$$P = V * I,$$

где P – мощность, V – напряжение, I – ток.

В соответствии с формулой приблизительная мощность данного передатчика при питании от батарейки 9 В составляет примерно 0.27 Вт. Данную мощность необходимо перевести в децибел-милливатт:

$$dBm = 10 * \log_{10}\left(\frac{P}{1\ \text{мВт}}\right) = 24.31$$

Для правильной работы данной схемы требуется подключение антенны длиной 5-7 см, представленной в виде медной проволоки.

Катушка индуктивности в данной схеме состоит из 8 витков провода диаметром 0,5 мм, намотанных на оправке диаметром 6 мм.

Номиналы всех остальных элементов на схеме, следующие: C1 = 22 нФ, C2 = 4,7 пФ, C3 = 1 нФ, C4 = 10-40 пФ, R1 = 330 Ом, R2 = 4,7 кОм, DC = 3-9 В.

Все элементы кроме выключателя и батареи питания, монтируются на макетной плате. Смонтированная плата ЭДРЗУ показана на рис. 2.

ЭДРЗУ, собранное по схеме рисунка 1,

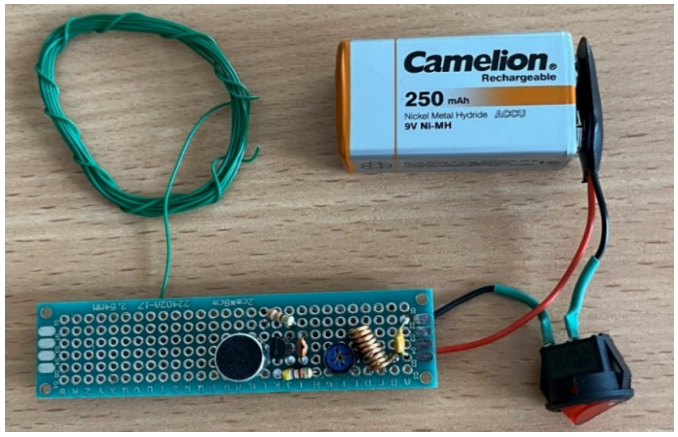


Рис. 2. Смонтированная плата ЭДРЗУ

должно вещать в FM диапазоне. Для определения частоты вещания радиопередатчика необходимо воспользоваться программно-аппаратным комплексом радиоконтроля «Кассандра С6» [4]. Для этого диапазон сканирования выставляется 90 – 100 МГц и фиксируется представленный результат (рис. 3).

В процессе использования ЭДРЗУ, все аудиосигналы, которые попадают на микрофон, автоматически транслируются на предварительно установленную частоту, как показано на представленном выше графике сканирования.

По результатам сканирования, представленного на рисунке 3, видно, что ЭДРЗУ передает информацию на частоте около 94,5 МГц. Радиус действия, равный 12 м, был определен экспериментальным путем. Иными словами, при отдалении ЭДРЗУ от приемника больше чем на 12 м мощность сигнала была сравнима с радиошумом.

Для того, чтобы обеспечить защиту от РЗУ, рассмотрим для начала случай, когда есть возможность определить частоту на котором

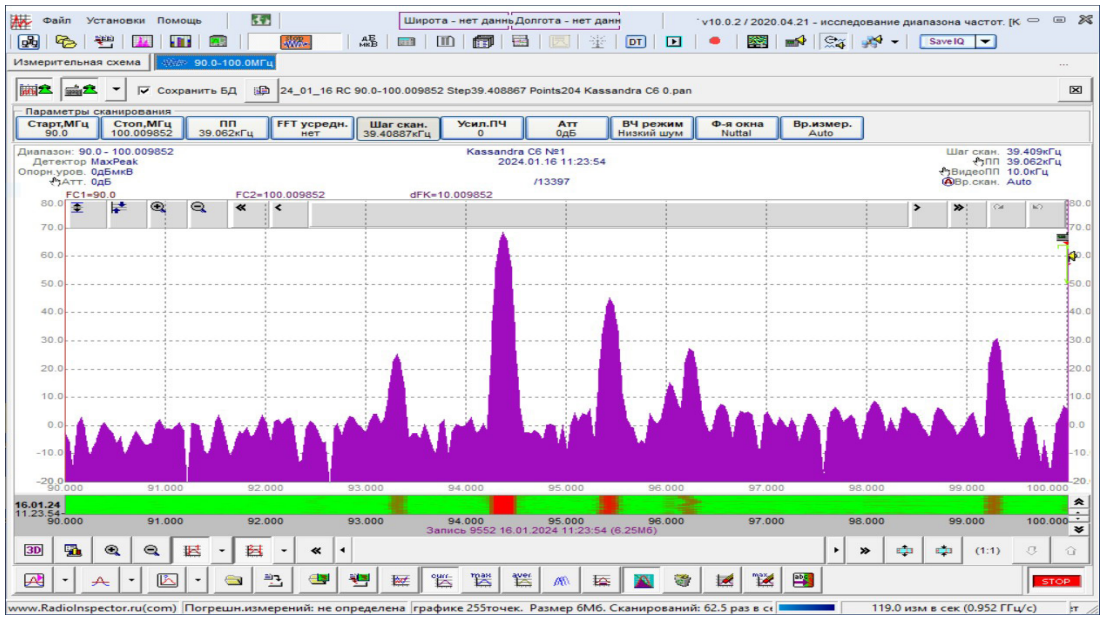


Рис. 3. Сканирование радиоэфира с включенным ЭДРЗУ

работает РЗУ. Для этого случая используют метод подавления сигнала.

Радиоподавляющее устройство

В ряде ситуаций возникает потребность в подавлении нежелательных радиопередач, создаваемых РЗУ, которые вмешиваются в работу незаконным образом и могут нарушить нормальный ход работы. Для этой цели существуют специальные устройства РПУ.

Принципиальная схема РПУ на двух транзисторах представлена на рис. 4.

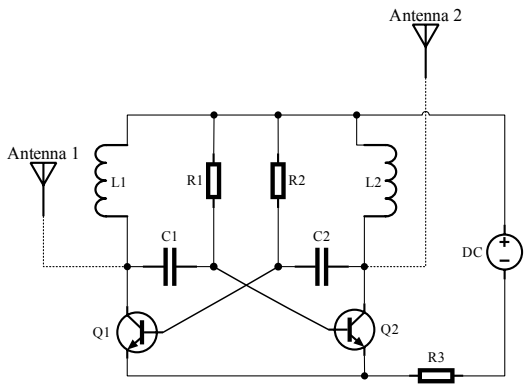


Рисунок 4. Принципиальная схема РПУ на двух транзисторах

Данная схема состоит из двух биполярных транзисторов Q1 и Q2 типа 2CS3355, двух резисторов R1 и R2 и двух конденсаторов C1 и C2, и функционирует как мультивибратор, определяя необходимую выходную частоту. В нагрузке для каждого транзистора используются катушки индуктивности. Помимо этого, схема включает отдельный резистор R3 для обратной связи питания эмиттеров транзисторов [5-6].

Перед сборкой схемы необходимо рассчитать несколько важных параметров, а именно резонансная частота, мощность и длинна волны, на которой будет работать РПУ.

Резонансная частота для схемы рассчитывается следующим образом:

$$f = \frac{1}{2\pi\sqrt{\frac{1}{L_1 C} + \frac{1}{L_2 C}}}$$

Резонансная частота рассчитывается для понимания частоты устройства, а также для эффективной работы на настроенной частоте.

Расчет мощности передатчика можно выполнить с использованием закона Ома и закона электромагнитной совместимости (ЭМС).

Мощность рассчитывается по закону Ома для цепи постоянного тока:

$$P = V * I,$$

где P – мощность, V – напряжение, I – ток.

В соответствии с формулой приблизительная мощность данного передатчика при питании от батарейки 9 В составляет примерно 0.45 Вт.

Мощность переводится в децибел-милливатт:

$$dBm = 10 * \log_{10}(\frac{P}{1\ \text{мВт}}) = 26.53$$

Мощность рассчитывается для понимания эффективной дальности передачи, а также, чтобы оценить, насколько долго устрой-

ство может работать от автономного источника питания.

Для расчета длин антенн для вещания в диапазоне 80-110 МГц, используется формула, связывающая частоту и длину волны:

$$\lambda = \frac{c}{f} = 3 \text{ м},$$

где λ – длинна волны, c – скорость света, f – частота в герцах.

Длинна волны рассчитывается для подбора антенн и подбора компонентов под конкретный диапазон.

Для правильной работы данной схемы требуется подключение двух антенн разной длины, представленных в виде медного провода. Первая антенна имеет длину 14 см, так как это $\frac{1}{16}$ длины волны нижнего диапазона. В то время как вторая антенна – 45 см, так как это $\frac{1}{8}$ длины волны верхнего диапазона.

Катушки индуктивности в данной схеме состоят из 7 витков провода диаметром 0,8 мм, намотанных на оправке диаметром 4 мм. Конденсаторы и резисторы и резистор R3 выполняют функцию сглаживания генерируемых импульсов, что способствует стабильности работы устройства.

Номиналы всех остальных элементов на схеме, следующие: C1, C2 = 1,0 мкФ, R1, R2 = 56 кОм, R3 = 100 кОм, DC = 9 В.

Все элементы монтировались на весу. Смонтированное РПУ на двух транзисторах представлено на рисунке 5.

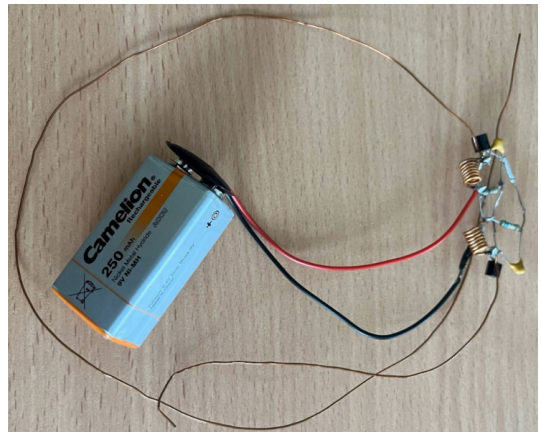


Рис. 5. Смонтированное РПУ на двух транзисторах

Определим диапазон работы схемы, для этого подключим антенну 0–600 МГц, подключим питание к устройству и запустим сканирование (рис. 6).

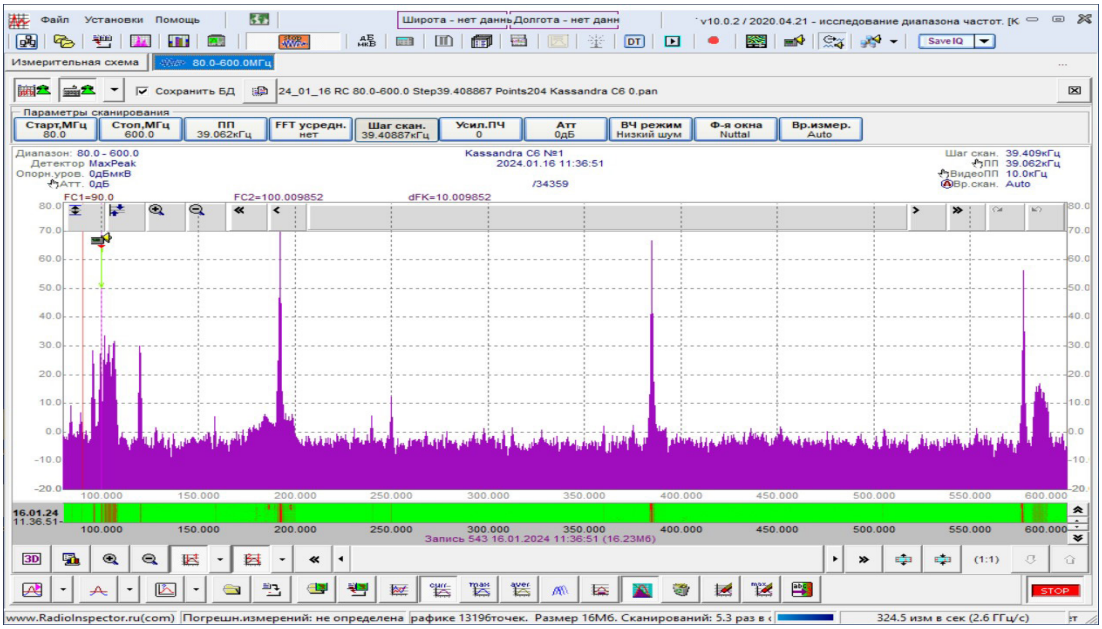


Рис. 6. Сканирование радиоэфира 80 – 600 МГц

При использовании РПУ возникают радиопомехи, которые начинают перекрывать и заглушать сигналы, передаваемые на определенных радиочастотах. РПУ обладает мощным сигналом, что позволяет успешно подавлять слабые радиопередачи, такие как РЗУ. Представленный выше график показывает, что мощность сигнала от РПУ превышает мощность сигнала от РЗУ. Из-за этого, при попытке прослушивания частоты, на которой работает РЗУ, пользователь слышит только шум и помехи, не воспринимая информативный сигнал.

По результатам сканирования, представ-

ленного на рис. 6, видно, что устройство генерирует сигналы через каждые 100 – 110 МГц.

Диапазон работы данного устройства составляет примерно 4000 МГц, основная мощность приходит на первые 1000 МГц, далее постепенно уменьшается. Дальность работы сигнала составляет до 15 метров.

Рассмотрим случай, когда нет возможности определить частоту на котором работает РЗУ, для этого используют метод обнаружения источника сигнала.

Индикатор поля

Помимо того, что в ряде ситуаций можно подавить нежелательные радиопередачи, создаваемые РЗУ. Также возникают ситуации с потребностью обнаружения. Для этой цели существуют устройства «индикаторы поля».

Рассмотрим схему индикатора радиоизлучений для регистрации напряженности электромагнитного поля в высокочастотном диапазоне 3-30 МГц длин волн со встроенным усилителем на транзисторах, позволяющем улучшить чувствительность (рис. 7).

Схема начинается с проволочной антенны длиной 20 см, скрученной в спираль. Длина антенны влияет на чувствительность к частотам: короткая антенна лучше воспринимает высокие частоты, ориентируясь на четверть длины волны. Пойманный сигнал усиливается двумя NPN транзисторами, VT1, VT2 – KT3102EM для хорошей чувствительности. Остальные транзисторы (VT3 – VT10) и диоды (VD1, VD2) – маломощные компоненты.

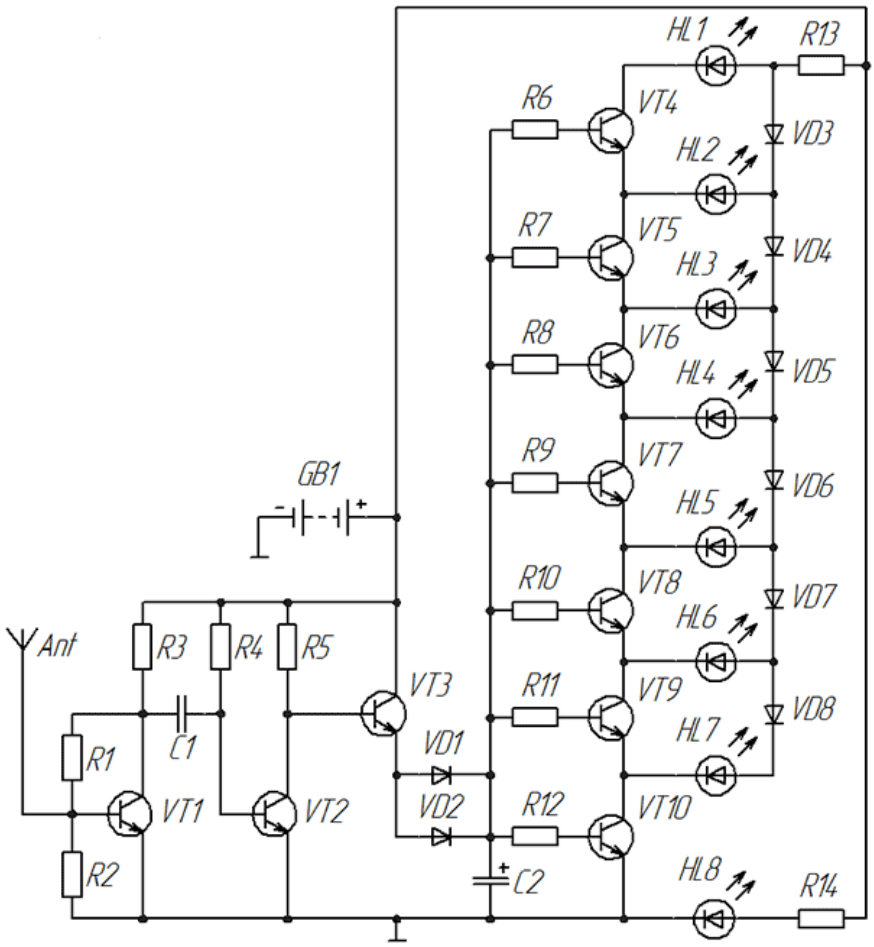


Рис. 7. Принципиальная схема индикатора ВЧ поля

Индикация осуществляется линейкой светодиодов HL1 – HL7, при этом каждый светодиод управляется своим транзистором. Используется пороговый диод (VD3 – VD8) для того, чтобы в каждый момент времени светился только один светодиод. Резистор R13 является токоограничителем для всей линейки, установлен с номиналом 680 Ом для яркости свечения светодиодов. Светодиоды для информативности оформлены в три цвета: зелёный в начале, оранжевый в середине и

красный в конце, предоставляя информацию о максимальном излучении. Схема питается от напряжения 9 В, при этом потребляемый ток не превышает 40 мА. В качестве источника питания используется крона, обеспечивающая несколько часов беспрерывной работы. Конденсатор С2 (22 мкФ) вводится для задержки гашения светодиодного столба, обеспечивая плавность в работе.

Номиналы всех остальных элементов на схеме, следующие: С1 = 10 нФ, R1, R4 = 1 МОм, R2 = 470 кОм, R3, R5 = 10 кОм, R6 – R12 = 1 кОм, R14 = 680 Ом.

Ввиду простоты схемы, индикатор собирается на макетной плате.

Учитывая вышеперечисленные условия, был изготовлен индикатора ВЧ поля (рисунок 9). Изготовленное устройство имеет чувствительность примерно от 20кГц до 2,45 ГГц. Светодиоды загораются снизу вверх, показывая уровень сигнала. Потому поиск скрытого РЗУ в исследуемом помещении осуществляется по нарастающей индикации светодиодов на устройстве.

При обнаружении РЗУ, сигнал будет слабым, так как частота РЗУ значительно меньше

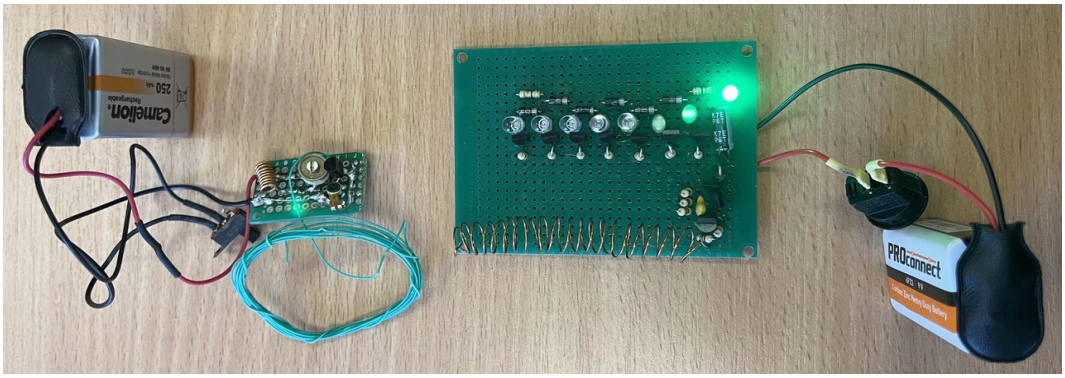


Рис. 9. Поиск РЗУ индикатором ВЧ поля

частоты на котором работает индикатор поля. В связи с этим загорится только нижний светодиод.

Заключение

В рамках данной работы были рассмотрены, проанализированы и разработаны три ключевых аспекта для повышения уровень безопасности в использовании беспроводных технологий: разработка устройства, эмулирующего работу РЗУ, применение РПУ, а также применение индикатора поля, предоставляющее возможность подавления и обнаружения РЗУ в исследуемом помещении.

Выбор между методами защиты от РЗУ – подавлением сигнала и обнаружением – зависит от конкретных требований и характера угрозы. Ниже описаны рекомендации для использования каждого метода.

Подавление сигнала является рекомендуемым методом в экстренных ситуациях, где требуется мгновенное прекращение связи с РЗУ из-за непосредственной опасности. Однако при использовании этого метода крайне важно соблюдать законы и нормативы связи, чтобы избежать возможных юридических проблем, связанных с нарушением законодательства.

С другой стороны, обнаружение сигнала может быть предпочтительным в случае необходимости точной локализации и идентификации источника РЗУ. Этот метод также может быть более безопасным, минимизируя коллатеральные повреждения и избегая создания помех для других беспроводных устройств в окружающей среде.

Таким образом, данная статья подчеркивает эффективность методов обнаружения и подавления РЗУ в современном информационном обществе. Понимание их работы и принципов функционирования существенно для обеспечения эффективности и безопасности радиочастотных систем. Полученные результаты оказывают влияние на развитие технологий связи и повышение надежности работы радиочастотных систем в разнообразных областях применения.

Литература

1. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. – М.: Горячая линия – Телеком, 2016. – 909 с.

2. Малогабаритная радиоаппаратура. Вопросы конструирования, производства и эксплуатации. – М.: Издательство иностранной литературы, 2014. – 372 с.

3. Горшелев, В. Д. Основы проектирования радиоприемников / В.Д. Горшелев, З.Г. Красноцветова, Б.Ф. Федорцов. – Москва: СИНТЕГ, 2015. - 384 с.

4. Михайлова У.В., Фаткуллин А.Р. Использование возможностей комплекса радиомониторинга «Кассандра» для обнаружения современных технических средств с передачей информации по радиоканалу// Безопасность информационного пространства. Сборник трудов XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. 2019. С. 124-127

5. Иванов-Цыганов, А. И. Электротехнические устройства радиосистем / А.И. Иванов-Цыганов. – М.: Высшая школа, 2019. – 490 с.

6. Фаткуллин А.Р., Михайлова У.В. Современные средства радиоразведки// Актуальные проблемы современной науки, техники и образования. Тезисы докладов 79-й международной научно-технической конференции. 2021. С. 402.

References

1. Buzov, Gennadiy Alekseyevich Zashchita informatsii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam / Buzov Gennadiy Alekseyevich. – M.: Goryachaya liniya – Telekom, 2016. – 909 c.

2. Malogabaritnaya radioapparatura. Voprosy konstruirovaniya, proizvodstva i ekspluatatsii. – M.: Izdatel'stvo inostrannoy literatury, 2014. – 372 c.

3. Gorshelev, V. D. Osnovy proyektirovaniya radiopriyemnikov / V.D. Gorshelev, Z.G. Krasnotsvetova, B.F. Fedortsov. – Moskva: SINTEG, 2015. - 384 c.

4. Mikhaylova U.V., Fatkullin A.R. Ispol'zovaniye vozmozhnostey kompleksa radiomonitoringa «Kassandra» dlya obnaruzheniya sovremennykh tekhnicheskikh sredstv s peredachey informatsii po radiokanalu// Bezopasnost' informatsionnogo prostranstva. Sbornik trudov KHVIII Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uche-nykh. 2019. S. 124-127

5. Ivanov-Tsyganov, A. I. Elektrotekhnicheskiye ustroystva radiosi-stem / A.I. Ivanov-Tsyganov. – M.: Vysshaya shkola, 2019. – 490 c.

6. Fatkullin A.R., Mikhaylova U.V. Sovremennyye sredstva radio-razvedki// Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazova-niya. Tezisy dokladov 79-y mezhdunarodnoy nauchno-tekhnicheskoy konferen-tsii. 2021. S. 402.

БАРАНКОВА Инна Ильинична, доктор технических наук, доцент, заведующая кафедрой информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Associate Professor, Head of the Department of Computer Science and Information Security of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru

КУЗЬМИНА Ульяна Владимировна, кандидат технических наук, доцент по специальности «Информационная безопасность автоматизированных систем», доцент кафедры информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: u.mihaylova@magtu.ru

KUZMINA Ulyana Vladimirovna, Candidate of Technical Sciences, Associate Professor in the specialty «Information Security of automated systems», Associate Professor of the Department of Computer Science and Information Security of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: u.mihaylova@magtu.ru

ФЕДОРОВА Анастасия Романовна, студент федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: anastasia.43ag@yandex.ru

FEDOROVA Anastasia Romanovna, student of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: anastasia.43ag@yandex.ru

КУЛЬЕВИЧ Юрий Ярославович, студент федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ykulevich01@mail.ru

KULEVICH Yuri Yaroslavovich, student of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: ykulevich01@mail.ru

КАЗАКОВ Олег Алексеевич, студент федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: oleg.kazakov.2013@bk.ru

KAZAKOV Oleg Alekseevich, student of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: oleg.kazakov.2013@bk.ru

УДК 004.056.5 Вестник УрФО № 1(51) / 2024, с. 14–21

Кротова Е.Л., Субботина Ю.В., Ермаков Д.Г., Тишин К.Л.

