ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 2(44) / 2022

Подписной индекс 73852 в каталоге «Почта России»

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

Свидетельство ПИ № ФС77-65765 от 20.05.2016

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

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

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

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 2(44) / 2022

FOUNDER

SOUTH URAL STATE UNIVERSITY (NIU)

SOUTH URAL LEGAL NEWSLETTER

Subscription index 73852

in the «Russian Post» catalog

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

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

Publisher: OOO « South Ural Legal Newsletter»

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

Electronic version of the magazine in the Internet:

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

16+

В НОМЕРЕ

РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

IN THIS ISSUE

RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

УДК 004.056 Вестник УрФО № 2(44) / 2022, с. 5–11

Хижников Д. И., Михайлова У.В., Баранкова И.И.

DOI: 10.14529/secur220201

РАЗРАБОТКА ОБУЧАЮЩЕГО КОМПЛЕКСА ДЛЯ РАСЧЕТА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

В настоящее время защита выделенных помещений как никогда актуальна. Для оценки полноты и актуальности применяемых средств защиты, а также для анализа эффективности их применения используется специальные методические документы, разработанные ФСТЭК России.

В статье рассматривается обучающий тренажер для расчета побочных электромагнитных излучений. Данный тренажер имитирует реальное оборудование, предназначенного для обучения студентов ВУЗов методике проведения специсследования.

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

Khizhnikov D. I., Mikhailova U.V., Barankova I.I

DEVELOPMENT OF A TRAINING COMPLEX FOR CALCULATING INCIDENTAL ELECTROMAGNETIC EMISSIONS

At present, protection of allocated premises is more relevant than ever. To assess the completeness and relevance of the protection means used, as well as to analyze the effectiveness of their use, special methodological documents developed by FSTEC of Russia.

This article describes a training simulator for calculating incident electromagnetic emissions. This simulator simulates real equipment designed to teach students of higher education institutions the methods of special investigation

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

В настоящий момент технические средства (ТС), представляют большую ценность, поскольку могут обрабатывать большое количество информации за малый промежуток времени. Однако при обработке информации ТС возникает побочное электромагнитное излучение (ПЭМИ), перехватив которое злоумышленник получает доступ к обрабатываемой информации. Частотный диапазон ПЭМИ, сопровождающих информативный сигнал, простирается от единицы кГц до ГГц. В связи с этим у организации возникает потребность в защите информации и соответственно в устранении данного технического канала утечки информации.

Главное направление защиты информации от утечки за счет ПЭМИ - уменьшение отношения информативного сигнала к помехе до предела, определяемого «Нормами эффективности защиты АСУ и ЭВМ от утечки информации за счет ПЭМИ». Нормы определяют числовой коэффициент, при котором восстановить исходные данные невозможно. Решение этой задачи достигается снижением уровня излучений информационных сигналов, или увеличением уровня помех в частотных диапазонах.

Согласно ГОСТ Р 50922-2006 [1], специальные исследования (СИ) – комплекс мероприятий с использованием контрольно-измерительной аппаратуры, направленных на выявление и измерение информативных сигналов в каналах возможной утечки за счет побочных электромагнитных излучений и наводок, несущие скрываемую или защищаемую информацию, а также оценка защищенности информации требованиям нормативных документов по защите информации.

Для определения защищённости, исследуемой ТС в условиях эксплуатации, измеряется затухание до границы контролируемой зоны (КЗ). С учетом полученного затухания, используя данные лабораторных исследований (специальных исследования) делается вывод о защищенности объекта информатизации, а также размер зоны R2 [2].

“Зона 2” (R2) - это расстояние между ТС и условной границей, за пределами которой не возможен эффективный прием вследствие естественного затухания сигнала на фоне помех.

СИ проводятся с использованием современной измерительной аппаратуры, сертифицированной и поверенной, в соответствии с требованиями нормативных документов ФСБ России, а также ФСТЭК России. Для проведения СИ используется дорогостоящие оборудование: анализаторы спектра (Rohde&Schwarz FSH8, АКИП-4204/TG, Protek A734) с антеннами (П6-124, П6-122, П6-121).

