ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 2(36) / 2020

УЧРЕДИТЕЛИ

ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

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.
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

№ 2(36) / 2020

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

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

SHRABER 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
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

ИССЛЕДОВАНИЕ И ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

МЕТОДЫ АНАЛИЗА ДАННЫХ

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКАЯ И ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

IN THIS ISSUE

RESEARCH AND DESIGN OF TECHNICAL FACILITIES

INFORMATION TECHNOLOGY AND COMPUTER SECURITY

METHODS OF DATA ANALYSIS

ORGANIZATIONAL, TECHNICAL AND LEGAL PROTECTION OF INFORMATION

TOPICAL PROBLEMS OF CYBERSECURITY

УДК 004.048.44 + 620.179 Вестник УрФО № 2(36) / 2020, с. 5–9

Швырев Б. А., Тимонов Д. А.

DOI: 10.14529/secur200201

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ НА ANDROID OS ОБНАРУЖИТЕЛЯ УТЕЧКИ ИНФОРМАЦИИ ПОСРЕДСТВОМ МОДУЛЯЦИИ ВИДИМОГО СВЕТА

Передача информации посредством модуляции интенсивности видимого света подтверждена работами многих авторов и существованием сети передачи данных Li-Fi. Повсеместное использование светодиодного освещения, управляемого контроллерами, потенциально формирует канал утечки акустической информации посредством модуляции видимого света. В работе авторы рассматривают структурную схему устройства обнаружения канала утечки информации. Авторы предлагают использовать современный смартфон под управлением Android OS для определения модуляции интенсивности освежения, регистрируемого датчиком освещенности смартфона.

Ключевые слова: *модуляция видимого света, светодиод, фотодиод, датчик освещенности, обнаружение канала утечки информации.*

Shvyrev B. A., Timonov D. A.

SOFTWARE IMPLEMENTATION ON ANDROID OS OF THE INFORMATION LEAK DETECTOR BY MEANS OF VISIBLE LIGHT MODULATION

The transmission of information by means of visible light intensity modulation is confirmed by the works of many authors and the existence of a Li-Fi data transmission network. The widespread use of led lighting controlled by controllers potentially creates a channel for acoustic

information leakage through visible light modulation. In this paper, the authors consider the block diagram of the device for detecting the channel of information leakage. The authors suggest using a modern smartphone running Android OS to determine the modulation of the refresh rate detected by the smartphone's light sensor.

Keywords: *visible light modulation, led, photodiode, light sensor, information leakage channel detection.*

Утечка акустической информации посредством модуляции видимого света рассмотрена в работах [1-3]. Очевидность существования такого канала утечки подтверждается существование сети передачи данных

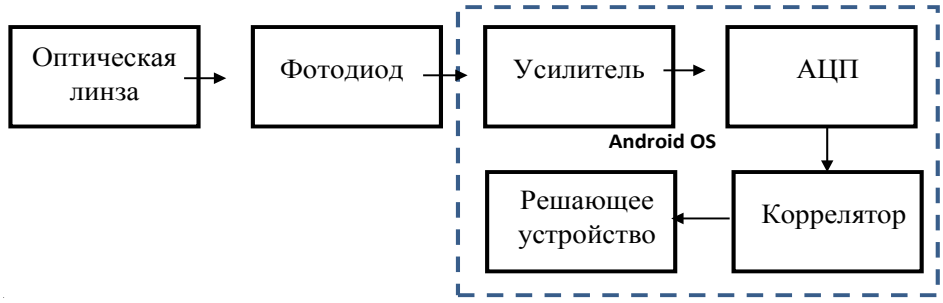

Рис.1. Структурная схема устройства обнаружения утечки информации посредством модуляции видимого света

Li-Fi [4-6]. Существованию оптических скрытых каналов посвящена публикация [7]. Подробное описание оптической фильтрации простого оптического приемника, подключенного к параллельному порту старого компьютера, приводится в [8]. Известна работа [9] посвященная утечки информации и взлому компьютера, физически не соединённому ни с какой информационной сетью посредством перехвата видимого излучения от информационных светодиодов расположенных на системном блоке. В работе [10] рассматривается атака с использованием потребительских лампочек дневного освещения с функциями интернета вещей IoT для скрытой коммуникации через различные уровни интенсивности света.

Структура канала утечки посредством модуляции видимого света рассмотрена авторами в [11], а его характеристики в [12]. В настоящее время остается актуальным разработка устройства обнаружения утечки информации посредством модуляции видимого света от осветительных светодиодов. Перспективным направлением является использование для этих целей современные смартфоны под управление Android OS.

Структурная схема устройства обнаружения утечки информации посредством модуляции видимого света представлена на рисунке 1. Рассмотрим схему основного автомата LTR-579ALS[1] (ALS) датчика освещенности смартфона под управлением Android OS на рис. 2.

Во время работы ALS и датчика приближения (proximity sensor PS) измерения ALS можно активировать, установив бит ALS_ Enable в 1 и PS измерение можно активировать, установив бит PS_Enable в 1. Как только датчики PS и / или ALS станут активироваться с помощью команды I2C, внутренние блоки поддержки становятся включены. После того, как напряжения и токи установлены (обычно через 5 мс), конечный автомат проверяет наличие событий запуска из планировщика измерений для запуска ALS или PS преобразования в соответствии с выбранными скоростями повторения измерений. После того, как PS_Enable или ALS_Enable будут изменен до 0, текущее преобразование на соответствующем канале будет завершено, и соответствующие АЦП и блоки поддержки станут отключены.

Люкс Формула. Lux_Calc - это рассчитанное значение в люксах, а ALS DATA - цифровое представление (выходной АЦП) окружающей среды. Уровень освещенности сохраняется в регистрах (Адрес: 0x0D-0x0F) независимо от источников света

$$Lux_{calc} = \frac{0.8 * ALS_{DATA}}{(GAIN * INT)}$$

Если датчик располагается под тониро-

[1] Optical SensorProduct Data SheetLTR-579ALS-01. https://optoelectronics.liteon.com/upload/download/DS86-2015-0005/LTR-579ALS-01_FINAL_DS_V1.1.PDF

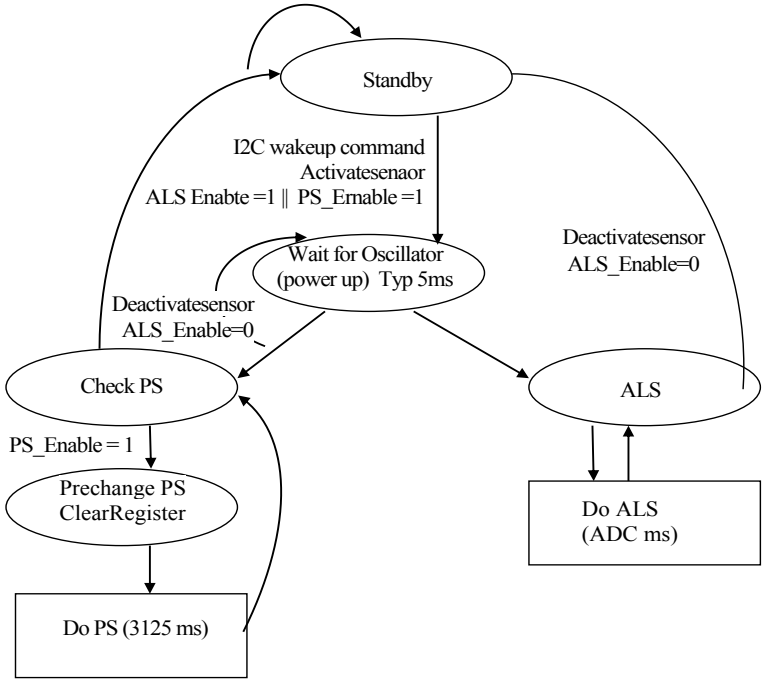

Рис. 2. Схема функционирования конечного автомата датчика освещенности смартфона приемника оптического сигнала

ванным стеклом необходимо воспользоваться соотношением

$$Lux_{Calc} = \frac{0.8 * ALS_{DATA}}{(GAIN * INT)}$$

вается, когда данные выбранного источника прерывания выше верхнего или ниже нижнего порога для заданного количества последовательных измерений, установленных в ALS Persist в регистре INT_PST (0x1A). Сигнал пре-

Таблица 1

ALS Gain	GAIN
X1	1
X2	3
X3	6
X4	9
X5	18

Resolution (bit) / Integration Time (ms)	INT
16-bit, 25ms	0.25
17-bit, 50ms	0.5
18-bit, 100ms	1
19-bit, 200ms	2
20-bit, 400ms	4

Особенности прерывания датчика освещенности. Это устройство генерирует независимые сигналы прерывания ALS и PS, которые можно мультиплексировать и выводить на выход INT (см. табл. 1). Условия прерывания всегда оцениваются после завершения нового преобразования каналов ALS и PS. Режим логики PS имеет приоритет над любым другим сигналом прерывания. Если выбрано (PS Logic Mode = 1), прерывание ALS не может сигнализировать на выходе INT. ALS и PS прерывания, а также режим PS Logic активны на низком уровне на выводе INT. Прерывание ALS активируется битом 2 (контакт ALS INT включен) регистра INT_CFG (0x19). Прерывание ALS Источник - канал ALS. INT устанавли-

рывания также сохраняется в регистре MAIN_ STATUS (0x07) как бит флага в бите 4 (состояние ALS INT). Это бит флага состояния очищается чтением регистра MAIN_STATUS. Сброшенный флаг также очистит сигнал прерывания на контакте INT. Прерывание PS активируется битом 0 (разрешение контакта прерывания PS). Оно срабатывает, когда результат преобразования PS выше верхнего или нижнего порога PS для заданного количества последовательных измерений, установленных в PS Persist в INT_PST регистр (0x1A). Логический сигнал PS, бит 2 регистра MAIN_STATUS (0x07), устанавливается в 0, когда данные PS ниже нижнего PS порога, и он установлен в 1, если данные PS выше верхнего порога PS.

Существует два варианта указания сигнала прерывания PS на выводе INT: в виде непрерывного логического сигнала или в виде, инициируемом фронтом сигнал прерывания, который очищается при следующем считывании из регистра MAIN-STATUS. Сигнал прерывания PS также сохраняется в регистре MAIN_STATUS (0x07) как бит флага в бите 1 (состояние PS INT). Это бит флага состояния очищается чтением регистра MAIN_STATUS.

Для управления датчиком освещенности разработана программа позволяющая регистрировать изменения интенсивности освещения. Для обработки полученных данных освещенности и обнаружения в них передачи информации в работе использовалось выявление коррелированных данных в потоке, для этого рассчитывалась автокорреляционная функция.

Рассмотрим реализация автокорреляционной функции. Поток данных представляет собой дискретные значения освещенности. Запишем автокорреляционную функцию дискретного сигнала как:

$$B_u(n) = \sum_{j=-\infty}^{\infty} u_j u_{j-n}$$

где u_j – отсчеты дискретного сигнала освещенности, n – задержка сигнала (целочисленный аргумент, указывающий, на сколько позиций сдвинута копия сигнала относительно оригинала).

При $n = 0, B_u(n)$ она максимальна и равна энергии сигнала, однако функция в общем случае не является четной функцией и необязательно достигает максимума при $n = 0$. При передачи дискретных сообщений с неизвестной фиксированной частотой дискретизации максимум автокорреляционной функции $B_u(n)$ соответствует временной задержке равной интервалу дискретизации исследуемого процесса. Такой подход позволяет определить наличие связанных данных в изменениях интенсивности освещения.

Решающим устройством является программный компаратор. Выносящий суждение при значительном превышении текущих значений $B_u(n)$. Что сигнализирует о возникновении канала утечки в контролируемом помещении посредством модуляции видимого света.

Разработанная программное средство позволяет обнаружить передачу информации в оптическом диапазоне посредством модуляции видимого света, излучаемого осветительными светодиодами.

Литература

1. Канал утечки акустической информации посредством модуляции видимого света // Швырев Б.А., Тимонов Д.А. / Вестник УрФО. Безопасностьвинформационнойсфере. 2019. № 1 (31). С. 11-16.

2. Occurrence channel of leakage of the acoustic due to the modulation of the visible light // Shvyrev B.A., Vlasenko A.V., Makaryan A.S., Timanov D.A./ Industry 4.0. 2019. Т. 4. № 4. С. 161-163.

3. Mathematical model of the leakage channel of acoustic information by modulating the light flux // Shvyrev B.A., Vlasenko A.V., Timanov D.A./Mathematical Modeling. 2019. Т. 3. № 1. С. 30-31.

4. «Comprehensive Summary of Modulation Techniques for LiFi. LiFi Research». www.lifi.eng.ed.ac.uk. Retrieved 2018-01-16.

5. Harald Haas. «Harald Haas: Wireless data from every light bulb». ted. com. Archived from the original on 8 June 2017.

6. H. Haas, L. Yin, Y. Wang, C. Chen, What is LiFi?, J. Light. Technol. 34 (6) (2016). PP. 1533-1544

7. Information leakage from optical emanations. J Loughry, DA Umphress. ACM Transactions on Information and System Security (TISSEC) 5 (3), 20021, p.262-289. http://www.applied-math.org/optical_tempest.pdf

8. Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. April 15, 2005. by Michal Zalewski. https://www.amazon.com/Silence-Wire-Passive-Reconnaissance-Indirect/dp/1593270461

9. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. Mordechai Guri ; Boris Zadov ; Andrey Daidakulov ; Yuval Elovici. 2018 16th Annual Conference on Privacy, Security and Trust (PST). DOI: 10.1109/PST.2018.8514196. https://arxiv.org/ftp/arxiv/papers/1706/1706.01140.pdf.

10. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. Eyal Ronen, Adi Shamir. 2016 IEEE European Symposium on Security and Privacy (EuroS&P). DOI:10.1109/EuroSP.2016.13. Corpus ID: 206649455. http://www.wisdom.weizmann.ac.il/~eyalro/EyalShamirLed.pdf

11. Параметры канала утечки акустической информации за счет модуляции видимого света//Власенко А.В., Швырев Б.А., Тимонов Д.А./ Прикаспийский журнал: управление и высокие технологии. 2019. № 1 (45). С. 188-192.

12. Акустические аспекты модели угроз утечки информации по средствам модуляции видимого света// Швырев Б.А., Тимонов Д.А./Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 3. С. 120-124.

References

1. Kanal utechki akusticheskoj informacii posredstvom modulyacii vidimogo sveta [Channel leakage of acoustic information by modulating the visible light] // SHvyrevB.A., TimonovD.A. / VestnikUrFO. Bezopasnost' vinformacionnojsfere. 2019. № 1 (31). S. 11-16.

2. Occurrence channel of leakage of the acoustic due to the modulation of the visible light // Shvyrev B.A., Vlasenko A.V., Makaryan A.S., Timanov D.A./ Industry 4.0. 2019. T. 4. № 4. C. 161-163.

3. Mathematical model of the leakage channel of acoustic information by modulating the light flux // Shvyrev B.A., Vlasenko A.V., Timanov D.A./Mathematical Modeling. 2019. T. 3. № 1. C. 30-31.

4. «Comprehensive Summary of Modulation Techniques for LiFi. LiFi Research». www.lifi.eng.ed.ac.uk. Retrieved 2018-01-16.

5. Harald Haas. «Harald Haas: Wireless data from every light bulb». ted. com. Archived from the original on 8 June 2017.

6. H. Haas, L. Yin, Y. Wang, C. Chen, What is LiFi?, J. Light. Technol. 34 (6) (2016). PP. 1533-1544

7. Information leakage from optical emanations. J Loughry, DA Umphress. ACM Transactions on Information and System Security (TISSEC) 5 (3), 20021, p.262-289. http://www.applied-math.org/optical_tempest.pdf

8. Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. April 15, 2005. by Michal Zalewski. https://www.amazon.com/Silence-Wire-Passive-Reconnaissance-Indirect/dp/1593270461

9. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. Mordechai Guri ; Boris Zadov ; Andrey Daidakulov ; Yuval Elovici. 2018 16th Annual Conference on Privacy, Security and Trust (PST). DOI: 10.1109/PST.2018.8514196. https://arxiv.org/ftp/arxiv/papers/1706/1706.01140.pdf.

10. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. Eyal Ronen, Adi Shamir. 2016 IEEE European Symposium on Security and Privacy (EuroS&P). DOI:10.1109/EuroSP.2016.13. Corpus ID: 206649455. http://www.wisdom.weizmann.ac.il/~eyalro/EyalShamirLed.pdf

11. Parametry kanala utechki akusticheskoj informacii za schet modulyacii vidimogo sveta [Parameters of the acoustic information leakage channel due to visible light modulation]//Vlasenko A.V., SHvyrev B.A., Timonov D.A./Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii. 2019. № 1 (45). S. 188-192.

12. Akusticheskie aspekty modeli ugroz utechki informacii po sredstvam modulyacii vidimogo sveta [Acoustic aspects of the threat model of information leakage by means of visible light modulation]// SHvyrev B.A., Timonov D.A./Sovremennaya nauka: aktual'nye problem teorii i praktiki. Seriya: Estestvennye i tekhnicheskie nauki. 2019. № 3. S. 120-124.

ШВЫРЕВ Борис Анатольевич, кандидат физико-математических наук, главный научный сотрудник ФКУ Научно-исследовательский институт ФСИН России. 125130, г. Москва, ул. Нарвская, д. 15а, стр. 1. E-mail: bor2275@yandex.ru

ТИМОНОВ Дмитрий Александрович, начальник лаборатории Научно-исследовательского центра Краснодарского высшего военного училища имени генерала армии С.М. Штеменко. 350063, г. Краснодар, ул. Красина, дом 4. E-mail: dmitrii-timonov@bk.ru

SHVYREV Boris, Candidate of Physical and Mathematical Sciences, Chief Researcher, PKU Research Institute of the Federal Penitentiary Service of Russia. Bld. 15a, p. 1, Narvskaya Str., Moscow, 125130. E-mail: bor2275@yandex.ru

TIMONOV Dmitry, the head of laboratory of the research center of Krasnodar higher military school named after Army General S.M. Shtemenk. Bld. 4, KrasinaStr., Krasnodar, 350063. E-mail: dmitrii-timonov@bk.ru

УДК 004.588 Вестник УрФО № 2(36) / 2020, с. 10–16

Шпак В. А., Кремлев Е. С., Михайлова У. В.

DOI: 10.14529/secur200202

РАЗРАБОТКА ВИРТУАЛЬНОГО ТРЕНАЖЕРА ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ В КОНТРОЛИРУЕМОМ ПОМЕЩЕНИИ

Статья посвящена разработке виртуального тренажера для обучения специалистов по информационной безопасности аспектам аудита помещений по требованиям акустической безопасности, в том числе поиску скрытых закладных устройств. Рассмотрены функциональные достоинства внедрения виртуальных тренажеров в учебный процесс высших учебных заведений на постоянной основе, такие как ускорение и удешевление процесса обучения. Описаны преимущества и возможности разработанного виртуального тренажера для оценки защищенности акустической информации в контролируемом помещении.

Ключевые слова: *информационные технологии, образование, виртуальные тренажеры, информационная безопасность.*

Shpak V. A., Kremlev E. S., Mikhailova U. V.

DEVELOPMENT OF A VIRTUAL TRAINER FOR ASSESSING THE PROTECTION OF ACOUSTIC INFORMATION IN A CONTROLLED ROOM

The article is devoted to the development of a virtual trainer for training information security specialists in the audit of premises in terms of acoustic safety requirements, including the search for secret intelligence device. The functional advantages of introducing virtual simulators into the educational process of higher education, such as accelerating and cheapening the learning process, are examined. The advantages and capabilities of the developed virtual trainer for assessing the security of acoustic information in a controlled room are described.

Keywords: *information technology, education, virtual trainers, information security.*

Большинство современных предприятий независимо от вида деятельности и форм собственности не может успешно вести свою деятельность без обеспечения системы защиты своей информации, включающей организационно-нормативные меры и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах.

В бизнесе промышленный шпионаж используется для получения секретной информации, являющейся коммерческой тайной и дальнейшее ее использование с целью уменьшения убытков на конкурентную борьбу предприятий, преодоления технологического отставания, увеличения клиентской базы.

Вне зависимости от типа тайны, интерес злоумышленника зависит от характера информации и физических носителей, на которых она представлена. Поэтому основными формами информации, подлежащими защите, являются: документальные, акустические, телекоммуникационные, видовые. С целью предотвращения хищения таких форм информации любое предприятие нуждается в квалифицированных специалистах в области информационной безопасности.

Для обеспечения необходимых результатов обучения специалистов ВУЗы должны иметь соответствующие программно-аппаратную и специализированную технические базы для проведения практических занятий. Развитие информационных технологий и постоянно изменяющиеся профессиональные условия, в которых выпускник обязан разбираться, подталкивает ВУЗы своевременно реагировать и постоянно адаптироваться к условиям отрасли и рынка труда.

Наиболее серьезная проблема, характерная всей образовательной системе подготовки и повышения квалификации специалистов технических специальностей, являет собой отставание материально-технического обеспечения от требований жизни. Внедрение виртуальных тренажеров в практику образования специалистов информационной безопасности позволит нивелировать временное отставание между появлением нового оборудования на рынке и началом использования его в образовательных целях.

В связи с переходом образовательного процесса в виртуальную среду, можно выделить такие достоинства, как:

а) удешевление обучения без потери качества образования;

б) ускорение овладения навыками использования специального оборудования большими группам студентов;

в) возможность проведения лекционных занятий с демонстрированием практической части на виртуальном тренажере;

г) облегчение дистанционного обучения;

д) безопасное воспроизведение аварийных ситуаций и корректировка поведения в ней человека.

е) автоматизированный сбор аттестационных данных

Для эффективной подготовки специалистов информационной безопасности и повышения их профессиональных навыков используют виртуальные тренажеры и имитаторы средств защиты информации. Разработанный тренажер предназначен для визуализации практической работы и обучения проведению аттестационных мероприятий или поиска закладных устройств с использованием специальных технических средств.