DOI: 10.14529/secur240102

ОСОБЕННОСТИ РАЗРАБОТКИ И ВНЕДРЕНИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Работа посвящена сравнительному анализу традиционного и электронного голосования. Определены основные проблемы, возникающие при внедрении электронного формата голосования, определенные Федеральным законом от 12.06.2002 N 67-ФЗ (ред. От 31.-7.2020) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации». На базе сформулированных критериев, следование которым свидетельствовало бы об улучшении решений и несоблюдение которых, на данный момент, является их слабой стороной. Сформулированы требования, которые предъявляются к любой системе голосования. Предложен вариант обхода существующих недостатков разрабатываемых и внедряемых систем электронного голосования.

Ключевые слова: *протокол электронного голосования, криптография, блокчейн.*

Krotova E.L., Subbotina Yu.V., Ermakov D.G., Tishin K.L.

PECULIARITIES OF DEVELOPMENT AND IMPLEMENTATION OF THE ELECTRONIC VOTING SYSTEM

The work is devoted to a comparative analysis of traditional and electronic voting. The main problems arising from the implementation of the electronic voting format, defined by the Federal Law of June 12, 2002 N 67-FZ (as amended on July 31, 2020) "On the basic guarantees of electoral rights and the right to participate in a referendum of citizens of the Russian Federation," are identified. Based on the formulated criteria, adherence to which would indicate an improvement in decisions and non-compliance with which, at the moment, is their weakness, the requirements that apply to any voting system are formulated. An option is proposed to bypass the existing shortcomings of electronic voting systems being developed and implemented.

Keywords: *electronic voting protocol, cryptography, blockchain.*

Голосование – это форма принятия решения, при которой общее мнение голосующей группы формулируется путем подсчета голосов ее членов.

Рассмотрим традиционную систему голосования (бумажную) и электронную систему голосования.

Традиционная аналоговая система голосования подразумевает под собой голосование с урной и бумажными бюллетенями на традиционном участке, где избиратель приходит на участок, предъявляет документ, который удостоверяет личность избирателя. Далее член избирательной комиссии при наличии избирателя в списке выдает ему бюллетень под роспись. Затем, избиратель проходит в индивидуальную кабину для голосования, где заполняет бюллетень и после опускает его в урну.

Электронная голосование – форма принятия решения, с помощью традиционного голосования, но с применением специальных электронных средств голосования и технических электронных средств, с помощью которых подсчитываются голоса и оглашаются результаты [1-3]. Стоит понимать, что, говоря о технических электронных средствах, мы в том числе подразумеваем под этим и сканеры избирательных бюллетеней. В менее обширном понимании электронным голосованием считается голосование с использованием машин прямой записи результатов без использования бумажных бюллетеней. Это новая концепция основана на криптографии. Система поддерживает полнофункциональное голосование онлайн на любых устройствах. Результаты опроса рассчитываются автоматически и анонимно.

Сравним традиционное голосование с электронным, используя наиболее важные требования, которые предъявляются к любой системе голосования.

Таблица 1

Сравнение видов голосования по заданным критериям

	Скорость обработки голосов	Экономия времени заполнения бюллетеней	Ход голосования в реальном времени	Эффективная масштабируемость
Бумажное голосование	ниже	ниже	Не доступно	ниже
Электронное голосование	выше	выше	доступно	выше

Выводы, которые мы можем сделать исходя из таблицы сравнения видов голосования по заданным критериям:

– электронное голосование более экономичная система;

– электронное голосование более прозрачная система;

– электронное голосование более объективная система.

Также важно отметить, что традиционная (бумажная) форма требует личного присутствия при процедуре голосования и больших финансовых затрат, если речь идет о выборах государственного масштаба. Электронное голосование, в свою очередь, позволяет сократить время избирателей на посещение избирательного участка и время подсчета голосов.

Не смотря на положительные стороны электронного голосования, система имеет большой риск фальсификации и компрометации результатов подсчета, так как может быть взломана третьими лицами, или администратором, который имеет доступ к машине, производящей подсчет голосов, с целью их изменения.

В связи с этим, стоит обратить внимание на основные требования, которые предъявляются к любой системе голосования, как для традиционного, так и для электронного формата голосования, определенные Федеральным законом от 12.06.2002 N 67-ФЗ (ред. От 31.-7.2020) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» и включают в себя [4, 5]:

1. Голосование на выборах должно быть тайным и исключать возможность контроля за волеизъявлением в любом виде.

2. Иметь возможность голосования могут только те лица, которые обладают активным избирательным правом на этом голосовании.

3. Не мало важно соблюдать принцип «один избиратель – один голос». Иными словами, «двойное» голосование не допускается.

4. Для тех, кто голосует, т.е. для избирате-

лей, а также для наблюдателей процесс голосования должен быть открытым и гласным.

5. Важно обозначить, что возможность неизменности поданного голоса также должна обеспечиваться.

6. Также возможность подсчитать промежуточные итоги голосования до его завершения должна гарантировано отсутствовать.

Для того, чтобы снизить риски нарушения требований к системам электронного голосования, было разработано большое множество протоколов связанных с конфиденциальностью бюллетеней, индивидуальной проверкой, надежностью, доступностью и т.д., где реализованы различные технологии, в том числе технологии «слепая подпись», «гомоморфное шифрование», «кольцевая подпись», «Mix networks», «доказательство с нулевым разглашением» и т.п. [6-10].

Анализируя практику применения сканеров избирательных бюллетеней (СИБ), констатируем два основных недостатка:

– отсутствует решение по защите от одновременного принятия более одного бюллетеня (голоса);

– нестабильность работы оптической схемы, которая распознает информацию о голосовании.

Существование этих недостатков потребовало разработки новой модели электронного голосования.

Поэтому, в 2001 году был разработан первый комплекс обработки избирательных бюллетеней (КОИБ), куда был встроен компьютер, который обеспечивал работу устройства и сохранял итоги голосования на дискету. Именно тогда, распечатываемые КОИБ итоги голосования стали иметь юридическую силу. Помимо того, что был исключен ручной подсчет бюллетеней, что существенно увеличило скорость получения результатов голосования, к тому же повысилось доверие избирателей к результатам. Эта модель просуществовала в период с 2004 по 2011 гг., а затем усовершенствовалась и служила эффективным инструментом для голосования вплоть до 2020 года [11-15]. Также, при анализе практики применения КОИБ, констатируем два основных недостатка:

– сложность в обслуживании и высокая стоимость машин;

– невозможность проверки корректности работы оборудования для голосования независимыми экспертами.

Попытки исследователей достигнуть поставленных целей при поиске наиболее эффективного способа голосования и подсчета голосов привели их к использованию технологии blockchain. С 2015 года исследователи США были заинтересованы в разработке и апробации блокчейн-голосования на платформе с приложением Web 3.0. Такое голосование предусматривало интернет-регистрацию избирателя и голосование с помощью ID-голосования и избирательного бюллетеня с QR-кодами. В том же году, исследователи З. Жао и Т. Чан представили способ голосования с использованием технологии blockchain и zk-SNARK, которые обеспечивали соблюдения свойств конфиденциальности, своевременной проверяемости и неизменяемости. В 2016 году П. С. Джейсон, и К. Ючи предложили протокол с использованием карт Bitcoin и слепой подписи. Но, система голосования, основанная на платформе Bitcoin, имела недостаточную пропускную способность сети, а сама криптовалюта имела большую популярность, что приводило к низкой скорости обработки транзакций и повышению стоимости комиссий [16-18].

Анализ мирового опыта автоматизации голосования вместе с существующими решениями и их недостатками, позволяют нам выявить схожие и особенные характеристики/критерии, следование которым свидетельствовало бы об улучшении решений и несоблюдение которых, на данный момент, является их слабой стороной:

– критерий достаточной прозрачности процесса голосования. Подсчет голосов должен осуществляться корректным образом без возможности его фальсификации.

– критерий достаточной отказоустойчивости системы голосования. Недостаточность отказоустойчивости системы, может привести к тому, что если машина, занимающаяся обработкой голосов, выйдет из строя, то это приведет к нарушению всего процесса голосования.

– критерий надежности системы голосования. Принцип построения архитектуры системы голосования должен обеспечивать отсутствие единой «точки отказа» этой системы.

На основе критериев, которые мы сформулировали и требований, которые предъявляются к любой системе голосования, определенные Федеральным законом от 12.06.2002 N 67-ФЗ (ред. От 31.07.2020) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан

Российской Федерации» все чаще к рассмотрению предлагается протокол на основе технологии blockchain, который должен их удовлетворить [5].

Технология блокчейн основной базовый компонент большинства криптовалютных сетей, так как при записи и передачи данных использует прозрачный, надежный и доказуемый метод. Являясь децентрализованной, распределённой и общедоступной цифровой бухгалтерской книгой (DLT), технология отвечает за ведение постоянной записи цепочки блоков ранее всех подтвержденных транзакций. То есть, обобщая сказанное выше, мы можем сказать, что блокчейн – цепочка блоков, каждый из которых содержит в себе информацию о серии транзакций, которые были проведены в течении определенного промежутка времени. Термин «транзакция» представляет собой вычислительный процесс, который происходит в цепочке блокчейна или, иными словами, единицы данных, которые содержат сведения о транзакции и отметке времени [6-8]. Транзакции блокчейна происходят в одноранговой сети глобально распределённых компьютеров (рис. 1) peer-to-peer (P2P), где было введено свойство отсутствие доверия, которое позволяет проверять и хранить все транзакционные данные в общедоступном блокчейне. Система без доверия означает, что пользователям не нужно знать или доверять друг другу или третьей стороне, чтобы система функционировала, так как нет единого субъекта, имеющего контроль над всей системой. То есть, каждый компьютер (узел) сети поддерживает копию блокчейна, тем самым обеспечивает ей безопасность и функционирование.

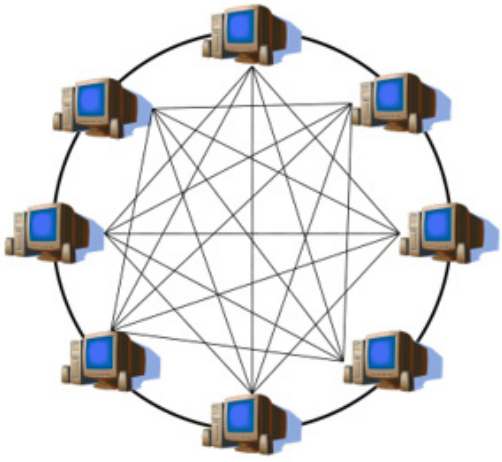


Рис. 1. Схематичное представление одноранговой сети P2P

Структура блока технологии состоит из четырех строк:

– первая строка адрес, который является публичным ключом. Он генерируется ассиметричным алгоритмом шифрования с помощью приватного ключа, который придумывает пользователь;

– вторая строка включает в себя дату и время того момента, когда был создан блок.

– третья строка содержит в себе хэш, который вычисляется с помощью хэш-функции (например, SHA256) от адреса предыдущего и суммы всех транзакций текущего блоков. Так как при вычислении хэш использует адреса предыдущего и текущего блока, его называют связующим. Именно он объединяет блоки в одну цепь;

– четвертая строка содержит само сообщение, т.е. информацию (сведения) о транзакциях. Эту строку также называют телом блока (рис. 2).

Рис. 2. Структура блока технологии blockchain

Предыдущий и последующий блоки связываются с помощью идентификатора блока (рис. 3), что позволяет сохранить надежность этой системы.

То есть, если мы не верим, что система надежна и решили внести изменения в данные одного из блоков в целях ее компрометации, то мы заметим, что идентификатор всех последующих блоков также изменится (рис. 4) и наша корректировка данных будет обнаружена и признана невалидной.

При анализе существующих систем электронного голосования в РФ с помощью применения СИБ были выявлены следующие недостатки:

– отсутствует решение по защите от одно-

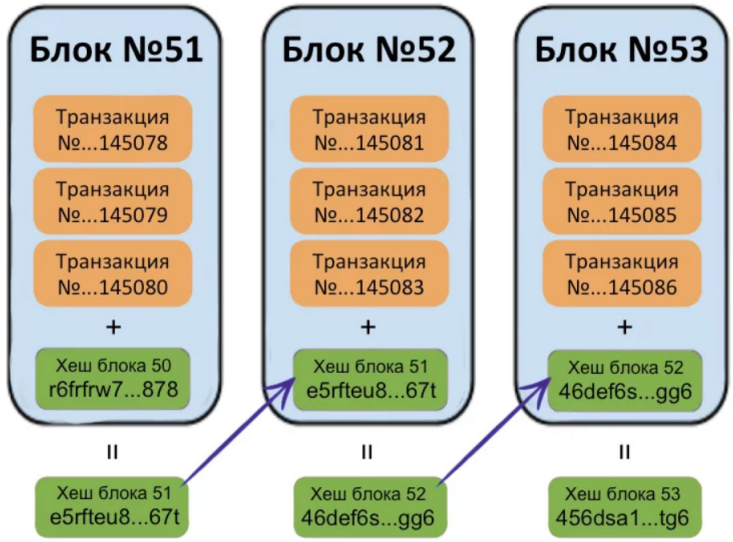


Рис. 3. Связь блоков между собой в технологии blockchain

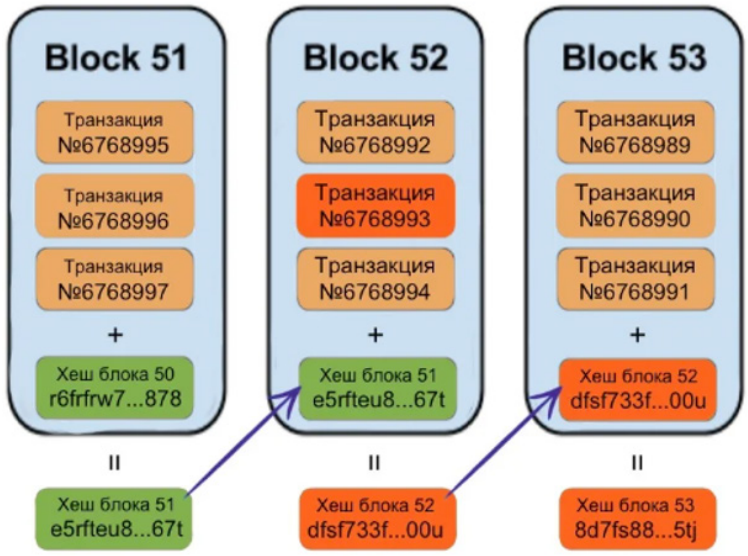


Рис. 4. Иллюстрация попытки изменения данных в блоке

временного принятия более одного бюллетеня (голоса);

– нестабильность работы оптической схемы, которая распознает информацию о голосовании.

Также, при анализе СЭГ в РФ с помощью применения КОИБ в качестве недостатков мы сформулировали следующее:

– сложность в обслуживании и высокая стоимость машин;

– невозможность проверки корректности работы оборудования для голосования независимыми экспертами.

В ходе аналитической работы был выявлен ряд целей, к которым стремиться любая система электронного голосования:

– повышение скорости подсчета голосов;

– сокращение роли человека в подсчете голосов;

– повышение доверия к результатам голосования.

Исходя из этого, была сформулирована следующая проблема: принимая во внимание обстоятельства последних двух лет и несоответствие им существующих решений избирательной системы, возникает необходимость создания безопасного и защищенного от фальсификаций метода электронного голосования на основе прогрессивных технологий.

Литература

1. Российский центр обучения избирательным технологиям при ЦИК.

2. России [Электронный ресурс]. URL: http://www.rcoit.ru/main/tech/tech/17065/.

3. Cyberleninka.ru / Электронное голосование: «За» и «Против» [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/elektronnoe-golosovanie-za-i-protiv.

4. Сапожников Д.В., Полякова Е.Н. Правовое обеспечение информационной безопасности российских телематических сетей на примере ГАС «Выборы» // Безопасность информационного пространства: сб. материалов XV Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых. Курган: Курган. гос. ун-т. 2016. С. 62–65.

5. Худолей Д. М., Худолей К. М. Электронное голосование в России и за рубежом // Вестник Пермского университета. Юридические науки. 2022. Вып. 57. С. 476–503. DOI: 10.17072/1995-4190-2022-57-476-503.

6. Lilleker D.G. Koc-Michalska K. What Drives Political Participation? Motivations and Mobilization in a Digital Age // Political Communication. 2016. Vol. 33. P. 1–23. DOI: 10.1080/10584609.2016.1225235.

7. Володенков С.В., Артамонова Ю.Д. Информационные капсулы как структурный компонент современной политической интернет-коммуникации // Вестник Томского государственного университета. Философия. Социология. Политология. 2020. № 53. С. 188–196. DOI: 10.17223/1998863X/53/20.

8. Прасти Н. Блокчейн. Разработка приложений, // Н. Прасти, В.С. Яценков. — СПб.: БХВ-Петербург, 2018. – 256 с.

9. Равал С. Децентрализованные приложения. Технология Blockchain в действии, // С. Равал. — СПб.: Питер, - 2017. - 192 с.

10. Тапскотт Д., Тапскотт А. Технология блокчейн - то, что движет финансовой революцией сегодня, // Д. Тапскотт, А. Тапскотт. — М.: Эксмо, 2017. – 448 с.

11. Насколько надежно электронное голосование [Электронный ресурс]. – Режим доступа: https://www.svoboda.org/a/269300.html, свободный.

12. Норвегия официально отказалась от электронного голосования на выборах: оно контрпродуктивно [Электронный ресурс]. – Режим доступа: http://www.mk.ru/politics/world/2014/06/30/norvegiya-otkazalasv-politike-ot-elektronnogo-golosovaniya.html, свободный.

13. Block The Vote: Could Blockchain Technology Cybersecure Elections? [Электронный ресурс]. – Режим доступа: http://www.forbes.com/sites/realspin/2016/08/30/block-the-votecouldblockchain-technology-cybersecure-elections, свободный.

14. California: The Top to Bottom Review [Электронный ресурс]. – Режим доступа: http://www.votetrustusa.org/index.php?option=com_content&task=view&id =2554&Itemid=113, свободный.

15. IGS Votomatic Prototype Goes to the Smithsonian [Электронный ресурс]. – Режим доступа: https://web.archive.org/web/20070713201451/http://www.igs.berkeley.edu/publications/par/winter2001/votomatic.htm, свободный.

16. Kiwi. Bitcoin testnet sandbox. [Электронный ресурс]. – Режим доступа: https://testnet.manu.backend.hamburg/faucet, свободный.

17. NSW election result could be challenged over iVote security flaw [Электронный ресурс]. – Режим доступа: https://www.theguardian.com/australia-news/2015/mar/23/nsw-electionresult-could-be-challenged-over-ivote-security-flaw, свободный.

18. Peer-to-peer [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf, свободный.

References

1. Rossiyskiy tsentr obucheniya izbiratel'nym tekhnologiyam pri TSIK.

2. Rossii [Elektronnyy resurs]. URL: http://www.rcoit.ru/main/tech/tech/17065/.

3. Cyberleninka.ru / Elektronnoye golosovaniye: «Za» i «Protiv» [Elektronnyy resurs]. URL: https://cyberleninka.ru/article/v/elektronnoe-golosovanie-za-i-protiv.

4. Sapozhnikov D.V., Polyakova Ye.N. Pravovoye obespecheniye informatsionnoy bezopasnosti rossiyskikh telematicheskikh setey na primere GAS «Vybory» // Bezopasnost' informatsionnogo prostranstva: sb. materialov XV Vseros. nauch.-prakt. konf. studentov, aspirantov i molodykh uchenykh. Kurgan: Kurgan. gos. un-t. 2016. S. 62–65.

5. Khudoley D. M., Khudoley K. M. Elektronnoye golosovaniye v Rossii i za rubezhom // Vestnik Permskogo universiteta. Yuridicheskiye nauki. 2022. Vyp. 57. C. 476–503. DOI: 10.17072/1995-4190-2022-57-476-503.

6. Lilleker D.G. Koc-Michalska K. What Drives Political Participation? Motivations and Mobilization in a Digital Age // Political Communication. 2016. Vol. 33. P. 1-23. DOI: 10.1080/10584609.2016.1225235.

7. Volodenkov S.V., Artamonova YU.D. Informatsionnyye kapsuly kak strukturnyy komponent sovremennoy politicheskoy internet-kommunikatsii // Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya. 2020. № 53. S. 188–196. DOI: 10.17223/1998863X/53/20.

8. Prasti N. Blokcheyn. Razrabotka prilozheniy, // N. Prasti, V.S. Yatsenkov. — SPb.: BKHV-Peterburg, 2018. – 256 s.

9. Raval S. Detsentralizovannyye prilozheniya. Tekhnologiya Blockchain v deystvii, // S. Raval. — SPb.: Piter, - 2017. - 192 s.

10. Tapskott D., Tapskott A. Tekhnologiya blokcheyn - to, chto dvizhet finansovoy revolyutsiyey segodnya, // D. Tapskott, A. Tapskott. — M.: Eksmo, 2017. – 448 s.

11. Naskol'ko nadezhno elektronnoye golosovaniye [Elektronnyy resurs]. – Rezhim dostupa: https://www.svoboda.org/a/269300.html, svobodnyy.

12. Norvegiya ofitsial'no otkazalas' ot elektronnogo golosovaniya na vyborakh: ono kontrproduktivno [Elektronnyy resurs]. – Rezhim dostupa: http://www.mk.ru/politics/world/2014/06/30/norvegiya-otkazalasv-politike-ot-elektronnogo-golosovaniya.html, svobodnyy.

13. Block The Vote: Could Blockchain Technology Cybersecure Elections? [Electronic resource]. - Access mode: http://www.forbes.com/sites/realspin/2016/08/30/block-the-votecouldblockchain-technology-cybersecure-elections, free.

14. California: The Top to Bottom Review [Electronic resource]. - Access mode: http://www.votetrustusa.org/index.php?option=com_content&task=view&id =2554&Itemid=113, free.

15. IGS Votomatic Prototype Goes to the Smithsonian [Electronic resource]. - Access mode: https://web.archive.org/web/20070713201451/http://www.igs.berkeley.edu/publications/par/winter2001/votomatic.htm, free.

16. Kiwi. Bitcoin testnet sandbox. [Electronic resource]. - Access mode: https://testnet.manu.backend.hamburg/faucet, free.

17. NSW election result could be challenged over iVote security flaw [Electronic resource]. - Access mode: https://www.theguardian.com/australia-news/2015/mar/23/nsw-electionresult-could-be-challenged-over-ivote-security-flaw, free.

18. Peer-to-peer [Electronic resource]. - Access mode: https://bitcoin.org/bitcoin.pdf, free.

КРОТОВА Елена Львовна, кандидат физико-математических наук, доцент кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

KROTOVA Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Territory, Perm, Komsomolsky prospect, 29. E-mail: lenkakrotova@yandex.ru

СУББОТИНА Юлия Владимировна, ведущий инженер кафедры «Высшая математика», аспирант кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: yulyia.urazbaeva@mail.ru

SUBBOTINA Yulia Vladimirovna, leading engineer of the Department of Higher Mathematics, postgraduate student of the Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Territory, Perm, Komsomolsky prospect, 29. E-mail: yulyia.urazbaeva@mail.ru

ЕРМАКОВ Дмитрий Германович, кандидат физико-математических наук, старший научный сотрудник отдела дифференциальных уравнений Лаборатории научно-информационных ресурсов, Федеральное государственное бюджетное учреждение науки Институт математики и механики им. Н. Н. Красовского Уральского отделения Российской академии наук (ИММ УрО РАН). 620108, г. Екатеринбург, ул. Софьи Ковалевской, д. 16.; кандидат физико-математических

наук, доцент, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, Екатеринбург, ул. Мира, 19. E-mail: Dmitry.Ermakov@mail.ru

YERMAKOV Dmitry Germanovich, PhD in Physics and Mathematics, Senior Researcher, Differential Equations Department, Laboratory of Scientific and Information Resources, Federal State Budgetary Institution of Science Institute of Mathematics and Mechanics named after N. N. Krasovsky Ural Branch of the Russian Academy of Sciences (Institute of Mathematics and Mechanics of the Ural Academy of Sciences). N. N. Krasovsky Institute of Mathematics and Mechanics of the Ural Branch of the Russian Academy of Sciences (IMM Ural Branch of the Russian Academy of Sciences), 620108, Ekaterinburg, Sofya Kovalevskaya St., 16.; candidate of Physical and Mathematical Sciences, Associate Professor, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: Dmitry.Ermakov@mail.ru

ТИШИН Константин Львович, аспирант кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: konstantinlvovich777@gmail.com

TISHIN Konstantin Lvovich, postgraduate student, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Territory, Perm, Komsomolsky prospect, 29. E-mail: konstantinlvovich777@gmail.com

УДК 004.056.5 Вестник УрФО № 1(51) / 2024, с. 22–29

Карелова О.Л., Лисин Г.А.

DOI: 10.14529/secur240103

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕЖСЕТЕВЫХ ЭКРАНОВ НОВОГО ПОКОЛЕНИЯ

В статье проведен сравнительный анализ межсетевых экранов нового поколения, реализованных в виде программно-аппаратных комплексов. Рассмотрены представленные на отечественном рынке варианты таких средств защиты информации, а также отобраны критерии их сравнения.