Не многие ВУЗы для подготовки молодых специалистов по информационной безопасности имеют возможность закупить необходимое программно-аппаратное обеспечение, из-за чего студенты могут ознакомиться с методом проведения СИ только в теории. Виртуальные тренажеры способны заменить дорогостоящее оборудование и поспособствовать эффективной подготовке и развитию профессиональных навыков будущих специалистов информационной безопасности. Для решения данной проблемы разработан виртуальный тренажер позволяющий:

1. Изучить основные методики проведения СИ;

2. Освоить специальное оборудование, используемое специалистами информационной безопасности на современных предприятиях;

3. Получить навыки поиска и измерения ПЭМИ.

Разработанный виртуальный тренажер представляет собой программный комплекс, позволяющий проводить физические опыты на компьютере без непосредственного контакта с реальным оборудованием или лабораторным стендом. Он предназначен для приобретения первичных навыков в эксплуатации типовых программно-аппаратных комплексов поиска и измерения ПЭМИ.

Тренажер разработан в среде разработки Unity. Unity очень удобен для разработки средних и крупных проектов в 3D пространстве. Движок использует для написания скрипов язык программирования C#.

Разработанный виртуальный тренажер содержит меню библиотеки с информацией об оборудовании. В этом меню студент имеет возможность ознакомиться с основными характеристиками оборудования, его общим видом и габаритами. В плане дальнейшего развития тренажера предусмотрено расширение библиотеки (добавление нового оборудования, нормативные и технические документы и т.п.). На текущий момент разработана модель анализатора спектра Rohde & Schwarz FSH8 (модель 28) (рис. 1), которая имеет абсолютно те же параметры и интерфейс, что и у реального образца.

Тренажер позволит обучающимся изучить возможности специализированного обо-

а б

Рис. 1. Анализатора спектра Rohde & Schwarz FSH8, где а - реальный, б - модель в тренажере

рудования, произвести СИ с использованием специальных методик, а также осуществить поиск сигнала и проанализировать его.

В качестве исследуемого объекта используется модель монитора. На экране можно задать разрешение и частоту кадров, из этих показателей будет рассчитываться частота излучения для дальнейшего нахождения этого сигнала на анализаторе спектра. Так же на экране можно задать центральную частоту.

Тренажер с правами доступа студент предусматривает два режима работы:

• В первом режиме (easy) студент знакомится с методом проведения СИ, для этого в тренажере предусмотрена система подсказок, которая будет направлять каждое действие учащегося.

• Во втором режиме (hard) студенту будет необходимо самостоятельно провести СИ, опираясь на знания полученные в ходе прохождения режима easy.

В тренажере предусмотрены различные права доступа:

• администратор (преподаватель) который может:

1. возможность изменения планировки;

2. изменения параметра исследуемых объектов (мощности сигнала выходе, μВт);

3. задавать настройки для уровня hard.

• пользователь (студент) который может:

1. изменять настройки исследуемого объекта (разрешение и частоту обновления экрана);

2. возможность изменения расположения антенны;

3. изменять свойства стен (кирпичная кладка, дерево, полистирол, бетон, пенополистирол).

Место установки исследуемого объекта не статично, как преподаватель, так и студент имеют возможность перемещения исследуемых объектов в пространстве спроектированного помещения.

Перед началом измерений студенту необходимо установить антенну измерителя напряженности поля на расстоянии R0 от исследуемого ОТСС. После этого необходимо произвести настройку ОТСС.

На ОТСС эмулируется работы Windows 7 в которой установлено два ПО:

Программа “Тест сигнал” эмитирует работу монитора и излучаемый им ПЭМИ сигнал, когда пользователь нажимает первую кнопку то на экране запускается тестовый сигнал, который генерирует частоты работы ОТСС с уровнем мощности сигнала.

После полученный данных на выявленных частотах необходима измерить уровень шума при выключенном ОТСС. Для этого нужно нажать вторую кнопку для запуска измерителя шумов.

После получения всех необходимых данных студенту становится доступна панели расчетов, в которой студенту необходимо рассчитать R2.

“Настройка” данное ПО эмитирует про-

граммно-аппаратный комплекс "Зонд-3" для воспроизведения стабильного по частоте и мощности сигнала. Для этого пользователю представлена два поля для ввода.