Таким образом, представленный виртуальный тренажер позволит решить следующие задачи:

а) изучать основные методики проведения оценки защищенности акустической информации в помещении;

б) осваивать специальное оборудование, используемое специалистами информационной безопасности на современных предприятиях;

в) получать навыки поиска и идентификации скрытых закладных устройств.

Разработанный виртуальный тренажер представляет собой программный комплекс, позволяющий проводить физические опыты на компьютере без непосредственного контакта с реальной лабораторной установкой или стендом. Мультимедийная учебная лаборатория сочетает в себе имитационную динамическую модель оборудования и программную оболочку, включающую методическое сопровождение лабораторной работы, информацию об оборудовании и инструментах, их технических характеристиках.

Тренажер разработан в среде разработки UnrealEngine 4 (UE4). UE4 очень удобен для разработки средних и крупных проектов в 3D пространстве. Также плюсом UE4 можно назвать его отличительную черту – язык визуального программирования Blueprints, разработанный Epic Games. UE4 предлагает разработчикам удобный редактор классов, в котором можно спокойно манипулировать полями и компонентами класса.

В разработанный виртуальный тренажер добавлено меню библиотеки с информацией об оборудовании, инструментах и методиках измерений. В этом меню студент имеет возможность ознакомиться с основными характеристиками оборудования, его общим видом и габаритами (рис. 1). В плане дальнейшего развития тренажера предусмотрены изменения общего вида библиотеки (добавление трехмерных моделей оборудования, кнопки просмотра текучих лицензий специальных устройств и проч.).

на предмет защищенности по акустическому каналу с использованием специальных методик, а также предусмотрена возможность поиска закладных устройств. Места расположения закладных устройств не являются постоянными и имеется возможность модерации администратором.

Расстановка оборудования реализована на основе технологии трассировки лучей. Так, из камеры, имитирующей персонажа-специалиста по информационной безопасности раз в несколько тиков выпускается пучок

Рис. 1. Информация об оборудовании на примере АИ-3М

В программе спроектирована возможность самостоятельно расставлять генератор шума, акустические излучатели, закладные устройства, шумомеры. На текущий момент разработки у всего расставляемого оборудования используется условная 3D-модель. При этом у каждого из этих специальных инструментов изменяются абсолютно те же параметры и интерфейс, что и у их реального прототипа (рис. 2). В дальнейшем планируется заменить ползунки на панели управления прототипов.

Тренажер предусматривает два режима работы:

а) теоретический – при помощи интерфейса тренажера студенты могут изучить основные технические характеристики специализированного оборудования, то как выглядит это оборудование, ознакомится с интерфейсом данного оборудования;

б) практический – позволяет обучающимся изучить возможности специализированного оборудования, исследовать помещение

лучей в сторону центра экрана с некоторым разбросом. После пересечения луча с какой-либо трехмерной моделью засекается угол, на который отклонился данный луч и расстояние между камерой и местом пересечения луча с некоторой поверхностью.

На основе полученных данных, обработанных в классе работы с лучом, воспроизводится вывод о том, возможно ли в данную местность поставить оборудование, и если возможно, то на какой угол нужно повернуть оборудование, чтобы оно смотрелось в данной точке естественно. Для удобства место будущей установки отображается с помощью куба (рис. 3).

Объектной базой для реализации комплекса-тренажера выбрана абстрактная схема-офиса (рис. 4). Данный офис имеет такие помещения, как шоурум, конференц-зал, кухня, санузел, серверная, ресепшн и несколько офисных пространств.

В общем случае среда распространения носителя акустической информации от ис-

Рис. 2. Панель управления параметрами тренажерного оборудования

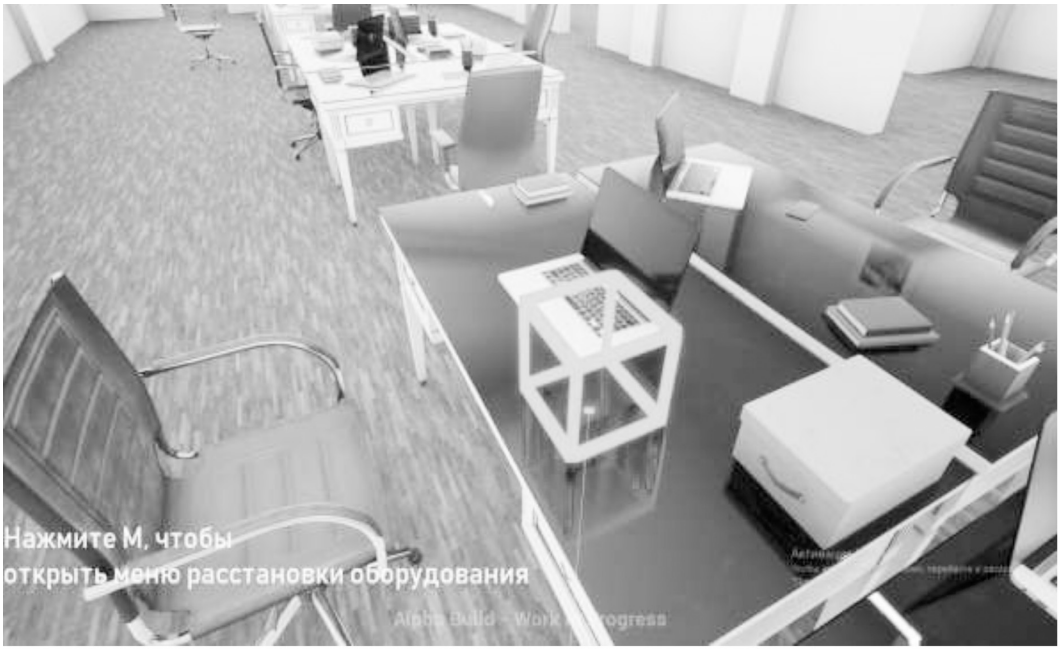

Рис. 3. Система расстановки оборудования

точника к приемнику может быть однородной и неоднородной, т.е. образованной последовательными участками различных физических сред: воздуха, древесины дверей, стекол окон, бетона или кирпича стен, различными породами земной поверхности и т.д.

Данная модель помещения, позволяет проводить занятия, моделирующие некоторые аспекты аудита помещения по требованиям акустической безопасности. Виртуальный тренажер учитывает реалистичную модель распространения акустических волн в помещении с однородными и неоднородными стенами, мебелью и т.д. Предусмотрен выбор материала для модерирования стен и дверей с возможностью дополнительного экранирования. На карте офиса располагается мебель, в выдвижные ящики которой можно прятать закладные устройства.

При расстановке закладных устройств можно выбрать диапазон частот, на котором оно будет вещать (Wi-Fi, GSM и т.д.), после этого производится выбор самой частоты веща-

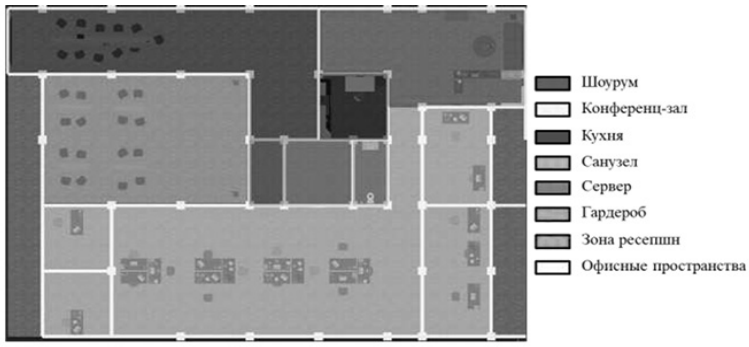

Рис. 4. Схема помещений офиса

ния. Так как злоумышленник может установить закладное устройство как с заходом в помещение (позволяя спрятать закладное устройство рационально с точки зрения скрытности закладки), так и без захода (путем заброса в помещение, выстрелом из пневматического оружия и иными способами), преподаватель или товарищ студент может заранее спрятать закладное устройство самостоятельно или выбрать предустановку из списка, в том числе и снаружи помещения.

После этого студенту предлагается с помощью устройств поиска скрытых закладных устройств определить местоположение закладного устройства. На данный момент единственным таким средством в тренажере является BugHunterprofessionalBH-02, но в дальнейшем планируется добавить другие модели BugHunter'ов и анализаторы спектра, в том числе Кассандра К6.

Заключение

Качественное улучшение подготовки специалистов в области информационной безопасности на данный момент актуально, поэтому существует необходимость разработки новых учебных программных средств и виртуальных тренажеров.

Внедрение в образовательную программу ВУЗов виртуального тренажера имитатора средств акустической защиты информации повысить компетентность, технологическую грамотность и инициативность студентов, обучающихся по направлению «Информационная безопасность автоматизированных систем». Так же данный тренажер будет полезен таким направлениям, как «Комплексная защита объектов информатизации» и «Техническая защита информации».

Литература

1. Технические Средства и Методы Защиты Информации / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. - Москва: Машиностроение, 2009. – 507 с.

2. Белов, В.В. Компьютерная Реализация Решения Научно-Технических и Образовательных Задач: Учебное Пособие / В.В. Белов, И.В. Образцов, В.К. Иванов, Е.Н. Коноплев // Тверь: ТвГТУ, 2015. 108 с.

3. Рагозин Ю.Н. Инженерно-Техническая Защита Информации: Учебное Пособие по Физическим Основам Образования Технических Каналов Утечки Информации и по Практикуму Оценки их Опасности/ Рагозин Ю.Н. - Электрон. Текстовые Данные -СПб.: Интермедия, 2018 – 168 с.– Режим доступа: http://www.iprbookshop.ru/73641.html – ЭБС «IPRbooks».

4. Баранкова И.И., Михайлова У.В., Быкова Т.В. Сложности, возникающие при проведении аудита информационной безопасности на предприятии / Вестник УРФО. Безопасность в информационной сфере. 2019. №1 (31). С. 53–56.

5. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии / Международная конференция «Наука. Исследования. Практика». – 2019. – с. 341–345.

6. Михайлова У.В., Лукьянов Г.И. Защита информации в помещении от утечки по акустическому каналу / Актуальные проблемы современной науки, техники и образования Тезисы докладов 76-ой международной научно-технической конференции. 2018. С. 294.

7. Думенков Д.Ю., Лукьянов Г.И., Михайлова У.В. Разработка комплекса оценки акустической защищенности помещения / Безопасность информационного пространства: Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых: в 2 томах. 2018. С. 22–28.

8. Баранкова И.И., Михайлова У.В.,Лукьянов Г.И. Анализ методик оценки звукоизоляционных свойств ограждающих конструкций / Актуальные проблемы современной науки, техники и образования. 2017. Т. 1. С. 211–214.

9. Баранкова И.И., Михайлова У.В. Особенности формирования оценочных средств для оценки уровня сформированности компетенций специалиста по информационной безопасности / Информационной противодействие угрозам терроризма. 2015. Т. 2. №25. С. 26–30.

10. Пешонов С.А., Баранкова И.И., Романько. Е.А., Михайлова У.В. Имитационный тренажер для изучения устройства и принципа разработки подземных горнодобывающих систем / Имитационный тренажер. Магнитогорск 2011.

11. Баранкова И.И., Михайлова У.В., Романько. Е.А., Борисов В.О. Имитационный тренажер для изучения устройства и принципа работы теодолита / Магнитогорск 2011.

References

1. Tekhnicheskie Sredstva i Metody Zashchity Informatsii / A.P. Zaytsev, A.A. Shelupanov, R.V. Meshcheryakov i dr. - Moskva: Mashinostroenie, 2009. – 507 s.

2. Belov, V.V. Komp'yuternaya Realizatsiya Resheniya Nauchno-Tekhnicheskikh i Obrazovatel'nykh Zadach: Uchebnoe Posobie / V.V. Belov, I.V. Obraztsov, V.K. Ivanov, E.N. Konoplev // Tver': TvGTU, 2015. 108 s.

3. Ragozin Yu.N. Inzhenerno-Tekhnicheskaya Zashchita Informatsii: Uchebnoe Posobie po Fizicheskim Osnovam Obrazovaniya Tekhnicheskikh Kana-lov Utechki Informatsii i po Praktikumu Otsenki ikh Opasnosti/ Ragozin Yu.N. - Elektron. Tekstovye Dannye - SPb.: Intermediya, 2018 – 168 c. – Re-zhim dostupa: http://www.iprbookshop.ru/73641.html – EBS «IPRbooks».

4. Barankova I.I., Mikhailova U.V., Bykova T.V. Slozhnosti, vozni-kayushchie pri provedenii audita informatsionnoy bezopasnosti na predpriya-tii / Vestnik URFO. Bezopasnost' v informatsionnoy sfere. 2019. №1 (31). S. 53–56.

5. Mikhaylova U.V., Bykova T.V. Audit informatsionnoy bezopasno-sti na predpriyatii / Mezhdunarodnaya konferentsiya «Nauka. Issledovaniya. Praktika». – 2019. – s. 341–345.

6. MikhailovaU.V., Luk'yanovG.I. Zashchita informatsii v pomeshche-niiotutechkipoakusticheskomuka nalu / Aktual'nye problemy sovremennoy nauki, tekhnikii obrazovaniya Tezisy Dokladov 76-oymezhdunarodnoynauch-no-tekhnicheskoykonferentsii. 2018. S. 294.

7. Dumenkov D.Yu., Luk'yanov G.I., Mikhaylova U.V. Razrabotka kom-pleksa otsenki akusticheskoy zashchishchennosti pomeshcheniya / Bezopasnost' in-formatsionnogo prostranstva: Sbornik trudov XVII Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh: v 2 tomakh. 2018. S. 22-28.

8. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Analiz metodik otsenki zvukoizolyatsionnykh svoystv ograzhdayushchikh konstruktsiy / Aktual'-nye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2017. T. 1. S. 211-214.

9. Barankova I.I., Mikhaylova U.V. Osobennosti formirovaniya otsenochnykh sredstv dlya otsenki urovnya sformirovannosti kompetentsiy spe-tsialista po informatsionnoy bezopasnosti / Informatsionnoy protivodey-stvie ugrozam terrorizma. 2015. T. 2. №25. S. 26-30.

10. Peshonov S.A., Barankova I.I., Roman'ko. E.A., Mikhaylova U.V. Imitatsionnyy trenazher dlya izucheniya ustroystva i printsipa razrabotki podzemnykh gornodobyvayushchikh sistem / Imitatsionnyy trenazher. Magnito-gorsk 2011.

11. Barankova I.I., Mikhailova U.V., Roman'ko. E.A., Borisov V.O. Imitatsionnyy trenazher dlya izucheniya ustroystva i printsipa raboty teo-dolita / Magnitogorsk 2011.

ШПАК Виталий Алексеевич, студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: xxx-yyy-2014@inbox.ru

КРЕМЛЕВ Егор Сергеевич, студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: rabitsenpai@gmail.com

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: ylianapost@gmail.com

SHPAK Vitaliy, student, Department, Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: xxx-yyy-2014@inbox.ru

KREMLEV Egor, student, Department, Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: rabitsenpai@gmail.com

MIKHAILOVA Uliana, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security of Magnitogorsk State Technical University named after G. I. Nosova. Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com

УДК 004.056 Вестник УрФО № 2(36) / 2020, с. 17–23

Аверин А. С., Зюляркина Н. Д., Ижбердеева Е. М.

DOI: 10.14529/secur200203

ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ЧЕЛОВЕКО-МАШИННОГО ВЗАИМОДЕЙСТВИЯ

Статья посвящена разработке и анализу программного генератора случайных чисел основанного на человеко-машинном взаимодействии для программных и криптографических приложений. Описан метод генерации случайных чисел основанный на человеко-машинном взаимодействии, с использованием времени и положения курсора на дисплее компьютера или смартфона. На основе этого метода разработан и программно реализован генератор случайных чисел. Проведен предварительный анализ алгоритма, в ходе, которого было сгенерировано 11000 чисел. Создано тестовое программное обеспечение для данного метода, рассмотрены предварительные показатели генерируемых случайных чисел. Показано, что функция распределения случайных чисел имеет равномерный вид. Преимуществом рассматриваемого генератора является простота в изготовлении и эксплуатации.

Ключевые слова: человеко-машинное взаимодействие, генератор, случайные числа, криптография, статистическое тестирование.

Averin A. S., Zyulyarkina N. D., Izhberdeeva E. M.

RANDOM NUMBER GENERATOR BASED ON HUMAN-COMPUTER INTERACTION

The paper is devoted to the development and analysis of a software random number generator based on human-computer interaction for software and cryptographic applications. Described is a method of generating random numbers based on human-computer interaction, using time and position of a cursor on a computer or smartphone display. Based on this method, a random number generator has been developed and programmatically implemented. A preliminary analysis of the algorithm was performed, during which 11,000 numbers were generated. The test software for this method has been created, preliminary indicators of generated random numbers have been considered. The random number distribution function is shown to be uniform. The advantage of this generator is its ease of manufacture and operation.

Keywords: *human-computer interaction, generator, random numbers, cryptography, statistical testing.*

Введение. В настоящее время крайне актуальной является проблема генерации случайных чисел с дальнейшей целью применения их в системах защиты информации. Характеристики систем безопасности в большинстве своем зависят от характеристик их криптографических подсистем, которые определяются, как правило, показателями используемых генераторов случайных чисел, так как на их базе создаются ключи шифрования и защитные последовательности [1]. Так же, можно отметить важную роль генераторов случайных чисел в таких областях знаний как, численный анализ, тория игр, теория принятия решений и моделирование.

Для генерации таких чисел используется несколько подходов. Первый из них связан с созданием и применением специальных устройств, использующих какие-либо физические источники шума. Второй подход связан с получением случайных величин на обычном персональном компьютере без применения дополнительного оборудования. Учитывая это, актуальным может стать способ, связанный с использованием стандартных устройств компьютера. Наиболее распространенным методом генерации случайных чисел, использующим этот подход, является генерация случайных чисел с использованием счетчика тактов процессора. К его недостаткам можно отнести чувствительность фазового шума генераторов частоты к внешним помехам, а значит, возможность влиять на генератор случайных чисел извне [2]. Так же генераторы случайных чисел могут строиться на фундаментальных законах физики, функциональных или «паразитных» свойствах электронных приборов и компьютерных систем, свойствах элементов электронных схем [3].

Целью данной работы является описание алгоритма генерации случайных чисел основанного на человеко-машинном взаимодействии, с использованием времени и положения курсора на дисплее компьютера или смартфона. Генератор случайных чисел, представленный в этой работе, разрабатывался как часть алгоритма консенсуса для блокчейн систем.

Существующие решения. В настоящее время существует большое количество предлагаемых решений в области генерации случайных чисел. Рассмотрим некоторые из них:

1. Аппаратный генератор случайных чисел, представленный в статье [1] Р.О. Султановым и Д.В. Лопатиным. Для связи с ПК в описанном генераторе авторами используется микроконтроллер с оригинальным программным обеспечением. Для работы с шиной USB использовалась открытая библиотека пользовательских функций, создано программное обеспечение для типовых задач, рассмотрены качественные показатели генерируемых случайных чисел. Показано, что функция распределения случайных чисел имеет равномерный вид. В преимуществах аппаратного генератора случайных чисел отмечается то, что он обладает простотой в изготовлении (тиражировании) и эксплуатации [1].

2. Генератор случайных чисел на базе звуковой карты, представленный в статье [4] Д.Б. Беспаловым и С.В. Белим. В качестве источника внешней энтропии рассматривается линейный вход звуковой карты. Этот разъем предназначен для подключения источников аналогового звукового сигнала, принимаемого на входе звуковой карты. Сигнал переводится в последовательность байтов с помощью аналого-цифрового преобразователя, к действию полезного сигнала постоянно добавляется шум, вызванный электромагнитными наводками от других элементов цепи, тепловым шумом в цепях питания и прочими флуктуациями в подсистеме аналогового входа [4]. Для считывания данных с линейного входа звуковой карты авторами была написана программа. Программа позволяет составить список устройств. Преимуществом называется цена «создания» работающего устройства, пользователь платит за программное обеспечение, а аппаратной составляющей не требуется.

3. Генератор случайных чисел с неравномерным распределением с помощью вебкамеры компьютера представленный в статье «Генератор Случайных Чисел С Неравномерным Распределением» [5] Р.М. Михерского, М.В. Исаева и Д.М. Полянчука. Для генерации случайных чисел с неравномерным распределением необходимо, чтобы веб-камера, подключенная к ноутбуку или компьютеру,

находилась в темном помещении или была закрыта [5]. Размер каждого снимка – 640 на 480 пикселей, из каждой фотографии извлекается матрица пикселей. Далее для 24-х разрядного изображения каждый пиксель содержит в себе информацию о трех цветах (для цветовой модели RGB) – соответственно красном, зеленом и синем. На каждый цвет отводится 8 бит, то есть максимально возможное значение в десятичном представлении – 255, а минимальное 0. Значению 255 соответствует максимальная интенсивность цвета, а значению 0 – минимальная. На следующем шаге, в общем случае формируется двумерный массив, в который записываются соответствующие значения разностей компонент цвета двух изображений для каждого из пикселей. Полученные разности могут изменяться от – 255 до 255. Эти разности и являются случайными числами [5].

4. Особо интересным примером реализации является генератор случайных чисел от компании «Код безопасности», разработчик криптографического комплекса «Континент», получила патент на биологический датчик случайных чисел. С описанием патента, возможно, ознакомиться на сайте Роспатента и доступно по ссылке: http://www1.fips.ru/fips_servl/fips_servlet?DB=RUPAT&DocNumber=2628213&TypeFile=html). В основе случайности лежит реакция пользователя на показанное ему изображение. «Компания уверяет, что до нее такие технологии в мире не патентовались». Датчик генерирует случайные последовательности, основываясь на скорости и точности реагирования руки пользователя на изменение изображения на экране ПК или планшета, для ввода используются мышь или тачскрин. В случайные моменты времени, определяемые кликами пользователя, измеряются меняющиеся во времени значения определенного набора величин, связанных с псевдослучайным процессом. Затем полученные случайные значения величин процесса отображаются в последовательность бит, к которой применяется функция хеширования. Так же компания на своем официальном сайте https://www.securitycode.ru/ пишет о том что: «Известные исследования подтверждают, что движения мышью или нажатия клавиш порождают предсказуемые последовательности чисел, которые нельзя напрямую использовать в задачах криптографии. Таким образом, общеизвестные способы требуют модификации и доработки» [7].