Для нахождения оптимального решения из имеющихся альтернатив использован метод анализа иерархий, учитывающий субъективную важность выбранных критериев.

В ходе исследования продемонстрирована эффективность данного метода в ситуациях, когда сравнение ведется по совокупности критериев и нет явного лидера по каждому из них.

По результатам анализа предложено воспользоваться многоступенчатым подходом для сравнения межсетевых экранов нового поколения. Прежде всего необходимо выбрать желаемую реализацию данных средств защиты (в виде программного обеспечения или программно-аппаратного комплекса) и определить подлежащую защите информации. На основании этих сведений следует отобрать необходимые критерии, по которым ведется сравнение, добавив в качестве одного из них полноту программного функционала, после чего целесообразно обратиться к методу анализа иерархий.

Ключевые слова: *информационная безопасность, средства защиты информации, межсетевой экран, UTM, NGFW, метод анализа иерархий, программно-аппаратный комплекс.*

Karelova O.L., Lisin G.A.

COMPARATIVE ANALYSIS OF NEW GENERATION FIREWALLS

The article provides a comparative analysis of new generation firewalls implemented in the form of software and hardware complexes. The variants of such information protection tools presented on the domestic market were reviewed, and criteria for their comparison were selected.

To find the most optimal solution from the available alternatives, the hierarchy analysis method was applied, taking into account the subjective importance of the selected criteria.

The study demonstrated the effectiveness of this method in situations where the comparison is based on a set of criteria and there is no clear leader for each of them.

Based on the results of the analysis, it was proposed to use a multi-step approach to compare new generation firewalls. First of all, it is necessary to choose the desired implementation

of these security measures (in the form of software or hardware and software complex) and determine the information to be protected. Based on this information, it is necessary to select the necessary criteria for comparison, adding the completeness of the software functionality to one of them, after which it is advisable to turn to the analytic hierarchy process.

Keywords: *information security, information security tools, firewall, UTM, NGFW, analytic hierarchy process, hardware and software complex.*

Введение

В настоящее время, как показывают недавние исследования [1], основную угрозу для бесперебойного функционирования корпоративных сетей организаций представляют вредоносные программы и направленные атаки, приводящие к сбоям в работе информационной системы компаний вне зависимости от формы их собственности и размера. Чтобы обезопасить внутренние ресурсы предприятий, ИТ-специалисты прибегают к различным организационным и техническим мерам. Одной из таких мер является внедрение различных средств программно-аппаратной защиты: систем защиты информации от несанкционированного доступа, антивирусных программ, межсетевых экранов, систем обнаружения и предотвращения вторжений, средств криптографической защиты информации и некоторых других [2].

В данной статье рассмотрено одно из таких средств – межсетевые экраны (файрволы, брандмауэры). В классическом понимании они представляют собой комплекс, предназначенный для защиты сети от различных видов угроз и атак путем контроля и фильтрации проходящего через него сетевого трафика. Файрволы работают на основе ряда правил и политик безопасности, которые определяют, в зависимости от адреса отправителя, используемых сетевых сервисов, портов и протоколов, какие пакеты могут свободно передаваться по сети, а какие должны блокироваться [3]. Кроме того, межсетевые экраны могут выполнять функцию NAT (Network Address Translation), сохраняя количество общедоступных адресов, используемых в компании, а также позволяя более строго контролировать доступ к ресурсам как с внутренней, так и с внешней стороны брандмауэра.

Однако помимо классических файрволов существуют их более усовершенствованные аналоги – универсальные шлюзы безопасности (UTM – Unified Threat Management) и межсетевые экраны нового поколения (NGFW – Next Generation Firewall). Строго говоря, между ними есть небольшая разница: несмотря на то, что они выполняют одни и те же функции, системы NGFW являются многопоточными, в то время как UTM-решения работают с одним потоком, что можно расценивать как их недостаток [4]. На практике же для многих компаний эта разница не является существенной, поэтому при принятии решения о приобретении данных средств защиты их рассматривают совместно, а выбор между ними осуществляется по принципу соотношения желаемой организацией функциональности к оптимальной для нее, с точки зрения пользователя, производительности.

В общем случае класс UTM/NGFW-решений сочетает в себе как базовые возможности привычного многим файрвола, так и некоторый дополнительный функционал: построение защищенных каналов связи (VPN), антивирусная фильтрация, обнаружение и предотвращение вторжений, инспектирование SSL трафика, контроль приложений, контент-фильтрация [5], благодаря которому снижается количество компонентов, необходимое для обеспечения информационной безопасности в целом. Наглядно сравнение функционала классических межсетевых экранов и решений следующего поколения представлено в табл. 1.

Так как межсетевые экраны нового поколения обладают рядом преимуществ по сравнению с классическими файрволами, многие компании, особенно крупные, отдают предпочтение именно более современным вариантам.

Отбор альтернатив

На сегодняшний день класс UTM/NGFW-решений представлен в виде программных и программно-аппаратных комплексов. Однако для того, чтобы не зависеть от технических характеристик компьютера или сервера, на которые устанавливается защитное программное обеспечение, для данного исследования был выбран исключительно второй вариант реализации межсетевых экранов нового поколения. Кроме того, анализ был ограничен крупными корпоративными решения-

Таблица 1

Сравнение файрволов с UTM/NGFW-решениями

Характеристика	Классический файрвол	Межсетевые экраны нового поколения
Контроль пакетов	✓	✓
Фильтрация трафика	✓	✓
NAT	✓	✓
VPN	×	✓
Антивирус	×	✓
Система обнаружения и предотвращения вторжений	×	✓
Инспектирование SSL трафика	×	✓
Контроль приложений	×	✓
Контент-фильтрация	×	✓
Глубокая инспекция пакетов	×	✓

ми с максимальной производительностью, рассчитанными на наибольшее число пользователей, так как малые и средние предприятия прибегают зачастую к классическим файрволам ввиду низкой стоимости последних.

В результате были отобраны и рассмотрены следующие альтернативы современных шлюзов безопасности:

A1 – Континент 4 IPC-R3000 от ООО «Код Безопасности» – российский межсетевой экран, обеспечивающий комплексную защиту сети. Данное решение гарантирует стабильно высокую пропускную способность и фиксированное время обработки данных вне зависимости от интенсивности трафика и количества правил. Имеет действующий сертификат ФСТЭК России [6].

A2 – UserGate F8000 от ООО «Юзергейт» – еще один отечественный межсетевой экран нового поколения, который работает на мощных платформах и процессорах, обеспечивая эффективность выполнения множества защитных функций даже для большого числа пользователей. В его состав входят все необходимые инструменты для защиты корпоративной сети от современных видов угроз и атак. Кроме того, он также сертифицирован ФСТЭК России [7].

A3 – ViPNet xFirewall 5 xF5000 Q2 от АО «ИнфоТеКС» – также российский современный шлюз безопасности, сочетающий в себе функции классического межсетевого экрана с расширенными функциями анализа и фильтрации трафика. Данное средство защиты информации также позволяет создать гранулированную политику безопасности на основе учетных записей пользователей. Является сертифицированным ФСТЭК России средством защиты [8, 9].

A4 – Traffic Inspector Next Generation L1500+-AQ от ООО «СМАРТ-СОФТ» – отечественный универсальный шлюз безопасности, который может являться единственным самодостаточным средством защиты сети организации. Одним из его главных достоинств является простота настройки, благодаря которой данное решение может начать полноценно функционировать за достаточно короткое время. Имеет сертификат соответствия ФСТЭК России [10].

A5 – Zyxel USG FLEX 700H от тайваньской компании Zyxel – данный универсальный шлюз безопасности обеспечивает достаточно хорошую производительность в UTM режиме, а также многоуровневую защиту сетевой инфраструктуры и подключенных пользователей. Такая максимальная производительность достигается за счет многоядерного процессора нового поколения, технологии Fastpath, а также новой операционной системы [11].

A6 – Dionis DPS-7000 от ООО «Фактор-ТС» – российский программно-аппаратный комплекс, выполняющий различные функции и позволяющий решать задачи разной степени сложности: от предоставления безопасного доступа в Интернет сотрудникам компании до объединения множества филиалов организации в единую защищенную сеть. Его преимуществами выступают высокий уровень производительности и надежность ядра сети организации. Отличительной особенностью данного решения является наличие действующих сертификатов соответствия не только ФСТЭК России, но и ФСБ России [12].

A7 – Ideco EX от ООО «Айдеко» – передовая отечественная модель, разработанная специально для крупных корпораций с количеством пользователей больше 3000. Как и другие представленные на российском рынке аналоги, данная платформа защищает сеть компании от внутренних и внешних угроз, обеспечивает анализ и фильтрацию трафика, позволяет наращивать ресурсы вычислительной системы, а также выполняет иные функции безопасности. Данное средство защиты также сертифицировано ФСТЭК России [13].

Подбор критериев

Следующий этап исследования посвящен выявлению присущих всем отобранным UTM/NGFW-решениям характеристик, которые являются наиболее важными с точки зрения производительности и информационной безопасности.

K1 – полнота программного функционала. Это один из наиболее существенных параметров при сравнении вышеупомянутых альтернатив. Так как межсетевые экраны нового поколения характеризуются разнообразными свойствами, среди них были выделены десять наиболее сопоставимых опций, являющихся ключевыми для данных решений. Все альтернативы были проанализированы на предмет наличия («1») или отсутствия («0») отобранных функций, после чего был рассчитан процент ненулевых характеристик относительно общего их числа – это и есть искомое значение K1 по каждой из альтернатив. Наглядно данное сравнение UTM/NGFW-решений представлено в табл. 2.

Таблица 2

Сравнение альтернатив по программным характеристикам

Характеристика	A1	A2	A3	A4	A5	A6	A7
Контроль пакетов и фильтрация трафика	1	1	1	1	1	1	1
VPN	1	0	0	1	1	1	1
Антивирус	0	1	1	1	1	1	1
Глубокая инспекция пакетов	1	1	1	1	0	0	0
Система обнаружения и предотвращения вторжений	1	1	1	1	1	1	1
Контент-фильтрация	1	1	1	1	1	0	1
Контроль приложений	1	1	1	1	1	0	1
Инспектирование SSL трафика	1	1	1	1	1	1	1
Отказоустойчивость	1	1	1	1	0	1	1
Двухфакторная аутентификация	0	1	0	1	1	0	1
Полнота программного функционала, %	80	90	80	100	80	60	90

Остальные критерии характеризуют производительность и масштабируемость межсетевых экранов нового поколения.

K2 – производительность в режиме межсетевого экрана. Данный параметр определяет скорость и эффективность обработки сетевого трафика и потому является достаточно важным при выборе UTM/NGFW-решения.

K3 – производительность в комбинированном режиме. Это очень важный критерий, так как от его величины зависит возможность совмещения высоких сетевых нагрузок с обеспечением достаточного уровня безопасности.

K4 – максимальное рекомендуемое количество пользователей. Данный критерий имеет немаловажное значение для крупных компаний, так как в случае увеличения числа их сотрудников требуется масштабируемость такого сетевого решения.

K5 – удельная производительность при максимальной нагрузке в комбинированном режиме. Данный критерий получается как частное от деления K3 на K4 и вводится для определения достаточности заявленной наибольшей производительности при максимальной нагрузке на сеть.

Набор данных

Для дальнейшего анализа необходимо свести воедино как значения критерия K1, рассчитанные в предыдущем разделе, так и значения других критериев, взятые из паспортов программно-аппаратных комплексов соответствующих производителей. Полученный набор данных отражен в табл. 3.

Данные значения будут использованы в

Таблица 3

Значения альтернатив по критериям

	К1, %	К2, Гбит/с	К3, Гбит/с	К4, чел.	К5, Мбит/с
А1	80	50	8	3 000	2,67
А2	90	60	8	10 000	0,8
А3	80	45	1,531	6 000	0,26
А4	100	25	1,2	1 500	0,8
А5	80	15	4	4000	1
А6	60	90	8	2000	4
А7	90	42	5	3000	1,67

следующем разделе для проведения непосредственно сравнительного анализа.

Сравнение методом анализа иерархий

В проведенных ранее исследованиях [14] уже был проведен анализ межсетевых экранов нового поколения методом простой ранжировки по нескольким критериям, однако в данной статье для целей сравнения использовался метод анализа иерархий.

В рамках этого метода прежде всего нужно проранжировать отобранные критерии в соответствии с субъективной оценкой их важности [15]. В результате критерии К1-К5 были упорядочены так, как показано в табл. 4, после чего с учетом этих значений был получен вектор приоритетов для критериев ($\overline{a}$).

Следующим этапом данного метода является ранжирование альтернатив по выбран-

Таблица 4

Ранжирование критериев

Критерий	К1	К2	К3	К4	К5
Ранг	4	2	1	5	3
$\overline{a}$	0,10551249	0,2713178	0,3875969	0,0590009	0,17657192

ным критериям на основании числовых параметров, приведенных в таблице 3. Результат представлен в таблице 5.

Приведенные выше данные позволяют получить векторы приоритетов для альтернатив ($\overline{b_i}$) по каждому из пяти критериев, что в дальнейшем даст возможность перейти уже к заключительному этапу исследования, по результатам которого будет выявлено наиболее оптимальное решение.

Результаты исследования

Все полученные на предыдущем этапе анализа значения векторов приоритетов $\overline{a}$, $\overline{b_1}$, $\overline{b_2}$, $\overline{b_3}$, $\overline{b_4}$ и $\overline{b_5}$ сводятся в итоговую таблицу, на основании которой определяются искомые приоритеты альтернатив, что наглядно показано в таблице 6.

Данные итоговой таблицы позволяют окончательно проранжировать выбранные для анализа решения следующим образом:

1. Dionis DPS-7000 (А6);
2. UserGate F8000 (А2);
3. Континент 4 IPC-R3000 (А1);
4. Ideco EX (А7);
5. ViPNet xFirewall 5 xF5000 Q2 (А3);
6. Zyxel USG FLEX 700H (А5);

Таблица 5

Ранжирование альтернатив по критериям

	К1	К2	К3	К4	К5
А1	4	3	1	4	2
А2	2	2	1	1	5
А3	4	4	6	2	7
А4	1	6	7	7	5
А5	4	7	5	3	4
А6	7	1	1	6	1
А7	2	5	4	4	3

Таблица 6

Итоговая таблица

$\bar{a}$	0,10551249	0,2713178	0,3875969	0,0590009	0,17657192	Приоритеты
A1	0,09316335	0,1744857	0,2507642	0,1129243	0,23452822	0,20244015
A2	0,20594004	0,2369332	0,2507642	0,3023758	0,07188385	0,213742
A3	0,09316335	0,12214	0,0434658	0,2295816	0,02775659	0,07826242
A4	0,28243205	0,0490397	0,0251958	0,0281044	0,07188385	0,06722213
A5	0,09316335	0,0285737	0,071217	0,16612	0,11535738	0,07535605
A6	0,02619781	0,3085642	0,2507642	0,0479695	0,30889083	0,2410503
A7	0,20594004	0,0802634	0,1078286	0,1129243	0,16969928	0,12192694

7. Traffic Inspector Next Generation L1500+-AQ (A4).

Таким образом, на основе полученных методом анализа иерархий результатов модель программно-аппаратного межсетевого экрана нового поколения Dionis DPS-7000 является наиболее оптимальным выбором с точки зрения функциональной полноты и аппаратной производительности.

Однако стоит отметить, что представленный в данном исследовании перечень критериев не является исчерпывающим и не учитывает цели внедрения того или иного средства защиты информации. В случае, если целью является защита коммерческой тайны, имеет смысл рассмотреть в качестве одного из критериев критерий стоимости, присвоив ему ранг в соответствии со степенью важности данного критерия для конкретной организации. В тех же случаях, когда речь идет о защите персональных данных, сведений, составляющих государственную тайну, и иной информации, обрабатываемой в информационных или автоматизированных системах определенного уровня защищенности, необходимо в обязательном порядке включить в перечень критериев критерий наличия сертификата ФСТЭК России или ФСБ России, подтверждающим соответствие средств защиты информации предъявляемым к ним требованиям, и присвоить ему наивысший ранг.

Кроме того, необходимо принять во внимание субъективность результатов данного метода принятия решений, несмотря на его структурированность и системность. Это обусловлено особенностью самого метода анализа иерархий, в основе которого лежит отбор и последующее ранжирование необходимых критериев, по которым будет производиться оценка рассматриваемых альтернатив. В большинстве же случаев выбираемые параметры и присваиваемые им ранги зависят исключительно от предпочтений того, кто принимает решение, и потому не существует однозначного способа подбора и упорядочения критериев по степени их важности.

Заключение

Проведенное исследование показывает необходимость в многоступенчатой методике подбора межсетевого экрана нового поколения. Для начала следует определиться с необходимой реализацией данного средства защиты, которое может быть представлено как в виде специализированного программного обеспечения, так и в виде программно-аппаратного комплекса, а также принять решение о том, какая информация подлежит защите. На основании этого должны быть отобраны те критерии, по которым будет вестись сравнение, при этом в случае программно-аппаратных комплексов важно учитывать не только характеристики аппаратной платформы, но и некоторые программные критерии, как, например, полнота программного функционала. На заключительном этапе стоит воспользоваться методом анализа иерархий, который при всей своей зависимости от ранжирования критериев позволяет в случае правильной расстановки приоритетов сделать оптимальный выбор.

Литература

1. Барыбина А.З. Моделирование угроз информационной безопасности сценарным подходом. // Естественно-гуманитарные исследования, 2022. № 4 (42). С. 35–44.

2. Малий Ю.В., Прокушев Я.Е. Концептуальная модель выбора средств программно-аппаратной защиты. // Computational nanotechnology, 2020. № 1. С. 63–71. DOI: 10.33693/2313-223X-2020-7-1-63-71.

3. Орехов А.В., Орехов А.А. Автоматическое обнаружение аномалий сетевого трафика при DDoS-

атаках. // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления, 2023. Том 19. № 2. С. 251–263. DOI: 10.21638/11701/spbu10.2023.210.

4. Баранов А.В., Корепанов П.М., Кузнецов Е.Е. Обеспечение информационной безопасности научного суперкомпьютерного центра. // Программные продукты и системы, 2023. Том 36. № 4. С. 615–631. DOI: 10.15827/0236-235X.142.615-631.

5. Бирюков А.С. Защита информации в компьютерной сети предприятия. // Молодой ученый, 2020. № 15 (305). С. 81–84.

6. Код Безопасности. Континент 4. Доступно по: https://www.securitycode.ru/products/kontinent-4/?tab=models (дата обращения: 04.03.2024).

7. UserGate. UserGate. Доступно по: https://www.usergate.com/ru/products/usergate-f (дата обращения: 04.03.2024).

8. ИнфоТэКС. ViPNet xFirewall 5. Доступно по: https://infotecs.ru/products/vipnet-xfirewall-5/ (дата обращения: 04.03.2024).

9. Родионычева Е.Д., Голубев А.С. Оценка стоимости приобретения программно-аппаратного комплекса для обеспечения информационной безопасности информационных систем в сфере здравоохранения. // Известия высших учебных заведений. Серия «Экономика, финансы и управление производством» [Ивэкофин], 2021. № 3 (49). С. 124-129. DOI: 10.6060/ivecofin.2021493.558.

10. Смарт-Софт. Traffic Inspector Next Generation. Доступно по: https://www.smart-soft.ru/ (дата обращения: 04.03.2024).

11. Zyxel. Zyxel. Доступно по: https://www.zyxel.com/ru/ru/products/next-gen-firewall/usg-flex-firewall-usg-flex-700h/license-and-spec (дата обращения: 04.03.2024).

12. Фактор-ТС. Dionis. Доступно по: https://dps.factor-ts.ru/produkciya/utm-dionis-dps/dionis-dps-5000-6000-7000-series/#anchor2 (дата обращения: 04.03.2024).

13. Ideco. Ideco. Доступно по: https://ideco.ru/apparatnye-resheniya#!/tproduct/596522077-1685701471282 (дата обращения: 04.03.2024).

14. Шаханова М.В., Четверик М.А., Шаханова В.С. Сравнение различных характеристик отечественных файрволов. // Международный журнал информационных технологий и энергоэффективности, 2024. Том 9. № 1 (39). С. 90–95.

15. Саати Т.Л. Принятие решений: Метод анализа иерархий // Пер. с англ. Вачнадзе Р.Г. // – М.: Радио и связь; 1993. – 314 с.

References

1. Barybina A.Z. Modelirovaniye ugroz informatsionnoy bezopas-nosti stsenarnym podkhodom. // Yestestvenno-gumanitarnyye issledovaniya, 2022. № 4 (42). S. 35–44.

2. Maliy YU.V., Prokushev YA.Ye. Kontseptual'naya model' vybora sredstv programmno-apparatnoy zashchity. // Computational nanotechnology, 2020. № 1. S. 63–71. DOI: 10.33693/2313-223X-2020-7-1-63-71.

3. Orekhov A.V., Orekhov A.A. Avtomaticheskoye obnaruzheniye anoma-liy setevogo trafika pri DDoS-atakakh. // Vestnik Sankt-Peterburgskogo universiteta. Prikladnaya matematika. Informatika. Protsessy upravleniya, 2023. Tom 19. № 2. S. 251–263. DOI: 10.21638/11701/spbu10.2023.210.

4. Baranov A.V., Korepanov P.M., Kuznetsov Ye.Ye. Obespecheniye in-formatsionnoy bezopasnosti nauchnogo superkomp'yuternogo tsentra. // Programmnyye produkty i sistemy, 2023. Tom 36. № 4. S. 615–631. DOI: 10.15827/0236-235X.142.615-631.

5. Biryukov A.S. Zashchita informatsii v komp'yuternoy seti pred-priyatiya. // Molodoy uchenyy, 2020. № 15 (305). S. 81–84.

6. Kod Bezopasnosti. Kontinent 4. Dostupno po: https://www.securitycode.ru/products/kontinent-4/?tab=models (data ob-rashcheniya: 04.03.2024).

7. UserGate. UserGate. Available at: https://www.usergate.com/ru/products/usergate-f (accessed 04.03.2024).

8. InfoTeKS. ViPNet xFirewall 5 [Infotecs. ViPNet xFirewall 5]. Available at: https://infotecs.ru/products/vipnet-xfirewall-5/ (accessed 04.03.2024).

9. Rodionycheva Ye.D., Golubev A.S. Otsenka stoimosti priobreteniya programmno-apparatnogo kompleksa dlya obespecheniya informatsionnoy bezopasnosti informatsionnykh sistem v sfere zdravookhraneniya. // Iz-vestiya vysshikh uchebnykh zavedeniy. Seriya «Ekonomika, finansy i upravleniye proizvodstvom» [Ivekofin], 2021. № 3 (49). S. 124-129. DOI: 10.6060/ivecofin.2021493.558.

10. Smart-Soft. Traffic Inspector Next Generation. Available at: https://www.smart-soft.ru/ (accessed 04.03.2024).

11. Zyxel. Zyxel. Available at: https://www.zyxel.com/ru/ru/products/next-gen-firewall/usg-flex-firewall-usg-flex-700h/license-and-spec (accessed 04.03.2024).

12. Faktor-TS. Dionis. Available at: https://dps.factor-ts.ru/produkciya/utm-dionis-dps/dionis-dps-5000-6000-7000-series/#anchor2 (accessed 04.03.2024).

13. Ideco. Ideco. Available at: https://ideco.ru/apparatnye-resheniya#!/tproduct/596522077-1685701471282 (accessed 04.03.2024).

14. Shakhanova M.V., Chetverik M.A., Shakhanova V.S. Sravneniye raz-lichnykh kharakteristik otechestvennykh fayrvolov. // Mezhdunarodnyy zhurnal informatsionnykh tekhnologiy i energoeffektivnosti, 2024. Tom 9. № 1 (39). S. 90–95.

15. Saati T.L. Prinyatiye resheniy: Metod analiza iyerarkhiy // Per. s angl. Vachnadze R.G. // – M.: Radio i svyaz'; 1993. – 314 s

КАРЕЛОВА Оксана Леонидовна, доктор физико-математических наук, доцент, профессор кафедры «Международная информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный лингвистический университет». 119034, г. Москва, ул. Остоженка, 38, стр. 1.; Профессор кафедры «Прикладные информационные технологии» федерального государственного бюджетного образовательного учреждения высшего образования «Президентская академия». 119571, г. Москва, проспект Вернадского, 82, стр. 1. E-mail: okarelova@yandex.ru

KARELOVA Oksana Leonidovna, Doctor of Physical and Mathematical Sciences, Associate Professor, Professor at the Department of International Information Security of the Federal State Budgetary Educational Institution of Higher Education «Moscow State Linguistic University». 119034, Moscow, Ostozhenka str., 38, bld. 1.; Professor at the Department of Applied Information Technologies of the Federal State Budgetary Educational Institution of Higher Education «Presidential Academy». 119571, Moscow, Vernadskogo ave., 82, bld. 1. E-mail: okarelova@yandex.ru

ЛИСИН Георгий Андреевич, обучающийся 4-го курса направления подготовки «Информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный лингвистический университет». 119034, г. Москва, ул. Остоженка, 38, стр. 1. E-mail: gal060303@gmail.com

LISIN Georgiy Andreevich, student of the 4th year of the training course «Information Security» of the Federal State Budgetary Educational Institution of Higher Education «Moscow State Linguistic University». 119034, Moscow, Ostozhenka str., 38, bld. 1. E-mail: gal060303@gmail.com

УДК 004.056.5 Вестник УрФО № 1(51) / 2024, с. 30–38

Абрамова Т.В.