Анализатор не может автоматически определить частоту, на которой монитор излучает сигнал, поэтому изначально на экране анализатора спектра изображен спектр шума (рис.2). Настройка анализатора спектра пошагово и подробно показывается пользователю в виде всплывающих окон (только в режиме easy), которые меняются после успешно проведенного действия.

Если все значения посчитаны правильно на экране анализатора появится спектр сигнал + шум. На рис. 3 показана спектрограмма сигнала + шум, найденная на частоте 29 МГц мощностью 85 dBμV, который рассчитывается по формуле $dB\mu V=20Log_{10}(V_{вых}/1мкВ)$, где $V_{вых}$ – выходное напряжение, dBμV(дБмкВ) – абсолютное напряжение в децибелах относительно 1 мкВ. Полученный сигнал позволяет определить критерии защищенности.

На рис.4 показана модель помещения, в котором происходит СИ. Виртуальный тренажер учитывает реальную модель распростра-

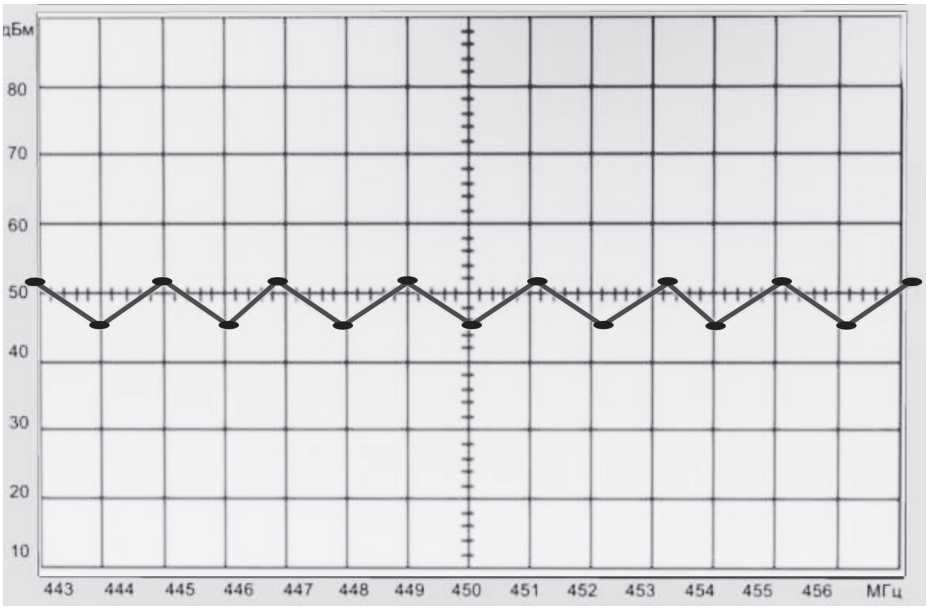


Рис. 2. Спектр шума

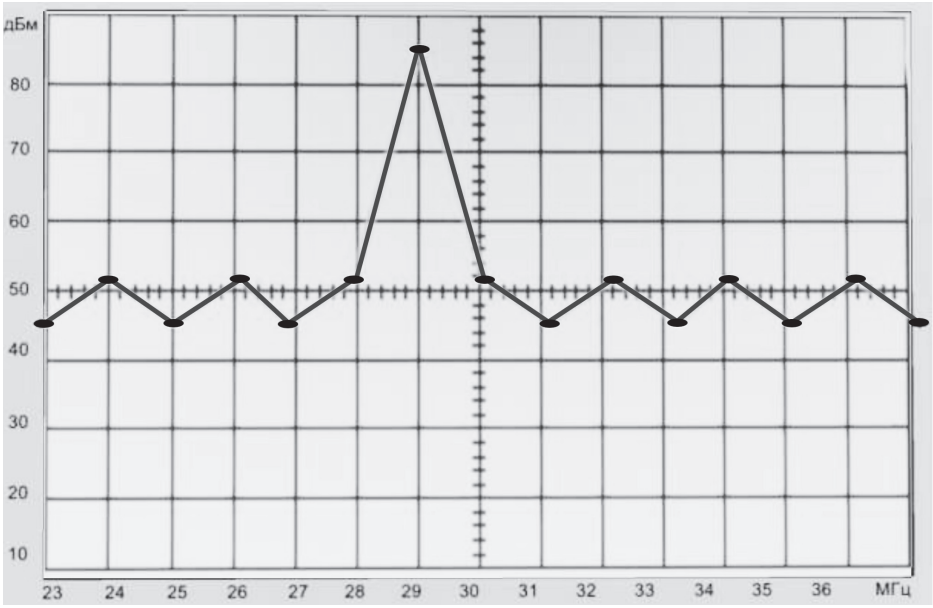


Рис. 3. Спектр сигнал+шум

нения сигнала в пространстве. Поэтому при расчетах учитываются:

1. воздушная среда;

2. заграждающие объекты без учета металлических конструкций.