Предлагаемый алгоритм генерации случайных чисел на основе человеко-машинного взаимодействия. Был проведен анализ того, как часто люди взаимодействует с компьютерами и смартфонами, на январь 2020 года. Согласно отчету о состоянии цифровой сферы Digital 2020, который каждый год готовят We Are Social и Hootsuite количество интернет-пользователей в мире составляет 4,54 миллиарда и более 5,19 миллиарда человек пользуются мобильными телефонами. Так же стоит заметить, что среднестатистический человек проводит онлайн 6 ч 40 мин в сутки, в то время как в 2018 году проводил только 6 ч, а суммарно люди проведут онлайн за 2020 год один миллиард двести пятьдесят тысяч лет. Это говорит о том, что способ использования такого ресурса, как человеко-машинное взаимодействие может быть крайне эффективен. Важным преимуществом разрабатываемого алгоритма генерации случайных чисел является его независимость от дополнительных устройств, достаточно встроенных в любой смартфон дисплея и манипулятора.

В ходе разработки алгоритма консенсуса для блокчейн систем был создан алгоритм генерации случайных чисел на основе человеко-машинного взаимодействия. Данный алгоритм использует в своей работе функцию от времени и координат курсора в реальном времени (см. рис. 1).

Результатом является вектор из 24 случайных величин, из которых нами рассматриваются 19 (с 3 по 21). Это объясняется тем, что визуальный анализ показывает несоответствие рассматриваемому критерию - равной вероятности появления для всех цифр на каждой позиции. Процесс генерации случайных чисел происходит в момент взаимодействия пользователя с компьютером, планшетом или смартфоном. При этом процесс генерации случайных чисел проходит в фоновом режиме, то есть, остается незаметным для пользователя. В сравнении с генератором случайных чисел от компании «Код безопасности», предложенному алгоритму не требуется входных данных.

Предварительно функция от времени и координат курсора в реальном времени использует результаты делений реального времени на каждую координату дисплея поддельности, и сумму полученных результатов. Используется непрерывное течение времени в микросекундах и положение курсора, полу-

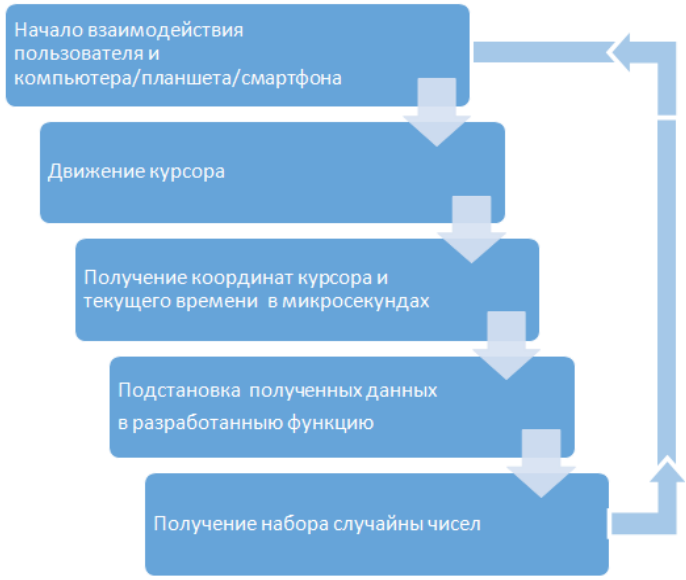

Рис. 1. Процесс получения случайных чисел

Таблица 1

Статистика значений случайных величин

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	0	1219	1127	1113	1125	1139	1089	1096	1093	1122	1146	1090	1119	1053	1120	1097	1146	1083	1120	1051	1113	1164	1312	2145
1	2513	1192	1079	1129	1124	1108	1130	1103	1104	1123	1069	1081	1121	1059	1139	1056	1086	1155	1088	1118	1072	1085	909	0
2	1764	1140	1080	1068	1061	1076	1138	1127	1110	1090	1121	1104	1133	1109	1067	1122	1111	1126	1096	1084	1106	1154	1227	2236
3	1375	1140	1063	1148	1095	1111	1081	1101	1102	1128	1088	1082	1118	1131	1076	1107	1166	1114	1068	1070	1077	1044	843	0
4	1173	1152	1068	1036	1111	1087	1134	1041	1086	1063	1117	1112	1013	1150	1091	1094	1155	1006	1117	1088	1112	1149	1324	2131
5	1021	1061	1154	1112	1179	1096	1035	1058	1144	1089	1102	1124	1145	1044	1100	1131	1088	1082	1134	1138	1122	1060	905	0
6	920	1036	1104	1071	1076	1097	1040	1143	1134	1101	1123	1040	1115	1086	1049	1118	1052	1102	1155	1103	1127	1164	1359	2229
7	824	1041	1048	1137	1084	1043	1140	1082	1135	1150	1051	1124	1122	1104	1143	1088	1060	1108	1071	1141	1063	1045	875	0
8	720	1094	1144	1123	1056	1133	1100	1116	1013	1088	1108	1126	1044	1156	1111	1079	1068	1093	1070	1097	1105	1077	1314	2260
9	691	926	1134	1064	1090	1111	1114	1134	1080	1047	1076	1118	1071	1109	1105	1109	1069	1132	1082	1111	1104	1059	933	0
X^2 набл	3776,9	61,8	11,54	11,47	10,89	6,30	12,37	8,71	11,50	8,04	6,84	6,09	14,99	12,72	7,51	4,06	14,40	13,17	7,38	6,63	3,90	21,55	402,9	11013,3

Таблица 2

Критические области для хи-квадрат распределения

n - 1	.995	.990	.975	.950	.900	.750	.500	.250	.100	.050	.025
9	1.73493	2.08790	2.70039	3.32511	4.16816	5.89883	8.34283	11.38875	14.68366	16.91898	19.02277

ченные данные подставляются в функцию, полученную экспериментальным. Процесс получения случайных чисел представлен на рис. 1. В ходе предварительного анализа, была собрана тестовая выборка из 11000 сгенерированных чисел. Данная выборка собиралась на экране с разрешением 1366 на 768 px. Далее в табл. 1, представлена статистика того какие значения и как часто принимались случайными величинами.

Из табл. 1 следует, что крайние значения в выборке, очевидно, не удовлетворяют искомым требованиям, поэтому в дальнейшем мы исключаем их анализа. Далее на рис. 2 показана статистика из табл. 1 в виде графиков распределения для каждой рассматриваемой случайной величины:

Следует отметить, что на графиках демонстрируется частота появления значений, в результате генерации, для всех случайных величин на каждой позиции (с 3 по 21) близка к равномерному. На графиках черная линия соответствует 1100.

Была проведена проверка гипотезы о равномерном распределении при помощи критерия согласия Пирсона. Ее результаты представлены в нижней части на табл. 1. а так же на табл. 2. (Критические области для хи-квадрат распределения) можно сравнить соответствие уровню значимости полученных результатов.

Согласно результатам, для вертикальных выборок от 3 до 21 можно сказать, что: при уровне значимости a = 0,05 выборочные данные не противоречат тому, что данные случайные величины имеют дискретное равномерное распределение.

Из анализа представленных данных мож-

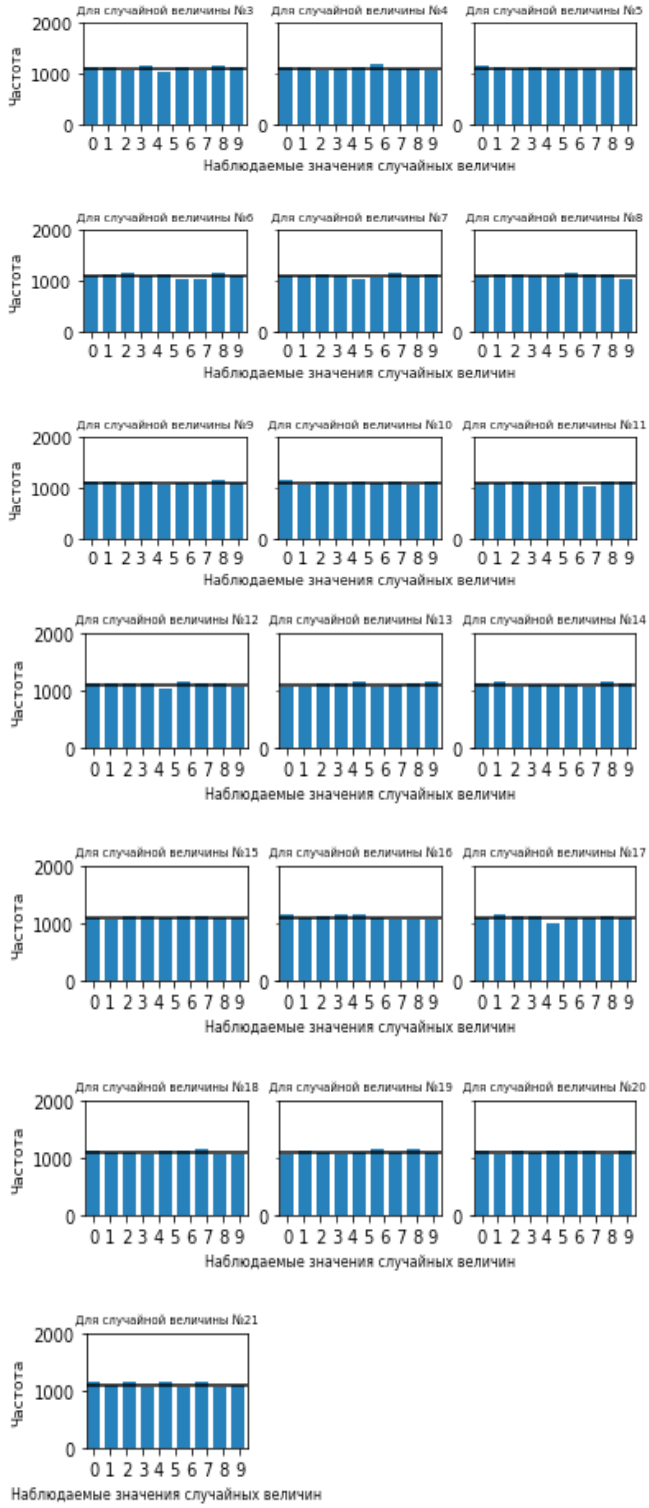

Рис. 2. Графики распределения случайных величин

но сделать вывод, что дальнейшее исследование и анализ генератора случайных чисел, основанного на человеко-машинном взаимодействии, является целесообразным.

Заключение. В результате данной работы был описан алгоритм генерации случайных чисел на основе человеко-машинном взаимодействии, с использованием времени и положения курсора на дисплее компьютера или смартфона.

Было рассмотрено несколько ранее опубликованных решений в сфере генерации случайных чисел. В том числе решение, пред-

ставленное компанией «Код безопасности». В сравнении с данными решениями алгоритм генерации случайных чисел на основе человеко-машинном взаимодействии имеет ряд преимуществ:

• не требуется дополнительное оборудование, будь то: микроконтроллер, аудио разъем или веб-камера;

• отсутствует необходимость использования, каких-либо изображений для работы генератора;

• генератор способен работать в фоновом режиме, абсолютно не заметно для пользователя.

Проведен предварительный анализ алгоритма, в ходе которого было сгенерировано 11000 чисел. Создано тестовое программное обеспечение для представленного метода, рассмотрены предварительные показатели генерируемых случайных чисел. Получено, что выборочные данные соответствуют тому, что распределение случайных величин является дискретным равномерным.

Безусловно, в дальнейшем необходимо увеличить количество итераций и провести исследование полученных материалов на критерий соответствия требованиям, предъявляемых к генераторам случайных чисел. Дальнейшее исследование и анализ генератора случайных чисел, основанного на человеко-машинном взаимодействии, является целесообразным и может быть продолжено в дальнейшем.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Султанов Р. О., Лопатин Д. В. Аппаратный генератор случайных чисел // Гаудеамус. 2013. №2 (22). URL: https://cyberleninka.ru/article/n/apparatnyy-generator-sluchaynyh-chisel (дата обращения: 25.04.2020).

2. Реализация генераторов случайных чисел / А. В. Ковалев // Научная сессия МИФИ. 2007. Том 12. С. 176–177.

3. Григорьев А. Ю. Методы тестирования генераторов случайных и псевдослучайных последовательностей// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017, № 1, С. 22–28.

4. Беспалов Д. Б., Белим С. В. Реализация генератора случайных чисел на базе звуковой карты // МСиМ. 2010. №1 (21). URL: https://cyberleninka.ru/article/n/realizatsiya-generatora-sluchaynyh-chisel-na-baze-zvukovoy-karty (дата обращения: 25.04.2020).

5. Михерский Р.М., Исаев М.В., Полянчук Д.М. ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ С НЕРАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ // Вестник Физико-технического института Крымского федерального университета имени В. И. Вернадского. 2018. №1. URL: https://cyberleninka.ru/article/n/generator-sluchaynyh-chisel-s-neravnomernym-raspredeleniem (дата обращения: 25.04.2020).

References

1. Sultanov R. O., Lopatin D. V. Apparatnyy generator sluchaynykh chisel // Gaudeamus. 2013. №2 (22). URL: https://cyberleninka.ru/article/n/apparatnyy-generator-sluchaynyh-chisel (data obrashcheniya: 25.04.2020).

2. Realizatsiya generatorov sluchaynykh chisel / A. V. Kovalev // Nauchnaya sessiya MIFI. 2007. Tom 12. C. 176–177.

3. Grigor'yev A. YU. Metody testirovaniya generatorov sluchaynykh i psevdosluchaynykh posledovatel'nostey// Uchenyye zapiski UlGU. Ser. Matematika i informatsionnyye tekhnologii. UlGU. Elektron. zhurn. 2017, № 1, S. 22–28.

4. Bespalov D. B., Belim S. V. Realizatsiya generatora sluchaynykh chisel na baze zvukovoy karty // MSiM. 2010. №1 (21). URL: https://cyberleninka.ru/article/n/realizatsiya-generatora-sluchaynyh-chisel-na-baze-zvukovoy-karty (data obrashcheniya: 25.04.2020).

5. Mikherskiy R.M., Isayev M.V., Polyanchuk D.M. GENERATOR SLUCHAYNYKH CHISEL S NERAVNOMERNYM RASPREDELENIYEM // Vestnik Fiziko-tekhnicheskogo instituta Krymskogo federal'nogo universiteta imeni V. I. Vernadskogo. 2018. №1. URL: https://cyberleninka.ru/article/n/generator-sluchaynyh-chisel-s-neravnomernym-raspredeleniem (data obrashcheniya: 25.04.2020).

АВЕРИН Андрей Сергеевич, аспирант кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). Россия, 45408, г. Челябинск, пр. Ленина, 76. E-mail: andreaverin24@gmail.com.

ЗЮЛЯРКИНА Наталья Дмитриевна, доктор физико-математических наук, доцент, профессор кафедры «Защита информации» ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). Россия, 454080, г. Челябинск, пр. Ленина, 76. E-mail: ziuliarkinand@susu.ru.

ИЖБЕРДЕЕВА Елизавета Монировна, студент кафедры теории управления и оптимизации ФГБОУ ВО «Челябинский государственный университет». Россия, 454001, г. Челябинск, ул. Братьев Кашириных, 129. E-mail: elizaveta.izhberdeeva@gmail.com.

AVERIN Andrey, Postgraduate Student, Department of Information Security, South Ural State University (National Research University). 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: andreaverin24@gmail.com.

ZYULYARKINA Natalya, Doctor of Physics and Mathematics, Associate Professor, Professor of the Department of Information Security, "South Ural State University (national research university)". 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: ziuliarkinand@susu.ru.

IZHBERDEEVA Elizaveta, student of the Department of Control Theory and Optimization, "Chelyabinsk State University". Russia, 454001, Chelyabinsk, Kashirin Brothers Street, 129. E-mail: elizaveta.izhberdeeva@gmail.com.

УДК 004.056.55 Вестник УрФО № 2(36) / 2020, с. 24–28

Зырянова Т. Ю., Распопов Н. А.

DOI: 10.14529/secur200204

РЕАЛИЗАЦИЯ ПРОТОКОЛА ДИФФИ–ХЕЛЛМАНА В НЕЗАЩИЩЁННОМ ОТ ПЕРЕХВАТА КАНАЛЕ

В статье рассматривается реализация протокола Диффи–Хеллмана в незащищённом от перехвата канале. Суть данного метода заключается в применении стеганографии для передачи открытого ключа в незащищённом канале передачи данных. Открытый ключ зашифровывается при помощи блочного шифра и встраивается в изображение стеганографическим методом LSB. Уникальность изображения и невозможность изменения ключа обеспечивается за счёт лавинного эффекта. Реализация протокола Диффи–Хеллмана в незащищённом канале передачи данных уже давно остаётся актуальной, хотя и существует решение с использованием технологии инфраструктуры открытых ключей. В статье предложено новое решение данной проблемы.

Ключевые слова: *асимметричная криптография, блочное шифрование, инфраструктура открытых ключей, незащищённый канал, протокол Диффи–Хеллмана, стеганография.*

Zyryanova T. Yu., Raspopov N. A.

IMPLEMENTATION OF THE DIFFIE-HELLMAN PROTOCOL IN A CHANNEL UNLESS PROTECTED FROM INTERCEPT

This article discusses the implementation of the Diffie-Hellman protocol in an unprotected channel. The essence of this method is to use steganography to transmit the public key in an unsecured channel. The public key is encrypted using a block cipher and encoded into the picture using the LSB method. The uniqueness of the picture and the impossibility of changing the key is ensured by the avalanche effect. The implementation of the Diffie-Hellman protocol in an insecure channel has long remained relevant, although there is a solution in the form of public key infrastructure, but in this article a new solution to this problem was proposed.

Keywords: *asymmetric cryptography, block encryption, Diffie-Hellman protocol, public key infrastructure, steganography, unprotected channel.*

В 1974 году Уитфилд Диффи и Мартин Хеллман решили проблему, остро стоявшую перед криптографией – безопасное распределение ключей шифрования. На тот момент не существовало метода, который позволил бы вырабатывать общий ключ для его использования в симметричной системе шифрования. Данный протокол основан на эксплуатации задачи вычисления дискретного логарифма[1].

При работе алгоритма каждый пользователь:

1. Генерирует случайное натуральное число a – закрытый (или секретный) ключ;

2. Совместно с другим пользователем устанавливает открытые параметрыри g (обычно значения p и g генерируются на одной стороне и передаются другой), где

• p является случайным простым числом,

• (p – 1)/ 2 также должно быть случайным простым числом (для повышения безопасности),

• g является первообразным корнем по модулю p (также является простым числом);

3. Вычисляется открытый ключ A, используя преобразования над закрытым ключом: $A = g^a mod p$;

4. Обменивается открытыми ключами с удалённой стороной.

5. Вычисляет общий секретный ключ K, используя открытый ключ удалённой стороны B и свой закрытый ключ a: $K = B^A mod p$.

Ключ получается равным с обеих сторон, потому что: $B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p$. В практических реализациях в качествеаи b используются числа порядка 10^{100} и рпорядка 10^{300}. Число gнеобязательно должно быть большим и обычно имеет значение в пределах первого десятка.

Протокол Диффи–Хеллмана позволил решить проблему распределения ключей, но, как и у всего, у него есть недостатки. Таким недостатком является то, что невозможно однозначно установить, является ли открытый ключ, который был получен в ходе реализации протокола легальным, а не подменённым злоумышленником. Именно поэтому данный протокол уязвим к атаке «человекпосередине». Суть атаки «человекпосередине» или MITM (Men-in-the-middle) заключается в том, что злоумышленник получает возможность не только читать весь поток передаваемых сообщений, но и осуществляет вмешательство в протокол передачи, удаляя или искажая информацию (рис. 1). Злоумышленник тайно ретранслирует и при необходимости изменяет связь между сторонами. Данная атака особенно опасна тем, что практически незаметна для пользователей. Пользователи сети могут даже не догадываться, что весь сетевой трафик проходит через злоумышленника.

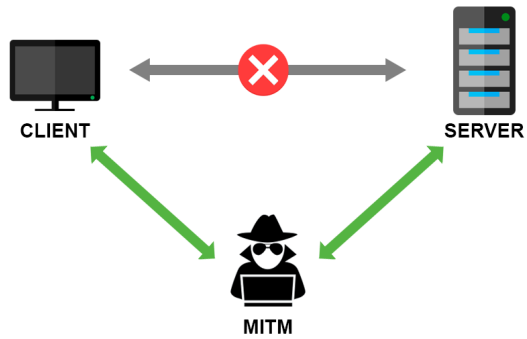

Рис. 1. Реализация атаки «человекпосередине»

Атака обычно начинается с прослушивания канала связи и заканчивается тем, что криптоаналитик пытается подменить перехваченное сообщение, извлечь из него полезную информацию, перенаправить его на какой-либо внешний ресурс. Предположим, Алиса планирует передать Бобу информацию. Злоумышленник Ева обладает знаниями о структуре и свойствах используемого метода передачи данных, а также о факте планируемой передачи информации, которую она планирует перехватить. Для совершения атаки Ева «представляется» Алисе Бобом, а Бобу как Алиса. Алиса, ошибочно думая, что ведёт обмен информацией с Бобом, на самом деле посылает данные Еве. Ева в своём случае совершает манипуляции с перехваченной информацией (скопировав, модифицировав) пересылает её Бобу; Боб в своём случае полагает, что данная информация пришла от Алисы. Одним из примеров атак типа «человек посередине» является активное прослушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передаёт сообщения между ними. Тем самым он заставляет жертв поверить, что они разговаривают непосредственно друг с другом через частную связь, фактически же весь разговор управляется злоумышленником. Злоумышленник должен уметь перехватывать все передаваемые между двумя жертвами сообщения, а также вводить новые. В большинстве случаев это довольно просто, например, злоумышленник может вести себя как «чело-

век посередине» в пределах диапазона приёма беспроводной точки доступа (Wi-Fi).