DOI: 10.14529/secur240104

МНОГОАСПЕКТНЫЙ АНАЛИЗ ЧАСТНЫХ РЕШЕНИЙ В ЗАДАЧЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МОНИТОРИНГА СЕТЕВОГО ТРАФИКА

В статье рассмотрены вопросы анализа эффективности частных технических решений при разработке систем защиты информации (СЗИ). Предложена многоаспектная интерактивная матричная модель (МИМ) для системного анализа характеристик технических решений, вариант применения МИМ для анализа методов и средств защиты информации на основе мониторинга сетевого трафика. Проведен многоаспектный анализ частных решений на примере методов и средств защиты информации в компьютерных сетях (КС) автоматизированных систем управления технологическим процессом (АСУ ТП) транспортировки нефтегазового сырья. Представленные в работе результаты способствуют повышению качества процесса разработки СЗИ.

Ключевые слова: *методы и средства защиты информации, многоаспектный анализ, интерактивная матричная модель, автоматизированные системы управления, мониторинг сетевого трафика.*

MULTI-ASPECT ANALYSIS OF PARTICULAR SOLUTIONS IN THE PROBLEM OF INFORMATION SECURITY BASED ON NETWORK TRAFFIC MONITORING

The article discusses the issues of analyzing the effectiveness of private technical solutions in the development of information security systems. A multi-aspect interactive matrix model (IMM) is proposed for system analysis of the characteristics of technical solutions, and an option for using IMM to analyze methods and means of information security based on network traffic monitoring. A multi-aspect analysis of particular solutions was carried out using the example of methods and means of protecting information in computer networks of automated control systems for the technological process of transporting oil and gas raw materials. The results presented in the work contribute to improving the quality of the information security development process.

Keywords: *methods and means of information security, multi-aspect analysis, interactive matrix model, automated control systems, network traffic monitoring.*

Введение

Одним из факторов успешного создания систем защиты информации (СЗИ) является наличие и рациональное использование инструментальной базы средств поиска технических решений (ТР) и оценки их эффективности на всех стадиях и этапах построения СЗИ. Большая организационная и техническая сложность проектных работ обусловила использование наряду с традиционными новых решений для повышения качества проекта, а вместе с этим – и необходимость оценки эффективности этих решений.

В научной литературе известен представительный ряд публикаций, посвященных тематике настоящей работы. В частности, в статьях [1, 2] рассматриваются вопросы оценки эффективности проектов и внедряемых систем, в [3] представлены результаты исследований вкладов отдельных технических решений в общую эффективность проекта, в [4, 5] приводятся результаты разработки систем автоматизации проектных работ по созданию СЗИ. Однако представленные в публикациях решения не позволяют в полной мере оценить эффективность конкретных методов и средств в совокупности других результатов разработок сложных проектов. Подобные задачи нередко возникают в процессе выявления актуальных стратегий при управлении проектами, а также в процессе обсуждения и принятия решений о соответствии результатов научных исследований системе требований к научно-квалификационным работам.

Целью настоящей работы является повышение качества процесса разработки СЗИ на основе системного анализа эффективности частных технических решений с использованием многоаспектной матричной модели. Для достижения цели разработана структура многоаспектной интерактивной матричной модели для системного анализа характеристик технических решений по созданию СЗИ, представлен вариант применения МИМ для анализа эффективности разработанных методов и средств в задаче построения СЗИ на ос-

нове мониторинга сетевого трафика, проведен многоаспектный анализ частных решений на примере методов и средств защиты информации в КС АСУ транспортировкой нефтегазового сырья.

Объектом исследования в настоящей работе являются СЗИ в промышленных сетях на примере КС АСУ транспортировкой нефтегазового сырья. Предметом исследования – множество методов М и множество средств С, являющихся техническими решениями для построения и совершенствования СЗИ на основе мониторинга сетевого трафика.

Структура многоаспектной интерактивной матричной модели для системного анализа характеристик технических решений по созданию СЗИ

Ниже представлена структура многоаспектной интерактивной матричной модели, демонстрирующая особенности декомпозиции процесса создания СЗИ по стадиям, структуре СЗИ и ее компонентам.

Множество аспектов А, позволяющих определить систему оценок качества технических решений, содержит следующие элементы.

1. Структурный аспект S, определяющий уровень детализации СЗИ: система, подсистема, функциональный блок. Выбор перечня функциональных блоков обусловлен особенностями решения задачи, требованиями нормативных документов к СЗИ для рассматриваемого класса систем, а так же необходимостью расширения функциональной полноты существующих средств защиты в соответствии с требованиями проекта.

2. Технологический аспект Т, определяющий стадии создания СЗИ или ее компонентов.

3. Аспект К, определяющий качество ТР на основе показателей технического, экономического, социального или иного эффекта.

Таким образом, каждое техническое решение может быть описано фасетным кодом Ф (1):

$$Ф = \{S; T; K\} \quad (1)$$

В зависимости от задачи анализа результатов исследований и разработки перечень составляющих фасетного кода дополняется такими компонентами, как: уровень актуальности R, достоверности D, практической значимости Z или другими атрибутами результатов.

Для систематизации разработанных методов и средств в модели использован способ классификации и кодирования по методике, представленной в работе [6]. Согласно предложенному способу, разработанному решению присваивается код, каждый блок которого характеризует определенный аспект анализа ТР и содержит коды подсистем СЗИ, стадий проектирования и видов эффекта, относящихся к анализируемому методу или средству.

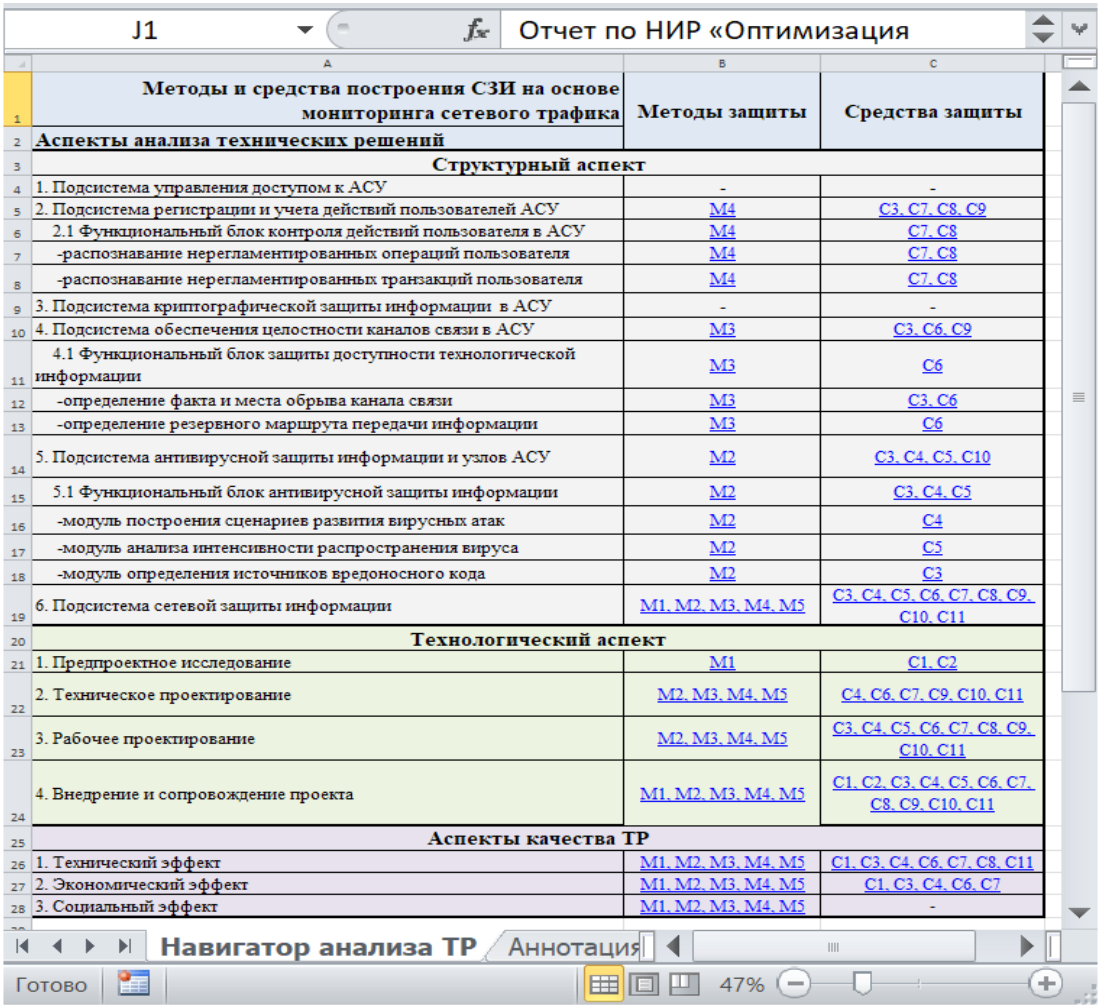
Вариант применения МИМ для анализа методов и средств защиты информации на основе мониторинга сетевого трафика

На рис. 1–3 приводится вариант реализации МИМ на основе табличного процессора MS Excel для многоаспектного анализа технических решений [7, 8], полученных по итогам научных исследований по теме гранта РФФИ № 18-47-560012 «Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков» [9]. МИМ включает навигатор анализа ТР, аннотации технических решений и характеристику решений по каждому из аспектов, представленных в выражении (1).

На рис. 1 представлена экранная форма навигатора анализа технических решений, отображающего общую структуру МИМ и позволяющего определить место разработанных решений в структуре СЗИ, этапы проектирования, на которых они применяются, и вид получаемого эффекта. Ввод сведений о технических решениях осуществляется с использованием специальных опросных анкет, реализованных в табличном процессоре MS Excel.

На рис. 2 представлен фрагмент аннотации ТР, содержащей код и наименование решения, общие сведения о ТР и ссылки на соответствующие электронные ресурсы в сети Internet.

Переход к сведениям о ТР и результатам анализа их эффективности осуществляется со страницы навигатора по гиперссылкам, обеспечивающим интерактивность модели и быструю навигацию между сведениями о решении, результатами анализа по различным аспектам и соответствующими электронными ресурсами сети Internet. Например, при нажатии на ссылку М2 в поле навигатора (рис. 1), характеризующего определенный аспект анализа, выводится информация об эффективности метода М2 «Метод восстановления

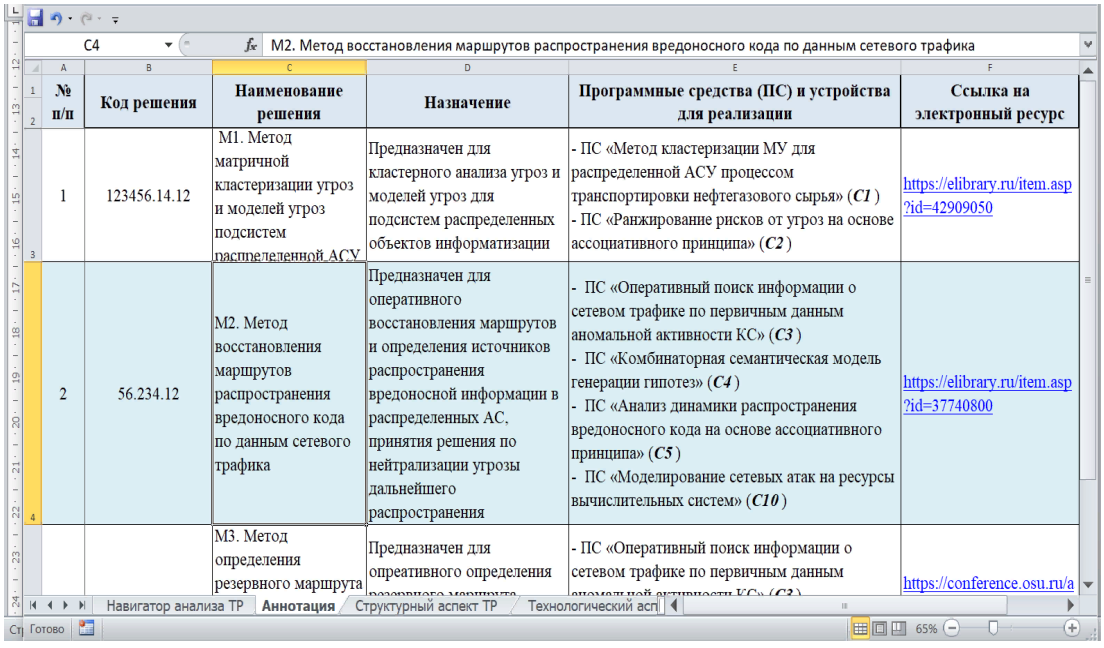


J1 | Отчет по НИР «Оптимизация

Методы и средства построения СЗИ на основе мониторинга сетевого трафика	Методы защиты	Средства защиты
Аспекты анализа технических решений		
Структурный аспект		
1. Подсистема управления доступом к АСУ	-	-
2. Подсистема регистрации и учета действий пользователей АСУ	M4	C3, C7, C8, C9
2.1 Функциональный блок контроля действий пользователя в АСУ	M4	C7, C8
-распознавание нерегламентированных операций пользователя	M4	C7, C8
-распознавание нерегламентированных транзакций пользователя	M4	C7, C8
3. Подсистема криптографической защиты информации в АСУ	-	-
4. Подсистема обеспечения целостности каналов связи в АСУ	M3	C3, C6, C9
4.1 Функциональный блок защиты доступности технологической информации	M3	C6
-определение факта и места обрыва канала связи	M3	C3, C6
-определение резервного маршрута передачи информации	M3	C6
5. Подсистема антивирусной защиты информации и узлов АСУ	M2	C3, C4, C5, C10
5.1 Функциональный блок антивирусной защиты информации	M2	C3, C4, C5
-модуль построения сценариев развития вирусных атак	M2	C4
-модуль анализа интенсивности распространения вируса	M2	C5
-модуль определения источников вредоносного кода	M2	C3
6. Подсистема сетевой защиты информации	M1, M2, M3, M4, M5	C3, C4, C5, C6, C7, C8, C9, C10, C11
Технологический аспект		
1. Предпроектное исследование	M1	C1, C2
2. Техническое проектирование	M2, M3, M4, M5	C4, C6, C7, C9, C10, C11
3. Рабочее проектирование	M2, M3, M4, M5	C3, C4, C5, C6, C7, C8, C9, C10, C11
4. Внедрение и сопровождение проекта	M1, M2, M3, M4, M5	C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11
Аспекты качества ТР		
1. Технический эффект	M1, M2, M3, M4, M5	C1, C3, C4, C6, C7, C8, C11
2. Экономический эффект	M1, M2, M3, M4, M5	C1, C3, C4, C6, C7
3. Социальный эффект	M1, M2, M3, M4, M5	-

Навигатор анализа ТР | Аннотация | Готово | 47%

Рис. 1. Экранная форма навигатора анализа технических решений



C4 | M2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика

№ п/п	Код решения	Наименование решения	Назначение	Программные средства (ПС) и устройства для реализации	Ссылка на электронный ресурс
1	123456.14.12	M1. Метод матричной кластеризации угроз и моделей угроз подсистем распределенной АСУ	Предназначен для кластерного анализа угроз и моделей угроз для подсистем распределенных объектов информатизации	- ПС «Метод кластеризации МУ для распределенной АСУ процессом транспортировки нефтегазового сырья» (***C1***) - ПС «Ранжирование рисков от угроз на основе ассоциативного принципа» (***C2***)	https://elibrary.ru/item.asp?id=42909050
2	56.234.12	M2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	Предназначен для оперативного восстановления маршрутов и определения источников распространения вредоносной информации в распределенных АС, принятия решения по нейтрализации угрозы дальнейшего распространения	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (***C3***) - ПС «Комбинаторная семантическая модель генерации гипотез» (***C4***) - ПС «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» (***C5***) - ПС «Моделирование сетевых атак на ресурсы вычислительных систем» (***C10***)	https://elibrary.ru/item.asp?id=37740800
		M3. Метод определения резервного маршрута	Предназначен для опреативного определения	- ПС «Оперативный поиск информации о сетевом трафике по первичным данным	https://conference.osu.ru/a

Навигатор анализа ТР | Аннотация | Структурный аспект ТР | Технологический асп | Готово | 65%

Рис. 2. Экранная форма аннотации технических решений

маршрутов распространения вредоносного кода по данным сетевого трафика» по соответствующему аспекту. Строка сведений об анализируемом методе выделяется цветом.

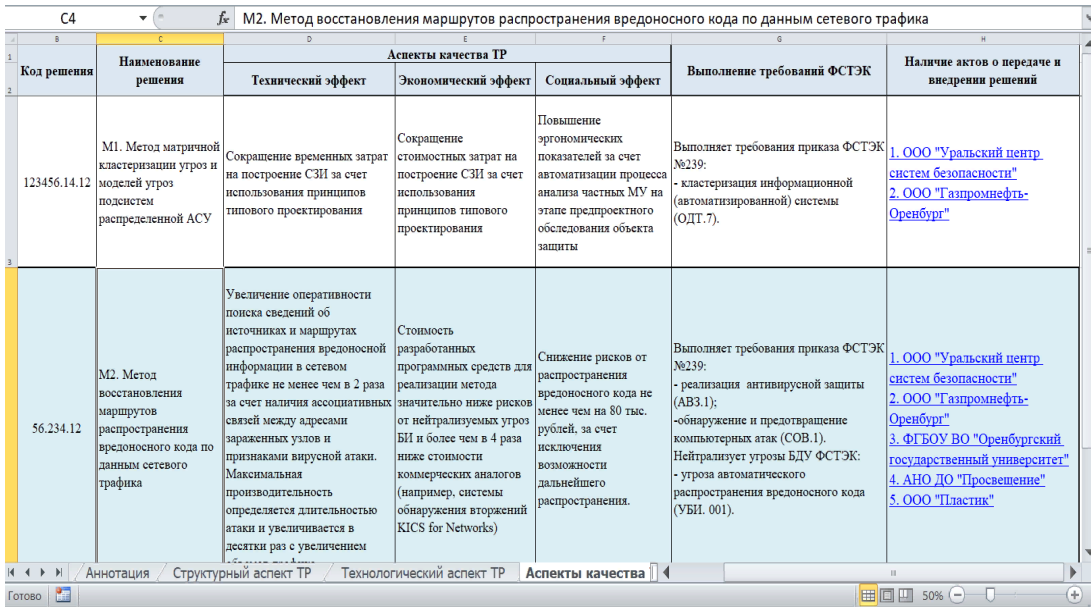
Многоаспектный анализ частных решений на примере методов и средств защиты информации в КС АСУ транспортировкой нефтегазового сырья

Анализ решений по *структурному аспекту* осуществляется согласно требованиям стандарта [10]. Относительно представленного в примере метода М2 можно сделать вывод, что метод используется в подсистемах антивирусной и сетевой защиты информации и позволяет повысить функциональную полноту средств антивирусной защиты за счет функций построения маршрутов и определения источников распространения вредоносного кода в КС.

Анализ решений по *технологическому аспекту* осуществляется согласно положениям стандарта [11]. В результате анализа делается вывод о том, на каком этапе проекта используется разработанное решение. Например, модели, разработанные при реализации метода М2, используются на этапе технического проектирования, а программное обеспечение – на этапах рабочего проектирования, внедрения и сопровождения проекта.

Анализ решений по *аспектам качества ТР* проводится с учетом технического, экономического и социального эффекта от его использования. Численные значения показателей эффекта выводятся на основе данных опросных анкет, заполняемых авторами разработанных решений. Результаты анализа позволяют оценить эффективность от внедрения ТР, степень выполнения требований нормативных документов Федеральной службы по техническому и экспортному контролю (ФСТЭК России), наиболее значимых при построении СЗИ для исследуемого объекта, нейтрализуемые угрозы из банка данных угроз ФСТЭК [12] и степень снижения рисков от угроз.

На рис. 3 в качестве примера представлена экранная форма результатов анализа эффективности метода М2 по аспектам качества ТР.


C4 | M2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика

Код решения	Наименование решения	Аспекты качества ТР: Технический эффект	Аспекты качества ТР: Экономический эффект	Аспекты качества ТР: Социальный эффект	Выполнение требований ФСТЭК	Наличие актов о передаче и внедрении решений
123456.14.12	М1. Метод матричной кластеризации угроз и моделей угроз подсистем распределенной АСУ	Сокращение временных затрат на построение СЗИ за счет использования принципов типового проектирования	Сокращение стоимостных затрат на построение СЗИ за счет использования принципов типового проектирования	Повышение эргономических показателей за счет автоматизации процесса анализа частных МУ на этапе предпроектного обследования объекта защиты	Выполняет требования приказа ФСТЭК №239: - кластеризация информационной (автоматизированной) системы (ОДТ.7).	1. ООО "Уральский центр систем безопасности" 2. ООО "Газпромнефть-Оренбург"
56.234.12	М2. Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика	Увеличение оперативности поиска сведений об источниках и маршрутах распространения вредоносной информации в сетевом трафике не менее чем в 2 раза за счет наличия ассоциативных связей между адресами зараженных узлов и признаками вирусной атаки. Максимальная производительность определяется длительностью атаки и увеличивается в десятки раз с увеличением	Стоимость разработанных программных средств для реализации метода значительно ниже рисков от нейтрализуемых угроз БИ и более чем в 4 раза ниже стоимости коммерческих аналогов (например, системы обнаружения вторжений KICS for Networks)	Снижение рисков от распространения вредоносного кода не менее чем на 80 тыс. рублей, за счет исключения возможности дальнейшего распространения.	Выполняет требования приказа ФСТЭК №239: - реализация антивирусной защиты (АВЗ.1); -обнаружение и предотвращение компьютерных атак (СОВ.1). Нейтрализует угрозы БДУ ФСТЭК: - угроза автоматического распространения вредоносного кода (УБИ. 001).	1. ООО "Уральский центр систем безопасности" 2. ООО "Газпромнефть-Оренбург" 3. ФГБОУ ВО "Оренбургский государственный университет" 4. АНО ДО "Просвещение" 5. ООО "Пластик"

Аннотация | Структурный аспект ТР | Технологический аспект ТР | Аспекты качества

Готово 50%

Рис. 3. Экранная форма результатов анализа эффективности метода по аспектам качества ТР

Сведения о наличии актов о передаче и внедрении технических решений на отраслевых предприятиях необходимы для подтверждения новизны и достоверности анализируемых методов и средств.

Результаты многоаспектного анализа частных решений на примере методов и средств защиты информации в КС АСУ транспортировкой нефтегазового сырья, полученных при выполнении проекта [9], представлены в табл. 1.

Предложенная модель отличается применением принципов многоаспектности и интерактивности, что позволяет оперативно проводить системный анализ эффективности частных технических решений на всех стадиях разработки СЗИ и способствует повышению качества процесса разработки.

Таблица 1

Результаты многоаспектного анализа эффективности методов и средств защиты информации в КС АСУ транспортировкой нефтегазового сырья

Метод	Результаты анализа	Средства для реализации метода
Метод матричной кластеризации угроз и моделей угроз (МУ) подсистем распределенной АСУ (М1)	– предназначен для кластерного анализа моделей угроз (МУ) для подсистем распределенных объектов информатизации на этапах предпроектного исследования, внедрения и сопровождения проекта; – используется во всех подсистемах СЗИ; – позволяет повысить функциональную полноту методов и средств кластеризации элементов АС, согласно мерам ОДТ. 7 приказа ФСТЭК №239; – позволяет снизить временные и стоимостные затраты на построение СЗИ.	– ПС «Метод кластеризации МУ для распределенной АСУ процессом транспортировки нефтегазового сырья» (С1); – ПС «Ранжирование рисков от угроз на основе ассоциативного принципа» (С2).
Метод восстановления маршрутов распространения вредоносного кода по данным сетевого трафика (М2)	– предназначен для оперативного восстановления маршрутов и определения источников распространения вредоносной информации в распределенных АС и принятия решения по нейтрализации угрозы дальнейшего распространения; – используется на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем антивирусной и сетевой защиты информации; – позволяет повысить функциональную полноту методов и средств антивирусной защиты, согласно мерам АВ3.1 и СОВ.1 приказа ФСТЭК №239; – позволяет повысить оперативность поиска данных о распространении вредоносной информации в сетевом трафике не менее чем в 2 раза за счет принципов ассоциативности и снизить риски от угрозы распространения вредоносного кода в КС не менее чем на 80 тыс. рублей	– ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (С3); – ПС «Комбинаторная семантическая модель генерации гипотез» (С4); – ПС «Анализ динамики распространения вредоносного кода на основе ассоциативного принципа» (С5); – ПС «Моделирование сетевых атак на ресурсы вычислительных систем» (С10).
Метод определения резервного маршрута на основе принципов обхода аномальных участков промышленных КС (М3)	– предназначен для определения резервного маршрута передачи информации при блокировании одного или нескольких участков основного канала связи; – используется на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем обеспечения целостности и доступности технологической информации и сетевой защиты информации; – позволяет повысить функциональную полноту средств защиты доступности информации в АС, согласно мерам ЗИС. 6 и ДНС.4 приказа ФСТЭК №239; – позволяет снизить риски потери информации о состоянии объекта защиты не менее чем на 14% за счет использования принципов горячего резервирования и оперативного определения резервного маршрута передачи данных.	– ПС «Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности КС» (С3); – ПС «Маршрутизация сетевых потоков в режимах переключения на резервные каналы связи» (С6).