В связи с политической напряженностью,

Рис. 4. Модель помещения

обострившейся вокруг России в последний год, стали особенно востребованы молодые квалифицированные специалисты в области информационной безопасности. Поэтому внедрение в образовательную программу ВУЗов виртуального тренажера обучающего комплекса для расчета ПЭМИ позволит повысить технологическую грамотность и инициативность студентов. Разработанный тренажер будет способствовать наиболее эффективному обучению по направлению информационная безопасность в части технической защиты информации, а также будет полезен специальностям: «Информационная безопасность телекоммуникационных систем» (10.05.02), «Информационная безопасность автоматизированных систем» (10.05.03).

Литература

1. Национальный стандарт российской федерации. ГОСТ Р 50922-2006 «ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ» [Текст], Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст. – 2021. – 4 с.

2. Хорев А. А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники// Специальная техника. 2010. № 2. – С. 2–15.

3. [Электронный ресурс] – Режим доступа: https://searchinform.ru/analitika-v-oblasti-ib/utechki

informatsii/sluchai-utechki-informatsii/utechka-informatsii-po-kanalam-pemin/razrabotka-meropriyatij-po-zaschite-informatsii-ot-utechki-po-kanalam-pemin/ (Дата обращения: 20.03.2022).

4. Технические Средства и Методы Защиты Информации / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. - Москва: Машиностроение, 2009. – 45 с.

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

6. 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: https://books.google.ru/books?id=GJOqBb3vtNUC&printsec =copyright&hl=ru#v=onepage&q&f=false

7. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Техническая защита информации / Международная конференция «Наука. Исследования. Практика». – 2017. – С. 7–10.

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

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. Имитационный тренажер для изучения устройства и принципа разработки подземных горнодобывающих систем / Имитационный тренажер. Магнитогорск, 2011.

11. Михайлова У.В., Аименева А.А., Полехина А.В. Технические средства защиты информации / Актуальные проблемы современной науки. Безопасность в информационной сфере. 2012. – С. 27–30.

References

1. Natsional'nyy standart rossiyskoy federatsii. GOST R 50922-2006 «OSNOVNYYe TERMINY I OPREDELENIYA» [Tekst], Prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 27 dekabrya 2006 g. N 373-st. - 2021. – 4 s.

2. Khorev A. A. Tekhnicheskiye kanaly utechki informatsii, obrabatyvayemoy sredstvami vychislitel'noy tekhniki// Spetsial'naya tekhnika. 2010. № 2. – S. 2–15.

3. [Elektronnyy resurs] – Rezhim dostupa: https://searchinform.ru/analitika-v-oblasti-ib/utechki informatsii/sluchai-utechki-informatsii/utechka-informatsii-po-kanalam-pemin/razrabotka-meropriyatij-po-zaschite-informatsii-ot-utechki-po-kanalam-pemin/ (Data obrashcheniya: 20.03.2022).

4. Tekhnicheskiye Sredstva i Metody Zashchity Informatsii / A.P. Zaytsev, A.A. Shelupanov, R.V. Meshcheryakov i dr. - Moskva: Mashinostroyeniye, 2009. – 45 s. 5. Mikhaylova U.V., Bykova T.V. Audit informatsionnoy bezopasnosti na predpriyatii / Mezhdunarodnaya konferentsiya «Nauka. Issledovaniya. Praktika». – 2019. – S. 341–345.