На сегодняшний день известно решение данной проблемы – это инфраструктура открытых ключей PublicKeyInfrastructure (PKI) [2]. Основная идея PKI заключается в том, что удостоверяющий центр создает электронный документ — сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, а открытый ключ (publickey) свободно передается в сертификате. Недостатком данной системы является то, что сертификат может быть скомпрометирован, и тогда злоумышленник сможет под видом легального пользователя отправлять сообщения получателю. PKI позволяет нейтрализовать уязвимость протокола Диффи–Хеллмана, но это решение является слишком громоздким, так как оно ставит между абонентами удостоверяющий центр, который даёт гарантию, что ключ, полученный абонентом является легальным. Наличие третьей стороны, принимающей участие в обмене информации, увеличивает её стоимость. PKI помогает обойти уязвимость протокола Диффи–Хеллмана, но она не решает эту проблему полностью. Инфраструктура открытых ключей помогает только тем, кто готов платить за сертификат. На сегодняшний день необходима альтернатива PKI, так как сфера информационных технологий развивается бурными темпами, и необходимо решение, которое не будет ставить абонентов в зависимость от третьей стороны. В статье предлагается метод решения проблемы уязвимости данной технологии к атаке MITM. Предлагаемое решение совмещает в себе стеганографические и криптографические методы.

Научная новизна предлагаемого метода обусловлена нестандартным подходом к использованию криптографии и стеганографии. В данном случае шифрование используется как средство, придающее уникальность выбранному ключу. Придание уникальности обеспечивается за счёт «лавинного эффекта». Стеганографическая часть протокола также используется нестандартным образом. В данном случае при помощи стеганографии мы будем кодировать зашифрованный ключ методом RGB. Это позволит получить изображение с уникальной палитрой цветов.

Обозначим предполагаемых санкционированных участников обмена сообщениями как Алиса и Боб, а в качестве злоумышленника будет выступать Ева.

Предлагаемый алгоритм включает следующие этапы.

1. Алиса и Боб вырабатывают открытые ключи в соответствии с протоколом Диффи – Хеллмана.

2. Алиса и Боб выбирают ключи для шифрования шифром AES и публикуют их как открытую информацию. Данные ключи могут не совпадать, так как в этом случае шифрование используется исключительно для реализации «лавинного эффекта».

3. Алиса и Боб встраивают ключи в контейнер, который вмещает в себя ключ выбранной длины. Изображение-контейнер с встроенными ключами также публикуется как открытая информация. «Лавинный эффект» обеспечивает уникальность полученного изображения, и малейшие изменения в ключе приведут к сильному искажению изображения.

4. Алиса и Боб обмениваются изображениями.

5. Алиса и Боб сравнивают полученные изображения с изображением, опубликованным ранее и, если изображения совпадают, то переходят к следующему этапу. Сравнение изображений происходит при помощи сканирования структуры изображений, полученных методом RGB. Если существует различие хотя бы в 1 байт, то изображение считается скомпрометированным и соединение разрывается. Данная процедура может считаться также барьером защиты. Злоумышленнику необходимо будет подобрать изображение идентичное изображению Алисы и Боба. Эта процедура подбора подобна поиску коллизий 2 рода хэш-функции второго рода.

6. Алиса и Боб декодируют изображение и расшифровывают свои открытые ключи при помощи ранее опубликованных ключей AES.

7. Алиса и Боб вырабатывают общий ключ, следуя протоколу Диффи–Хеллмана.

Обобщённая модель алгоритма представлена на рис. 2.

В случае перехвата Евой изображения с встроенным в него ключом, она сможет лишь раскодировать изображение и получить открытый ключ, но, чтобы заменить его на свой, ей будет необходимо потратить значительное количество времени на подбор такого ключа, который при кодировании будет давать изображение, идентичное изображению

Рис. 2. Реализация алгоритма

Алисы и Боба. Так же злоумышленнику необходимо скомпрометировать два изображения, а это увеличивает время работы в два раза. Обмена сообщениями между Алисой и Бобом происходит за относительно небольшой промежуток времени, любая задержка в момент обмена сообщениями может выдать злоумышленника. Это делает атаку нецелесообразной для злоумышленника, так как затраты на атаку начнут превышать её стоимость и как следствие утратится целесообразность атаки. Также данная атака будет требовать значительного количества времени или же больших вычислительных ресурсов.

Преимущество данного алгоритма заключается в том, что пользователи являются независимыми от центров сертификации. Пользователям достаточно использовать предлагаемый алгоритм, для того чтобы выработать общий ключ. Также данный алгоритм применим в сетях, которые не используют интернет, так как в данном случае единственное, что необходимо двум абонентам для выработки общего ключа – это канал связи. Именно поэтому данный алгоритм может найти место применение в военной сфере. Алгоритм не обладает данными, которые необходимо держать в секрете. Это исключает вероятность несанкционированной утечки информации и облегчает работу с ней. Также в качестве достоинства предложенного решения можно выделить его относительную простоту. Это позволяет упростить порог квалификации, необходимой для эксплуатации данного решения. В принципе реализацию данного алгоритма может использовать любой человек, имеющий базовые познания в криптографии. Стоит отметить, что такой протокол является легко масштабируемым, так как при выработке не имеет ограничительных мер.

Если рассматривать финансовую сторону, то данный протокол является менее затратным вариантом в сравнении с сертификатами, которые необходимо продлевать по истечению срока. Он позволяет увеличить количество интернет-ресурсов, которые будут использовать защищённое соединение, так как потребует лишь небольшого увеличения вычислительных мощностей сервера. Это гораздо выгоднее, нежели использовать сертификат. Это открывает сектор коммерческих организаций. Данный алгоритм предлагает более выгодные условия для рынка, нежели сертификаты. Предложенный вариант решения проблемы реализации протокола Диффи–Хеллмана в незащищённом от перехвата канале предлагает необычный взгляд на использование криптографических и стеганографических примитивов, так как в данном случае шифрование не используется для обеспечения конфиденциальности, а кодирование стегонтейнера не используется для сокрытия факта передачи информации. Шифрование позволяет обеспечить невозможность внесения изменений в ключ или его полной замены, кодирование позволяет придать данному ключу оболочку в виде изображения.

С точки зрения производительности данный алгоритм несильно отличается от обычного варианта алгоритма Диффи–Хеллмана. Все операции не являются вычислительно сложными, единственное, что может составить задержку – это проверка изображения при получении. Данный алгоритм реализуем на таких объектно-ориентированных языках программирования как C#.

Область применения данного метода довольно обширна. Любая система, которая требует шифрования потока сообщений между двумя абонентами, может использовать его в своей деятельности. В частности, винтернет-пространстве любой информационный ресурс, использующий технологию https может использовать данный алгоритм для организации защиты информации. Также алгоритм подходит для реализации частной пе-

переписки в мессенджерах. Например, данная функция может использоваться в качестве дополнительного шифрования переписки. Если пользователи считают, что их переписка может попасть не в те руки и хотят обезопасить себя и свои данные, то предложенный алгоритм является адекватным решением. Он позволит пользователям генерировать персональный ключ шифрования, который будет известен только им. Это позволит обеспечить конфиденциальность информации. В том числе данный протокол может найти своё применение в прикладных программах, направленных на защиту информации. Он позволит упростить процедуру генерации общего ключа на основе протокола Диффи–Хеллмана, если компания не может обеспечить защиту канала передачи информации. Это в свою очередь позволит снизить затраты на обеспечение информационной безопасности или же усилить уязвимые места в системе безопасности.

Если рассматривать протокол с точки зрения злоумышленника, то потенциальными уязвимостями могут быть изображения, полученные входе кодирования зашифрованного открытого ключа. Если будет найден алгоритм, который за полиномиальное время позволит получать идентичное изображение, но с другим встроенным ключом, то данный алгоритм можно будет считать скомпрометированным. В остальных случаях он является хорошим сдерживающим фактором для злоумышленника, так как для реализации атаки требуется значительное количество вычислительных ресурсов и высокий уровень квалификации.

В данной статье был предложен новый метод решения проблемы реализации протокола Диффи–Хеллмана в незащищённом от перехвата канале. Также был предложен нестандартный взгляд на криптографические и стеганографические примитивы. В итоге был получен алгоритм, не требующий высокой вычислительной мощности со стороны пользователей и являющийся простым в использовании. Были рассмотрены сферы применения, где данный алгоритм может применяться и успешно доказывать свою эффективность в сравнении с PKI.

Литература

1. ДиффиУ., Хеллман М.Новые направления в криптографии. IEEETransactionsonInformationTheory, vol. IT-22, Nov. 1976, pp: 644—654.

2. Горбатов В. С., Полянская О. Ю. Основытехнологии PKI. – М.: Горячаялиния – Телеком, 2003.

References

1. Diffi U., Khellman M. Novyye napravleniya v kriptografii. IEEETransactionsonInformationTheory, vol. IT-22, Nov. 1976, pp: 644—654.

2. GorbatovV. S., PolyanskayaO. YU. Osnovytekhnologii PKI. – M.: Goryachayaliniya – Telekom, 2003.

ЗЫРЯНОВА Татьяна Юрьевна, доцент кафедры «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, кандидат технических наук. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: tzyryanova@usurt.ru

РАСПОПОВ Никита, студент 2 курса электротехнического факультета по направлению подготовки Информационная безопасность Уральского государственного университета путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: nastyazavedenskaya@yandex.ru

ZYRYANOVA Tatiana Yuryevna, associate professor of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorovastr., Yekaterinburg, 620034. E-mail: tzyryanova@usurt.ru.

RASPOPOV Nikita, 2-yearstudentof Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorovastr., Yekaterinburg, 620034. E-mail: wildpro6@gmail.com

УДК 004.056 + 003.26 Вестник УрФО № 2(36) / 2020, с. 29–33

Казаковцев М. С., Рогачев С. С., Михайлова У. В.

DOI: 10.14529/secur200205

ИСПОЛЬЗОВАНИЕ ОСОБЫХ ТОЧЕК ОТПЕЧАТКОВ ПАЛЬЦЕВ В БИОКРИПТОГРАФИИ И КОДИРОВАНИИ ИНФОРМАЦИИ

В статье рассмотрен процесс создания криптографической последовательности из биометрических данных человека. Представлены краткие сведения о признаках папиллярного узора, а также алгоритмах предварительной обработки изображения отпечатка пальца. Проведена сравнительная характеристика алгоритмов на этапах генерации, хранения и сравнения информации о ключе. Результатом проведенного исследования является выбор наиболее эффективных алгоритмов создания биокриптографического ключа и защиты информации о нем.

Ключевые слова: *биокриптография, отпечаток пальца, последовательность, бинаризация, алгоритм, ключ.*

Kazakovtsev M. S., Rogachev S. S., Mikhailova U. V.

USE OF FINGERPRINT SPECIFIC POINTS IN BIOCRYPTOGRAPHY AND INFORMATION CODING

This article discusses the process of creating a cryptographic sequence from human biometric data. Brief information about the features of the papillary pattern, as well as algorithms for the preliminary processing of the fingerprint image are presented. A comparative characteristic of the algorithms at the stages of generation, storage and comparison of key information is carried out. The result of the study is the selection of the most effective algorithms for creating a biocryptographic key and protecting information about it.

Keywords: *biocryptography, fingerprint, sequence, binarization, algorithm, key.*

В разрезе современных тенденций цифровизации и киберфизических систем появилось и такое понятие как биокриптография. Это весьма интересная коллаборация биометрии и криптографии. Появилась она в связи с всеобщей цифровизацией общества и поиском более удобных способов для хранения ключевой информации. Основная ее область исследования – применение биометрических данных, в нашем случае отпечатков пальцев.

Для идентификации личности наиболее часто используются такие биометрические данные, как отпечатки пальцев и сканирование радужной оболочки, в качестве преимуществ первого можно выделить:

• устойчивость отпечатков к изменениям с возрастом человека;

• крайне малая вероятность встречи идентичных отпечатков, как у разных людей, так и у одного человека. В истории пока не случалось совпадений или их просто не находили;

• невозможность утери.

У любого отпечатка существуют две категории признаков:

• глобальные;

• локальные.

Признаки первого типа можно увидеть без использования специальных приборов. Они состоят из счетчика линий, ядра, пункта «дельта», области образа и папиллярного узора. Уникальные точки малого размера являются в свою очередь признаками второго типа - они не повторяются на разных пальцах, в отличие от глобальных признаков. Их уникальность обеспечивается с помощью минуций – точек, где линии заканчиваются, делятся или меняют направление. Все по причине того, что линии отпечатков пальцев не образуют прямые линии ни при каких обстоятельствах, ведь они постоянно разветвляются, ломаются и заканчиваются.

Процесс идентификации, как правило, состоит из двух этапов. Первым этапом проходит классификация отпечатков по признакам, видным невооруженным глазом, для разделения на классы. Второй этап заключается в распознавании отпечатка пальца на основе сравнения структуры и коэффициента совпадения точек минуции.

Немаловажным будет упомянуть и предварительный этап в улучшении изображения отпечатка фильтром Габора. Все потому, что на изображении до обработки из-за помех разного рода, как грязь, складки и других, линии отпечатков могут деформироваться, а это в свою очередь влечет за собой ошибки распознавания признаков. С целью устранения этих ошибок изображение улучшают. При нем падает зашумленность изображения, а достоверность модели возрастает.

Функция фильтра Габора в классическом виде выглядит следующим образом:

Стоит отметить, что параметры σ и f относятся к маске фильтра, а угол θ – к ориентации маски над изображением. Формула является произведением гауссиана и периодической функции, что подразумевает улучшение монотонных областей повторяющихся частей изображения.

$$h(x,y) = e^{\left(-\frac{x^2+y^2}{2\sigma^2}\right)} cos2\pi f(xsin\theta + ycos\theta)$$

Эмпирическим путем были определены значения параметров σ и f, которые равны 7 и 10, соответственно. Это означает снижение коэффициентов от центра окружности по радиусу длинной в 7 точек и периодическое повторение изображение через 10.

Таблица 1

Параметр	Значение
x, y	Координаты точек
σ	Стандартное отклонение предполагаемого нормального распределения
f	Частота
θ	Ориентация фильтра

Далее следует алгоритм Базена, основополагающий смысл которого состоит в перпендикулярности линий отпечатка пальца градиенту изображения отпечатка, соответствующему перепадам цветов от белого к черному. Таким образом, определяется поле направлений (рис. 1).

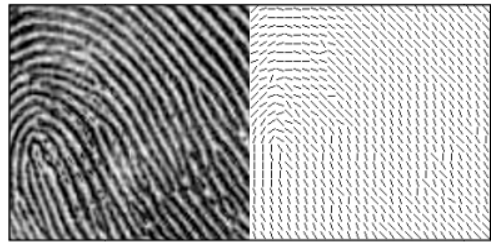

Рис. 1. Определение поля направлений

После этого происходит фильтрация и бинаризация изображения, которая наглядно изображена на рис. 2.

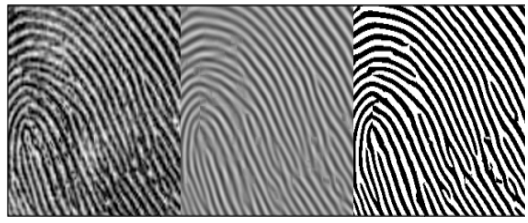

Рис. 2. Фильтрация и бинаризация изображения

Слева – начальное изображение, посередине – темное фильтрованное, а справа уже бинаризованное конечное улучшенное изображение.

Следующим этапом идет генерация биометрической последовательности.

Справиться с задачей преобразования входного набора биометрических данных в последовательность битов помогает блок ге-

нерации биометрической последовательности. Полученная последовательность требуется в дальнейшем для того, чтобы сформировать криптографический ключ.

Для получения биометрической последовательности предлагается использование n, t-пороговой схемы Шамира. Схожим алгоритмом действия обладают такие схемы, как, например, схема Шнорра и схема Блэкли. Однако первая не подходит для идентификации с помощью отпечатка пальца по причине того, что, в сравнении со схемой Шамира, она имеет меньший размер цифровой подписи. Вторая же менее эффективна: в схеме Шамира каждая часть такого же размера, как и секрет, а в схеме Блэкли каждая часть в t раз больше.

По центру папиллярного узора ставится точка O, которая является центром новой системы координат (эта и последующие операции производятся на уже обработанном изображении).

Сначала вычисляются особые точки, являющиеся элементами конечного поля, что задано простым числом. Над этим полем формируется многочлен таким образом, что его график проходит через подмножество особых точек. На базе построенного полинома выбираются случайные точки, после чего из них вычисляются координаты, из которых формируется множество. Данным образом получается система, информацию о которой можно открыто хранить в базе данных. Биометрическая последовательность получается посредством соединения элементов полинома и аналогично не требует защищенного хранения, ибо воссоздается из вновь полученного отпечатка пальца.

За тем эта информация сравнивается с ранее имеющейся информацией, также сформированной из особых точек отпечатка. С помощью интерполяционного многочлена Лагранжа образуется полином, который должен совпадать с эквиваленцией исходного и вновь полученного множеств особых точек папиллярного узора, не меньше значения t.

Выполнение всех вычислений в пределах конечного поля приводит к высокой точности системы, а использование проблемы восстановления полинома из определенного числа точек – к высокой степени безопасности.

Далее в формировании биокриптографического ключа идет блок fuzzy extractor.

В стандартных системах идентификации с помощью отпечатка пальца есть один существенный недостаток – это относительная постоянность совпадений поступающей и исходной биометрической последовательностей, из-за чего в случае получения доступа к информации посторонним лицом, заменить ее не представляется возможным. В таком случае необходимо внедрить следующие требования к биометрической системе:

• каждый новый криптографический ключ в процедуре регистрации пользователя должен отличаться от предыдущего;

• один из входных параметров функции генерации ключа должен быть случайным;

• случайный параметр в открытом виде не должен нигде храниться, как и биометрическая последовательность.

Реализация подобных требований стала возможна после появления блока fuzzy extractor. Добавление в генерацию криптографического ключа стала хоть и необязательной, но очень желательной для добавления. Также данный блок способен сформировать случайную последовательность из вновь сгенерированной биометрической и открытой информации.

Для достижения наилучшего результата мы для алгоритма рассмотрели 3 блока fuzzy и выбрали fuzzy extractor, а не один из других двух, потому что методы fuzzy commitment и fuzzy vault имеют ограничения, в том числе – неспособность генерировать много несвязанных шаблонов из одного и того же набора биометрических данных. Один из возможных способов преодоления этой проблемы - применение функции трансформации черт к биометрическому шаблону до того, как она будет защищена с помощью биометрической криптосистемы. Биометрические криптосистемы, которые объединяют трансформацию с генерацией защищенного эскиза, называют гибридными.

Создание алгоритмов, основанных на биометрии и криптографии, позволит разработать системы, в которых отсутствуют недостатки обоих направлений, например, возможность хищения закрытого криптографического ключа или незащищенность биометрического образа.

Литература

1. Схемы идентификации [Электронный ресурс] URL: http://www.dialektika.com/PDF/978-5-9908462-4-1/part.pdf

2. Биометрическая аутентификация: защита систем и конфиденциальность пользователей [Электронный ресурс] URL: https://www.osp.ru/os/2012/10/13033122

3. В.Ю. Гудков, А.В. Бойцов. Улучшение изображений отпечатков пальцев с помощью фильтра Габора [Электронный ресурс] URL: https://cyberleninka.ru/article/n/15705550

4. Juels A., Wattenberg M.A Fuzzy Commitment Scheme [Электронный ресурс] URL: https://www.arijuels.com/wp-content/uploads/2013/09/JW99.pdf

5. Uludag U., Pankanti S., Jain A.K. Fuzzy Vault for Fingerprints [Электронный ресурс] URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.5939&rep=rep1&type=pdf

6. Fuzzy extractor [Электронный ресурс] URL: https://en.bitcoinwiki.org/wiki/Fuzzy_extractor

7. Коновалов М.В., Михайлова У.В., Хусаинов А.А. и др. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2. № 71. С. 159–-161.

8. Михайлова У.В., Коновалов М.В., Гуринец К. и др. Идентификация личности // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2.№ 71. С. 164–166

9. Михайлова У.В., Лукьянов Г.И., Дончан Д.М. Анализ биометрической аутентификации на устойчивость при воздействии внешних факторов // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 76-ой междунар. науч.-техн. конф. Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. Т. 1. С. 295–295.

References

1. Skhemy identifikatsii [Elektronnyy resurs] URL: http://www.dialektika.com/PDF/978-5-9908462-4-1/part.pdf

2. Biometricheskaya autentifikatsiya: zashchita sistem i konfidentsial'nost' pol'zovateley [Elektronnyy resurs] URL: https://www.osp.ru/os/2012/10/13033122

3. V.YU. Gudkov, A.V. Boytsov. Uluchsheniye izobrazheniy otpechatkov pal'tsev s pomoshch'yu fil'tra Gabora [Elektronnyy resurs] URL: https://cyberleninka.ru/article/n/15705550

4. Juels A., Wattenberg M.A Fuzzy Commitment Scheme [Elektronnyy resurs] URL: https://www.arijuels.com/wp-content/uploads/2013/09/JW99.pdf

5. Uludag U., Pankanti S., Jain A.K. Fuzzy Vault for Fingerprints [Elektronnyy resurs] URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.5939&rep=rep1&type=pdf

6. Fuzzy extractor [Elektronnyy resurs] URL: https://en.bitcoinwiki.org/wiki/Fuzzy_extractor

7. Konovalov M.V., Mikhaylova U.V., Khusainov A.A. i dr. Algoritmy shifrovaniya dannykh // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2013. T. 2. № 71. S. 159–161.