Продолжение табл. 1

Метод мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций (М4)	– предназначен для контроля управляющих операций и транзакций в АС; – используется на этапах технического и рабочего проектирования, внедрения и сопровождения подсистем регистрации и учета, сетевой защиты информации; – позволяет повысить функциональную полноту методов и средств контроля действий пользователей в АС, согласно мерам АУД. 9 и ОЦЛ. 5 приказа ФСТЭК №239; – метод позволяет снизить риски от угрозы несанкционированных действий персонала АСУ не менее чем в 2 раза за счет контроля последовательности и очередности подачи управляющих команд	– ПС «Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus TCP» (С7); – ПС «Моделирование сетевого трафика на базе протокола TCP/ModBUS» (С9); – устройство для контроля поведения пользователя (С8).
Метод обнаружения аномалий в сетевом трафике на основе дихотомического подхода (М5)	– предназначен для обнаружения аномалий в сетевом трафике КС; – используется на этапах технического и рабочего проектирования, внедрения и сопровождения подсистемы сетевой защиты информации; – позволяет повысить функциональную полноту методов и средств анализа сетевого трафика, согласно мерам АУД. 5 и СОВ.1 приказа ФСТЭК №239; – метод обладает большей оперативностью и меньшей вычислительной сложностью на этапе распознавания аномалии не менее чем на порядок по сравнению с базовыми, в частности, нейросетевыми методами.	– ПС «Метод дихотомического распознавания аномалий в сетевом трафике» (С11).

Заключение

Разработанная интерактивная матричная модель позволяет:

– автоматизировать процедуру обоснования и доказательства применимости результатов научных исследований;

– выявить избыточность или дефицит методов и средств защиты информации для конкретного этапа проекта;

– оценить эффективность результатов конкретных решений в совокупности других результатов разработок сложных проектов;

– оценить вклад разработанных методов и средств в общий результат проекта.

Представленные результаты могут быть использованы при составлении отчетов по научно-исследовательской работе с учетом актуальности и значимости конкретных технических решений.

Литература

1. Вишнякова Т.О., Васильев В.И. Анализ эффективности систем физической защиты при помощи марковской сетевой модели // Вестник УГАТУ = Vestnik UGATU. 2007. №7. URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-sistem-fizicheskoy-zaschity-pri-pomoschi-markovskoy-setevoy-modeli (дата обращения: 23.12.2023).

2. Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты // Программные продукты и системы (SOFTWARE&SYSTEMS). – 1998. – №2. – С.6-9.

3. Коломойцев В.С. Модели и методы оценки эффективности систем защиты информации и обоснование выбора их комплектации: автореферат дис. ... кандидата технических наук: 05.13.19 / Коломойцев Владимир Сергеевич; [Место защиты: С.-Петерб. гос. ун-т телекоммуникаций им. М.А. Бонч-Бруевича]. - Санкт-Петербург, 2018. - 20 с.

4. Домарев В.В. Моделирование процессов создания и оценки эффективности систем защиты информации [Электронный ресурс]. - URL: http://citforum.ru/security/articles/model_proc. (дата обращения 23.12.2023).

5. Касимов А.Ф. Автоматизация проектирования систем защиты информации с использованием

методов многоальтернативной оптимизации : автореферат дис. ... кандидата технических наук: 05.13.12 / Воронеж. гос. техн. ун-т. - Воронеж, 2005. - 17 с.

6. Смирнова, Г.Н. Проектирование экономических информационных систем [Текст]: учебное пособие / Г.Н. Смирнова, Ю. Ф. Тельнов; Международный консорциум «Электронный ун-т», Московский гос. ун-т экономики, статистики и информатики, Евразийский открытый ин-т. - Москва: МЭСИ, 2004. - 22 см.; ISBN 5-7764-0405-3.

7. Патент 2675896 Российская Федерация, МПК G06K9/62. Устройство для контроля поведения пользователя/Абрамова Т.В., Аралбаев Т.З., Каскинов И.И., Хатеев М.Д./заявитель и патентообладатель ОГУ. – № 2018100997/08; заявл. 10.01.2018; опубл. 25.12.2018, Бюл. № 36. – 17 с.

8. Университетский фонд электронных ресурсов. Оренбургский государственный университет. - URL: https://ufer.osu.ru/ (дата обращения 23.12.2023).

9. Аралбаев, Т.З. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография/Т.З. Аралбаев, Г.Г. Аралбаева, Т.В. Абрамова, Р.Р. Галимов, А.В. Манжосов. - Оренбург: ОГУ, 2018.

10. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. [Электронный ресурс]. – URL: https://itsec2012.ru/gosudarstvennyy-standart-rossiyskoy-federacii-gost-r-51624-2000-zashchita-informacii (дата обращения 23.12.2023).

11. ГОСТ Р 59793-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания [Электронный ресурс]. – URL: https://www.astoni.ru/upload/iblock/2d4/GOST-34.601_90.pdf (дата обращения 23.12.2023).

12. Банк данных угроз безопасности информации. Федеральная служба по техническому и экспортному контролю ФСТЭК России, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – URL: https://bdu.fstec.ru/ (дата обращения 31.01.2024).

References

1. Vishnyakova T.O., Vasil'ev V.I. Analiz effektivnosti sistem fizicheskoy zashchity pri pomoshchi markovskoy setevoy modeli // Vestnik UGATU = Vestnik UGATU. 2007. №7. URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-sistem-fizicheskoy-zaschity-pri-pomoschi-markovskoy-setevoy-modeli (data obrashcheniya: 23.12.2023).

2. Khubaev G.N. Sravnenie slozhnykh programmnykh sistem po kriteriyu funktsional'noy polnoty // Programmnye produkty i sistemy (SOFTWARE&SYSTEMS). – 1998. – №2. – S.6-9.

3. Kolomoytsev V.S. Modeli i metody otsenki effektivnosti sistem za-shchity informatsii i obosnovanie vybora ikh komplektatsii: avtoreferat dissertatsii na soiskanie uchenoy stepeni kandidata tekhnicheskikh nauk: 05.13.19 / Kolomoytsev Vladimir Sergeevich; [Mesto zashchity: Sankt-Peterburgskiy. gos. un-t telekommunikatsiy im. M.A. Bonch-Bruevicha]. - Sankt-Peterburg, 2018. - 20 s.

4. Domarev V.V. Modelirovanie protsessov sozdaniya i otsenki effektivnosti sistem zashchity informatsii [Elektronnyy resurs]. - URL: http://citforum.ru/security/articles/model_proc. (data obrashcheniya 23.12.2023).

5. Kasimov A.F. Avtomatizatsiya proektirovaniya sistem zashchity informatsii s ispol'zovaniem metodov mnogoal'ternativnoy optimizatsii: avtoreferat dissertatsii na soiskanie uchenoy stepeni kandidata tekhnicheskikh nauk: 05.13.12 / Voronezh. gos. tekhnicheskiy un-t. - Voronezh, 2005. - 17 s.

6. Smirnova, G.N. Proektirovanie ekonomicheskikh informatsionnykh sistem [Tekst]: uchebnoe posobie / G. N. Smirnova, Yu. F. Tel'nov; Mezhdunarodnyy konsortsium "Elektronnyy un-t", Moskovskiy gos. un-t ekonomiki, statistiki i informatiki, Evraziyskiy otkrytyy in-t. - Moskva: MESI, 2004. - 22 sm.; ISBN 5-7764-0405-3.

7. Patent 2675896 Rossiyskaya Federatsiya, MPK G06K9/62. Ustroystvo dlya kontrolya povedeniya pol'zovatelya/Abramova T.V., Aralbaev T.Z., Kaskinov I.I., Khateev M.D./zayavitel' i patentoobladatel' OGU. – № 2018100997/08; zayavl. 10.01.2018; opubl. 25.12.2018, Byul. № 36. – 17 s.

8. Universitetskiy fond elektronnykh resursov. Orenburgskiy gosudarstvennyy universitet. - URL: https://ufer.osu.ru/ (data obrashcheniya 23.12.2023).

9. Aralbaev, T.Z. Optimizatsiya metodov kontrolya tekhnicheskogo sostoyaniya raspredelennykh avtomatizirovannykh sistem v usloviyakh vozdeystviya prostranstvenno-vremennykh ugroz na osnove monitoringa setevykh informatsionnykh potokov: monografiya/T.Z. Aralbaev, G.G. Aralbaeva, T.V. Abramova, R.R. Galimov, A.V. Manzhosov. - Orenburg: OGU, 2018.

10. GOST R 51624-2000. Zashchita informatsii. Avtomatizirovannye siste-my v zashchishchennom ispolnenii. Obshchie trebovaniya. [Elektronnyy resurs]. – URL: https://itsec2012.ru/gosudarstvennyy-standart-rossiyskoy-federacii-gost-r-51624-2000-zashchita-informacii (data obrashcheniya 23.12.2023).

11. GOST R 59793-2021 Informatsionnye tekhnologii. Kompleks standartov na avtomatizirovannye sistemy. Avtomatizirovannye sistemy. Stadii sozdaniya [Elektronnyy resurs]. – URL: https://www.astoni.ru/upload/iblock/2d4/GOST-34.601_90.pdf (data obrashcheniya 23.12.2023).

12. Bank dannykh ugroz bezopasnosti informatsii. Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu FSTEK Rossii, Gosudarstvennyy nauchno-issledovatel'skiy ispytatel'nyy institut problem tekhnicheskoy za-shchity informatsii FAU «GNIII PTZI FSTEK Rossii». – URL: https://bdu.fstec.ru/ (data obrashcheniya 31.01.2024).

АБРАМОВА Таисия Вячеславовна, старший преподаватель кафедры вычислительной техники и защиты информации федерального государственного бюджетного образовательного учреждения «Оренбургский государственный университет». 460018, г. Оренбург, проспект Победы, д. 13. E-mail: taya357@gmail.com

ABRAMOVA Taisiya Vyacheslavovna, senior lecturer at the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education «Orenburg State University». 460018, Orenburg, ave. Pobeda, 13. E-mail: taya357@gmail.com

УДК 004.324 Вестник УрФО № 1(51) / 2024, с. 39–44

Куц Д.В., Поршнев С.В., Соколов И.П., Куц М.П.

DOI: 10.14529/secur240105

АНАЛИЗ ПРОБЛЕМЫ НАДЁЖНОГО УДАЛЕНИЯ ФАЙЛОВ НА ТВЕРДОТЕЛЬНЫХ НАКОПИТЕЛЯХ И ПОДХОДОВ К ЕЕ РЕШЕНИЮ

В статье проводится анализ проблемы надёжного удаления отдельных файлов на твердотельных накопителях, обусловленные их структурно-функциональными особенностями, которые являются основной причиной, не позволяющей реализовать их эффективное удаление с данного типа накопителей, например, используя для этого штатные средства операционной системы, специализированное программное обеспечение от производителя накопителя или специализированные программные решения, доказавшие свою эффективность для накопителей на жёстких магнитных дисках.

Описаны известные методы решения данной проблемы. Предложена классификация данных методов. Приведены оценки возможности практического использования данных методов.

Ключевые слова: *TRIM, deallocate, восстановление данных, solid-state drive, NTFS, твердотельный накопитель, выравнивание износа, сборка мусора гарантированное уничтожение, гарантированное затирание файлов.*

Kuts D.V., Porshnev S.V., Sokolov I.P., Kuts M.P.

WAYS TO SOLUTION THE PROBLEM OF RELIABLE DELETION OF INDIVIDUAL FILES ON SOLID-STATE DRIVES

The article analyzes the problem of reliable deletion of individual files on solid-state drives, due to their structural and functional features, which are the main reason that does not allow their effective removal from this type of drive, for example, using standard operating system tools, specialized software from drive manufacturer or specialized software solutions that have proven their effectiveness for hard disk drives. Known methods for solving this problem are described. A classification of these methods is proposed. Assessments of the possibility of practical use of these methods are given.

Keywords: *TRIM, deallocate, data recovery, solid-state drive, NTFS, wear leveling, garbage collection, file sanitizing, data sanitizing.*

Введение

Твердотельный накопитель (англ. Solid-State Drive, SSD), в отличие от более традиционных накопителей, например, таких как жёсткий диск, имеет более сложную структуру организации хранения информации в ячейках памяти. Данное обстоятельство обусловлено ограниченным ресурсом ячеек памяти после каждого стирания данных, находящихся в ячейке, происходит её постепенная деградация на физическом уровне. Для продления длительности жизни накопителя контроллер SSD реализует такой режим записи данных на диск, в котором количество стираний данных в ячейках, а, следовательно, и количество записей в каждую ячейку накопителя было одинаковым. Этим обеспечивается максимальная продолжительность жизни накопителя. Равномерный износ ячеек памяти обеспечивается реализацией в накопителе технологии «выравнивания износа» (англ. Wear Leveling, WL).

Технология WL [1] основана на совместном использовании абстрагированного логического адресного пространства SSD-накопителя и физических адресов ячеек памяти микросхем. Что, в свою очередь, обеспечивается технологией, реализующей алгоритм трансляции адресов флеш-памяти (англ. Flash Translation Layer, FTL), которая позволяет установить взаимно однозначное соответствие между логическими и физическими адресами ячеек флэш-памяти (англ. not and, NAND) SSD-накопителей. В данном алгоритме в случае записи новых данных на SSD-накопитель логические адреса физических адресов NAND-ячеек памяти заменяются на адреса менее изношенных NAND-ячеек, что и обеспечивает равномерный износ каждой ячейки памяти носителя на твердотельном накопителе [2].

Описанные выше особенности технологии FTL, приводят к тому, что при попытке стирания файла, путём перезаписи его содержимого, контроллер SSD с большой вероятностью подменит адреса ячеек и запись произойдёт в другие ячейки памяти. При этом ранее использованные ячейки, которых размещалось содержимое данного файла останутся не затёртыми. В этой связи в [2] был сделан обоснованный вывод о невозможности осуществления гарантированного затирания отдельных файлов на твердотельных накопителях в процессе его эксплуатации с помощью методов, рекомендованных действующей нормативно-правовой базой и зарубежными стандартами.

В настоящей статье авторами будет проведён анализ известных методов, обеспечивающих по мнению их авторов, гарантированное затирание отдельных файлов, удаляемых с SSD-носителя.

Анализ методов затирания отдельных файлов на твердотельных накопителях

Проблема стирания отдельных файлов на SSD-накопителях была впервые поднята исследовании «Reliably Erasing Data From Flash-Based Solid State Drives» [3], авторы которого описали результаты серии проведённых ими экспериментов, указывающих на невозможность осуществить полное затирание файлов традиционными инструментами, которые эффективно работали на жестких дисках. Таким образом, оказалось, что стирание определенных областей на SSD-накопителях, в связи с отсутствием соответствующих инструментов, является нетривиальной задачей.

Для ее решения в [3] предложено модифицировать слой абстракции твердотельного накопителя (FTL) с целью проведения процедуры принудительной сборки мусора контроллером SSD, для стирания данных файла сразу после завершения процедуры его удаления. В качестве альтернативного способа решения проблемы авторы предложили одновременно проводить фоновую сборку мусора удалённых файлов и продемонстрировали, что применение данного способа позволяет увеличить скорость работы накопителя. Ещё один предложенный авторами метод - затирание со сканированием. В процессе его практического использования контроллер твердотельного накопителя сканирует свободные области накопителя и, в случае обнаружения блоков, занятых данными, осуществляет их стирание. Все три метода были опробованы на модели твердотельного накопителя и, в целом, показали достаточную эффективность. Однако, практическое применение данных методов вызывает серьёзные сомнения. Во всех случаях требуется модификация прошивки контроллера SSD, что трудноосуществимо, учитывая многообразие производителей и решений в этой области.

Во всех случаях снижалась производительность и долговечность устройства.

Еще два подхода решению проблемы затирания отдельных файлов предложен в [4]. В основу первого подхода положены идеи использовании криптографических методов, обеспечивающих безопасное удаление данных без их перемещения, которые, однако, используют существенные вычислительные ресурсы, что приводит к существенному уменьшению скорости записи/считывания данных с SSD-накопителя. В основу второго подхода – стирание информации на уровне блоков данных SSD-накопителей (изменение каждого из битов данного блока, используемых для хранения не удаленных данных с нуля на единицу), использование которого, однако, приводит к увеличению энергопотребления, снижению производительности и сокращению срока службы SSD, поскольку каждый блок может выдержать лишь ограниченное количество циклов записи/стирания. Результаты проведенных авторами [3] экспериментов показали достаточную эффективность второго подхода и незначительное снижение производительности SSD-накопителя. Однако, оказалось, что его практическое использование требует существенной доработки прошивки SSD-накопителя, что затрудняет его применение.

Еще один метод, призванный обеспечить гарантированное удаление информации на SSD-носителях, предложены в [5]. Он основан на использовании программного шифрования данных и, по своей сути оказывается близким к системе шифрования данных EFS (англ. Encrypting File System), реализующей шифрование на уровне файлов в операционных системах Microsoft Windows NT для файловой системы NTFS. В данном методе каждый файл шифруется индивидуальным ключом, который получается путём хеширования пароля пользователя, общего для всей системы, и добавляемой соли, в роли которой выступает имя файла. В криптографии соль – последовательность данных, добавляемая к хешируемому блоку данных, в нашем случае – паролю пользователя, с целью чтобы хэш – функция от одинаковых блоков данных имела разные значения. При этом для обеспечения надёжного удаления файла, стирается информация о ключе шифрования из главной файловой таблицы (Master File Table, MFT) NTFS, данные же файла, затираются с помощью команды TRIM интерфейса SATA (англ. Serial Advanced Technology Attachment), позволяющей операционной системе уведомить твердотельный накопитель о том, какие блоки данных (страницы) не несут полезной нагрузки и их можно не хранить физически.

Однако данный метод оказывается не вполне надёжным, так как стойкость шифрования будет во многом обеспечиваться стойкостью пароля пользователя. Хотя имя файла также хранится в зашифрованном виде, для многих файлов его легко установить с помощью методов компьютерной криминалистики и реализовать атаку перебора пароля по хешу с известной солью. На современных высокопроизводительных платформах скорость такого перебора может достигать 1 трлн паролей в секунду и выше, что позволяет перебирать даже весьма сложные пароли за обозримый интервал времени. Кроме того, затирание данных на твердотельном накопителе с помощью команды TRIM не всегда эффективно. Например, в [6] демонстрировано, что программное восстановление удалённых данных на некоторых SSD-накопителях даже с включёнными командами TRIM или Deallocate вполне может быть результативным, особенно, для файлов небольшого размера.

Кроме того, в [3] продемонстрировано, что даже при успешно отработавшей команде TRIM, удаляемые данные могут оставаться на накопителе ещё достаточно продолжительное время, пока до них не доберётся сборщик мусора. Отдельные области в MFT, где хранятся метаданные удаляемого файла, можно затирать только программно, т.к. в этом случае команда TRIM оказывается бесполезной, т.к. файловая система воспринимает MFT как отдельный файл, чем, по сути, она и является. В этом случае весьма высока вероятность восстановить метаданные файла. В текущей реализации обсуждаемый метод также не сможет работать с файловой системой, отличной от NTFS.

В этой связи в данном методе используется исключительно программное шифрование, что также негативно сказывается на производительности системы. Подводя итоги, можно сказать, метод, предложенный в [5], не является универсальным в части поддерживаемых файловых систем, не обладает достаточной надёжностью и не имеет достаточной производительности. В тоже время, метод не требует модификации прошивки контроллера твердотельного накопителя, существенно усложняет процесс восстановления удалён-

ных данных на SSD-накопителе и, при некоторой доработке, может быть использован для других файловых систем, например, семейства EXT в операционных системах Linux. Однако главную задачу – надёжного удаления отдельного файла на твердотельном накопителе данный метод решает не в полной мере.

В [7] предложено встраивать систему страничного шифрования в общий уровень трансляции флэш-памяти FTL твердотельного накопителя. Суть метода состоит в следующем. Шифрование осуществляется для каждой страницы перед сохранением ее во флэш-памяти NAND и перед извлечением данных осуществляется их расшифровка для каждой страницы. Хранение ключей организуется в определенном участке флэш-памяти, известном как Зона Хранения Ключей. При удалении определённого файла, удаляется блок, в котором расположены ключи шифрования файла. Ключи шифрования хранятся в заголовке страницы памяти NAND. Очистка производится на каждом блоке области хранения ключей. При очистке выбирается новый блок области хранения ключей для копирования использующихся ключей, находящиеся в тех же местах. Эксперименты, проведённые авторами, подтвердили высокую эффективность предложенного метода. Однако, как и в ряде предыдущих работ, данный метод требует модификации прошивки контроллера, что весьма затруднительно на практике.

В [8] предложен метод частичной очистки данных в многоуровневых ячейках Multi Level Cell (MLC) флэш-памяти с использованием однократной записи. В данном методе применяется однократная запись для затирания данных на страницах MSB (Most Significant Bit, хранящих два старших бита ячейки) и LSB (Least Significant Bit, хранящих два младших бита ячейки). Проведенные авторами [8] эксперименты показали, что затирание лишь половины данных в ячейке памяти, в первую очередь LSB, является достаточно надёжным методом, и не позволяет осуществить эффективное восстановление данных. Однако метод не применим на более современной памяти твердотельных накопителях типа TLC (Triple Level Cell, с трехуровневыми ячейками памяти) и QLC (Quad Level Cell, с четырёхуровневыми ячейками памяти), о чём пишут сами авторы в [8], в связи с иной, более сложной организацией хранения данных.

Результаты проведенного нами анализа известных методов затирания отдельных файлов, находящихся на SSD-накопителях, в обобщенном виде оказывается удобным представить в виде сводной таблицы (табл. 1).

Таблица 1

Результаты сравнительного анализа методов затирания файлов, находящихся на SSD-накопителях

Метод затирания файла	Программная универсальность	Аппаратная независимость	Производительность	Срок службы	Надёжность затирания
Принудительная сборка мусора	Не зависит от файловой системы и ОС	Требуется модификация прошивки контроллера	Существен-но снижена	Сущес-твен-но снижен	Высокая
Криптографическое стирание с принудительной сборкой мусора	Не зависит от файловой системы и ОС	Требуется модификация прошивки контроллера	Незначи-тель-но снижена	Незначи-тельно снижен	Высокая
Программное шифрование данных	Работает только на NTFS в среде Windows.	Не зависит от типа SSD и его производителя	Существен-но снижена	Не влияет	Низкая
Шифрование, встроенное в FTL	Не зависит от файловой системы и ОС	Требуется модификация прошивки контроллера	Незначи-тель-но снижена	Незначи-тельно снижен	Высокая
Метод частичной очистки данных	Не зависит от файловой системы и ОС	Требуется модификация прошивки контроллера	Незначи-тель-но снижена	Незначи-тельно снижен	Высокая

Из табл. 1 видно.

1. Сегодня не существует единого универсального метода стирания файлов на SSD-носителях.

2. Все известные методы могут быть классифицированы на следующие группы:

1) методы, требующие модификации прошивки контроллера, оказывающиеся неприменимыми на практике, так как на защищаемых компьютерах устанавливаются твердотельные накопители от разных производителей с различными микросхемами памяти и внутренними алгоритмами работы контроллера;

2) программные методы, которые, не смотря на свою аппаратную независимость, зачастую не обладают достаточной надёжностью затирания данных, что не исключает их последующего восстановления;

3) технологии криптографического стирания данных, реализованные во многих твердотельных накопителях, предназначены не для затирания отдельных файлов, но затирания сразу всего накопителя. Использование аппаратных возможностей SSD для криптографического стирания отдельных файлов требуют модификации прошивки контроллера.

Следовательно, разработка надежного универсального алгоритма гарантированного удаления файлов, размещенных на SSD-накопителях, имеющего приемлемую, с точки зрения практики, скорость работы, и наказывающего существенного влияния на его производительность и срок службы является актуальной. Результаты проводимых авторами исследований в данной области являются предметом последующих публикаций.

Литература

1. Куц Д.В., Поршнев С.В., Соколов И.П., Куц М.П: К постановке проблемы затирания отдельных файлов на твердотельных накопителях. Сетевой научный журнал «Инженерный вестник Дона», №2, 2024. URL: http://www.ivdon.ru/uploads/article/pdf/IVD_16__2y24_kuts_porshnev_sokolov_kuts.pdf_82cac7b31d.pdf (дата обращения: 25 марта 2023 г.).

2. Куц Д.В., Поршнев С.В., Куц М.П: Анализ механизмов удаления файлов на твердотельных накопителях//Вестник УРФО. Безопасность в информационной сфере. 2022, № 3(45) 2022, с. 17–23.

3. Michael Wei, Laura Grupp, Steven Swanson: Reliably Erasing Data From Flash-Based Solid State Drives. Proceedings of the FAST, Volume 11,2011.

4. Chen Liu, Hoda Aghaei Khouzani, and Chengmo Yang: ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives. Proceedings of the Privacy Enhancing Technologies; 2017 (1):132–148.

5. Younsung Choi, Donghoon Lee, Woongryul Jeon, Dongho Won: Password-Based Single-File Encryption and Secure Data Deletion for Solid-State Drive. ICUIMC '14: Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. January 2014. No.: 5. Pages 1–7.