6. Ragozin YU.N. Inzhenerno-Tekhnicheskaya Zashchita Informatsii: Uchebnoye Posobiye po Fizicheskim Osnovam Obrazovaniya Tekhnicheskikh Kanalov Utechki Informatsii i po Praktikumu Otsenki ikh Opasnosti/ Ragozin YU.N. - Elektron. Tekstovyye Dannyye -SPb.: Intermediya, 2018 – 168 c.– Rezhim dostupa: https://books.google.ru/books?id=GJOqBb3vtNUC&printsec =copyright&hl=ru#v=onepage&q&f =false

7. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Tekhnicheskaya zashchita informatsii / Mezhdunarodnaya konferentsiya «Nauka. Issledovaniya. Praktika». – 2017. – S. 7–10.

8. Barankova I.I., Mikhaylova U.V., Roman'ko. Ye.A., Borisov V.O. Imitatsionnyy trenazher dlya izucheniya ustroystva i printsipa raboty teodolita / Magnitogorsk 2011. 9. Barankova I.I., Mikhaylova U.V. Osobennosti formirovaniya otsenochnykh sredstv dlya otsenki urovnya sformirovannosti kompetentsiy spetsialista po informatsionnoy bezopasnosti / Informatsionnoy protivodeystviye ugrozam terrorizma. 2015. T. 2. №25. – S. 26–30.

10. Imitatsionnyy trenazher dlya izucheniya ustroystva i printsipa razrabotki podzemnykh gornodobyvayushchikh sistem / Imitatsionnyy trenazher. Magnitogorsk 2011.

11. Mikhaylova U.V., Aimeneva A.A., Polekhina A.V. Tekhnicheskiye sredstva zashchity informatsii / Aktual'nyye problemy sovremennoy nauki. Bezopasnost' v informatsionnoy sfere. 2012. – S. 27–30.

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующая кафедрой Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: inna_barankova@mail.ru

ХИЖНИКОВ Дмитрий Игоревич, студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: strelok454@list.ru

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

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Informatics and Information Security f Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000. E-mail: inna_barankova@mail.ru

KHIZHNIKOV Dmitry Igorevich, student of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000. E-mail: strelok454@list.ru

MIKHAILOVA Uliana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000. E-mail: ylianapost@gmail.com

УДК 004.056.2; 316.334.3:324(470+571) Вестник УрФО № 2(44) / 2022, с. 12–24

Поршнев С.В., Рябко Н.Ю.

DOI: 10.14529/secur220202

ОПЫТ ПРИМЕНЕНИЯ МЕТОДА БЕРРА И СКАККО ДЛЯ ПРОВЕРКИ ДОСТОВЕРНОСТИ ЭЛЕКТОРАЛЬНЫХ ДАННЫХ

В статье обсуждаются результаты анализа электоральных данных участковых избирательных комиссий (УИК) Свердловской области (СО) по результатам выборов в 2018 г. Президента Российской Федерации (РФ). Цель анализа – проверка гипотезы об отсутствии фальсификаций использованных электоральных данных. В качестве инструмента исследований использован метод Бебера и Скакко.

Получены оценки чувствительности данного метода, свидетельствующие о возможности выявления потенциальных фальсификаций электоральных данных в случаях, когда количество чисел, заканчивающихся цифрами «0» и «5» не менее, чем на 8% превышает аналогичную величину в случае их отсутствия.

Вычислены оценки плотностей вероятностей второй после запятой цифры в электоральном показателе «отношение числа проголосовавших избирателей на данном избирательном участке к общему числу зарегистрированных избирателей», а также появления одинаковых цифр в первом и во втором разрядах после запятой, которые свидетельствуют об отсутствии в СО на этих выборах фальсификаций электоральных данных.

Ключевые слова: *выборы, электоральные данные, фальсификация электоральных данных, метод Бебера и Скакко, плотность распределения, критерий хи-квадрат.*

Porshnev S.V., Raybko N.Yu.

EXPERIENCE IN APPLYING THE BURR AND SCACCO METHOD TO VERIFY THE RELIABILITY OF ELECTORAL DATA

The article discusses the results of the electoral data of the Precinct Election Commissions (PECs) of the Sverdlovsk Region (SO) analysis that based on the results of the elections in 2018 of the President of the Russian Federation (RF). The purpose of the analysis is to test the hypothesis

about the absence of falsifications of the used electoral data. The method of Beber and Scacco was used as a research tool.