8. Mikhaylova U.V., Konovalov M.V., Gurinets K. i dr. Identifikatsiya lichnosti // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2013. T. 2.№ 71. S. 164–166

9. Mikhaylova U.V., Luk'yanov G.I., Donchan D.M. Analiz biometricheskoy autentifikatsii na ustoychivost' pri vozdeystvii vneshnikh faktorov // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. Tezisy dokladov 76-oy mezhdunar. nauch.-tekhn. konf. Izd-vo Magnitogorsk. gos. tekhn. un-ta im. G.I. Nosova, 2018. T. 1. S. 295–295.

КАЗАКОВЦЕВ Михаил Сергеевич, студент 2 курса кафедры Информатики и Информационной Безопасности Магнитогорского Государственного Технического Университета им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: misha.mk74@mail.ru

РОГАЧЕВ Станислав Сергеевич, студент 2 курса кафедры Информатики и Информационной Безопасности Магнитогорского Государственного Технического Университета им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: misha.mk74@mail.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и Информационной Безопасности Магнитогорского Государственного Технического Университета им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ylianapost@gmail.com

KAZAKOVCEV Mihail, 2-year student o department of Informatics and Information Security Nosov Magnitogorsk State Technical Universit., 455000, Magnitogorsk, av. Lenina, 38. E-mail: misha.mk74@mail.ru

ROGACHEV Stanislav, 2-year student o department of Informatics and Information Security Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, av. Lenina, 38. E-mail: misha.mk74@mail.ru

MIKHAILOVA Uliana, candidate of technical sciences, associate professor of the Department of Informatics and Information Security Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, av. Lenina, 38. E-mail: ylianapost@gmail.com

УДК 004.421.6:519.115.1 Вестник УрФО № 2(36) / 2020, с. 34–42

Мищенко Е. Ю., Соколов А. Н.

DOI: 10.14529/secur200206

ОПРЕДЕЛЕНИЕ ЭФФЕКТИВНОСТИ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ НАРУШИТЕЛЯ

В статье рассматривается модель нарушителя, как средство проверки эффективности некоторых методов обезличивания персональных данных (ПД), основанных на искажениях состава и структуры базы ПД. Отсутствие методик определения эффективности обезличивания ПД является препятствием для широкого применения на практике процедуры обезличивания, как способа защиты ПД. Приведено описание модели нарушителя, а также алгоритм воздействия на обезличенную базу данных, целью которого является раскрытие алгоритма искажения состава (или структуры). Критерием успеха алгоритма воздействия является минимум итераций. В то же время, отсутствие успеха алгоритма модели нарушителя указывает на достаточную эффективность алгоритма метода обезличивания. В результате эксперимента получены рекомендации по использованию конкретных параметров для методов обезличивания.

Ключевые слова: *модель нарушителя, метод изменения состава или семантики, метод перемешивания, обезличивание персональных данных, вероятность идентификации.*

DETERMINATION OF THE EFFECTIVENESS OF ANONYMIZATION OF PERSONAL DATA USING THE INTRUDER'S MODEL

The article discusses the violator's model as a means of testing the effectiveness of some methods of anonymization of personal data (PD) based on distortions of the composition and structure of the PD database. The lack of methods for determining the effectiveness of anonymization of PD is an obstacle to the widespread use of the procedure of anonymization in practice as a way to protect PD. A description of the intruder's model is given, as well as an algorithm for influencing an impersonal database, the purpose of which is to disclose an algorithm for distorting the composition (or structure). The criterion for the success of the impact algorithm is the minimum of iterations. At the same time, the lack of success of the intruder model algorithm indicates the sufficient efficiency of the depersonalization method algorithm. As a result of the experiment, recommendations were obtained on the use of specific parameters for methods of depersonalization.

Keywords: *intruder's model, method of changing the composition or semantics, mixing method, depersonalization of personal data, identification probability.*

1. Введение

Обезличивание ПД имеет главной целью нейтрализацию попыток злоумышленника использовать эти ПД во вред физическому лицу. Главная особенность Российского законодательства о ПД в отличие от зарубежного заключается в том, что в соответствие с Законом «О персональных данных» [1], обезличивание не позволяет определить принадлежность ПД физическому лицу без применения дополнительной информации, т.е. наиболее важным свойством обезличенных данных является возможность их деобезличивания. Эта возможность позволяет обрабатывать ПД после их восстановления из обезличенной формы.

В 2013 году Приказом Роскомнадзора [2] были определены четыре основных метода обезличивания: введение идентификаторов, изменение состава или семантики, декомпозиция и перемешивание.

Принципиальное отличие методов состоит в отношении к идентифицирующей информации:

– методы идентификаторов и декомпозиции основаны на отделении идентифицирующей информации от обезличенных данных, при этом идентифицирующая часть недоступна для злоумышленника во время хранения, но может быть доступна во время прочих сеансов обработки;

– методы изменения состава/семантики и перемешивания основаны на скрытии (искажении) расположения идентифицирующей информации в базе обезличенных данных, поэтому для них проблемой является уязвимость алгоритма во время сеанса работы. При этом идентифицирующая часть продолжает находиться в искаженной базе, поэтому может быть извлечена злоумышленником (например, путем перебора или вычисления вариантов);

Общей проблемой всех методов, важной с точки зрения затрат (финансовых), является необходимость модификации структуры базы данных и прикладного программного обеспечения до начала применения метода обезличивания, а для искажающих методов

для работы в прозрачном режиме также велика зависимость вычислительных затрат от сложности алгоритма. Особенно важным это становится в режимах модификации обезличенной базы.

Рассмотрим варианты реализации искажающих методов обезличивания персональных данных с учетом имеющегося опыта их внедрения и возможности их взлома с помощью модели нарушителя.

2. Искажающие методы обезличивания персональных данных и модель нарушителя

Анализ состояния проблемы является результатом исследования авторами имеющихся научных публикаций по теме обезличивания ПД в России, а также разработки модели нарушителя, позволяющей вычислить таблицу. Все варианты реализации искажающих методов можно условно разделить на две группы по применяемым методам обезличивания.

2.1. Алгоритмы реализации метода изменения состава или семантики.

Согласно Приказа [2] суть данного метода состоит в внесении обратимых изменений (искажений) в идентифицирующие атрибуты каждой записи ПД, без использования информации из других записей базы. При этом алгоритм искажений не регламентируется, это может быть замена символов на другие символы либо перемещение символов внутри строки. Изменения могут производиться по таблице или по формуле, при этом таблица необязательно должна быть одинаковой для разных записей базы.

Единственный обнаруженный вариант внедрения данного метода представлен в работе И.Ю. Кучина [3], в которой предлагается способ кодирования идентифицирующих атрибутов на базе разработанного алгоритма. Предлагаемый алгоритм кодирует каждую запись базы отдельным кодом с использованием значений идентификаторов и параметров операционной системы. Этот алгоритм был внедрен в сфере страхования, но вопрос обеспечения безопасности решается только при хранении персональных данных небольшого объема, только в хранилище на базе определенной операционной системы.

Однако, использование различных таблиц замен для разных записей базы большого объема представляется авторам не целесообразным с точки зрения производительности, поэтому в данной работе рассматривается возможность применения одной таблицы для всех записей.

2.2. Алгоритмы реализации метода перемешивания.

Согласно Приказа [2] суть данного метода состоит в обратимом изменении (искажении) положения идентифицирующих атрибутов каждой записи в другие записи, но с сохранением семантики перемещаемых атрибутов (их места в строке). При этом алгоритм искажений не регламентируется, группа записей, внутри которой производится перемещение, может быть произвольной по количеству. Изменения могут производиться по таблице или по формуле, при этом таблица необязательно должна быть одинаковой для разных групп записей базы.

Среди обнаруженных внедренных вариантов можно отметить работу В.В. Воронина и Н.Л. Нехай [4], в которой авторы разработали алгоритм с различными циклическими сдвигами для каждого атрибута-идентификатора и внедрили его в сфере обслуживания автотранспорта. В предложенном алгоритме перемешивание осуществляется не в группе записей (сегменте базы), а в группах разной величины для различных идентификаторов. Данный подход можно назвать несегментированным.

В работе И.П. Карповой [5] приводятся рассчеты производительности несегментировааного подхода, из которых можно сделать вывод о нецелесообразности его применения для баз большого объема.

В других разработанных алгоритмах, рассчитанных на базы ПД большого объема, производится предварительное разделение базы на равные сегменты, в границах которых и производится перемешивание. Например, в работе К.О. Бондаренко и В.А. Козлова [6], размер сегмента составляет 256 записей, в сегменте перемешиваются сначала полные строки, затем идентификаторы между строками. Параметры перемешивания задаются криптографическими методами.

Авторы данной работы являются сторонниками сегментированного подхода, но считают, что применение криптографических методов в значительной мере нивелирует экономическую эффективность любых методов обезличивания.

2.3. Модель нарушителя. В своей работе авторы использовали экспериментальную базу ПД объемом 310 тыс. физических лиц, где в качестве идентифицирующих атрибутов

использовались фамилия, имя, отчество, название улицы проживания, номер дома и номер квартиры, в сумме составляющие строку длиной 73 символа. В качестве алгоритмов искажения рассматривались следующие:

– перестановка символов внутри полной строки идентификаторов;

– перестановка бит внутри идентификатора;

– перемешивание полей (с сохранением структуры строки) внутри группы из 256 записей базы;

– перемешивание символов (с сохранением места в строке) внутри группы из 256 записей базы.

– формула (таблица) смещения принималась произвольной, но одинаковой для всех строк (для метода изменения состава) или сегментов записей (для метода перемешивания).

Модель нарушителя, разработанная для идентификации физических лиц в обезличенной базе, может быть названа «Моделью внедренного пользователя» и имеет следующие параметры:

– нарушитель имеет неограниченный доступ к обезличенной базе;

– нарушитель знает структуру (размер полей и записи в целом), но не знает точной семантики исходной базы;

– нарушитель знает, что искажению подверглись только идентификаторы, т.е. прочие данные не искажены;

– нарушитель не знает формулы (таблицы) обезличивания базы, за исключением того, что все данные одного лица содержатся в одной записи базы (для метода изменения состава) или в одном сегменте не более 256 записей (для метода перемешивания);

– нарушитель знает только ФИО искомого лица, хочет узнать другие идентификаторы и прочие данные этого лица;

– нарушитель знает, что в базе есть данные некоторого числа знакомых ему лиц, которые он знает, причем прочие (неискаженные) данные может найти в базе;

– количество лиц в обезличенной базе, полная информация о которых известна нарушителю - не менее 3 и не более 5;

– нарушитель не может разрабатывать программное обеспечение аналитического типа для вскрытия алгоритма искажений, но может пользоваться готовыми программными средствами (например, для поиска или сравнения символов).

Алгоритм действий нарушителя следующий:

– нарушитель находит (вручную или автоматизированным путем) в базе прочие (неискаженные) данные первого известного ему лица;

– нарушитель оценивает возможность ошибки (одинаковые прочие данные могут быть у нескольких лиц). Оценка производится по составу символов искаженной строки или составу полей в сегменте из 511 записей (по 255 в обе стороны от найденной);

– нарушитель составляет таблицу смещений символов в строке или полей в сегменте по известным ему символам/полям знакомого лица. Таблица составляется по первому найденному значению и неизбежно будет частично ошибочной из-за совпадающих символов/полей, но определенная ее часть будет абсолютно точной;

– нарушитель использует для устранения ошибочной части таблицы данные второго известного ему лица по описанному выше алгоритму. Для устранения оставшихся ошибок можно использовать третью запись и т.д;

– если нарушитель не получил точную таблицу смещений при использовании всех знакомых ему записей, данная модель считается неэффективной;

– нарушитель использует полученную точную таблицу смещений для получения данных о любом лице в данной базе, в этом случае модель считается эффективной.

2.3.1. Перемешивание символов внутри строки.

При определении смещений символов в перемешанной строке длиной N путем посимвольного сравнения с значением известной строки проблему представляют совпадающие (повторяющиеся) символы. Анализ частотного распределения символов в идентификаторах должен показать, какие символы наиболее вероятно встречаются в общей строке идентификаторов не менее двух раз и каково их общее количество - m. По причине строго заданной длины идентификаторов более всего будет повторяющихся пробелов, но их условно можно считать незначимыми и игнорировать в расчетах. При использовании нарушителем второй записи необходимо учитывать следующее:

– вторая строка независима от первой, поэтому в ней также останется m ошибочных мест, но они не совпадут с ошибочными местами возникшими после первой записи;

– минимальное количество совпадений ошибок двух строк = 0 (эти случаи возможны, если удвоенное количество ошибок меньше длины строки (в нашем случае условие m*2 < N соблюдается)), но полное несовпадение сразу заполняет таблицу смещений и нас не интересует;

– если одному ошибочному месту первой записи соответствует точное место второй записи, то количество ошибок уменьшается на одно место;

– хотя повторяющиеся символы отличаются друг от друга, даже если место одного повторяющегося символа в первой строке совпадет с местом другого повторяющегося символа во второй строке, сам факт ошибки останется, поэтому все повторяющиеся символы условно считаем одним ошибочным символом.

Для расчета наиболее вероятного количества совпадений была применена формула:

$$C_{max} = M(F_v(c)), \quad \{1\}$$

где M - математическое ожидание, $F_v(c)$ - функция зависимости количества вариантов совпадений от количества совпадений с. Сама функция Fv(c) является дискретной и представляет собой произведение количества различных вариантов расположения с ошибочных символов в строке удвоенной длины ошибок на количество различных вариантов расположения оставшихся ошибочных символов в оставшейся части удвоенной строки, т.е.:

$$F_v(c) = P_{(2m-1)c} * P_{(2m-1-c)(m-c)}, \quad \{2\}$$

где m -количество ошибочных мест,

P_{ab}=a!/b!(a-b)! – количество различных вариантов расположения b символов в строке длиной a (см. [7]). Сама функция $F_v(c)$ является симметричной, математическое ожидание будет соответствовать середине диапазона значений $C_{max} = C_{ср}$, хотя при большом диапазоне более правильным будет использовать полосу значений от C_{max} - D до C_{max} + D, где D - среднеквадратичное отклонение.

Теоретически при использовании третьей записи количество ошибок уменьшается вдвое, но поскольку ошибочные символы все-таки разные, их повторяемость уменьшится пропорционально и может стать меньше двух. Т.е. эти символы перестанут быть повторяющимися, и реальное количество ошибок уменьшится в большей степени.

Кроме того, необходимо учитывать, что сочетаемость различных букв любого языка не является равномерной. Анализ частотного распределения пар символов в идентификаторах должен показать, какие сочетания символов наиболее вероятно встречаются в общей строке идентификаторов. Этот факт в результате еще более уменьшает количество ошибок.

2.3.2. Перемешивание бит внутри идентификатора.

В работе Е.Ю. Мищенко [8], где приводятся результаты исследования влияния различных идентификаторов на процесс идентификации, показано, что наиболее вероятную длину атрибута «фамилия» можно принять равной 8 (см. табл.1), остальные - пробелы. Если для упрощения расчетов абстрагироваться от пробелов и от кодов страниц различных языков, то в фамилии содержится 64 бита. Наиболее вероятное распределение - 33 бита 1 и 31 бит 0. Применить тот же подход, что при перемешивании символов можно, но необходимо учесть следующее:

– все биты 1 и 0 являются значимыми, т.е. теоретически ошибочными могут быть все 64 места и предыдущий подход в прямом виде применять нельзя (2*64 > 64);

– подход усложняется и применяется по частям - сначала учитываются совпадения битов 1 друг с другом, затем учитываются совпадения битов 0 друг с другом, затем совпадения 1 и 0, в итоге количества вариантов соответствующих сочетаний перемножаются, и рассчитывается полная функция $F_v(c)$ и ее матожидание;

– поскольку есть только биты 1 и 0, то никакие дополнительные условия уменьшения количества совпадений не срабатывают.

2.3.3. Перемешивание полей внутри группы записей.

Поскольку сегментированный подход подразумевает перемешивание идентификаторов в группе из 256 записей, то применяя первую известную запись, нарушитель должен найти в базе один из идентификаторов, и приняв в качестве точки отсчета абстрактный номер записи (его наличие необходимо во всех алгоритмах перемешивания), отступить в обе стороны от него по 255 записей и вести поиск прочих идентификаторов в этой области из 511 записей. Успех поиска зависит от возможности повтора известных значений идентификаторов в этой области. В работе [8] рассчитаны наиболее вероятные количества повторений значений различных идентификаторов в уже рассмотренной эксперимен-

тальной базе (см. столбец Мат.ожидание в табл.1).

Таблица 1

Атрибут	Мат. ожидание	Вероятность идентификации
Фамилия	7,5	0,133
Имя	132	0,008
Отчество	183	0,005
Улица	26	0,038
№ дома	132	0,008
№ квартиры	59	0,017

Используя мат. ожидание M, полученное для полной базы (310000 записей), можно определить количество повторений в группе 511 записей $M_{повт}$ по формуле:

$M_{повт} = (M-1)*510/310000,$

а вероятность повторения того же идентификатора при использовании второй записи - это и есть вероятность идентификации по данному атрибуту (см. табл.1).

2.3.4. Перемешивание символов внутри группы записей.

Если группу из 511 записей по 73 символа представить в виде повернутой таблицы из 73 записей по 511 символов, то для определения смещения символа в такой строке можно попытаться применить подход, описанный в п.2.3.1. и рассчитать количество необходимых знакомых записей для нарушителя.

3. Результаты применения модели нарушителя

3.1. Перемешивание символов внутри строки.

Для идентификаторов экспериментальной базы авторами произведен анализ частотного распределения символов, результаты которого приведены на рис.1.

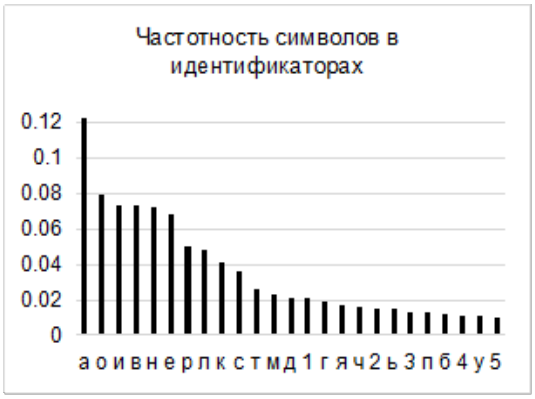

Рис. 1

В строке идентификаторов длиной N=73 символа наиболее вероятно повторяются следующие символы: пробел - 34 раза, «а» - 5 раз, «в», «е», «и», «н», «о» - по 3 раза, «к», «л», «р» - по 2 раза. Не повторяются - 13 символов. Пробелы при сравнении игнорируются, следовательно, в формируемой таблице смещений останется m=26 ошибочных мест.

Рис. 2

Из рис. 2 видно, что Fv(c) имеет явный максимум при Cmax=13, которое и является математическим ожиданием, а среднеквадратичное отклонение для нашего случая D = 2,5, т.е. наибольшая часть вариантов находится в диапазоне от c=11 до c=15. При таком значении с применение второй знакомой записи нарушителем было неизбежно. Поскольку ошибочные символы все-таки разные, их повторяемость уменьшается пропорционально и становится меньше двух (для символов «к», «л», «р»). Повторяющихся символов стало меньше - совпадения сократились в три раза. Авторы также провели анализ сочетаемости букв в экспериментальной базе, который показал, что более 40% сочетаний являются маловероятными и даже невозможными (см. рис. 3).

Рис. 3

В результате количество совпадений

уменьшилось до 2-3х. При таком значении с использование третьей знакомой записи нарушителем может оказаться необязательным. А ее использование приведет к решению однозначно.

3.2. Перемешивание бит внутри идентификатора.

Применение аналогичного подхода к расчетам сначала для битов 1, затем для битов 0, затем для их сочетаний (см.п.2.3.2.) для первой записи дало значение C_{max}=35, для второй - C_{max}=32, для третьей - C_{max}=28, что показало неэффективность модели нарушителя даже для одного идентификатора, не говоря уже о полной строке идентификаторов.

Поскольку количество совпадений Cmax хотя и медленно, но снижается, то возможно, что при наличии у нарушителя знакомых записей в количестве гораздо большем, чем 5 (параметр данной модели), задача построения таблицы смещений будет решена полностью.

Для проверки этой гипотезы авторы сняли ограничение количества известных записей и частично сняли ограничение на разработку программного обеспечения. В остальном концепция модели была сохранена и использована для обучения нейронной сети скомпанованной на базе стандартной библиотеки для распознавания бит в строке. Параметрами нейронной сети были размер и количество полносвязных слоев. Роль обучающих записей выполняли записи, известные нарушителю. Количество нейронов выходного слоя - 64 (по количеству бит в идентификаторе). количество промежуточных слоев варьировалось от 2 до 4. Результаты эксперимента показаны на рис. 4.

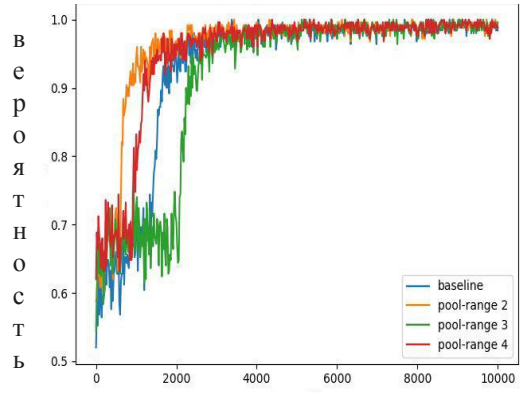

Рис. 4. Количество шагов (записей)

Заданная точность распознавания 0,95 была быстрее всего достигнута в двухслойной архитектуре сети при использовании около 500 обучающих записей.

Данные результаты можно рассматривать в качестве дополнительного подтверждения неэффективности применения модели нарушителя при перестановке бит в строке.

3.3. Перемешивание полей внутри группы записей.

Эксперимент, проведенный для группы из 511 записей и 6 идентификаторов, показал, что наиболее вероятно повторение значения только одного из идентификаторов, например, для отчества Мповт = 0,3. А вероятность повторения отчества при использовании второй записи уже будет равна 0,005. Т.е. ее использование приведет к решению задачи однозначно.