6. Куц Д.В., Куц М.П: Deleted Data Recovery on Solid-State Drives by Software Based Methods. Proceedings of the 2022 Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT).

7. Singh, Bhupendra, Ravi Saharan, Gaurav Somani, Gaurav Gupta: Secure File Deletion for Solid State Drives. Proceedings of the IFIP International Conference on Digital Forensics, pp. 345-362. Springer, Cham, 2016.

8. Instant Data Sanitization on Multi-Level-Cell NAND Flash Memory. Proceedings of the 15th ACM International Conference on Systems and Storage. June 2022, p. 85–95.

References

1. Kuts D.V., Porshnev S.V., Kuts M.P: Analiz mekhanizmov udaleniya fajlov na tverdotel'nyh nakopitelyah. "Vestnik URFO. Bezopasnost' v informacionnoj sfere" ISSN 2225-5435, № 3(45) / 2022, str. 17-23. URL: http://www.ivdon.ru/uploads/article/pdf/IVD_16__2y24_kuts_porshnev_sokolov_kuts.pdf_82cac7b31d.pdf (date of the application: 25 march 2023 г.).

2. Kuts D.V., Porshnev S.V., Sokolov I.P., Kuts M.P: K postanovke problemy zatiraniya otdel'nyh fajlov na tverdotel'nyh nakopitelyah. Setevoj nauchnyj zhurnal «Inzhenernyj vestnik Dona» №2 2024. ISSN 2073-8633

3. Michael Wei, Laura Grupp, Steven Swanson: Reliably Erasing Data From Flash-Based Solid State Drives. Proceedings of the FAST, Volume 11,2011.

4. Chen Liu, Hoda Aghaei Khouzani, and Chengmo Yang: ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives. Proceedings of the Privacy Enhancing Technologies, 2017 (1), p 132–148.

5. Younsung Choi, Donghoon Lee, Woongryul Jeon, Dongho Won: Password-Based Single-File Encryption and Secure Data Deletion for Solid-State Drive. ICUIMC '14: Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. January 2014. No.: 5. Pages 1–7.

6. Kuts D.V., Kuts M.P: Deleted Data Recovery on Solid-State Drives by Software Based Methods. Proceedings of the 2022 Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT).

7. Singh, Bhupendra, Ravi Saharan, Gaurav Somani, Gaurav Gupta: Secure File Deletion for Solid State Drives. Proceedings of the IFIP International Conference on Digital Forensics, pp. 345-362. Springer, Cham, 2016.

8. Instant Data Sanitization on Multi-Level-Cell NAND Flash Memory. Proceedings of the 15th ACM International Conference on Systems and Storage. June 2022, p. 85–95.

КУЦ Дмитрий Владимирович, старший преподаватель Учебно-научного центра «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: d.v.kutc@urfu.ru

KUTS Dmitry Vladimirovich, senior teacher of the Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: d.v.kutc@urfu.ru

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: s.v.porshnev@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Full Professor, Head of Unit, Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: s.v.porshnev@urfu.ru

СОКОЛОВ Илья Петрович, старший преподаватель Учебно-научного центра «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: ipsokolov@urfu.ru

SOKOLOV Ilya Petrovich, senior teacher of the Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: ipsokolov@urfu.ru

КУЦ Мария Петровна, преподаватель кафедры Иностранных языков и образовательных технологий, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Куйбышева, 48а. E-mail: m.p.kutc@urfu.ru

KUTS Maria Petrovna, teacher of the Department of Foreign Languages and Educational Technologies, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Ekaterinburg, Kuibysheva street, 48a. E-mail: m.p.kutc@urfu.ru

УДК 004.922 Вестник УрФО № 1(51) / 2024, с. 45–52

Грибачёв А.С., Кальщиков В.В., Ручай А.Н. DOI: 10.14529/secur240106

МЕТОДЫ, АЛГОРИТМЫ И БАЗЫ ДАННЫХ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

В современных реалиях, передача, обработка и хранение информации производится преимущественно в электронном виде. Процесс обработки и анализа электронных данных происходит куда быстрее и удобнее и, что не мало важно, намного дешевле: достигается это благодаря хранению информации в специализированных базах данных. Цифровизация – это современный инструмент, позволяющий человеку получать интересующую его информацию за короткий промежуток времени. Использование продуктов цифровизации позволяет более рационально использовать время, однако, информация о человеке более уязвима. Сегодня мы можем наблюдать как информация подвергается различным мошенническим атакам: телефонные мошенники, целью которых является банковские сведения человека, шпионское программное обеспечение внедряется для использования компьютерных мощностей пользователя для преступных целей, кража личной информации и переписки в социальных сетях для последующей публикации в открытом доступе и, как следствие, серьезный урон репутации человека или компании. Часто бывает так, что данным угрожают не злоумышленники, а недостаточно квалифицированные пользователи, либо ошибки в программном обеспечении, что в обоих случаях, приводит к потери информации. Огромное количество угроз в цифровой сфере обосновывает необходимость обеспечивать не только доступность цифровых сервисов, но и их безопасность. Обеспечение защиты информации на объектах критической информационной инфраструктуры для страны является одной из главных задач. Поэтому превентивная защита, своевременная реакция на данные виды атак, а также принятие мер по противодействию киберугрозам является приоритетной задачей. Цель данной работы состоит в изучении типов компьютерных угроз, существующих типов баз данных, методов обнаружения кибератак и способов противодействия им.

Ключевые слова: *кибербезопасность, критическая информационная инфраструктура, обнаружение атак, информационная безопасность, машинное обучение, базы данных.*

Gribachev A.S., Kalshikov V.V., Ruchay A.N.

METHODS, ALGORITHMS AND DATABASES FOR DETECTING COMPUTER INCIDENTS

In modern realities, the transfer, processing and storage of information is carried out digitally. Processing and analyzing digital data are much faster and more convenient and much

cheaper: this is achieved by storing information in specialized databases. Digitalization is a modern tool that allows a person to obtain interest information in a short period of time. The use of digitalization products allows for more efficient use of time, however, information about a person is more assailable. Today information is subjected to various scam attacks: phone scammers whose goal is a person's banking information, spyware is introduced to use the user's computer power for criminal purposes, theft of personal information and correspondence in social networks for publication in the public domain, and, as a result, serious damage to the reputation of a person or company. Often, data is threatened not by attackers, but by insufficiently qualified users, or by software errors, which in both cases leads to loss of information. The huge number of threats in the digital sphere justifies the need to ensure not only the availability of digital services, but also their security. Ensuring the protection of information at objects of critical information infrastructure for the country is one of the main tasks. Therefore, preventive protection, timely response to these types of attacks, as well as taking measures to counter cyber threats are a priority. The purpose of this work is to study the types of computer threats, the types of databases, methods of cyberattacks detection and ways to counter it.

Keywords: *cybersecurity, critical information infrastructure, attack detection, information security, machine learning, databases.*

Введение

Сегодня превентивная защита и принятие мер по обнаружению и предотвращению киберугроз на информационные системы и компьютерное оборудование предприятий, на объекты критической информационной инфраструктуры одна из важнейших задач по обеспечению информационной безопасности страны. [1-2] Активное внедрение технологии интернета вещей в жизнь современного человека, цифровизации различных бизнес-процессов учреждений и предприятий, все это упрощает и облегчает существование и функционирование в различных сферах деятельности общества: медицина, сельское хозяйство, экономика и многие другие. Однако, это также является благоприятной средой для киберпреступности, что подтверждается каждодневным ростом кибератак на объекты критической информационной инфраструктуры. Кибератака представляет собой определенное действие, которое связанно с проникновением в компьютерную систему, минуя систему защиты. Обнаружение такого незаконного неавторизованного доступа в систему называют выявлением кибератаки. [3] Статья представлена в 4 разделах: 1, 2 и 3 разделы посвящены кибератакам и методам их обнаружения, в 4 разделе приводится обзор имеющихся структур баз данных, использующихся в построении SIEM-систем, а также примеры наборов данных современных атак.

Виды и типы кибератак на критическую информационную инфраструктуру

Действия киберпреступников направлены на получение несанкционированного доступа к информационным системам и каналам связи инфраструктуры для перехвата управлением, либо получения данных, имеющих определенную ценность. [4] Такие действия подразделяются на два вида: целевые и распределенные кибератаки. Одни нацелены на определенную компанию или отрасль, такой вид атаки подразумевает получение доступа к ресурсам инфраструктуры и минимизация риска обнаружения киберпреступника в системе, то есть злоумышленник может находиться в сети долгое время, до момента его обнаружения. Для реализации такого типа атак необходимы автоматизированные инструменты и высокоспециализированные хакеры. Другие направлены на огромное количество информационных систем компаний, для таких атак применяются специальные роботизированные сети.

Существуют различные типы атак на критическую информационную инфраструктуру:

1. Боты. Происходит имитация поведения человека, однако робот выполняет задачи быстрее самого пользователя. Доступность ботов и их возможность совершать огромное количество атак одновременно существенно упрощает работу злоумышленникам. Киберпреступники применяют комбинированный подход при обходе механизмов защиты информационных систем от ботнетов, то есть используют комбинацию автоматизированных скриптов и действий реального человека. Такие гибридные кибератаки гораздо сложнее обнаружить. Зачастую ботов исполь-

зуют для подготовки к атаке, для сбора информации и создания информационной базы. Проводятся направленные кибератаки с максимальной имитацией действий человека, таким способом избегают блокировок системой защиты. Современные боты могут очень точно имитировать действия реального человека благодаря применению технологии машинного зрения.

2. Атака «грубой силой» – представляет собой метод получения доступа в информационную систему путем взлома учетных записей. Получив данные адресов электронной почты или имена пользователей информационных систем, злоумышленник методом перебора паролей пытается получить доступ к таким системам. Обычно используются специализированное программное обеспечение, позволяющее создавать списки учетных данных для аутентификации. Данный вид атаки требует значительных временных трат, так как перебор всех возможных комбинаций имен пользователей и паролей до тех пор, пока не будет найдена корректная требует времени. Применение парольной политики и ограничивая количество запросов на авторизацию для одного аккаунта и с одного IP-адреса можно существенно снизить успешность атаки «грубой силы» на информационные ресурсы.

3. Отказ в обслуживании - эти атаки нагружают систему большим количеством запросов, в результате происходит снижение пропускной способности, а система недоступной. Данный тип кибератак относится к типу сетевых атак. Возможны два варианта реализации такого рода атак: отправка огромного объема данных с такой скоростью, что их обработка станет невозможной, либо могут передаваться пакеты данных, в которых содержатся ошибки, при обработке таких данных системы тратят много времени, начинают работать медленно и выходят из строя. Основными способами защиты от «DDoS-атак» является уменьшение зон, доступных для атаки, анализ сетевого трафика, увеличение пропускной способности и производительности серверов, достаточной для нейтрализации и поглощения кибератак.

4. Фишинг – использование почтовых рассылок, замаскированных под обычные сообщения компании, либо создание поддельных страниц регистрации с целью получения идентификационных данных. Для атак на критическую информационную инфраструктуру может быть использован направленный фишинг, то есть нацеленная рассылка на определенный объект или организацию. В качестве защиты от фишинга необходимо использовать надежную систему защиты, применять двухфакторную аутентификацию в системах, применять парольную политику, при передаче данных внимательно изучать сетевые-ресурсы и почтовых отправителей.

5. Атака через посредника. При таком типе атаки в момент передачи сообщений происходит утечка данных третьей стороне. [5-10] Киберпреступники, перехватывая трафик, могут перенаправлять его, либо пропускать, анализирую информацию в момент ее поступления. Злоумышленник выступает в роли посредника между отправителем и адресатом. Такой вид атак очень распространен, например в общедоступных сетях. Также в целях шпионажа или кражи данных могут быть установлены мошеннические точки доступа даже в частных сетях. IP, ARP, DNS, HTTPS, SSL спуфинги, перехват сеансов, внедрение пакетов, SSL-стриппинг применяются для подмены данных и передачи их злоумышленнику. Защита от такого типа угроз представляет собой полный отказ от использования общедоступных сетей при работе с конфиденциальной информацией, использование стойкого шифрования при передаче данных между клиентом и сервером, а также аудит локально-вычислительных сетей на наличие несанкционированного оборудования.

Методы обнаружения кибератак

Современные системы обнаружения кибератак основываются на сборе данных о трафике сетевых соединений и журналируемых событиях серверов и ключевых компьютеров. Такие системы проводят наблюдение и анализируют события, которые происходят в информационной инфраструктуре, а также позволяют отслеживать различные сетевые атаки, такие как проникновение в сеть, отказ в обслуживании и сканирование портов. Анализ различных системных характеристик, либо отслеживание входящего/исходящего трафика позволяет обнаружить вредоносные действия. [11-12]

Методы обнаружения компьютерных угроз можно разделить на следующие блоки:

• Сигнатурный анализ базируется на рассмотрении содержимого исследуемого объекта сигнатур уже известных угроз. Для возможности обнаружения угрозы исследуются ее характерные признаки. Сравнение проис-

ходит по контрольным суммам. Такой подход значительно снижает размер записей в базах и позволяет сохранить корректность обнаружения угроз.

• Метод эмуляции исполнения. Основное применение заключается в детектировании полиморфных и шифрованных вирусов. Применяется специальная программная модель процессора и эмулятор (среда исполнения программ). Эмулятор работает с буфером эмуляции, при этом инструкции не передаются на центральный процессор для реального исполнения.

• Эвристический анализ основывается на наборе эвристик о характерных признаках вредоносного и безопасного исполняемого кода. Каждому признаку такого кода назначается определенный вес. Исходя из суммарного веса, эвристический анализатор производит расчет вероятности, что в исследуемом объекте содержится неизвестный код. Если такая вероятность превышает пороговое значение, то будет выдано заключение - анализируемый объект является вредоносным.

• Метод поведенческого анализа позволяют анализировать последовательность действий всех процессов в системе. При обнаружении признаков поведения вредоносной программы действия приложения блокируются.

• Метод машинного обучения. Данный метод используется для обнаружения угроз, которые отсутствуют в вирусных базах. Преимущество метода – распознавание угроз на основе их характеристик. Основывается на классификации кибератак согласно определенным признакам. Метод машинного обучения позволяет экономить ресурсы операционной системы, так как не требует исполнения кода для выявления угроз. [13-14]

Исследование систем обнаружения и предотвращения вторжений

Системы обнаружения вторжений представляют собой программные, либо программно-аппаратные средства, позволяющие выявлять факт неавторизованного, несанкционированного доступа к устройству.

Архитектура систем обнаружения вторжений включает:

• сенсорную подсистему, которая предназначена для сбора входящего трафика, регистрации событий, связанных с безопасностью защищаемой системы

• подсистему анализа, которая предназначена для определения кибератак и подозрительных действий на основе поступающих данных от сенсорной подсистемы

• хранилище, в котором накапливаются и систематизируются первичные события и результаты анализа

• консоль управления, которая позволяет сконфигурировать систему обнаружения вторжений, наблюдать за состоянием защищаемой системы и просматривать выявленные подсистемой анализа инциденты.

Возможны следующие исполнения системы обнаружения вторжений: сетевая, основанная на протоколах связи, основанная на прикладных протоколах, узловая и гибридная. [15]

Для реализации анализа могут применяться различные технологии. Изначально для обеспечения защиты применялись простые политики. Например, при превышении определенного количества данных передача таких данных либо полностью останавливалась, либо нуждалась в дальнейшем подтверждении. Анализ сигнатур позволяет сравнивать данные, которые собраны сенсорами с имеющимися базами киберугроз. Анализ аномалий позволяет вычислять необычные действия без заранее созданных баз данных. Например, поведенческий анализ, который может определить отклонение от статистических метрик и количества действий, найти аномалии в самом трафике или протоколах связи.

Существуют различные способы обнаружения попыток вторжения в информационную инфраструктуру: сетевой трафик, активность портов, в данных, которые передаются по отслеживаемым протоколам, а также на конечных узлах. В зависимости от способа установки и технологии анализа системы обнаружения и предотвращения вторжений способны детектировать действия вредоносного программного обеспечения, использование ботнетов для атаки, попытки несанкционированного доступа к защищаемым данным, а также нарушение правил и политики безопасности.

Базы данных и наборы данных

Для предотвращения потери информации под действием кибератак широко используются SIEM-системы. Для разработки SIEM-системы используются различные типы существующих баз данных. Базами данных называют упорядоченные наборы структурированных данных. В компьютерных системах такие данные хранятся в электронном виде.

Для управления базами данных применяется инструмент - система управления базами данных (СУБД). В современных типах баз данных принято хранить данные в виде столбцов и строк, которые образуют таблицы. Применяя такой метод хранения данных, намного проще совершать над ними различные операции: добавлять, изменять, удалять, обновлять, отслеживать и систематизировать. При обращении к данным (для осуществления записи или выполнения запросов к таких данных) в большинстве современных баз данных используется язык SQL (структурированные запросы).

При выборе базы данных под разработку конкретной SIEM-системы очень важно учитывать с какими данными придется работать и как они будут использоваться, какая будет структура у таких данных. Таким образом, важно понимать какой тип баз данных будет использоваться.

Рассмотрим простейшие типы баз данных:

1. Простые структуры данных. Простым способом хранения данных являются текстовые файлы. Управлять разделением полей можно используя специальный символ: запятую, точку с запятой, двоеточие или пробел.

2. Иерархические базы данных. Основным отличием от простых структур является появление связей между объектами. Каждая запись, в такой структуре, имеет одного родителя и классифицируется в соответствии с тем, как она относится к родительской цепочке записей.

3. Сетевые базы данных. Записи таких баз данных могут иметь более одного родителя, что позволяет моделировать более сложные взаимосвязи.

4. Реляционные базы данных. Организация данных в реляционных базах представлена в виде таблиц, состоящих из столбцов и строк. Столбцы таблиц реляционных баз данных имеют имена и типы, а строки в свою очередь представлены отдельными записями, которые содержащат определенное значение для каждого из столбцов.

5. Базы данных NoSQL. Предназначены для работы в веб-приложениях реального времени и больших данных. Высокая доступность и масштабируемость являются основными преимуществами баз данных NoSQL.

6. Комбинированные базы данных. Разновидность баз совмещает в себе SQL- и NoSQL-подходы к организации хранения и обработки данных. Этот класс баз включает в себя NewSQL и многомодельные решения.

7. Объектно-ориентированные базы данных – базы данных, в которых информация представлена в виде объектов, как в объектно-ориентированных языках программирования.

8. Облачная база данных — это совокупность структурированных или неструктурированных данных, размещенных на частной, общедоступной или гибридной платформе облачных вычислений.

Набор данных или датасет — это коллекция данных, которая касается определенной темы или отрасли. Наборы данных включают различные типы информации: текст, изображения, видео и аудио, и могут храниться в различных форматах, таких, как CSV, JSON или SQL. [16]

Например, набор данных CICIDS2017 содержит безопасные и самые современные распространенные атаки. Включают результаты анализа сетевого трафика с использованием CICFlowMeter с маркировкой потоков. (файлы CSV). [17] А в наборе данных CSE-CIC-IDS2018 авторы используют понятие профилей для систематического создания наборов данных, которые будут содержать подробные описания вторжений и абстрактные модели распространения для приложений, протоколов или сетевых объектов более низкого уровня. Эти профили смогут использоваться агентами или операторами для генерации событий в сети. [18] Набор данных UNSW-NB 15 содержит девять типов атак, а именно: фаззеры, анализ, бэкдоры, DoS, эксплойты, общие, разведывательные, шеллкоды и черви. [19]

Заключение

В данной работе рассмотрены различные типы компьютерных угроз, а также методы их обнаружения, а также рассмотрены структуры баз данных, которые могут применяться при построении SIEM-систем. Рост требований скорости работы и производительности систем привел к увеличению количества типов баз данных. Перед началом создания SIEM-системы необходимо выбрать тип используемой базы данных, а для этого необходимо учитывать не только удобство хранения, но и скорость получения и использования данных. Используя связи нескольких баз данных, можно сохранить удобство хранения данных и их классификацию, а также высокую скорость получения больших объемов информации за счет предварительной индекса-

ции. Анализ существующих наборов данных кибератак позволяет обобщить их основные характеристики и использовать в дальнейших исследованиях. Важными составляющими методов обнаружения аномалий поведения информационных систем являются анализ последовательности действий всех процессов и классификация угроз по определенным характеристикам и признаками. Для повышения эффективности важно достижение оптимальных значений достоверности, точности и снижения времени принятия решений, что возможно лишь с применением глубокого машинного обучения. Одним из возможных путей решения проблемы обнаружения угроз - применение систематизации данных угроз, что позволит понять технологию обнаружения этих атак и разработать метод их обнаружения.

Литература

1. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646.

2. Хлопов О.А. Проблемы кибербезопасности и защиты критической информационной инфраструктуры. Political Sciences. The scientific heritage № 45, 2020.

3. Серёдкин С.П. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях. Информационные технологии и математическое моделирование в управлении сложными системами. Электрон. науч. журн. №4(16), 2022, с. 56-66.

4. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. /В. Ф. Шаньгин//, Москва: ДМК Пресс, 2012. – 592 с.

5. Путято М.М., Евглевский В.Ю., Макарян А.С., Володин И.В. Исследование механизмов социальной инженерии и анализ методов противодействия. Научные труды КубГТУ, 2021, № 2. С. 57-68.

6. Н.С. Афанасьева, Д.А. Елизаров, Т.А. Мызникова. Классификация фишинговых атак и меры противодействия им. Инженерный вестник Дона, №5, 2022.

7. Баженов А.С. Обзор DDoS атак на IoT устройства. Наука настоящего и будущего, 2019, С. 122-125.

8. Савченко Е.В., Ниссенбаум О.В. Ботнет-атаки на устройства интернета вещей. Математическое и информационное моделирование. Сборник научных трудов, электронный ресурс. Тюмень, 2018, С. 347-356.

9. Ручай А.Н., Токарев И.В., Грибачёв А.С. Методы машинного обучения и искусственного интеллектав сфере информационной безопасности: анализ современного состояния и перспективы развития. Вестник УрФО No 4(46), 2022, С. 76–87.

10. Грибачёв А.С., Кальщиков В.В. Исследование методов и алгоритмов обнаружения компьютерных инцидентов. Сборник трудов XXII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. Безопасность информационного пространства. Челябинск, 2024, С. 290-293.

11. Крейсат А., Гондал И., Вамплью П. и др. Обзор систем обнаружения вторжений: методы, наборы данных и проблемы. Кибербезопасность 2, 20, 2019.

12. Rafal Kozik, Michal Choraś, Rafal Renk, Witold Holubowicz. A Proposal of Algorithm for Web Applications Cyber Attack Detection. 13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM), Nov 2014, Ho Chi Minh City, Vietnam. pp.680-687.

13. Г. Ван, Дж. Хао, Дж. Ма и Л. Хуанг. Новый подход к обнаружению вторжений с использованием искусственных нейронных сетей и нечеткой кластеризации, Приложение Expert Syst,, т. 37, № 9, С. 6225-6232, 2010.

14. Методы обнаружения угроз. Электронный ресурс [https://cdn-download.drweb.com/pub/drweb/windows/server/12.0/documentation/html/ru/index.html?intro_detectionmethods.html]

15. Платонов В. Программно-аппаратные средства защиты информации. М.: Академия, 2013.

16. Нестеров С. А. Базы данных: учебник и практикум для вузов / С. А. Нестеров// Москва: Издательство Юрайт, 2024, — 258 с.

17. Набор данных. Электронный ресурс [https://www.unb.ca/cic/datasets/ids-2017.html]

18. Набор данных. Электронный ресурс [https://www.unb.ca/cic/datasets/ids-2018.html]

19. Набор данных. Электронный ресурс [https://research.unsw.edu.au/projects/unsw-nb15-dataset]

References

1. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. Ukaz Prezidenta Rossijskoj Federacii ot 5 dekabrya 2016 g. № 646.

2. Hlopov O.A. Problemy kiberbezopasnosti i zashchity kriticheskoj informacionnoj infrastruktury. Political Sciences. The scientific heritage № 45, 2020.

3. Seryodkin S.P. Osobennosti kiberatak na ob"ekty kriticheskoj informacionnoj infrastruktury v sovremennyh usloviyah. Informacionnye tekhnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami. Elektron. nauch. zhurn. №4(16), 2022, s. 56-66.

4. Shan'gin V. F. Zashchita informacii v komp'yuternyh sistemah i setyah. /V. F. Shan'gin//, Moskva: DMK Press, 2012. – 592 s.

5. Putyato M.M., Evglevskij V.Yu., Makaryan A.S., Volodin I.V. Issledovanie mekhanizmov social'noj inzhenerii i analiz metodov protivodejstviya. Nauchnye trudy KubGTU, 2021, № 2. S. 57-68.

6. N.S. Afanas'eva, D.A. Elizarov, T.A. Myznikova. Klassifikaciya fishingovyh atak i mery protivodejstviya im. Inzhenernyj vestnik Dona, №5, 2022.

7. Bazhenov A.S. Obzor DDoS atak na IoT ustrojstva. Nauka nastoyashchego i budushchego, 2019, S. 122-125.

8. Savchenko E.V., Nissenbaum O.V. Botnet-ataki na ustrojstva interneta veshchej. Matematicheskoe i informacionnoe modelirovanie. Sbornik nauchnyh trudov, elektronnyj resurs. Tyumen', 2018, S. 347-356.