Sensitivity estimates of this method have been obtained, indicating the possibility of identifying potential falsifications of electoral data in cases where the number of numbers ending with the numbers «0» and «5» is at least 8% higher than the same value in case of their absence.

The distribution density of the second digit after the decimal point in the electoral indicator «the ratio of the number of voters who voted in a given polling station to the total number of registered voters» estimates and the identical numbers in the first and second digits after the decimal point appearance are calculated, which indicate the absence of falsification of electoral data in SO in these elections.

Keywords: *elections, electoral data, falsification of electoral data, Beber and Scacco method, distribution density, chi-square test.*

Введение

Сегодня в политологии и юриспруденции активно разрабатываются и обсуждаются различные аспекты правовой защиты политической системы и её институтов от, так называемой, электоральной преступности. Под данным понятием понимают (см., например, [1–5]) совокупность преступлений, ответственность за совершение которых предусмотрена статьями 141, 1411, 142 и 1421 Уголовного кодекса (УК) Российской Федерации (РФ), совершаемых в определенные периоды в пределах какой-либо территории. Термин «электоральная преступность» был введен в отечественную политическую криминологию в [3] в 2000 г. Обоснование целесообразности выделения электоральной криминологии, как самостоятельного научного направления, основным объектом исследования которой является электоральная преступность, отдельные формы и/или виды ее проявления, причины её существования и распространения, особенности личности преступника и жертвы, а также меры противодействия данному негативному явлению, приведено, например, в [4].

Один из подходов, призванных выявлять возможные фальсификации результатов выборов, основан на использовании статистических методов анализа данных, собранных во время проведения голосования. В англоязычной литературе в качестве обобщенного названия этих методов используется термин «electoral forensics» [6], который можно перевести как «электоральная криминалистика». В [7] выделены две группы методов электоральной криминалистики:

– к первой группе отнесены методы, основанные анализе частотных характеристик цифр количественных данных о результатах голосования;

– ко второй группе – методы, основанные на анализе соотношений между вычисляемыми характеристиками электоральных данных, например, уровнем явки избирателей и уровнем поддержки кандидатов.

При этом в обеих группах методов выявление фальсификаций основано на сравнении результатов анализа реальных электоральных данных с соответствующими оценками, вычисленными на основе использования математических моделей «идеальных» выборов, оценить адекватность которых, однако, не представляется возможным, так как для этого, в свою очередь, необходимо и электоральные результаты «идеальных» выборов, но при этом сначала требуется доказать, что выборы были проведены, действительно «идеально». (В известной мере ситуация изоморфна известному детскому стихотворению о попе и его собаке.)

Закономерно, что в данной ситуации возникает огромный простор для самостоятельного анализа и интерпретации результатов проводимых, в первую очередь в Российской Федерации (РФ), выборов в соответствие с занимаемой политической позицией конкретным исследователем (политологом) по отношению действующей в государстве власти, что противоречит требованиям Федерального закона «Об информации, информационных технологиях и о защите информации» (149-ФЗ) [8], который в соответствие со статьей 1 регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации,

и устанавливает принципы правового регулирования отношений в сфере информации,

информационных технологий и защиты информации [9, ст. 3], в том числе, принцип «достоверности информации и своевременности ее предоставления».

При этом по мнению исследователей электоральных результатов выборов (электоральных статистиков – ЭС), оппозиционно настроенных по отношению к власти РФ (оппозиционных ЭС – ОЭС), в XXI вв. в нашей стране не было проведено ни одних выборов, результаты которых не были бы фальсифицированы. В этом можно убедиться, ознакомившись, например, с архивом электронного международного журнала «Electoral Politics» [9]; материалами дискуссии «Возможности математических методов по выявлению электоральных фальсификаций» [10] и другими публикациями многочисленных ОЭС (см. например, [11–14] и др.), часть из которых при этом получали финансовую поддержку за счет грантов государственных научных фондов РНФ и РФФИ. При этом попытки критического анализа математических методов, используемых для выявления электоральных аномалий (см., например, [15]), которые сегодня реализованы в виде соответствующих online сервисов [16], встречают резкую критику со стороны ОЭС (см., например, [17]).

Принимая во внимание социальную и политическую значимость проблемы делигитимации выборов, проводимых в РФ, представляется актуальным проведение не ангажированных исследований электоральных данных и интерпретации получаемых результатов. В статье обсуждаются результаты анализа электоральных данных, представленных участковыми избирательными комиссиями, проводивших выборы Президента РФ в 2018 г. на территории Свердловской области (СО).