3.4. Перемешивание символов внутри группы записей.

Для использования подхода, описанного в п.2.3.1., необходимо соблюдение условия m*2 < N, где N=511, а значение m зависит от структуры таблицы и определяется форматом полей идентификаторов в базе, а именно: поле фамилии имеет длину 15 символов, которые в повернутой таблице займут 15 первых строк, причем в 3х первых вообще не будет пробелов (нет фамилий длиной менее 3х символов). И хотя наиболее вероятная длина фамилии - 8 символов, в 8й строке этой таблице наиболее вероятно будет всего 231 символ и 280 пробелов. Т.е. в каждой отдельно взятой строке вероятное количество пробелов, а также совпадений символов m будет различным. Например, в первых 3х строках символ «а» повторится 62 раза, символ «б» - 7 раз, и наиболее вероятна ситуация, когда все 511 мест будут заполнены различными, но повторяющимися символами. Расчеты показывают, что условие m*2 < N соблюдается только начиная с 7й строки. Для остальных идентификаторов условия аналогичные.

Таким образом, первые 6 строк фамилии должны рассчитываться по усложненному методу, как это показано в п.3.2. для перемешивания бит в строке. Поскольку длина строки символов в данном случае гораздо больше, чем использовалось в расчетах для перемешивания бит, можно сделать однозначный вывод о неэффективности модели нарушителя для данного варианта метода перемешивания.

4. Заключение

В данной работе рассматривались варианты реализации искажающих методов обе-

зличивания персональных данных с учетом имеющегося опыта их внедрения и возможности их взлома с помощью модели нарушителя. Опыт внедрения искажающих методов обезличивания явно недостаточен для серьезного анализа. Тем не менее, отсутствие методик расчета эффективности является причиной недоверия разработчиков к таким методам, а также причиной применения сложных алгоримов, отличающихся для различных частей базы данных, что значительно снижает производительность обработки и ограничивает их применение базами малого размера.

В данной работе авторы рассматривают простые алгоритмы, имеющие достаточную производительность обработки баз очень большого объема. Именно для проверки эффективности таких алгоритмов разработана модель нарушителя, использование которой также было продемонстрировано.

Таким образом, применение модели нарушителя, будучи эффективным для одних методов обезличивания (перестановка символов в строке идентификаторов, перемешивание полей в группе записей) и неэффективным для других (перестановка бит в строке идентификаторов, перемешивание символов в группе записей), показало неэффективность либо эффективность соответствующих методов обезличивания.

Использование различных параметров при моделировании действий нарушителя (например, количество известных нарушителю записей) позволяет принять для них нормативные значения и сформировать соответствующую нормативную базу.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Федеральный закон от 27.07.2006 «О персональных данных» № 152-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/ cons_doc_LAW_61801/, свободный (дата обращения: 14.05.2018).

2. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» [Электронный ресурс]. – Режим доступа: http://54.rkn.gov.ru/protection/acts/p13580/, свободный (дата обращения: 14.05.2018).

3. Кучин И.Ю. Обработка баз данных с персонифицированной информацией для задач обезличивания и поиска закономерностей / И.Ю. Кучин // Диссертация ктн. – Астрахань: Издательство Астраханского гос. технического ун-та, 2012. – 132 с.

4. Воронин В.В. Защита персональных данных в информационных системах методом обезличивания / В.В. Воронин, Н.Л. Нехай // Информационные технологии XXI века: сборник научных трудов. – Хабаровск: Издательство Тихоокеанского гос. ун-та, 2017. – С. 479–483.

5. Карпова И.П. О реализации метода обезличивания персональных данных / И.П. Карпова // Вестник компьютерных и информационных технологий. – Москва: Издательский дом «Спектр», 2013. – № 6, - С. 56–60.

6. Бондаренко К.О. Универсальный быстродействующий алгоритм процедур обезличивания данных / К.О. Бондаренко, В.А. Козлов // Известия ЮФУ. Технические науки. – Ростов-на-Дону: Издательство Южного фед. ун-та, 2015. – № 11 (172). – С. 130–142.

7. Виленкин Н.Я. Глава III. Комбинаторика кортежей и множеств. Размещения с повторениями/ Н.Я. Виленкин // Популярная комбинаторика. — М.: Наука, 1975. — С. 80. — 208.

8. Мищенко Е.Ю. Вероятность идентификации в базе персональных данных: Выбор идентифицирующих атрибутов / Е.Ю. Мищенко // Безопасность информационного пространства: сборник трудов XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2019. – С. 206-209.

References

1. Federal'nyy zakon ot 27.07.2006 «O personal'nykh dannykh» № 152-FZ [Elektronnyy resurs]. – Rezhim dostupa: http://www.consultant.ru/document/ cons_doc_LAW_61801/, svobodnyy (data obrashcheniya: 14.05.2018).

2. Prikaz Federal'noy sluzhby po nadzoru v sfere svyazi, informatsionnykh tekhnologiy i massovykh kommunikatsiy ot 05.09.2013 № 996 «Ob utverzhdenii trebovaniy i metodov po obezlichivaniyu personal'nykh dannykh» [Elektronnyy recurs]. – Rezhim dostupa: http://54.rkn.gov.ru/protection/acts/p13580/, svobodnyy (data obrashcheniya: 14.05.2018).

3. Kuchin I.YU. Obrabotka baz dannykh s personifitsirovannoy informatsiyey dlya zadach obezlichivaniya i poiska zako-nomernostey / I.YU. Kuchin // Dissertatsiya ktn. – Astrakhan': Izdatel'stvo Astrakhanskogo gos. tekhnicheskogo un-ta, 2012. – 132 s.

4. Voronin V.V. Zashchita personal'nykh dannykh v informatsionnykh sistemakh metodom obezlichivaniya / V.V. Voronin, N.L. Nekhay // Informatsionnyye tekhnologii XXI veka: sbornik nauchnykh trudov. – Khabarovsk: Izdatel'stvo Tikhookeanskogo gos. un-ta, 2017. – S. 479–483.

5. Karpova I.P. O realizatsii metoda obezlichivaniya personal'nykh dannykh / I.P. Karpova // Vestnik komp'yuternykh i informatsionnykh tekhnologiy. – Moskva: Izdatel'skiy dom «Spektr», 2013. – № 6, - S. 56–60.

6. Bondarenko K.O. Universal'nyy bystrodeystvuyushchiy algoritm protsedur obezlichivaniya dannykh / K.O. Bondarenko, V.A. Kozlov // Izvestiya YUFU. Tekhnicheskiye nauki. – Rostov-na-Donu: Izdatel'stvo Yuzhnogo fed. un-ta, 2015. – № 11 (172). – S. 130–142.

7. Vilenkin N.YA. Glava III. Kombinatorika kortezhey i mnozhestv. Razmeshcheniya s povtoreniyami/ N.YA. Vilenkin // Populyarnaya kombinatorika. — M.: Nauka, 1975. — S. 80. — 208.

8. Mishchenko Ye.YU. Veroyatnost' identifikatsii v baze personal'nykh dannykh: Vybor identifitsiruyushchikh atributov / Ye.YU. Mishchenko // Bezopasnost' informatsionnogo prostranstva: sbornik trudov XVIII Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh. – Magnitogorsk: Izd-vo Magnitogorsk. gos. tekhn. un-ta im. G.I. Nosova, 2019. – S. 206-209.

МИЩЕНКО Евгений Юрьевич, старший преподаватель кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, Россия, г. Челябинск, пр. Ленина, 76. E-mail: mishchenkoei@susu.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО "Южно-Уральский государственный университет (национальный исследовательский университет)". Россия, 454080 Челябинск, проспект Ленина, 76. E-mail: sokolovan@susu.ru

MISHCHENKO Evgeniy, Senior Lecturer of Department of Information Security, South Ural State University (national research university). 76, Lenina prosp., Chelyabinsk, Russia, 454080. Email: mishchenkoei@susu.ru

SOKOLOV Alexander, Ph.D., Associate Professor, Head of Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru

УДК 004.052.42+004.942 Вестник УрФО № 2(36) / 2020, с. 43–48

Моргунов Д. А.

DOI: 10.14529/secur200207

ВЫЯВЛЕНИЕ СКРЫТЫХ УЯЗВИМОСТЕЙ В ИСХОДНОМ КОДЕ МНОГОПОТОЧНЫХ ПРОГРАММ ПОСРЕДСТВОМ АНАЛИЗА ФУНКЦИОНАЛЬНЫХ ПЕРЕХОДОВ

В статье представлены новая теоретико-множественная модель и процедуры, позволяющие уменьшить временные затраты на обнаружение скрытых уязвимостей в исходном коде многопоточных компьютерных программ, а также результаты проведенного математического моделирования. Под скрытыми уязвимостями в статье понимаются уязвимости, приводящие к ситуациям «гонок» и взаимоблокировкам, поскольку они имеют стохастический характер проявления во время тестирования, что значительно усложняет их выявление. Представленная модель описывает состояния каждого потока многопоточной компьютерной программы исполняемой в настоящее время функцией и содержимым стека вызова функций. При этом сохраняется возможность использования модели в верификации методом Model Checking, а также исключается необходимость решения задачи поиска инварианта модели. Представленные процедуры позволяют формировать спецификации для метода проверки на модели, выполнение которых позволяет выявить уязвимости, приводящие к ситуациям «гонок» и взаимоблокировкам, в исходном коде многопоточных программ.

Ключевые слова: *верификация, математическое моделирование, выявление уязвимости, ситуация «гонки», взаимоблокировка.*

Morgunov D. A.

IDENTIFICATION OF HIDDEN VULNERABILITIES IN THE SOURCE CODE MULTI-THREAD PROGRAMS BY ANALYSIS OF FUNCTIONAL TRANSITIONS

The article presents a new set-theoretic model and procedures that reduce the time required to detect hidden vulnerabilities in the source code of multi-threaded computer programs, as well as the results of mathematical modeling. Hidden vulnerabilities in the article are understood as vulnerabilities leading to data races and deadlocks, since they have a stochastic nature of manifestation during testing, which greatly complicates their identification. The presented model describes the state of each thread of a multi-threaded computer program currently executing a function and the contents of the function call stack. At the same time, it remains possible to use the model in verification by the Model Checking method, and also eliminates the need to solve the problem of searching for the model invariant. The presented procedures make it possible to formulate specifications for the verification method on models, the implementation of which makes it possible to identify vulnerabilities leading to data races and deadlocks in the source code of multithreaded programs.

Keywords: *verification, mathematical modeling, vulnerability identification, data race, deadlock.*

Многопоточные компьютерные программы могут содержать в себе уязвимости, приводящие к отказам, имеющим случайный характер обнаружения при тестировании (скрытым отказам [1]). В данной статье такие уязвимости называются скрытыми. Скрытые уязвимости приводят к ситуациям «гонок» и взаимоблокировкам, которые в международной базе уязвимостей Common Weakness Enumeration имеют идентификаторы CWE-362 и CWE-833 соответственно.

Причиной возникновения уязвимостей, приводящих к ситуациям «гонок», является одновременный доступ различных потоков к одним и тем же функциям исходного кода без применения механизмов обеспечения монопольного доступа. Причиной возникновения уязвимостей, приводящих к взаимоблокировкам, является неверная организация доступа потоков к функциям исходного кода, в которых используются механизмы обеспечения монопольного доступа [2, 3].

Наиболее эффективным методом обнаружения скрытых уязвимостей является верификация проверкой на модели (Model Checking) [4, 5, 6], поскольку позволяет описывать свойства программы посредством темпоральной логики и проверять наличие описанных свойств без реального исполнения программы. Но при этом верификация многопоточной программы требует значительных временных затрат.

В целях уменьшения времени выполнения верификации была разработана теоретико-множественная модель, названная моделью функциональных переходов. Под функциональными переходами в данной статье понимается передача управления между функциями исходного кода. Состояние потока многопоточной программы в модели функциональных переходов описывается исполняемой в текущее время функцией и содержимым стека вызовов функций. Под переходом между состояниями понимается передача управления от одной функции к другой. Состояния и переходы между ними описываются отдельно для каждого потока.

В общем виде модель на основе функциональных переходов M_p многопоточной программы описывается выражением

$M_p = (M^i_t, Tb)$, $i = \overline{0, K_t - 1}$,

где M^i_t – модель на основе функциональных переходов i-го потока, *Tb* – множество метаданных о множестве *I* наборов инструкций исходного кода, K_t – количество потоков в программе при минимальном количестве потоков, исполняющих одинаковые наборы инструкций исходного кода (однородных потоков).

Модель M^i_t включает в себя:

– множество состояний i-го потока программы $S^i \subset S$, где *S* – множество, состоящее из множеств состояний каждого потока, S = {Sj}, $j = \overline{0, K_t - 1}$;

– множество переходов между состояниями i-го потока программы $R^i \subset R$, где *R* = {*Rj*}, $j = \overline{0, K_t - 1}$ – множество, состоящее из множеств переходов между состояниями каждого потока;

– множество меток во множестве наборов инструкций, исполняемых i-м потоком, $L^i \subset L$, где *L* = {*Lj*}, $j = \overline{0, K_t - 1}$ – множество, состоящее из множеств меток во множестве наборов инструкций, исполняемых каждым потоком.

В общем виде M^i_t описывается кортежем

$$M^i_t = (S^i, R^i, L^i). \qquad (1)$$

Множество меток Li во множестве l^i в (1) имеет вид $L^i = \{l^i_j\}$, $j = \overline{0, K^i_L - 1}$, где l^i_j – некоторая метка во множестве L^i, $K^i_L = |L^i|$ – количество меток во множестве l_i, причем для $\forall$ j, p выполняется $l_j \neq l_p$ при $j \neq p$, $l_j \in L$, $l_p \in L$.

Множество состояний S^i в (1) i-го потока программы имеет вид $S^i = \{S^i_p\}$, $p = \overline{0, K^i_s - 1}$, где S^i_p – некоторое состояние *i*-го потока программы, $K^i_s = |S^i|$.

Состояние Sip описывается набором меток:

$$S^i_p = \bigwedge_{r=0}^{K_L - 1} l^i_r,\ l^i_r \in L^i,$$

где K_L – количество меток. Здесь символ $\wedge$ означает одновременное наличие элементов в заданном порядке.

Начальное состояние i-го потока, которое обозначается Si0, соответствует пустому стеку вызовов функций, то есть не содержит ни одной метки из Li.

При этом множество состояний Si обладает следующим свойством наличия бесконечных путей: для $\forall p, r\ \exists \pi(S^i_p, S^i_r)$ при $p \neq r$, где $\pi(S^i_p, S^i_r)$ – путь из состояния S^i_p в состояние S^i_r. Под путем из S^i_p в S^i_r понимается последовательность состояний, начинающаяся в S^i_p и заканчивающаяся в S^i_r: $\pi(S^i_p, Sir) = (S^i_p, \ldots, S^i_r)$, причем на протяжении всего пути существует переход из S^i_t в $S^i_t + 1$ для $\forall t = \overline{p, r-1}$. Выполнение данного свойства позволяет использовать модель функциональных переходов для верификации программы методом проверки на модели [4, 5, 6].

Множество переходов между состояниями R^i в (1) i-го потока имеет вид $R^i = \{R^i_j\}$, $j = \overline{0, K^i_R - 1}$, где $R^i_j = (S^i_p, S^i_r)$ – переход из состояния S^i_p в состояние S^i_r, $p \neq r$, $K^i_R = |R^i|$ – количество переходов между состояниями *i*-го потока. Множество R^i в начальный момент времени объявляется пустым.

Множество метаданных имеет вид *Tb* = {Tb^i}, $i = \overline{0, K_t - 1}$, где Tb^i – множество метаданных о множестве I^i.

Множество метаданных о множестве Ii имеет вид $Tb^i = \left\{Tb^{f^i_j}\right\}$, $j = \overline{0, K^i_f - 1}$, где $Tb^{f^i_j}$ – кортеж метаданных о функции f^i_j.

Подробное описание модели на основе функциональных переходов и алгоритмов ее построения представлены в статье [7].

Разработанная модель многопоточной программы содержит много меньше состояний, в сравнении с моделью Крипке, а также позволяет определять пути исполнения до уязвимостей тестирования программы, в отличие от модели с динамической семантикой [8].

Процедура обнаружения уязвимостей, приводящих к ситуациям «гонок», позволяет выявить количество E^0 уязвимостей посредством обработки множества *Tb* метаданных о множестве *I* наборов инструкций исходного кода многопоточной программы. Определяются уязвимости, возникающие при организации обращения к критическим секциям как однородных потоков, так и потоков, исполняющих различные наборы инструкция исходного кода.

Процедура обнаружения уязвимостей, приводящих к ситуациям «гонок», представляет собой следующую последовательность действий:

1) преобразовать множество *Tb* в *Tb′* за счет объединения элементов, у которых различается только компонента *th*;

2) найти количество E^0_0 уязвимостей, возникающих при организации доступа разнородных потоков к критическим секциям по множеству *Tb′* – поиск элементов множества *Tb′*, используемых несколькими потоками при отсутствии механизмов обеспечения монопольного доступа;

3) найти количество E^0_1 уязвимостей, возникающих при организации доступа однородных потоков к критическим секциям по множеству *Tb'* – поиск элементов множества Tb', используемых одним потоком, не являющимся главным или родительским для текущего элемента, при отсутствии механизмов обеспечения монопольного доступа.

Общее количество уязвимостей в проверяемой программе, способных привести к ситуациям «гонок», $E^0 = E^0_0 + E^0_1$.

Процедура обнаружения уязвимостей, приводящих к взаимоблокировкам, позволяет определить количество E^1 уязвимостей посредством обработки построенной модели M_p многопоточной программы на основе функциональных переходов. Определяются блокировки потоком самого себя, взаимоблокировки потоков, исполняющих как одинаковые, так и различные наборы инструкций, а также ложные обнаружения уязвимостей.

Процедура обнаружения уязвимостей, приводящих к взаимоблокировкам, представляет собой следующую последовательность действий:

– сформировать множества $Tb^i \subset Tb$ метаданных о функциях, исполняемых каждым из потоков;

– сформировать множества данных об используемых средствах обеспечения монопольного доступа и соответствующих им метках для каждого из потоков;

– обнаружить взаимоблокировки:

1) построить и проверить спецификации, позволяющие определить каждом из потоков наличие путей исполнения, на которых начинает использоваться средство обеспечения монопольного доступа $prot_2$ во время использования другого средства обеспечения монопольного доступа $prot_1$ ($prot_1 \longrightarrow prot_2$);

2) для каждого потока, соответствующего хотя бы одной из ранее построенных спецификаций, построить и проверить новые спецификации, позволяющие определить наличие пути, содержащего ($prot_2 \longrightarrow prot_1$);

3) для каждого потока, соответствующего хотя бы одной спецификации из шага 2, выполнить проверку ложного обнаружения взаимоблокировки, то есть построить и проверить спецификации, позволяющие определить отсутствие путей ($prot_3 \longrightarrow prot_1 \longrightarrow prot_2$) и ($prot_3 \longrightarrow prot_2 \longrightarrow prot_1$); в случае одновременного существования таких путей обнаруженная взаимоблокировка является ложной.

Количество состояний по модели на основе функциональных переходов N и модели Крипке N' было найдено для ряда многопоточных программ. Результаты представлены в таблице 1. При нахождении количества состояний в модели Крипке изменение значений параметров цикла с неизвестным числом итераций было ограничено до 103 изменений вместо всего диапазона изменения значений.

Таблица 1

Количество состояний по модели на основе функциональных переходов и модели Крипке

Кол-во строк	*N*	*N'*
6921	1724	1,4 * 107
9417	2520	1,9 * 107
12014	3207	2,4 * 107
21569	4832	4,3 * 107
35720	9418	7,1 * 107
42548	10159	8,5 * 107
50071	12367	108
61593	14216	1,2 * 108
72553	18925	1,5 * 108
91326	22311	1,8 * 108

На рисунке 1 представлена динамика изменения количества состояний от числа строк кода модели Крипке (верхний график) и модели на основе функциональных переходов (нижний график) в одной из проверяемых программ с ограничением до 104 значений параметров цикла с неизвестным числом итераций. Из рисунка 1 видно, что для одного и того же исходного кода программы количество состояний в модели на основе функциональных переходов много меньше, чем в модели Крипке.

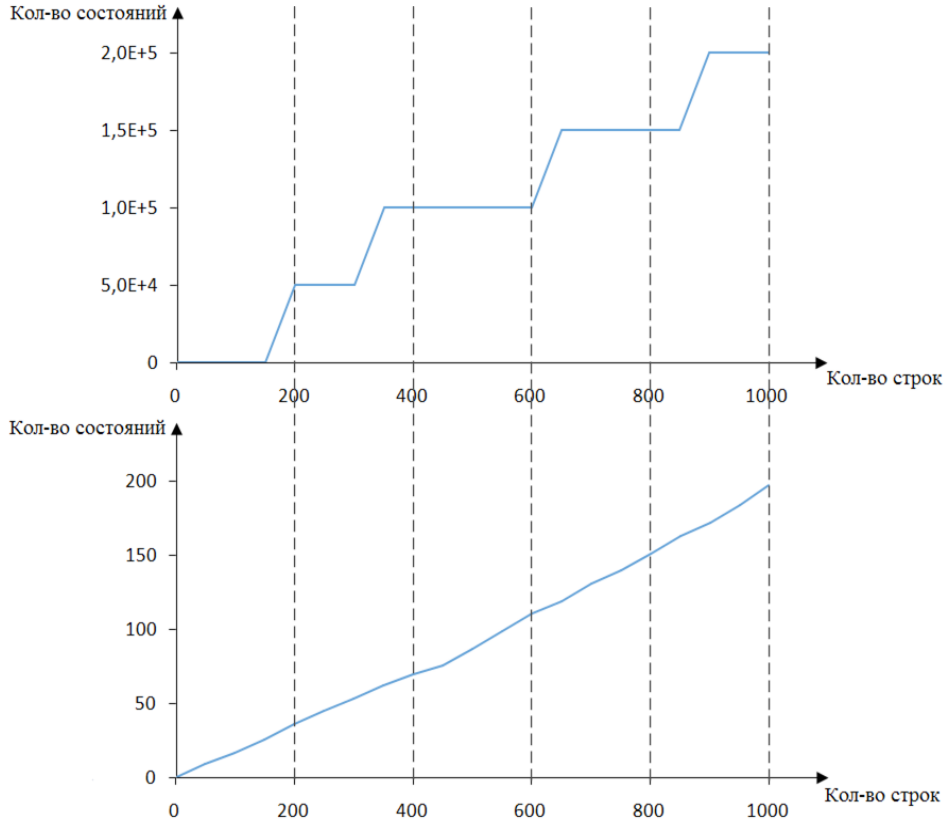

Рис. 1. Динамика изменения количества состояний от числа строк кода в модели Крипке (верхний график) и модели на основе функциональных переходов (нижний график)

Применение представленных в статье процедур позволяет более чем в 110 раз снизить временные затраты на выявление скрытых уязвимостей в сравнении с верификацией по модели Крипке.