9. Ruchaj A.N., Tokarev I.V., Gribachyov A.S. Metody mashinnogo obucheniya i iskusstvennogo intellektav sfere informacionnoj bezopasnosti: analiz sovremennogo sostoyaniya i perspektivy razvitiya. Vestnik UrFO No 4(46), 2022, S. 76–87.

10. Gribachyov A.S., Kal'shchikov V.V. Issledovanie metodov i algoritmov obnaruzheniya komp'yuternyh incidentov. Sbornik trudov XXII Vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molodyh uchyonyh. Bezopasnost' informacionnogo prostranstva. Chelyabinsk, 2024, S. 290-293.

11. Krejsat A., Gondal I., Vampl'yu P. i dr. Obzor sistem obnaruzheniya vtorzhenij: metody, nabory dannyh i problemy. Kiberbezopasnost' 2, 20, 2019.

12. Rafal Kozik, Michal Choraś, Rafal Renk, Witold Holubowicz. A Proposal of Algorithm for Web Applications Cyber Attack Detection. 13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM), Nov 2014, Ho Chi Minh City, Vietnam. pp.680-687.

13. G. Van, Dzh. Hao, Dzh. Ma i L. Huang. Novyj podhod k obnaruzheniyu vtorzhenij s ispol'zovaniem iskusstvennyh nejronnyh setej i nechetkoj klasterizacii, Prilozhenie Expert Syst,, t. 37, № 9, S. 6225-6232, 2010.

14. Metody obnaruzheniya ugroz. Elektronnyj resurs [https://cdn-download.drweb.com/pub/drweb/windows/server/12.0/documentation/html/ru/index.html?intro_detectionmethods.html]

15. Platonov V. Programmno-apparatnye sredstva zashchity informacii. M.: Akademiya, 2013.

16. Nesterov S. A. Bazy dannyh: uchebnik i praktikum dlya vuzov / S. A. Nesterov// Moskva: Izdatel'stvo Yurajt, 2024, — 258 s.

17. Nabor dannyh. Elektronnyj resurs [https://www.unb.ca/cic/datasets/ids-2017.html]

18. Nabor dannyh. Elektronnyj resurs [https://www.unb.ca/cic/datasets/ids-2018.html]

19. Nabor dannyh. Elektronnyj resurs [https://research.unsw.edu.au/projects/unsw-nb15-dataset]

ГРИБАЧЁВ Антон Сергеевич, аспирант (соискатель) математического факультета, Челябинский государственный университет. 454001, Челябинск, ул. Братьев Кашириных, 129. E-mail: a.gribachev@yandex.ru.

GRIBACHEV Anton Сергеевич, PhD candidate of the Faculty of Mathematics, Chelyabinsk State University. 454001, Chelyabinsk, st. Brothers Kashirinykh, 129. E-mail: a.gribachev@yandex.ru.

КАЛЬЩИКОВ Всеволод Владимирович, аспирант (соискатель) математического факультета, Челябинский государственный университет. 454001, Челябинск, ул. Братьев Кашириных, 129. E-mail: vkalschikov@gmail.com.

KALSHCHIKOV Vsevolod Vladimirovich, PhD candidate of the Faculty of Mathematics, Chelyabinsk State University. 454001, Chelyabinsk, st. Brothers Kashirinykh, 129. E-mail: vkalschikov@gmail.com

РУЧАЙ Алексей Николаевич, кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры, Челябинский государственный университет. 454001, Челябинск, ул. Братьев Кашириных, 129; доцент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ran@csu.ru.

RUCHAY Alexey Nikolaevich, PhD in Physics and Mathematics, Associate Professor, Head of the Department of Computer Security and Applied Algebra, Chelyabinsk State University. 454001, Chelyabinsk, st. Brothers Kashirinykh, 129.; Associate Professor, Department of Information Security, South Ural State University (National Research University), Chelyabinsk, 454080, Chelyabinsk, Lenina avenue, 76. E-mail: ran@csu.ru.

УДК 004.056.2 Вестник УрФО № 1(51) / 2024, с. 53–59

Плаван А.И.

DOI: 10.14529/secur240107

МЕТОД ВЫЯВЛЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ НА ОСНОВЕ ФИЛЬТРА КОЛМОГОРОВА-ВИНЕРА

В данной работе исследуется возможность применения оптимального линейного фильтра Колмогорова-Винера для задачи обнаружения аномалий в трафике. Метод основывается на возможности вычисления минимальной среднеквадратической ошибки фильтрации случайных процессов с известными автокорреляционными функциями.

Рассматриваются существующие статистические методы обнаружения аномалий, включая кибератаки, в сетевом трафике и предлагается новый метод обнаружения аномалий на основе среднеквадратической ошибки фильтрации.

Для оценки метода обнаружения аномалий используются записи трафика MAWI WIDE, строятся графики ROC-кривой и кривой Precision-Recall (точности-полноты) при различных пороговых значениях.

Продемонстрировано, что среднее значение метрики площади под кривой (AUC), равное 0,6 слишком мало для эффективного обнаружения аномалий в сетевом трафике и не позволяет использовать предложенный метод самостоятельно.

Предложено использовать числовые значения среднеквадратической ошибки фильтрации, получаемые в результате работы метода, в качестве дополнительного признака для повышения эффективности других методов на основе машинного обучения.

Ключевые слова: *обнаружение аномалий, сетевой трафик, фильтрация трафика, классификация трафика, среднеквадратическая ошибка, ROC-кривая, фильтр Колмогорова-Винера.*

Plavan A.I.

A METHOD FOR ANOMALY DETECTION IN NETWORK TRAFFIC BASED ON THE KOLMOGOROV-WIENER FILTER

This paper investigates the possibility of applying the optimal linear Kolmogorov-Wiener filter to the problem of anomaly detection in network traffic. The method is based on the capability of computing the minimum mean square error to filter random processes with known autocorrelation functions.

The existing statistical methods for detecting anomalies, including cyberattacks, in network traffic are reviewed and a new anomaly detection method based on mean square filtering error is proposed.

MAWI WIDE traffic records are used to evaluate the anomaly detection method, and the ROC and Precision-Recall curves are plotted at different threshold values.

It is demonstrated that the average value of the area under curve (AUC) metric of 0.6 is too small to effectively detect anomalies in network traffic and does not allow the proposed method to be used on its own.

It is suggested that the numerical values of mean square error obtained as a result of method execution can be used as an additional feature to improve the efficiency of other machine learning-based methods, which is to be further verified.

Keywords: *anomaly detection, network traffic, traffic filtering, traffic classification, MSE, ROC curve, Wiener filter.*

Введение

В современном информационном обществе сетевые технологии стали неотъемлемой частью повседневной жизни, обеспечивая передачу данных и обмен информацией на глобальном уровне. Однако с ростом зависимости от цифровых технологий также возрастает и риск кибератак, направленных на нарушение конфиденциальности, целостности и доступности данных. В этом контексте обеспечение безопасности сетей и выявление вторжений в сетевом трафике становятся критическими задачами. Одним из ключевых методов выявления вторжений является анализ сетевого трафика с использованием различных алгоритмов и техник.

Зачастую злоумышленники используют сеть в качестве транспорта для доставки вредоносных программ до целевой системы или для доступа к конфиденциальным данным, расположенным на недостаточно защищенных сетевых ресурсах. Один из принципов, на которых основаны системы обнаружения вторжений и другие средства защиты информации, состоит в том, что получить доступ к сетевому ресурсу невозможно, не повлияв на трафик в сети, то есть, не установив соединение с некоторым сервером и не послав пакеты с некоторыми данными. Возникновение нового источника трафика приводит к изменению общего состояния и значений статистических характеристик сети. Необычный трафик также может быть вызван ошибками в настройках сетевого оборудования. Такой трафик называется аномальным, или просто аномалией.

Обнаружение аномалий применяется не только в задачах выявления вредоносного трафика, но и во многих других областях, например, выявление мошенничества в банках. Методы, используемые при этом, можно разделить на две группы: обнаружение злоупотреблений (специфичных сигнатур) или обнаружений аномалий [1]. Основным преимуществом второй группы является то, что такие методы могут обнаруживать ранее неизвестные атаки. К таким методам относятся: классификация k-средних, метод главных компонент, метод «случайного леса» на основе ансамбля решающих деревьев и другие методы машинного обучения и нейронных сетей [2–4].

Целью данной статьи является исследование потенциала среднеквадратической ошибки фильтрации как признака наличия аномалий, включая кибератаки, в сетевом трафике.

Обзор литературы

Существует несколько уровней, на которых можно выполнять классификацию данных с целью обнаружения аномалий в трафике: на уровне отдельных пакетов, потоков (однонаправленных или двунаправленных), сетевых интерфейсов или всего трафика в целом [5].

Предварительно трафик необходимо специальным образом подготовить, разбив на набор наблюдений, которые и будет классифицированы. Обычно выделяют наборы сетевых потоков, идентифицируемых по следующим признакам [6]: IP-адрес отправителя, IP-адрес получателя, Порт отправителя, Порт получателя, Идентификатор протокола (опционально).

В работе [3] предлагается метод на основе классификации отдельных HTTP запросов с использованием гибридной нейронной сети для применения на уровне WAF (Web Application Firewall).

Для применения статистических методов требуется объем данных достаточного разме-

ра, чтобы выявить статистические закономерности. Объем сетевых потоков, измеряемый в количестве пакетов, может быть недостаточным для этой цели. Например в [7] было выявлено, что типичная длина TCP-потока составляет 122 пакета. Более предпочтительным является рассмотрение срезов общего трафика (пакетов всех потоков) за определенный интервал времени.

Известно, что сетевой трафик обладает свойством самоподобия, или фрактальности [8]. Этим свойством обладают как интервалы времени между поступлениями пакетов (inter-arrival times), так и суммарное количество пакетов или байт в единицу времени [9]. Самоподобие предполагает наличие автокорреляционной функции (АКФ) определенного вида. Соответственно, можно предположить, что ожидаемый трафик некоторой сети в определенное время суток может быть охарактеризован АКФ конкретного вида. Знание об этих закономерностях сетевого трафика должно учитываться при разработке новых способов обнаружения аномалий и атак для повышения их эффективности.

В [10] приводится обзор существующих подходов к обнаружению сетевых аномалий на основе методов фрактального и мультифрактального анализа, исходя из того, что сетевой трафик проявляет фрактальные свойства и может быть охарактеризован некоторыми значениями показателя Херста. При возникновении аномалии значения показателя Херста и фрактальной размерности могут отклоняться от ожидаемого.

В работе [11] предлагается метод на основе корреляции между значениями переменных MIB (Management Information Base) протокола SNMP. В течение периода обучения записывается матрица корреляции в каждый момент времени. Для обнаружения аномалий используется значение нормализованной минимальной среднеквадратической ошибки (СКО) фильтра Колмогорова-Винера, называемого также фильтром Винера. Пороговые значения индикатора вычисляются из собственных векторов корреляционной матрицы при нормальном режиме работы сети. Превышение этих значений СКО является признаком наличия аномалий в трафике.

В [12] также предлагается использовать метод на основе среднеквадратической ошибки (СКО) фильтрации, но применительно к последовательности интервалов времени между поступлениями пакетов. Значение импульсной характеристики фильтра может быть не оптимальным, и в этом случае ошибка будет отлична от нуля. Для случая оптимального фильтра ошибка должна быть равна нулю. Индикатором аномалии служит отклонение значения СКО от эталонного значения, полученного в течение периода обучения. Также в работе предлагается упрощенный вариант метода, основанный на сравнении корреляционных функций эталонного и текущего трафика в точке $\tau = 0$, но и в точке $\tau = \tau_0$, соответствующей интервалу корреляции.

В данной работе исследуется возможность применения оптимального линейного фильтра Винера для задачи обнаружения аномалий в трафике. При этом также учитывается «шум» наблюдений нормального трафика, вызванный изменениями в загрузке сети, значений MTU (maximum transmission unit, максимальный размер полезной нагрузки пакета), использованием альтернативных путей между отправителем и получателем и т.д.

Методология

Сетевой трафик, выражаемый в виде интервалов времени между поступлением пакетов, или количества пакетов или байт в единицу времени можно представить в виде случайной последовательности

$$x_k = \xi_k + \eta_k \quad k \in \{1,\ldots,N\},$$

где ξ_k – нормальный трафик, η_k – шум (случайная составляющая временного ряда), N – количество отсчетов.

Шум можно оценить с использованием одного из методов, рассмотренных в работе [13]. В данной работе шум будет рассматриваться как некоррелированный гауссовский процесс с оцениваемой дисперсией.

Фильтр Винера, позволяет получить оптимальную по критерию СКО оценку стационарного сигнала по аддитивной смеси полезного сигнала с шумом. При этом неизбежно возникает ошибка оценивания (фильтрации), которая определяется как

$$\varepsilon = \frac{1}{N}\sum_{k=1}^{N}\left(\hat{\xi}_k - \xi_k\right)^2,$$

где $\hat{\xi}_k$ – оценка k – го отсчёта нормального трафика.

Выражение для вычисления импульсной переходной функции $\mathbf{h} = \{h_1, h_2, \ldots, h_M\}$ фильтра Винера с порядком M в матричной форме выглядит следующим образом [14]

$$\mathbf{h} = \mathbf{B}_{\mathbf{x}}^{-1} \cdot \mathbf{b}_{\mathbf{x}\xi},$$

где $\mathbf{b}_{\mathbf{x}^{\xi}}$ – вектор взаимной корреляции между входным и ожидаемым полезным сигналом, представляющим нормальный трафик,

$$\mathbf{b}_{\mathbf{x}^{\xi}} = \left\{B_{x\xi}(0), B_{x\xi}(1), \ldots, B_{x\xi}(M)\right\},$$

здесь $B_{x\xi}(m)$ – корреляция значений отсчётов сигнала на входе фильтра и отсчётов сигнала, представляющего нормальный трафик,

$$B_{x\xi}(m) = E\left[(x_k - E[x])(\xi_{k+m} - E[\xi])\right],$$

$\mathbf{B}_{\mathbf{x}}$ – корреляционная матрица входного сигнала

$$\begin{pmatrix} B_x(0) & B_x(1) & \cdots & B_x(M) \\ B_x(1) & B_x(0) & \cdots & B_x(M-1) \\ \vdots & \vdots & \ddots & \vdots \\ B_x(M) & B_x(M-1) & \cdots & B_x(0) \end{pmatrix}.$$

При этом минимальная СКО фильтра записывается в виде

$$\varepsilon^2_{\min} = \boldsymbol{\sigma}^2_{\boldsymbol{\xi}} - \mathbf{h}^{\mathbf{T}} \cdot \mathbf{B}_{\mathbf{x}} \cdot \mathbf{h},$$

или (без использования импульсной переходной функции [14])

$$\varepsilon^2_{\min} = \boldsymbol{\sigma}^2_{\boldsymbol{\xi}} - \mathbf{b}^{\mathbf{T}}_{\mathbf{x}} \cdot \mathbf{B}^{-1}_{\mathbf{x}\boldsymbol{\xi}} \cdot \mathbf{b}_{\mathbf{x}\boldsymbol{\xi}}.$$

При дисперсии шума, близкой к нулю, минимальная СКО фильтра Винера тоже будет стремится к нулю. В случае отсутствия шума как такового, минимальная СКО будет равна нулю, но и сам фильтр при этом будет пропускать сигнал на входе без изменений, то есть фильтрация не будет производится. Импульсная характеристика фильтра в данном случае будет выглядеть как единичный импульс [15, 16], т.е.

$$\lim_{\sigma^2_{\eta} \to 0} \varepsilon^2_{min} = 0,$$

где σ^2_{η} – дисперсия шума.

Во время периода обучения производятся наблюдения нормального трафика. Трафик разбивается на интервалы, в течение которых он сохраняет стационарность. Будем считать, что в течение определенного времени суток трафик остается стационарным. Для каждого интервала определяется АКФ и дисперсия трафика. На основе этих характеристик синтезируется оптимальный линейный фильтр и определяется его минимальная СКО. Для определения аномалий, к трафику, наблюдаемому на текущем временном интервале, применяется соответствующий фильтр. Для сигнала на выходе фильтра вычисляется СКО и сравнивается с минимальным значением СКО для фильтра. Отклонение значения ошибки фильтрации от порогового значения служит признаком аномалии.

Для определения пороговых значений возможно использовать значение СКО, нормализованное относительно дисперсии нормального трафика [14]

$$m^2_{min} = 1 - \frac{\hat{\sigma}^2_{\xi}}{\sigma^2_{\xi}},$$

где $\hat{\sigma}^2_{\xi}$ – дисперсия оценки сигнала на выходе фильтра, σ^2_{ξ} – дисперсия ожидаемого сигнала, соответствующего нормальному трафику.

Таким образом задается верхняя граница допустимых значений, равная единице. Нижней границей является нормализованное значение минимальной СКО

$$m^2_{min} = \frac{\varepsilon^2_{min}}{\sigma^2_{\xi}}.$$

Преобразовав вычисленное для текущего трафика значение СКО из диапазона значений $\left[m^2_{min}\right]$ к диапазону [0, 1]

$$m^2_{norm} = \frac{m^2 - \varepsilon^2_{min}}{1 - \varepsilon^2_{min}},$$

и изменяя пороговое значение δ между 0 и 1, можно влиять на чувствительность классификатора и вероятность ложноположительных срабатываний. Таким образом, формулу для индикатора аномалий можно записать как:

$$m^2_{norm} = \begin{cases} > 1 & - \text{ аномалия} \\ \leq \delta & - \text{ нет аномалии} \\ < m^2_{min} & - \text{ аномалия} \end{cases}. \quad (1)$$

Результаты

Метод был проверен на наборе 15-минутных записей сетевого трафика из архива MAWI WIDE, собранного с 11 по 17 октября 2021 года. Трафик был разбит на минутные интервалы, каждый из которых рассматривался отдельно. Каждому интервалу была присвоена метка аномальности на основе того, присутствуют ли на этом интервале аномалии в исходном датасете. Аномальными были признаны 64 из 105 (60%) интервалов, то есть датасет является практически сбалансированным.

На записях трафика, собранных в один день, производилось «обучение модели» (синтез фильтров для каждого минутного интервала). Можно сказать, что для каждой минуты использовалась своя собственная модель. Шум считался гауссовским с дисперсией = σ^2_{ξ}. Для каждой соответствующей минутной записи за другие дни было вычислено значение индикатора по формуле (1). По ним были построены графики ROC-кривой и кривой Precision-Recall (точности-полноты) при различных значениях порогового значения δ, которые представлены на рис. 1.

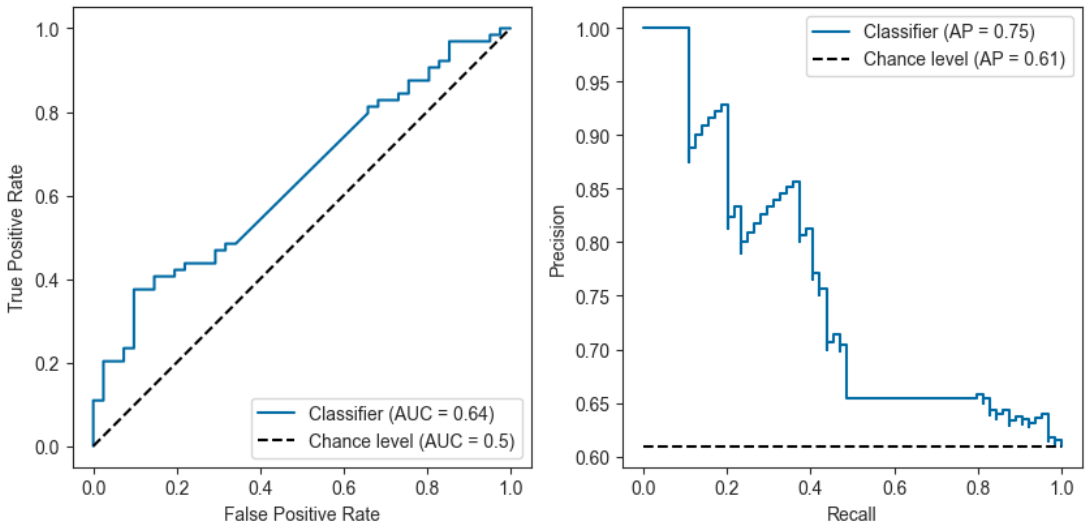


Рис. 1. Графики ROC-кривой и кривой Precision-Recall. Classifier – значения для предлагаемого метода, Chance level – значения для слепого угадывания, AUC – площадь под кривой, AP – средняя точность.

Обсуждение

ROC-кривая, или кривая рабочей характеристики приемника, первоначально появилась в теории обнаружении сигналов и использовалась для наглядной иллюстрации связи между относительным количеством правильных попаданий (детектировании сигнала при наличии шума) и ложных тревог (детектировании сигнала при его отсутствии). Аналогичным образом, ROC-кривая применяется для иллюстрации чувствительности бинарных классификаторов.

Классификатор с высокой точностью, но низким показателем полноты будет обнаруживать мало аномалий, но большинство предсказанных ей меток аномальности будут верными. Модель с высоким показателем полноты и низкой точностью наоборот будет отмечать много аномальных результатов, но при этом многие результаты будут ложноположительными. Это должно учитываться при выборе порогового значения δ.

Стоит отметить, что внешний вид графиков отличается в зависимости от того, для трафика какого дня производилось обучение. Но во всех случаях метрика площади под кривой (AUC) составляет около 0,6. Это говорит о том, что метод обладает предсказательной способностью, пусть и не очень высокой. Более того, при использовании методов машинного обучения обычно рассматривается несколько признаков [2, 3] в совокупности, здесь же рассматривается всего один. Можно предположить, что производительность существующих методов машинного обучения можно улучшить, добавив этот новый признак на основе минимальной СКО.

Также стоит отметить, что в случаях, когда обучение производилось для записей трафика, собранных в выходные дни (16 и 17 октября), метрика AUC оказывалась даже меньше 0,5. Это может говорить о том, что в выходные дни корреляционная структура трафика меняется (трафик не является стационарным), и для таких периодов необходимо использовать отдельные модели.

Вывод

В данной работе был предложен новый метод обнаружения аномалий в сетевом трафике на основе фильтра Колмогорова-Винера. Метод заключается в вычислении импульсной характеристики и минимальной СКО фильтра для последовательностей интервалов между поступлениями пакетов. Для каждого временного интервала, на котором эти интервалы сохраняют стационарность, вычисляется свой фильтр. Затем фильтр применяется к текущему трафику, полученная СКО нормируется и сравнивается с пороговым значением.

Полученное значение AUC не позволяет использовать данный метод для обнаружения аномалий самостоятельно, но, предположительно, получаемые значения могут быть использованы в качестве дополнительного признака для повышения эффективности других методов на основе машинного обучения.

Литература

1. Шелухин О.И. Обнаружение вторжений в компьютерные сети [сетевые аномалии] / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – М.: Горячая линия-Телеком, 2018. – 220 с.

2. Обзор методов обнаружения аномалий в потоках данных / В.П. Шкодырев [и др.] // Second Conference on Software Engineering and Information Management (SEIM-2017). – Санкт-Петербург, 2017. – С. 50

3. Методика раннего обнаружения компьютерных атак в сетевом трафике сети передачи данных / О.С. Лаута [и др.] // Сборник научных статей по материалам IV Всероссийской научно-технической конференции «Безопасность информационных технологий». – Пенза: ПГУ, 3 апреля 2022 г. – Т. 1. – С. 126

4. Дик Д.И. Обнаружение аномалий пользовательских сеансов веб-приложений с использованием рекуррентных нейронных сетей / Д.И. Дик, В.В. Москвин // Материалы II национальной научной конференции. Отв. редактор Е.Н. Полякова. НАУКА XXI ВЕКА: ТЕХНОЛОГИИ, УПРАВЛЕНИЕ, БЕЗОПАСНОСТЬ. – Курган: Курганский государственный университет, 21 апреля 2022 г. – С. 55-61

5. MAWILab: combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking / R. Fontugne [и др.] // Proceedings of the 6th International Conference Co-NEXT '10: Conference on emerging Networking Experiments and Technologies. – Philadelphia Pennsylvania: ACM, 2010. – MAWILab. – С. 1-12, DOI: https://doi.org/10.1145/1921168.1921179

6. Волков Д. Энтропия и выявление аномалий сетевого трафика [электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/neoflex/articles/561438/ (дата обращения: 05.08.2023)

7. Jurkiewicz P. Flow length and size distributions in campus Internet traffic / P. Jurkiewicz, G. Rzym, P. Boryło // Computer Communications. – 2021. – Т. 167. – С. 15-30, DOI: https://doi.org/10.1016/j.comcom.2020.12.016

8. On the self-similar nature of Ethernet traffic / W.E. Leland [и др.] // Conference proceedings on Communications architectures, protocols and applications. – 1993. – С. 183-193

9. Плаван А.И. Моделирование самоподобного трафика с использованием модели Poisson-Pareto-Burst-Process в симуляторе ns-3 / А.И. Плаван // XXVII Международная научно-техническая конференция «Современные средства связи». – Минск, Республика Беларусь: Белорусская государственная академия связи, 27–28 октября 2022 г. – С. 197-199

10. Басараб М.А. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа / М.А. Басараб, И.С. Строганов // Вопросы кибербезопасности. – 2014. – № 4 (7). – С. 30-40

11. Al-Kasassbeh M. Network intrusion detection with wiener filter-based agent / M. Al-Kasassbeh // World Appl. Sci. J. – 2011. – Т. 13. – № 11. – С. 2372-2384

12. Карташевский В.Г. Фильтрация наблюдаемого трафика как способ обнаружения вторжений / В.Г. Карташевский, И.С. Поздняк // Вестник УрФО. – 2019. – Т. 19. – № 1 (31). – С. 17-22, DOI: https://doi.org/10.14529/secur190103

13. Копырин А.С. Технологии обработки и очистки данных, выявления и устранения шумов на временном ряду / А.С. Копырин, Е.В. Видищева // Вестник Академии знаний. – 2020. – № 4 (39). – С. 220-228

14. Haykin S.S. Adaptive filter theory / S.S. Haykin. – 4th ed. – Upper Saddle River, N.J: Prentice Hall, 2002. – 920 с.

15. Плаван А.И. Выявление аномалий в сетевом трафике по критерию среднеквадратической ошибки фильтрации линейного преобразования / А.И. Плаван, И.С. Поздняк // VII Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности». – Таганрог: Южный федеральный университет, 5–11 апреля 2021 г. – С. 70-74

16. Плаван А.И. Среднеквадратическая ошибка фильтрации как критерий обнаружения аномалий сетевого трафика / А.И. Плаван, В.Г. Карташевский // Вестник Российского нового университета. Серия: Сложные системы модели, анализ и управление. – 2023. – № 1. – С. 94-101, DOI: https://doi.org/10.18137/RNU.V9187.23.01.P.94

References

1. Shelukhin O.I. Obnaruzhenie vtorzheniy v komp'yuternye seti [setevye anomalii] / O.I. Shelukhin, D.Zh. Sakalema, A.S. Filinova. – M.: Goryachaya liniya-Telekom, 2018. – 220 s.