2. Источник и структура анализируемых электоральных данных

Для проведения анализа особенностей мнений участников выборов Президента РФ в 2018 г. в СО, были использованы официальные данные, размещенные на сайте Центральной избирательной комиссии (ЦИК) [18]. В связи с тем, что сайт ЦИК не позволяет скачать одновременно все электоральные данные, собранные в ходе выборов Президента РФ в 2018 г., авторами был разработан специальный программный инструмент, обеспечивающий выгрузку этих данных в виде единого файла, имеющего формат Excel (далее файл «Данные ЦИК») [19]. Данный файл представляет собой таблицу, состоящую из 23 столбцов. Соответствие между названиями столбцов в файле «Данные ЦИК» и их контентом приведено в таблице 1.

Записи в файле «Данные ЦИК» упорядочены по алфавите в порядке убывания иерархии полей: «Название субъекта РФ», «Название ТИК», «Название УИК». После строки, содержащей электоральные сведения о последней УИК, созданной данной ТИК данного субъекта РФ, отображаются сводные данные по соответствующей ТИК. При этом в обсуждаемой строке поле с координатами (I3, «Номер обсуждаемой строки») остается пустым.

Таблица 1

Название столбца	Тип данных	Контент данных
I1	Текст	Название субъекта РФ
I2	Текст	Название территориальной избирательной комиссии (ТИК)
I3	Текст	Название участковой избирательной комиссии (УИК)
c1	Числовой	Число избирателей, включенных в список избирателей
c2	Числовой	Число избирательных бюллетеней, полученных участковой избирательной комиссией
c3	Числовой	Число избирательных бюллетеней, выданных избирателям, проголосовавшим досрочно
c4	Числовой	Число избирательных бюллетеней, выданных в помещении для голосования в день голосования
c5	Числовой	Число избирательных бюллетеней, выданных вне помещения для голосования в день голосования
c6	Числовой	Число погашенных избирательных бюллетеней
c7	Числовой	Число избирательных бюллетеней в переносных ящиках для голосования
c8	Числовой	Число бюллетеней в стационарных ящиках для голосования
c9	Числовой	Число недействительных избирательных бюллетеней
c10	Числовой	Число действительных избирательных бюллетеней

Окончание таблицы 1

Название столбца	Тип данных	Контент данных
c11	Числовой	Число утраченных избирательных бюллетеней
c12	Числовой	Число избирательных бюллетеней, не учтенных при получении
c13	Числовой	Число избирательных бюллетеней, поданных за Бабурина Сергея Николаевича
c14	Числовой	Число избирательных бюллетеней, поданных за Грудинина Павла Николаевича
c15	Числовой	Число избирательных бюллетеней, поданных за Жириновского Владимира Вольфовича
c16	Числовой	Число избирательных бюллетеней, поданных за Путина Владимира Владимировича
c17	Числовой	Число избирательных бюллетеней, поданных за Собчак Ксению Анатольевну
c18	Числовой	Число избирательных бюллетеней, поданных за Сурайкина Максима Александровича
c19	Числовой	Число избирательных бюллетеней, поданных за Титова Бориса Юрьевича
c20	Числовой	Число избирательных бюллетеней, поданных за Явлинского Григория Алексеевича

Соответственно, после строки, содержащей сводные данные о последней ТИК данного субъекта РФ, отображаются сводные данные по всем ТИК данного субъекта РФ. При этом в обсуждаемой строке поля с координатами (I2, «Номер обсуждаемой строки»), (I3, «Номер обсуждаемой строки») остаются пустыми. Выбранная структура файл «Данные ЦИК», как очевидно, позволяет извлекать электоральные данные как по отдельным УИК, отдельным ТИК выбранного субъекта РФ, так и по выбранному субъекту РФ, в целом, а также по выбранному Федеральному округу РФ.

Всего файл «Данные ЦИК» содержит 100579 строк (записей). При этом в первой строке файла размещаются названия столбцов, представленные в таблице 1. Отметим, что столбцы «c11», «c12» содержат только нулевые значения.