Разработанные процедуры снижают временные затраты на обнаружение скрытых уязвимостей, поскольку: модель на основе функциональных переходов содержит меньшее число состояний, чем модель Крипке; процедуры исключают решение задачи поиска инварианта модели [2, 3, 4]; позволяют находить пути исполнения программы до уязвимости без тестирования, в отличие от верификации модели на основе динамической семантики.

Представленные в статье модель и процедуры предоставляют возможность разработки средства автоматического обнаружения скрытых уязвимостей многопоточных компьютерных программ для некоторого языка программирования высокого уровня, что имеет практическую ценность при отладке, а также оценке качества программ во время проведения сертификации.

Литература

1. ГОСТ 27.002-2015 Надежность в технике (ССНТ). Термины и определения. Дата введения 2017-03-01.

2. Уильямс Э. Параллельное программирование на C++ в действии. Практика разработки многопоточных программ. Пер. с англ. Слинкин А.А. – М.: ДМК Пресс, 2014. – 672 с.: ил.

3. Шлее М. Qt. Профессиональное программирование. Разработка кроссплатформенных приложений на C++. – Пер. с англ. – СПб.: Символ-Плюс, 2011. – 560 с. : ил.

4. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программы: Model Checking. Пер. с англ. / Под ред. Р. Смелянского. – М.: МЦНМО, 2002. – 416 с. : ил.

5. Кулямин В.В. Методы верификации программного обеспечения. М.: Институт Системного Программирования РАН, 2008. – 117 с.

6. Карпов Ю.А. MODEL CHECKING. Верификация параллельных и распределенных программных систем. – СПб.: БВХ-Петербург, 2010. – 560 с.: ил. + CD-ROM.

7. Моргунов Д.А., Букин А.Г. Математическая модель многопоточной программы ЭВМ, построенная на основе переходов между функциями исходного кода // Известия Института инженерной физики, 2018, №2 (48), – С. 50-55.

8. Handbook of Model Checking. / Clarke, Edmund M. (Editor); Henzinger, Thomas A.; Veith, Helmut; Bloem, Roderick (Editor). Cham : Springer, 2018. 1210 p. ISBN 978-3-319-10574-1.

References

1. GOST 27.002-2015 Nadezhnost' v tekhnike (SSNT). Terminy i opredeleniya. Data vvedeniya 2017-03-01.

2. Uil'yams E. Parallel'noe programmirovanie na S++ v deystvii. Praktika razrabotki mnogopotochnykh programm. Per. s angl. Slinkin A.A. – M.: DMK Press, 2014. – 672 s.: il.

3. Shlee M. Qt. Professional'noe programmirovanie. Razrabotka krossplatformennykh prilozheniy na C++. – Per. s angl. – SPb.: Simvol-Plyus, 2011. – 560 s., il.

4. Klark E.M., Gramberg O., Peled D. Verifikatsiya modeley programmy: Model Checking. Per. s angl. / Pod red. R. Smelyanskogo. – M.: MTsNMO, 2002. – 416 s.: il.

5. Kulyamin V.V. Metody verifikatsii programmnogo obespecheniya. M.: Institut Sistemnogo Programmirovaniya RAN, 2008. – 117 s.

6. Karpov Yu.A. MODEL CHECKING. Verifikatsiya parallel'nykh i raspredelennykh programmnykh sistem. – SPb.: BVKh-Peterburg, 2010. – 560 s.: il. + CD-ROM.

7. Morgunov D.A., Bukin A.G. Matematicheskaya model' mnogopotochnoy programmy EVM, postroennaya na osnove perekhodov mezhdu funktsiyami iskhodnogo koda // Izvestiya Instituta inzhenernoy fiziki, 2018, №2 (48), – S. 50-55.

8. Handbook of Model Checking. / Clarke, Edmund M. (Editor); Henzinger, Thomas A.; Veith, Helmut; Bloem, Roderick (Editor). Cham : Springer, 2018. 1210 p. ISBN 978-3-319-10574-1.

МОРГУНОВ Дмитрий Андреевич, начальник отдела, Межрегиональное общественное учреждение «Институт инженерной физики». 142210, Российская Федерация, Московская область, г. Серпухов, Большой Ударный пер., д. 1а. E-mail: mor.dmitrij@gmail.com

MORGUNOV Dmitriy, Head of Department, Interregional Public Institution "Institute of Engineering Physics". 142210, Russian Federation, Moscow region, Serpukhov, Bolshoy Udarny per., 1a. E-mail: mor.dmitrij@gmail.com

УДК 343.85:004

Вестник УрФО № 2(36) / 2020, с. 49–55

Фельдман Е. В.

DOI: 10.14529/secur200208

ПРОТИВОДЕЙСТВИЕ СОВЕРШЕНИЮ БЕСКОНТАКТНЫХ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

В статье рассмотрены вопросы выявления способов совершения преступлений, связанных с незаконным оборотом наркотических веществ, а также приведенытипичные схемы контактного и бесконтактного распространения наркотических веществ на территории РФ. Более подробное внимание обращенона схему бесконтактного распространениянаркотических веществ и на проблемы противодействиясовершению бесконтактных преступлений с использованием цифровых технологий. Кроме того, в статье предложенысовременные организационно-правовые и технические направления борьбы с незаконным оборотом наркотических веществс применением цифровых технологий. Был сделан важный вывод, что успешное противодействие совершению бесконтактных преступлений возможно в тех случаях, в которых будетприменяться аналитическая система, позволяющая проводить оперативно-розыскные мероприятия с применениемцифровых технологий, машинного обучения и технологии Больших данных.

Ключевые слова: *незаконный оборот наркотических веществ, бесконтактный способ сбыта наркотических веществ, цифровые технологии, Интернет, Большие данные, машинное обучение.*

COUNTERACTION TO THE COMMISSION OF CONTACTLESS CRIMES USING DIGITAL TECHNOLOGY

The article discusses the issues of identifying methods of committing crimes related to the illicit trafficking of narcotic substances, as well as typical schemes of contact and contactless distribution of narcotic substances in the Russian Federation. More detailed attention is paid to the scheme of contactless distribution of narcotic substances and to the problems of counteracting the commission of contactless crimes using digital technologies. In addition, the article proposes modern organizational, legal and technical directions of the fight against drug trafficking using digital technologies. An important conclusion was made that successful counteraction to the commission of contactless crimes is possible in those cases in which an analytical system will be used to conduct operational-search measures using digital technologies, machine learning and Big Data technology.

Keywords: *drug trafficking, non-contact way of selling drugs, digital technology, Internet, Big data, machine learning.*

Наркотическим веществом называют вещество естественного или искусственного происхождения, которое влияет на психические функции организма с целью его изменения, а при многочисленном и продолжительном употреблении приводит к химической, физической и психической зависимости[1].

В настоящее время ситуация по употреблению наркотиков в РФ складывается катастрофическим образом [2]. Удельный вес синтетических наркотиков в общей массе изымаемых наркотических средств и психотропных веществ на протяжении последних 10 лет увеличился в 13 раз [3].

В связи со стремительным развитием цифровых технологий, глобальной информационной сети Интернет и современных операторов сотовой связи в последние годы злоумышленники начали активно использовать совершенно новые преступные схемы [4-6].

Если рассматривать контактную схему распространения наркотических веществ на территории РФ, то чаще всего их продажа происходит следующим образом [7]: поставщики наркотических средств организовывают их поставку в Россию, затем специально обученные для этих целей операторы, которые географически находятся в другом регионе, сообщают о прибытии «товара». Одновременно с этим они сообщают номера телефонов и счетов, на которые следует перевести деньги. Потенциальные покупатели переводят средства на полученный счет. Участники группировки создают тайник, адрес нахождения которого диспетчер отправляет сообщением уже самому потребителю. Непосредственного контакта при такой схеме «работы» между участниками группировки, покупателями и диспетчерами не происходит. Для дальнейшего сокрытия следов номера телефонов и счетов, на которые перечисляются деньги, заменяются не реже, чем раз в неделю [7].

Подробная схема бесконтактного распространения наркотических веществ описана в работах[8,9]. В этой схеме существуют должности, занявшие свои места по порядку подчинения. Должностные инструкции сотрудников подробно прописаны, соблюдаются меры безопасности. Названия должностей звучат следующим образом: кураторы, хакеры, кладовщики, закладчики или дропы, операторы, директор и другие.

Участники группировки общаются с помощью приложений-мессенджеров, например, таких как Viber, Telegram, WhatsApp, ICQ и

менее распространенных – XMPP (более известный, как Джабер), Brosix [10].

Сотрудники, «добросовестно» выполняющие свои функции, могут быть переведены на следующую по ступени должность с другим окладом. Также как и члены, допустившие ошибки в своей работе, подвергаются штрафу.

Все «работники» команды имеют подробные инструкции, где описывается, как вести себя в случае, если произошло задержание сотрудниками полиции. Также там имеется обучающая информация, касающаяся хранения, транспортировки, фасовки, пользования счетами, электронными платежами. Особенное внимание уделяется использованию анонимных методов общения в Интернете, а также посещению опасных или запрещенных страниц.

Среднестатистический пользователь персонального компьютера может зайти в интернет и установить специальные программы anonymizer и прокси-серверы для скрытия информации о компьютере и его IP-адресе.Самые часто используемые для этих целей являются такие программы, как hideme, webwarper, 2ip. Данные сервисы позволяют скрывать не только IP-адреса, но и информацию о географическом месте нахождения пользователя; браузере, который используется, а также переходить на запрещенные сайты, ранее заблокированные надзорными органами. Также программы-анонимайзеры позволяют загружать данные с файлообменников без временных требований и платной регистрации, посещать форумы и социальные сети, даже если они имеют статус заблокированных за нарушение правил сообществ.

С появлением сети VirtualPrivateNetwork или VPN, которая позволяет объединить несколько компьютеров, находящихся в разных концах мира, появилась такая возможность, как осуществление запрещенного доступа к ранее заблокированным платным и бесплатным сайтам. Суть использования этой сети в том, что зашифрованный секретный трафик с компьютера пользователя и интернет-провайдера отправляется на VPN-сервер, а далее происходит анонимный переход на заблокированный сайт. Пользователь может изменять IP-адрес своего компьютера, то есть со стороны он будет выглядеть как посетитель из другой страны, так как некоторые сервисы работают только для пользователей США и Европы.

Прокси-сервер – это промежуточный сервер, позволяющий клиентам осуществлять косвенные запросы к разным сетевым службам. То есть пользователь подключается в цепочку прокси-серверов и запрашивает какой-либо ресурс, расположенный на другом сервере. При этом сам запрос клиента или ответ сервера может быть изменен прокси-сервером для сохранения анонимность клиента.Разные прокси-серверы располагают разными возможностями. Например, одни из них позволяют скрыть данные об источнике запроса, другие – IP-адрес. Третьи изменяют адрес источника запроса. И если изначально эти серверы были направлены на использование в целях сохранения конфиденциальной информации о пользователе, то в последнее время их использование часто связано с получением доступа к запрещенным сайтам. Это объясняет популярность использования прокси-серверов для получения доступа к информационным ресурсам, запрещенным законом.

Отметим, что наркодилеры выделяют крупные суммы на покупку транспорта, устройств для использования сотовой и другой необходимой для работы связи, техники, оружия, разработки новых программ, аренду помещений, содержание «своего» персонала (охрана, водители, упаковщики), собственных лабораторий и т.п.

Незадолго до настоящего момента на территории Российской Федерации организационные моменты в схемах сбыта бесконтактными способами с использованием Интернета значительно изменились. Теперь буквально вся информация о разновидностях, массе, стоимости предлагаемого для продажи наркотических веществ, а также способах связи и оплаты размещается на определенных сайтах. Передача самого наркотического средства происходит посредством «закладок». Оплата осуществляется через разные электронные платежные сервисы (QIWI-кошелек, Яндекс.Деньги, WebMoneyTransfer, E-port.ru), на которые перечисляются виртуальные деньги.

Анализ предоставленной и собранной с помощью открытых источников информации дает возможность установить следующую схему сбыта наркотических средств, которая состоит из следующих этапов:

1) публикация информации о продаже наркотических веществ на сайтах, форумах в социальных сетях (VKontakte, Ok.ru и др.) на

сайтах знакомств и бесплатных досках объявлений, в даркнете, где в качестве контактных данных указываются никнейм (псевдоним) в программах Skype, Brosix, Jabber, адрес почтового ящика или номер телефона;

2) во время переписки продавец предлагает потенциальному покупателю подготовленный ранее прейскурант, где указано название вещества, стоимость и масса. А также сообщается информация о способах оплаты и получения желаемого вещества;

3) безналичная оплата предполагаемого заказа с помощью электронных платежных систем Qiwi, VisaWallet, WebMoneyTransfer, «Яндекс.Деньги». В последнее время отмечено использование пиринговой платежной системы Биткоин (BitCoin) и другой криптовалюты;

4) после подтверждения перевода денег происходит закладывание наркотического вещества в «тайники» или сообщаются заранее подготовленные точки с закладками;

5) заказчику описывают местонахождения «закладки» также с помощью переписки в интернете.

Также важно рассмотреть основные проблемы противодействия бесконтактного распространения наркотических веществ. Для более детального рассмотрения данного вопроса приведем схему преступной деятельности в межрегиональных и региональных крупных интернет-магазинах по сбыту наркотических веществ [11,12]. Она состоит из следующих пунктов:

1. Наличие самостоятельных структурных подразделений, имеющих свою иерархию, географически и функционально разделенных друг от друга, при этом находящихся под руководством одного лидера. Зачастую в каждом таком подразделении процесс преступной деятельности происходит от производства до незаконного сбыта. Количество структурных подразделений в зависимости от масштаба преступной деятельности может быть от двух до нескольких десятков. Например, у интернет-магазина «ХимПром», функционировавшего в форме организованной преступной группировки с годовым доходом 2,3 млрд рублей, филиалы были расположены в 14 регионах страны.

2. Многочисленный состав участников, доходящий до нескольких сотен человек с четко разделенными обязанностями (закладчики, диспетчеры, кассиры, курьеры, менеджеры по регионам, финансовые директоры, специалистов в области информационной безопасности и т.д.) При этом руководство группировок может использовать свой, неизвестный до этого в криминальном мире, сленг для еще большей конспирации.

3. Использование мессенджеров для обмена сообщениями и медиафайлами при общении между участниками преступного сообщества. Следует отметить, что если еще несколько лет назад для мгновенного обмена сообщениями наиболее часто использовались такие общедоступные и известные приложения, как Viber, WhatsApp и ICQ, то сейчас для затруднения прослушивания телефонных переговоров правоохранительными органами члены преступной группы все чаще применяют программы Telegram, Brosix, Pidgin, Xabber, Vipole, IM+, Psi и др.

4. Разработка и внедрение комплекса правил, позволяющих держать свои действия на высоком уровне секретности. Помимо использования вышеуказанных мессенджеров, также используются такие онлайн-сервисы для загрузки файлов, как Imgur, Radikal, Postimg. А для хранения и передачи покупателям фотографий мест тайников с наркотическими веществами, для передачи покупателям точных координат мест нахождения этих тайников используется картографический сервис GoogleMaps Сервисы OneTimeSecret, Privnote позволяют после прочтения полученных по ссылкам сообщений безвозвратно удалять их через определенный отправителем непродолжительный период времени.

Вышеперечисленные программы и сервисы позволяют усложнить работу сотрудникам правоохранительных органов, предотвратить утечку информации о преступной деятельности его участников и позволяют обезопасить руководство данного бизнеса от прямого участия в преступной деятельности.

В данный момент злоумышленники, распространяющие наркотические вещества, зачастую делают это с помощью площадок для обмена криптовалюты или биржи криптовалют [12]. По данным сайта, предоставляющем информацию об обменных пунктах и курсах обмена электронных денег – bestchange.ru, обходя законодательную сферу, в русскоязычном Интернете функционируют более 500 порталов для обмена криптовалюты на рубли.С помощью криптовалюты Ethereum и Bitcoin гонорары за работу получают сотрудники преступных группировок, кроме того,

при ее использовании для заказа «товара» в интернет-магазине цена товара снижается до 20%.

Для комплексной работы по борьбе с незаконным оборотом наркотических средств сотрудникам оперативных служб важно усилить работу по следующим направлениям [13]:

– начать сотрудничать с провайдером интернет-услуг, который на основании судебного решения предоставит следствию данные о посещаемых страницах компьютеров и телефонов подозреваемых;

– привлечь IT-специалиста для сбора и анализа информации сайтов, пропагандирующих незаконный оборот наркотических веществ, а также на установку программ, отслеживающих посещение интересующих интернет-ресурсов;

– подготовку запросов в Федеральную службу по надзору в сфере связи информационных технологий и массовых коммуникаций (Роскомнадзор) о блокировании подозрительных порталов;

– разработать аналитическую систему, которая позволит проводить оперативно-розыскные мероприятия с применением цифровых технологий, машинного обучения и технологии Больших данных.

Для комплексной оперативной работы при борьбе с преступной деятельностью наркодилеров важно систематически и комплексно осуществлять мониторинг сайтов и порталов, публикующих потенциально опасную информацию о наркотических веществах.

Быстроразвивающиеся современные цифровые технологии, доступность интернета для всех слоев населения, всеохватность социальных сетей создают препятствия для оперативной блокировки запрещенного контента.При этом сотрудники оперативных служб в рамках своих возможностей регулярно передают данные в Роскомнадзор для блокирования опасных сайтов посредством работы с провайдерами.

К минусам такого способа можно отнести время, которое приходится тратить, так как работа осуществляется при помощи человеческого ресурса. Поэтому автоматизирование с помощью специально настроенных программ для мониторинга позволило бы ускорить рабочий процесс и увеличить результат [14].

Для оперативного блокирования доступа пользователей интернета к контенту, содержащему противоправную информацию, было бы разумным взаимодействие с отечественными поисковыми сервисами, например, такими как Yandex, Mail.Ru, Rambler, Rutube, Aport, Webalta, Nigma.

Важно признать, что для получения положительного результата в борьбе с наркопреступностью важно выстроить работу с интернет-провайдерами, выяснить, как оперативно получить имеющуюся у них информацию. Еще одну сложность на этом этапе представляют иностранные фирмы, которые предоставляют интернет и при этом территориально находятся за границей.

Большим подспорьем в работе по сбору информации о злоумышленниках является информация, оставленная в Интернете самими участниками преступлений. Сюда относится случаи, когда пользователи восстанавливают пароль с помощью специальных серверов или оставляют свой номер телефона, а также другие личные данные на странице в социальных сетях.

Для улучшения работы сотрудников оперативных служб и ведомств, занимающихся разоблачением наркопреступлений в Интернет-пространстве, возможны следующие шаги для улучшения функционирования данного процесса [14]:

1) введение поправок в Федеральный закон «Об оперативно-розыскной деятельности», а именно дополнение положениями, которые позволят субъектам самостоятельно блокировать денежные переводы и счета (при наличии информации об их вовлеченности в сферу незаконного оборота наркотических веществ);

2) предоставление права субъектам оперативно-розыскной деятельности создавать сайты для обнаружения лиц, причастных к незаконному обороту наркотических средств;

3) постоянное совершенствование мониторинга и выявление интернет-ресурсов, созданных для сбыта наркотических средств;

4) привлечение на постоянной основе IT-специалистов, программистов для отслеживания посетителей сайтов, пропагандирующих незаконный оборот наркотических веществ;

5) создание банка данных нераскрытых преступлений, связанных с незаконным оборотом наркотических средств регионального уровня, а также автоматизированной информационной системы «Незаконный оборот

наркотических средств», состоящей из уже существующей и постоянно пополняющейся оперативной информации по части борьбы с незаконным оборотом наркотических средств.

Согласно проведенному исследованию важно на законодательном уровне рассмотреть следующие вопросы:

– введение обязательной регистрации юридических лиц, осуществляющих сделки с использованием цифровой валюты;

– запрет для некоммерческих организаций и банковских учреждений на проведение операций с криптовалютами с незарегистрированными в установленном порядке юрлицами;

– привлечение к уголовной ответственности за теневой оборот криптовалюты;

– арест на оборот криптовалюты в случае следственных и оперативно-розыскных мероприятий, а также закрепление списка требований для обменных пунктов, бирж, банкоматов для порядка изъятия криптовалюты;

– запрет и ответственность на законодательном уровне на массовую рассылку противоправной информации, а также приравнивание мессенджеров к организаторам распространения информации.

Литература

1. Кожемячкина М.Р. Информационная среда наркозависимых лиц // Сибирские уголовно-процессуальные и криминалистические чтения, 2016, №5(13).

2. Шалагин А.Е., Усманов И.М. Современная наркоситуация в Российской Федерации: тенденции, прогноз, меры противодействия // Вестник Казанского юридического института МВД России, 2016, №1(23).

3. Морозов, А.В. Особенности борьбы с наркопреступностью в сфере информационно-телекоммуникационных технологий / А.В. Морозов // Профессионал: научно-практический альманах МВД России, 2018, №3.