2. Obzor metodov obnaruzheniya anomaliy v potokakh dannykh / V.P. Shkodyrev [et al.] // Second Conference on Software Engineering and Information Management (SEIM-2017). – Sankt-Peterburg, 2017. – S. 50

3. Metodika rannego obnaruzheniya komp'yuternykh atak v setevom trafike seti peredachi dannykh / O.S. Lauta [et al.] // Sbornik nauchnykh statey po materialam IV Vserossiyskoy nauchno-tekhnicheskoy konferentsii «Bezopasnost' informatsionnykh tekhnologiy». – Penza: PGU, 3 aprelya 2022 g. – T. 1. – S. 126

4. Dik D.I. Obnaruzhenie anomaliy pol'zovatel'skikh seansov veb-prilozheniy s ispol'zovaniem rekurrentnykh neyronnykh setey / D.I. Dik, V.V. Moskvin // Materialy II natsional'noy nauchnoy konferentsii. Otv. redaktor E.N. Polyakova. NAUKA XXI VEKA: TEKhNOLOGII, UPRAVLENIE, BEZOPASNOST". – Kurgan: Kurganskiy gosudarstvennyy universitet, 21 aprelya 2022 g. – S. 55-61

5. MAWILab: combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking / R. Fontugne [et al.] // Proceedings of the 6th International Conference Co-NEXT '10: Conference on emerging Networking Experiments and Technologies. – Philadelphia Pennsylvania: ACM, 2010. – MAWILab. – S. 1-12, DOI: https://doi.org/10.1145/1921168.1921179

6. Volkov D. Entropiya i vyyavlenie anomaliy setevogo trafika [elektronnyy resurs]. – Rezhim dostupa: https://habr.com/ru/companies/neoflex/articles/561438/ (data obrashcheniya: 05.08.2023)

7. Jurkiewicz P. Flow length and size distributions in campus Internet traffic / P. Jurkiewicz, G. Rzym, P. Boryło // Computer Communications. – 2021. – T. 167. – S. 15-30, DOI: https://doi.org/10.1016/j.comcom.2020.12.016

8. On the self-similar nature of Ethernet traffic / W.E. Leland [et al.] // Conference proceedings on Communications architectures, protocols and applications. – 1993. – S. 183-193

9. Plavan A.I. Modelirovanie samopodobnogo trafika s ispol'zovaniem modeli Poisson-Pareto-Burst-Process v simulyatore ns-3 / A.I. Plavan // XXVII Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya «Sovremennye sredstva svyazi». – Minsk, Respublika Belarus': Belorusskaya gosudarstvennaya akademiya svyazi, 27–28 oktyabrya 2022 g. – S. 197-199

10. Basarab M.A. Obnaruzhenie anomaliy v informatsionnykh protsessakh na osnove mul'tifraktal'nogo analiza / M.A. Basarab, I.S. Stroganov // Voprosy kiberbezopasnosti. – 2014. – № 4 (7). – S. 30-40

11. Al-Kasassbeh M. Network intrusion detection with wiener filter-based agent / M. Al-Kasassbeh // World Appl. Sci. J. – 2011. – T. 13. – № 11. – S. 2372-2384

12. Kartashevskiy V.G. Fil'tratsiya nablyudaemogo trafika kak sposob obnaruzheniya vtorzheniy / V.G. Kartashevskiy, I.S. Pozdnyak // Vestnik UrFO. – 2019. – T. 19. – № 1 (31). – S. 17-22, DOI: https://doi.org/10.14529/secur190103

13. Kopyrin A.S. Tekhnologii obrabotki i ochistki dannykh, vyyavleniya i ustraneniya shumov na vremennom ryadu / A.S. Kopyrin, E.V. Vidishcheva // Vestnik Akademii znaniy. – 2020. – № 4 (39). – S. 220-228

14. Haykin S.S. Adaptive filter theory / S.S. Haykin. – 4th ed. – Upper Saddle River, N.J: Prentice Hall, 2002. – 920 s.

15. Plavan A.I. Vyyavlenie anomaliy v setevom trafike po kriteriyu srednekvadraticheskoy oshibki fil'tratsii lineynogo preobrazovaniya / A.I. Plavan, I.S. Pozdnyak // VII Vserossiyskaya nauchno-tekhnicheskaya konferentsiya «Fundamental'nye i prikladnye aspekty komp'yuternykh tekhnologiy i informatsionnoy bezopasnosti». – Taganrog: Yuzhnyy federal'nyy universitet, 5–11 aprelya 2021 g. – S. 70-74

16. Plavan A.I. Srednekvadraticheskaya oshibka fil'tratsii kak kriteriy obnaruzheniya anomaliy setevogo trafika / A.I. Plavan, V.G. Kartashevskiy // Vestnik Rossiyskogo novogo universiteta. Seriya: Slozhnye sistemy modeli, analiz i upravlenie. – 2023. – № 1. – S. 94-101, DOI: https://doi.org/10.18137/RNU.V9187.23.01.P.94

ПЛАВАН Алексей Игоревич, аспирант кафедры информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики». 443010, г. Самара, ул. Л. Толстого, д. 23. E-mail: aleksej-plavan@ya.ru

PLAVAN Aleksey Igorevich, Postgraduate student of the Department of Information Securityof the Federal State Budgetary Educational Institution of Higher Education "Povolzhskiy State University of Telecommunications and Informatics". 443010, Samara, L. Tolstoy str., 23. E-mail: aleksej-plavan@ya.ru

УДК 004.056.5 Вестник УрФО № 1(51) / 2024, с. 60–65

Кузьмина У.В., Михайлова О.Е., Афанасьев Ю.П. DOI: 10.14529/secur240108

РАЗРАБОТКА МОДУЛЯ КИБЕРПОЛИГОНА ДЛЯ ЗАЩИТЫ ВЕБ-СЕРВИСОВ ОТ АТАК НА ОСНОВЕ НЕЙРОСЕТИ

В данной статье разрабатывается модуль киберполигона для защиты веб-сервисов от атак на основе нейросетей. Этот модуль анализирует входящий HTTP-трафик для выявления пакетов, содержащих аномалии и попытки атак, далее генерирует предупреждение, которое заносится в логи и отправляется администратору сети. Также был разработан модуль для построения виртуальных сетевых лабораторий, что позволит исследователям и инженерам создавать, тестировать и анализировать как новые, так и старые методы защиты в контролируемых условиях.

Ключевые слова: *информационная безопасность, киберполигон, нейросети, веб-сервисы, фаервол.*

Kuzmina U.V., Mikhaylova O.E., Afanasyev Yu.P.

DEVELOPMENT OF A CYBERPOLYGON MODULE TO PROTECT WEB SERVICES FROM ATTACKS BASED ON A NEURAL NETWORK

In this article, a cyberpolygon module is being developed to protect web services from attacks based on neural networks. This module analyzes incoming HTTP traffic to identify packets containing anomalies and attack attempts, then generates a warning that is logged and sent to the network administrator. A module has also been developed for building virtual network laboratories, which will allow researchers and engineers to create, test and analyze both new and old protection methods in controlled conditions.

Keywords: *information security, cyberpolygon, neural networks, web services, firewall.*

Введение

В настоящее время широко применяют киберполигоны для моделирования сетевой инфраструктуры предприятия и ее тестирования на проникновения. Также киберполигоны могут использоваться для обучения правильного построения сетей, методологий атак и тактик защиты.

Задачей модуля киберполигона является полноценная имитация сети и составляющих ее устройств. В возможности полигона входят создание виртуальных машин на основе имеющихся шаблонов, создание новых шаблонов, построение связей между машинами и сохранение построенной сети с возможностью быстрой загрузки [1].

На текущий момент существуют и эксплуатируются полигоны Минкомсвязи России, Ernst & Young, Cyberbit Range, Cyber Range Hub, Cybersecurity Nexus (CSX). К основным минусам можно отнести необходимость в поддержании работы большого кол-ва реального оборудования, ограниченность сценариев атаки и защиты, сложность в масштабировании и реализации новой инфраструктуры и сценариев.

Популярность веб-приложений постоянно растет, поскольку с их помощью предприятия и корпорации размещают множество своих сервисов. Однако, организации попрежнему сталкиваются с уязвимостями в веб-приложениях. Для защиты веб-приложений используются различные инструменты, например WAF (Web Application Firewall), а также методологии по написанию безопасного кода и обработки входных данных.

Российский рынок Web Application Firewall, как и многие другие сферы, находится в периоде турбулентности. Изменения, вызванные уходом зарубежных поставщиков, ещё не закончились: отечественные вендоры активно осваивают освободившиеся пространства и развивают функциональные возможности своих систем, чтобы удовлетворить ожидания новых заказчиков. При этом значительная часть потенциальных клиентов вообще не использует WAF, предпочитая, очевидно, универсальные решения, такие как NGFW. Мысль о необходимости специализированной защиты веб-трафика зачастую приходит к таким компаниям слишком поздно — уже после взлома.

Однако не все атаки и уязвимости возможно исключить благодаря этим методам и инструментам. Зачастую требуется анализ специалистом информационной безопасности. Однако, обрабатывать весь объем входящих данных является затруднительной задачей.

Задачей модуля для защиты является защита веб-сервисов от типовых атак на веб-приложения и предупреждение администратора веб-сервиса. Модуль должен перехватывать HTTP-пакеты и анализировать с помощью нейросети на наличие вредоносных нагрузок и нетипичное содержание и структуру HTTP-пакетов. При обнаружении таких нагрузок модуль генерирует предупреждение, которое заносится в логи и отправляется администратору сети [2].

Перед началом разработки программной части модуля для построения виртуальных сетевых лабораторий были выдвинуты следующие требования к функционалу:

1. Возможность быстро развернуть приложение с модулем.

2. Поддержка создания пользовательских виртуальных машин в среде построения лаборатории.

3. Создание виртуальных сетевых интерфейсов у машин.

4. Создание изолированных виртуальных сетей для объединения виртуальных интерфейсов машин.

5. Удаленное подключение к виртуальным машинам.

6. Настройка виртуальных машин (ограничение используемой оперативной памяти и процессорного времени).

7. Сохранение конфигураций лабораторий, виртуальных сетей и машин.

8. Возможность создавать лаборатории с предустановленной конфигурацией сети и машин.

9. Наличие графического интерфейса для управления лабораторией.

Для реализации модуля построения виртуальных сетевых лабораторий с учетом описанных требований использовались следующие технологии и подходы:

• Контейнеризация - для изоляции процессов и ресурсов виртуальных машин друг от друга и хост-системы, а также для обеспечения быстрого развёртывания [3].

• Виртуализация устройств – для работы виртуальных машины выбрана система QEMU/KVM. Эта система позволяет эмулировать работу большинства устройств и операционных систем. Также некоторые устройства и операционные системы могут обрабатываться QEMU/KVM напрямую средствами рабочего контейнера, что увеличивает производительность [4].

• Виртуальные сетевые адаптеры – для создания виртуальных сетей и соединения виртуальных машин между собой и с внешними сетями. Использовались встроенные воз-

можности QEMU/KVM в связке с возможностями приложения контейнеризации [5].

• Языки программирования – для написания кода модуля использовался Python, так как позволяет работать на операционных системах Windows и Linux.

• Для хранения параметров и конфигураций лабораторий, виртуальных машин и сетей использовались xml-схемы.

• API – для управления виртуальными сетевыми лабораториями было разработано API на Python, с помощью которого можно автоматически создавать, настраивать и удалять виртуальные машины и сети.

Для достижения поставленных целей было разработано приложение для моделирования конфигурации сети. В приложении доступны следующие функции:

1. Создание и удаление виртуальных машин

2. Соединение виртуальных машин виртуальными сетевыми мостами

3. Удаленное подключение к виртуальным машинам

Приложение имеет графический интерфейс для создания, перемещения машин по экрану, созданию и удалению связей между машинами, а также текущий статус машины и связей. Данный интерфейс представлен на рис. 1.

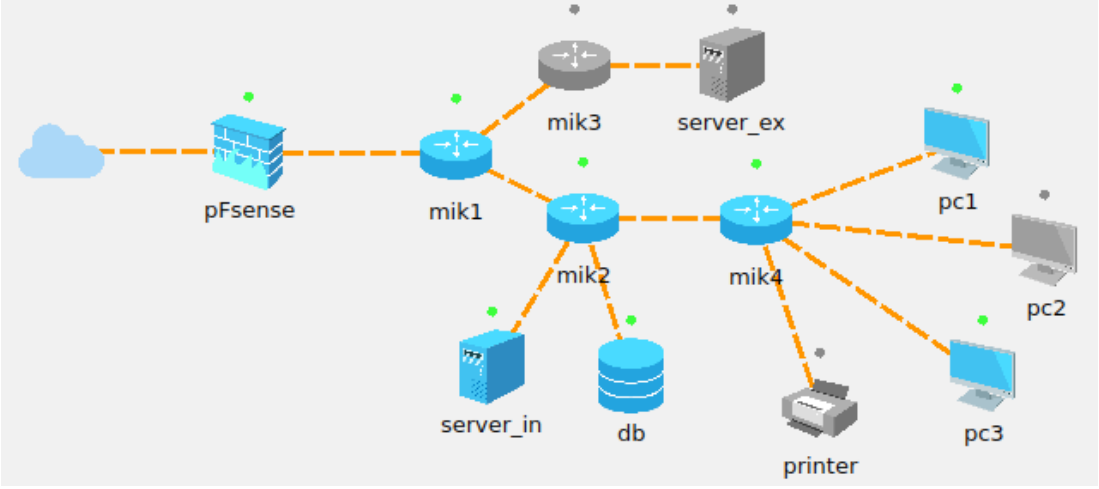


Рис. 1. Графический интерфейс приложения

Разрабатываемый модуль для защиты веб-сервисов разрабатывается на основе нейросети. Это поможет обнаруживать не только аномальные и вредоносные пакеты на основе существующих атак, но также и новые типы атак, еще не опубликованные исследователями и компаниями [6].

Приложение включает в себя механизм перехвата пакетов для анализа, модуль обученной нейросети для анализа входящего трафика, а также механизм логирования аномальных/вредоносных пакетов.

Для решения задачи анализа HTTP-трафика на предмет аномалий и атак можно использовать различные типы нейронных сетей, в зависимости от конкретной задачи и доступных данных.

Один из наиболее распространенных типов нейронных сетей для обнаружения аномалий в данных – это **автоэнкодеры** (англ. autoencoders). Автоэнкодеры – это нейронные сети, которые обучаются на входных данных и затем используются для восстановления этих данных. Если входные данные содержат аномалии, то автоэнкодеры могут обнаружить эти аномалии и выдать предупреждение [7].

Также для решения задачи анализа HTTP-трафика на предмет аномалий и атак можно использовать **сверточные нейронные сети** (англ. convolutional neural networks), которые могут анализировать временные ряды данных и выделять из них признаки, связанные с аномалиями [8].

Рекуррентные нейронные сети (англ. recurrent neural networks) также могут использоваться для анализа HTTP-трафика, особенно если данные имеют последовательную структуру.

Выбор конкретного типа нейронной сети зависит от характеристик данных и требований к точности и скорости обнаружения ано-

малий [9]. Для решения задачи было решено выбрать рекуррентные нейронные сети.

Так как длина HTTP-пакетов может быть довольно большой, а векторное представление слов для анализа не является возможным, в виду отсутствия семантического смысла, а также наличия различных типов данных помимо текстового, необходим тип рекуррентных нейронных сетей, способный 2обрабатывать длинную последовательность данных.

Для решения задачи было решено использовать рекуррентные сети типа LSTM и GRU, а после сравнения эффективности выбрать окончательный вариант.

Для перехвата пакетов и их дальнейшего анализа используется open-source инструмент mitmproxy. В данный инструмент входит функциональность обратного прокси-сервера, который, в отличие от обычного, работает на стороне сервера, а не клиента, что позволяет поддерживать HTTP-соединение со многими клиентами, при этом перехватывая и/или обрабатывая трафик.

Основной модуль перехватывает пакеты, а также производит первичную обработку (проверка на количество переноса строк в запросе).

Модуль нейросети использует методы для получения массивов данных из файлов с помощью библиотеки pickle, затем преобразование этих данных в массивы numpy и сохранение в файлы pickle (для оптимизации тестирования и работы). После этого происходит преобразование данных в нужный вид для обработки нейросетью. После чего создается непосредственно модель нейросети, ее обучение и тестирование с помощью keras – открытой библиотеки Python для работы с различными типа нейросетей. Фрагмент кода представлен на рис. 2.

```
# соединяем массивы
signs = np.concatenate((data_anomal1_sign, data_normal1_sign))

# вертикально соединяем массивы
data = np.vstack((data_anomal1, data_normal1))

# X - массив признаков, y - массив меток классов
X_train, X_test, y_train, y_test = train_test_split(data, signs, test_size=0.2, random_state=42)


# Создание модели
model = Sequential()
model.add(Dense(64, input_dim=X_train.shape[1], activation='relu'))
model.add(Dropout(0.5))
model.add(Dense(1, activation='sigmoid'))
model.compile(loss='binary_crossentropy', optimizer='adam', metrics=['accuracy'])

# Обучение модели
model.fit(X_train, y_train, epochs=100, batch_size=32, validation_data=(X_test, y_test))

# Оценка качества модели
score = model.evaluate(X_test, y_test, verbose=0)
print('Test loss:', score[0])
print('Test accuracy:', score[1])
```

Рис. 2. Фрагмент кода модуля нейросети.

В качестве тестирования была взята простая рекуррентная нейронная сеть. После обучения, коэффициент точности при тестировании составил 95%.

Заключение

Был разработан модуль киберполигона для построения виртуальных сетей, реализующий следующие функции:

• Поддержка создания пользовательских виртуальных машин в среде построения лаборатории.

• Создание виртуальных сетевых интерфейсов у машин.

• Создание изолированных виртуальных сетей для объединения виртуальных интерфейсов машин.

• Удаленное подключение к виртуальным машинам.

• Настройка виртуальных машин (ограничение используемой оперативной памяти и процессорного времени).

• Сохранение конфигураций лабораторий, виртуальных сетей и машин.

• Наличие графического интерфейса для управления лабораторией.

Для модуля защиты веб-сервисов на ос-

нове нейросети в результате анализа были выбраны нейросети типа LSTM и GRU. Также были выбраны инструменты для реализации выдвинутых требований к модулю, созданы основные модули программы, а также создана тестовая нейросеть. На основании полученных результатов можно сделать вывод, что разработка в данном направлении может открыть новые возможности для специалистов в области информационной безопасности.

Литература

1. Рахметов Р. Роль киберполигона в обеспечении ИБ / Рахметов Р. [Электронный ресурс] // Security Vision: [сайт]. – URL: https://www.securityvision.ru/blog/rol-kiberpoligona-v-obespechenii-ib/# (дата обращения 10.02.2024г.)

2. Сарычев Д. Как выбрать Web Application Firewall в 2023 году / Сарычев Д. [Электронный ресурс] // Anti-Malware [сайт]. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Web-Application-Firewall-in-2023#part34 (дата обращения: 11.02.2024г.)

3. Scott H. Software Containers: Used More Frequently than Most Realize / Scott H. [Электронный ресурс] // Network World [сайт]. – URL: https://www.networkworld.com/article/749098/cisco-subnet-software-containers-used-more-frequently-than-most-realize.html (дата обращения 10.02.2024г.)

4. Berl Andreas, Fischer Andreas, Hermann de Meer. Using System Virtualization to Create Virtualized Networks. — Berlin: Electronic Communications of the EASST, 2015. — 12 p.

5. Matthew Portnoy. Virtualization Essentials. – New York: Sybex, 2023. – 196 p.

6. Ian Goodfellow, Yoshua Bengio, and Aaron Courville. Deep Learning – Cambridge: MIT Press, 2016. – 555 p.

7. Питер Яворски. Ловушка для багов: полевое руководство по веб-хакингу. – СПб.: Питер, 2020. – 28 с.

8. Anthony Williams. Convolutional Neural Networks in Python: Introduction to Convolutional Neural Networks. – Scotts Valley: Createspace, 2019. – 57 p.

9. Aurélien Géron. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. – North Carolina: O'Reilly Media, 2019. – 152 p.

References

1. Rakhmetov R. Rol' kiberpoligona v obespechenii IB / Rakhmetov R. [Elektronnyy resurs] // Security Vision: [sayt]. – URL: https://www.securityvision.ru/blog/rol-kiberpoligona-v-obespechenii-ib/# (data obrashcheniya 10.02.2024g.)

2. Sarychev D. Kak vybrat' Web Application Firewall v 2023 godu / Sarychev D. [Elektronnyy resurs] // Anti-Malware [sayt]. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Web-Application-Firewall-in-2023#part34 (data obrashcheniya: 11.02.2024g.)

3. Scott H. Software Containers: Used More Frequently than Most Realize / Scott H. [Electronic resource] // Network World [website]. – URL: https://www.networkworld.com/article/749098/cisco-subnet-software-containers-used-more-frequently-than-most-realize.html (дата обращения 10.02.2024г.)

4. Berl Andreas, Fischer Andreas, Hermann de Meer. Using System Virtualization to Create Virtualized Networks. — Berlin: Electronic Communications of the EASST, 2015. — 12 p.

5. Matthew Portnoy. Virtualization Essentials. – New York: Sybex, 2023. – 196 p.

6. Ian Goodfellow, Yoshua Bengio, and Aaron Courville. Deep Learning – Cambridge: MIT Press, 2016. – 555 p.

7. Piter Yavorski. Lovushka dlya bagov: polevoe rukovodstvo po veb-khakingu. – SPb.: Piter, 2020. – 28 s.

8. Anthony Williams. Convolutional Neural Networks in Python: Introduction to Convolutional Neural Networks. – Scotts Valley: Createspace, 2019. – 57 p.

9. Aurélien Géron. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. – North Carolina: O'Reilly Media, 2019. – 152 p.

КУЗЬМИНА Ульяна Владимировна, кандидат технических наук, доцент по специальности «Информационная безопасность автоматизированных систем», доцент кафедры информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный техниче-

ский университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: u.mihaylova@magtu.ru

KUZMINA Ulyana Vladimirovna, Candidate of Technical Sciences, Associate Professor in the specialty «Information Security of automated systems», Associate Professor of the Department of Computer Science and Information Security of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: u.mihaylova@magtu.ru

МИХАЙЛОВА Ольга Евгеньевна, студент кафедры информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: olgamihailova01@mail.com

MIKHAYLOVA Olga Evgenevna, student of the department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: olgamihailova01@mail.com

АФАНАСЬЕВ Юрий Петрович, студент кафедры информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: yurashca19@mail.ru

AFANASYEV Yuri Petrovich, student of the department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: yurashca19@mail.ru

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76, ЮУрГУ,
Издательский центр

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(51) / 2024
Подписано в печать 08.04.2024. Дата выхода в свет 12.04.2024.
Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 5,78. Тираж 50 экз.
Заказ 100/200.
Цена свободная.

Отпечатано в типографии Издательского центра ФГАОУ ВО "ЮУрГУ (НИУ)".
454080, г. Челябинск, пр. им. В. И. Ленина, 76, ЮУрГУ, Издательский центр.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 1(51) / 2024
Signed to print April 08, 2024. Date of publication of the 12.04.2024.
Format 70×108 1/16. Screen printing. Conventional printed sheet 5,78. Circulation – 50 issues.
Order 100/200.
Open price.

Printed in the printing house of the Publishing Center of FGAOU VO "SUSU (NIU)".
SUSU, Publishing Center, 76, Lenina Str., Chelyabinsk, 454080