4. Осипенко А.Л., Миненко П.В. Оперативно-розыскное противодействие незаконному обороту наркотических средств, совершаемому с ИС пользованием телекоммуникационных устройств // Вестник ВИ МВД России, 2014, №1.

5. Дикарев В.Г., Олимпиев А.Ю. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России, 2016, №8.

6. Тимофеев С.В. Использование информационно-телекоммуникационных технологий при бесконтактном сбыте наркотических средств: проблемы противодействия и пути решения // Криминалистика: вчера, сегодня, завтра, 2018, №4(8).

7. Виноградов И.А., Загайнов В.В. Современные схемы «бесконтактного» сбыта наркотических средств и психотропных веществ // Криминалистика: вчера, сегодня, завтра, 2017, №2(2).

8. Богданов А.В., Ильинский И.И., Хазов Е.Н. Информационно-телекоммуникационная сеть Интернет как один из наиболее востребованных ресурсов в противодействии незаконному обороту наркотиков // Вестник Московского университета МВД России, 2018, №3.

9. Кушпель Е.В., Кулешов П.Е. Некоторые аспекты криминалистической характеристики незаконного сбыта наркотических средств, совершенного бесконтактным способом // Международный журнал прикладных и фундаментальных исследований, 2016, №2(1). С. 119–122.

10. Суходолов А.П. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков / А.П. Суходолов, А.М. Бычкова // Всероссийский криминологический журнал, 2019. Т. 13, № 1. С. 5–17.

11. Земцова С.И. Предмет допроса свидетелей при расследовании незаконного сбыта синтетических наркотических средств, совершенного с использованием интернет-магазинов // Криминалистика: вчера, сегодня, завтра, 2018, №3(7).

12. Земцова С.И. Интернет-магазины, осуществляющие незаконный сбыт синтетических наркотических средств: дифференциация и характерные признаки // Вестник Сибирского юридического института МВД России, 2019, №1(34).

13. Гурьянов К.В., Шатило Я.С. Организация противодействия распространению наркотиков через интернет Антинаркотическая безопасность, 2016, №1(6). С. 101–108.

14. Глушков Е.Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия // ППД, 2018, №2. С. 45–53.

References

1. Kozhemyachkina M.R. Informatsionnaya sreda narkozavisimykh lits // Sibirskiye ugolovno-protsessual'nyye i kriminalisticheskiye chteniya, 2016, №5(13).

2. Shalagin A.Ye., Usmanov I.M. Sovremennaya narkosituatsiya v Rossiyskoy Federatsii: tendentsii, prognoz, mery protivodeystviya // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii, 2016, №1(23).

3. Morozov, A.V. Osobennosti bor'by s narkoprestupnost'yu v sfere informatsionno-telekommunikatsionnykh tekhnologiy / A.V. Morozov // Professional: nauchno-prakticheskiy al'manakh MVD Rossii, 2018, №3.

4. Osipenko A.L., Minenko P.V. Operativno-rozysknoye protivodeystviye nezakonnomu oborotu narkoticheskikh sredstv, sovershayemomu s IS pol'zovaniyem telekommunikatsionnykh ustroystv // Vestnik VI MVD Rossii, 2014, №1.

5. Dikarev V.G., Olimpiyev A.YU. K voprosu o protivodeystvii beskontaktnomu sposobu sbyta narkotikov cherez set' Internet // Vestnik Moskovskogo universiteta MVD Rossii, 2016, №8.

6. Timofeyev S.V. Ispol'zovaniye informatsionno-telekommunikatsionnykh tekhnologiy pri beskontaktnom sbyte narkoticheskikh sredstv: problemy protivodeystviya i puti resheniya // Kriminalistika: vchera, segodnya, zavtra, 2018, №4(8).

7. Vinogradov I.A., Zagaynov V.V. Sovremennyye skhemy «beskontaktnogo» sbyta narkoticheskikh sredstv i psikhotropnykh veshchestv // Kriminalistika: vchera, segodnya, zavtra, 2017, №2(2).

8. Bogdanov A.V., Il'inskiy I.I., Khazov Ye.N. Informatsionno-telekommunikatsionnaya set' Internet kak odin iz naiboleye vostrebovannykh resursov v protivodeystvii nezakonnomu oborotu narkotikov // Vestnik Moskovskogo universiteta MVD Rossii, 2018, №3.

9. Kushpel' Ye.V., Kuleshov P.Ye. Nekotoryye aspekty kriminalisticheskoy kharakteristiki nezakonnogo sbyta narkoticheskikh sredstv, sovershennogo beskontaktnym sposobom // Mezhdunarodnyy zhurnal prikladnykh i fundamental'nykh issledovaniy, 2016, №2(1). S. 119–122.

10. Sukhodolov A.P. Tsifrovyye tekhnologii i narkoprestupnost': problemy protivodeystviya ispol'zovaniyu messendzhera «Telegram» v rasprostranenii narkotikov / A.P. Sukhodolov, A.M. Bychkova // Vserossiyskiy kriminologicheskiy zhurnal, 2019. T. 13, № 1. S. 5–17.

11. Zemtsova S.I. Predmet doprosa svideteley pri rassledovanii nezakonnogo sbyta sinteticheskikh narkoticheskikh sredstv, sovershennogo s ispol'zovaniyem internet-magazinov // Kriminalistika: vchera, segodnya, zavtra, 2018, №3(7).

12. Zemtsova S.I. Internet-magaziny, osushchestvlyayushchiye nezakonnyy sbyt sinteticheskikh narkoticheskikh sredstv: differentsiatsiya i kharakternyye priznaki // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii, 2019, №1(34).

13. Gur'yanov K.V., Shatilo YA.S. Organizatsiya protivodeystviya rasprostraneniyu narkotikov cherez internet Antinarkoticheskaya bezopasnost', 2016, №1(6). S. 101–108.

14. Glushkov Ye.L. Sbyt narkoticheskikh sredstv beskontaktnym sposobom posredstvom seti Internet: puti vyyavleniya i raskrytiya // PPD, 2018, №2. S. 45–53.

ФЕЛЬДМАН Елена Васильевна, доцент, кафедра «Компьютерной безопасности и прикладной алгебры», Челябинский государственный университет. 454001, г. Челябинск, ул. Бр. Кашириных, 129. E-mail: mila008.is@gmail.com

FELDMAN Elena, Associate Professor, Department of Computer Security and Applied Algebra, Chelyabinsk State University. 454001, Chelyabinsk, ul. Br. Kashirinykh, 129. E-mail: mila008.is@gmail.com

УДК 004.052

Вестник УрФО № 2(36) / 2020, с. 56–60

Афанасьева М. В., Абзалутдинов Д. Р., Бараков К. Я. DOI: 10.14529/secur200209

ПРИНЦИПЫ ПОСТРОЕНИЯ МОДЕЛИ НАДЕЖНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ АСУ ТП

В статье рассмотрена возможность применения теории надежности технических систем для количественной оценки уровня защиты системой управления кибербезопасностью АСУ ТП. Построена модель надежности и определена функция надежности для каждого компонента подсистемы. Также приведены аналитические выражения для расчета вероятности безотказной работы системы управления кибербезопасностью АСУ ТП в целом, построена модель надежности системы с учетом её подсистем.

Ключевые слова: *модель надежности, система управления кибербезопасностью, функция надежности, последовательно-параллельная схема.*

Afanaseva M. V., Abzalutdinov D. R., Barakov K. Y.

CYBERSECURITY MANAGEMENT OF INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS: PRINCIPLES OF RELIABILITY MODEL BUILDING

The article considers the possibility of applying the reliability engineering theory for the quantification of cyber security level of industrial automation and control systems security. The reliability model was built and the reliability function for each component of the subsystem was determined. Analytical expressions for the cybersecurity management system uptime probability calculation are also given, and a system reliability model was built taking into account its subsystems.

Keywords: *reliability model, cybersecurity management system, reliability function, serial-parallel circuit.*

Рис. 1. Структурная схема CSMS

В настоящее время при анализе эффективности систем защиты информации (СЗИ) в рамках оценки защищенности информации мало рассматривается оценка надежности защиты информации в связи с отсутствием моделей надежности, учитывающих специфику СЗИ и согласующихся с подходами, построенных на классической теории надежности технических систем [1]. Оценивая надежность защищенности АСУ ТП, необходимо учитывать факт, что безопасность АСУ ТП не сводится к обеспечению информационной безопасности (ИБ), т.е. обеспечению конфиденциальности собираемой, обрабатываемой и передаваемой информации [2–3]. Безопасность АСУ ТП должна заключаться прежде всего в обеспечении непрерывности и целостности самого ТП [3]. Эта особенность еще более усложняет анализ надежности защищенности АСУ ТП, поэтому вопрос о разработке модели надежности защиты промышленных объектов является важной и актуальной задачей.

Согласно ГОСТ Р МЭК 62443-2-1—2015 система управления кибербезопасностью (CSMS) АСУ ТП включает в себя следующие элементы, представленные на рис. 1.

Данная схема соединения компонентов CSMS имеет сложную комбинированную структуру, поэтому целесообразно предварительно произвести декомпозицию системы, разбив ее на простые подсистемы, которые, в свою очередь, так же разбить на более простые квазиэлементы.

Модель надежности CSMS представлен на рис. 2.

Данная структура имеет вид последовательного соединения, которое в теории надежности используется тогда, когда отказ одного элемента приводит к отказу всей системы [5]. Выбор такого типа соединения обусловлен следующими тремя ситуациями. Без проведения анализа рисков кибератак CSMS (отказ подсистемы «Анализ рисков») организация не сможет убедить руководство выделить средства на создание CSMS, и, следовательно, нечего будет совершенствовать, и наступит отказ всей системы CSMS. Также отказ CSMS наступит, если не будут приниматься меры по устранению рисков. И, наконец, без контроля и совершенствования CSMS будет неэффективной для защиты от постоянно появляющихся кибератак, и в итоге наступит отказ всей системы.

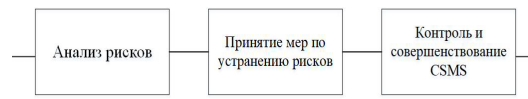

Рис. 2. Модель надежности CSMS

Функция надежности CSMSпринимает следующий вид:

$$P_{CSMS}(t) = P_{AP}(t) \cdot P_{ПМ}(t) \cdot P_{КС}(t), \quad (1)$$

где $P_{AP}(t)$– вероятность безотказной работы (ВБР) подсистемы «Анализ рисков», %;

$P_{ПМ}(t)$– ВБР подсистемы «Принятие мер по устранению рисков», %;

$P_{КС}(t)$– ВБР подсистемы «Контроль и совершенствование CSMS», %;

t – время, с.

Далее оценим надежность каждой подсистемы отдельно также применяя декомпозицию.

Подсистема «Анализ рисков»

Цель данной подсистемы – идентифицировать и документально описать уникальные потребности организации для устранения рисков кибератак в отношении АСУ ТП и определить комплекс кибер-рисков АСУ ТП, которые угрожают организации, и оценить вероятность и уровень серьезности таких рисков. Отсюда можно сделать вывод, что компоненты анализов рисков кибербезопасности, как одного из компонентов CSMS в целом на схеме ее надежности должны быть соединены последовательно (рис. 3).

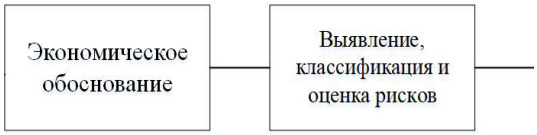

Рис. 3. Модель надежности подсистемы «Анализ рисков»

Функция надежности:

$$P_{АР}(t) = P_{ЭО}(t) \cdot P_{Р}(t), \quad (2)$$

где $P_{ЭО}(t)$ – ВБР компонента «Экономическое обоснование», %;

$P_{Р}(t)$– ВБР компонента «Выявление, классификация и оценка рисков», %;

Подсистема «Принятие мер по устранению рисков»

Рассмотрим причины и механизмы возникновения отказа в данной подсистеме.

Применительно к компоненту «Политика, организация и понимание необходимости безопасности»:

– не разработан формальный письменный документ с описанием сферы применения для программы обеспечения кибербезопасности;

– не организованы структурные единицы, ответственные за управление, проведение и оценку общей кибербезопасности объектов АСУ ТП;

– не разработана и не внедрена программа обучения по работе с системой ИБ;

– персонал не прошел первоначальное и периодическое обучение по вопросам работы с правильными процессами безопасности и правильному использованию объектов обработки информации, а также отсутствие процедуры аттестации программы обучения;

– не разработаны политика и процедуры безопасности и не доведены до персонала.

Применительно к компоненту «Избранные контрмеры по обеспечению безопасности»:

– не установлена политика в области безопасности персонала;

– не реализована физическая безопасность и защита от внешних воздействий;

Применительно к компоненту «Внедрение»:

– не принята схема управления рисками;

– не применен общий комплекс контрмер, направленных на физические риски и риски для информационной безопасности при идентификации определенного риска.

Так как при выходе из строя хотя бы одной из составляющих частей данной подсистемы вероятность кибератаки увеличится, но не приведет к отказу всей подсистемы в целом, и каждая часть подсистемы может функционировать вне зависимости от других, обеспечивая требуемый уровень защиты, поэтому все части рассмотренной подсистемы должны быть соединены параллельно (рис. 4).

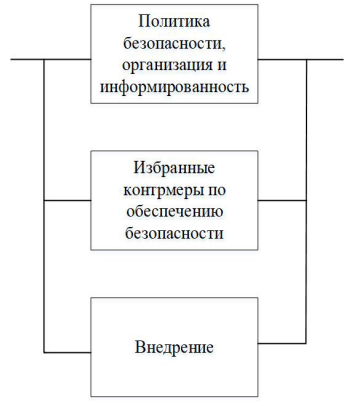

Рис. 4. Модель надежности подсистемы «Принятие мер по устранению рисков»

Функция надежности:

$$P_{ПМ}(t) = 1-(1-P_{ПБ}(t)) \cdot (1-P_{ИК}(t)) \cdot (1-P_{В}(t)), \quad (3)$$

где $P_{ПБ}(t)$– ВБР компонента «Политика безопасности»;

$P_{ИК}(t)$– ВБР компонента «Избранные контрмеры»;

$P_{В}(t)$ – ВБР компонента «Внедрение».

Подсистема «Контроль и совершенствование CSMS»

Данная подсистема обеспечивает соответствие CSMS, которое означает, что организация придерживается официальной политики, своевременно выполняет процедуры и составляет отчеты для последующего анализа. Также в рамках этой подсистемы обеспечивается анализ, совершенствование и поддержание CSMS. Отказ одного из компонентов не приведет к отказу подсистемы, следовательно, компоненты представляют собой параллельное соединение (рис. 5).

Рис. 5. Модель надежности подсистемы «Контроль и совершенствование CSMS»

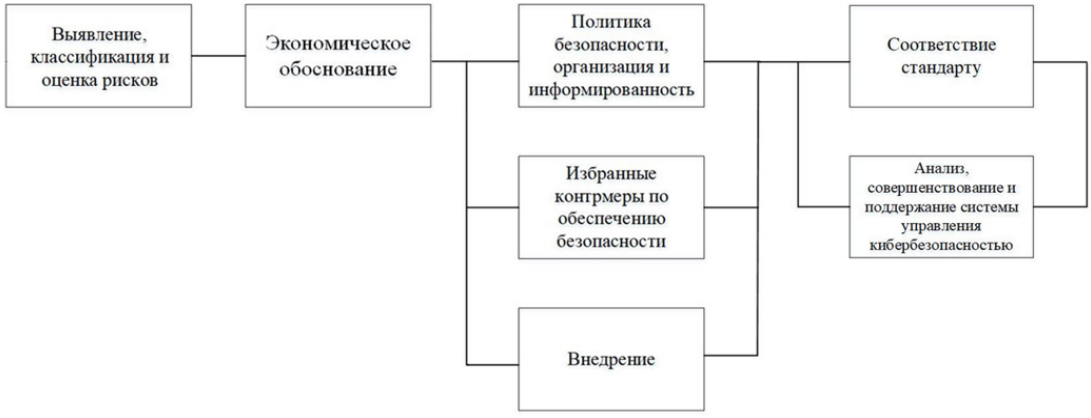

Рис. 6. Модель надежности CSMS с учетом структур ее подсистем

Функция надежности:

$P_{КС}(t) = 1-(1-P_{СС}(t)) \cdot (1-P_{АСПК}(t))$, (4)

где $P_{СС}(t)$ – ВБР компонента «Соответствие стандарту»;

$P_{АСПК}(t)$ – ВБР компонента «Анализ, совершенствование и поддержание системы управления кибербезопасностью».

Подставим в модель надежности CSMS модели надежности подсистем «Анализ рисков», «Принятие мер по устранению рисков» и «Контроль и совершенствование CSMS», чтобы получить модель надежности CSMS с учетом структур ее подсистем (рис. 6).

Подставим в (1) функции надежности (2), (3) и (4), чтобы получить функцию надежности CSMS с учетом структур ее подсистем:

$$P_{CSMS}(t) = P_{ЭО}(t) \cdot P_{Р}(t) \cdot P_{ПМ}(t) \cdot P_{КС}(t) \cdot [1-(1-P_{ПБ}(t)) \cdot (1-P_{ИК}(t)) \cdot (1-P_{В}(t))] \cdot [1-(1-P_{СС}(t)) \cdot (1-P_{АСПК}(t))].$$

С помощью полученной функции надежности CSMS можно оценивать эффективность мер защиты АСУ ТП и выявлять наиболее ненадежные компоненты системы. Таким образом, полученная информация о надежности системы в данной момент времени дополнит общую картину защищенности предприятия и позволит принять необходимые меры для повышения уровня защиты.

Литература

1. Булгаков О.М., Стукалов В.В., Кучмасов Е.А. Принципы построения модели надежности организационного компонента системы защиты информации объекта информатизации//Вестник Воронежского института МВД России. -2013. - № 2. - С.145–155.

2. Ярушевский Д. Кибербезопасность АСУ ТП – что это и зачем? [Электронный ресурс]. URL: https://www.dialognauka.ru/press-center/article/13226 (дата обращения 9.10.2019).

3. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии//Международная конференция «Наука. Исследования. Практика». – 2019. – С. 341–345.

4. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия//Актуальные проблемы современной науки, техники и образования. -2017. -Т. 1. С. 217–220.

5. Афанасьева М.В. Лабораторный практикум по курсу «Теоретические основы обеспечения надежности систем автоматизации и модулей мехатронных систем»: лабораторный практикум – Магнитогорск, 2019.

6. ГОСТ Р МЭК 62443-2-1-2015.

References

1. Bulgakov O.M., Stukalov V.V., Kuchmasov Ye.A. Printsipy postroyeniya modeli nadezhnosti organizatsionnogo komponenta sistemy zashchity informatsii ob»yekta informatizatsii//Vestnik Voronezhskogo instituta MVD Rossii. -2013. -№ 2. -S. 145–155.

2. Yarushevskiy D. Kiberbezopasnost' ASU TP – chto eto i zachem? [Elektronnyy resurs]. URL: https://www.dialognauka.ru/press-center/article/13226 (data obrashcheniya 9.10.2019).

3. Mikhaylova U.V., Bykova T.V. Audit informatsionnoy bezopasnosti na predpriyatii//Mezhdunarodnaya konferentsiya «Nauka. Issledovaniya. Praktika». – 2019. – S. 341–345.

4. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Prognozirovaniye lokal'nykh i vneshnikh ugroz na informatsionnyye servery predpriyatiya//Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. -2017. -T. 1. S. 217–220.

5. Afanas'yeva M. V. Laboratornyy praktikum po kursu «Teoreticheskiye osnovy obespecheniya nadezhnosti sistem avtomatizatsii i moduley mekhatronnykh sistem»: laboratornyy praktikum – Magnitogorsk, 2019.

6. GOST R MEK 62443-2-1-2015.

АФАНАСЬЕВА Маргарита Владимировна, старший преподаватель кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Россия, Челябинская область, г. Магнитогорск, пр. Ленина, 38. E-mail: nansy_stokli@mail.ru

АБЗАЛУТДИНОВ Данил Римович, студент второго курса Института энергетики и автоматизированных систем по направлению подготовки Информационная безопасность автоматизированных систем, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Россия, Челябинская область, г. Магнитогорск, пр. Ленина, 38. E-mail: abz-dan@yandex.ru

БАРАКОВ Камил Ялилевич, студент второго курса Института энергетики и автоматизированных систем по направлению подготовки Информационная безопасность автоматизированных систем, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Россия, Челябинская область, г. Магнитогорск, пр. Ленина, 38. E-mail: kamil.barakov@gmail.com

AFANASEVA Margarita, Senior lecturer at theDepartment of Computer Science and Cyber security, Nosov Magnitogorsk State Technical University. 455000, Russia, Chelyabinsk Region, Magnitogorsk, 38 Lenin avenue. E-mail: nansy_stokli@mail.ru

ABZALUTDINOV Danil, second-year student at the Power Engineering and Automated Systems Institute, Department of Computer Science and Cyber security, Nosov Magnitogorsk State Technical University. 455000, Russia, Chelyabinsk Region, Magnitogorsk, 38 Lenin avenue. E-mail: abz-dan@yandex.ru

BARAKOV Kamil, second-year student at the Power Engineering and Automated Systems Institute, Department of Computer Science and Cyber security, Nosov Magnitogorsk State Technical University. 455000, Russia, Chelyabinsk Region, Magnitogorsk, 38 Lenin avenue. E-mail: kamil.barakov@gmail.com

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 № 2(36) / 2020
Подписано в печать 30.06.2020.
Дата выхода в свет 04.09.2020. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 5,6. Тираж 100 экз. Заказ 234/243.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 2(36) / 2020
Signed to print June 30, 2020.
Date of publication of the 04.09.2020. Format 70×108 1/16. Screen printing.
Conventional printed sheet 5,6. Circulation – 100 issues. Order 234/243. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080