Далее для проведения последующего анализа из файла «Данные ЦИК» были извлечены электоральные данные по каждой из УИК, созданной на территории СО (общее число УИК – 2582).

3. Анализ электоральных данных, представленных УИК СО по результатам выборов Президента РФ в 2018 г.

Рассмотрим выбранные результаты анализа электоральных данных, представленных УИК СО по результатам выборов Президента РФ в 2018 г.

Зависимости числа зарегистрированных избирателей (Последовательность № 1 – П1) и числа проголосовавших избирателей от порядкового номера УИК СО (Последовательность № 2 – П2), а также аппроксимации их плотностей распределений (ПР), вычисленные с помощью функции ksdensity.m пакета MATLAB, представлены на рисунке 1.

Из рисунка 1 видно, что П1, П2 являются некоторыми выборками случайных процессов, имеющих двухмодальные ПР. Значения П1 принадлежат отрезку [11,3581], значения П2 – отрезку [5,2356]. Координаты локальных максимумов ПР анализируемых зависимостей оказываются равными 314 и 1889. Визуальный анализ П1, П2 и их ПР позволяет предположить, что существует линейная связь между числом зарегистрированных и числом проголосовавших избирателей.

Для подтверждения данного предположения была исследована зависимость числа проголосовавших избирателей на данном избирательном участке (B) числа зарегистрированных избирателей данной УИК (V), представленная на рисунке 2 (слева вверху), из которой видно, что точки с координатами (V_i, B_i) $i = \overline{1,2580}$ располагаются вдоль прямой

$$v = ax + b, \quad (1)$$

где a=0.6045, b=13.1407 – коэффициенты прямой, вычисленные с помощью метода наименьших квадратов. При этом значение коэффициента детерминации R^2, характеризующего величину линейной связи между показателями B и V, оказалось равным 0967.

Для оценки степени отклонения точек с координатами (V_i, B_i) от прямой (1) вычислены

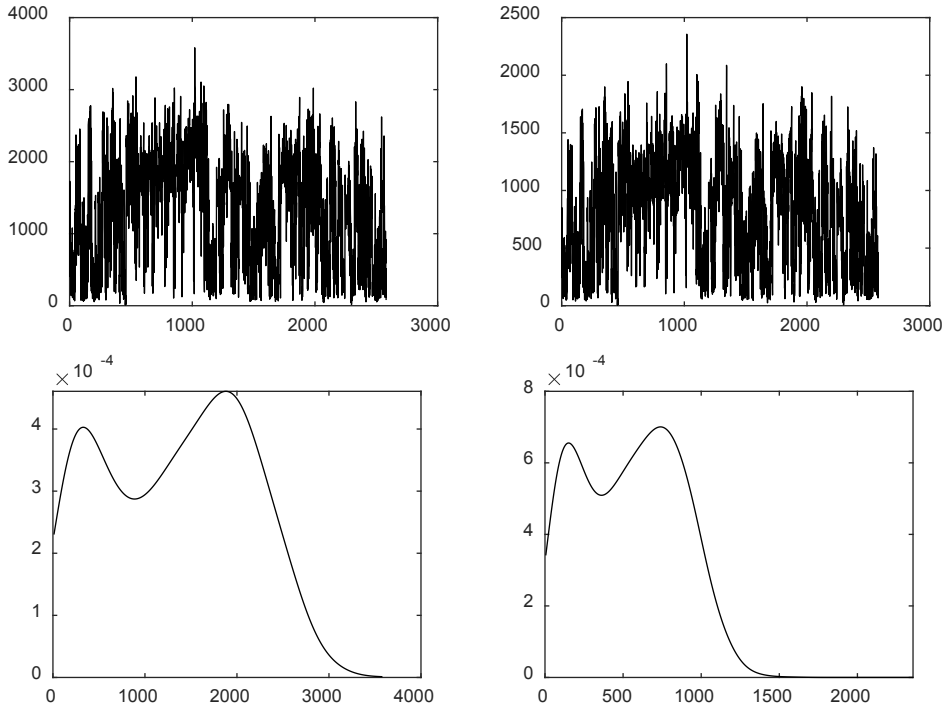


Рис. 1. Сверху: Последовательности № 1 (слева), № 2(справа); снизу аппроксимации их ПР (соответственно)

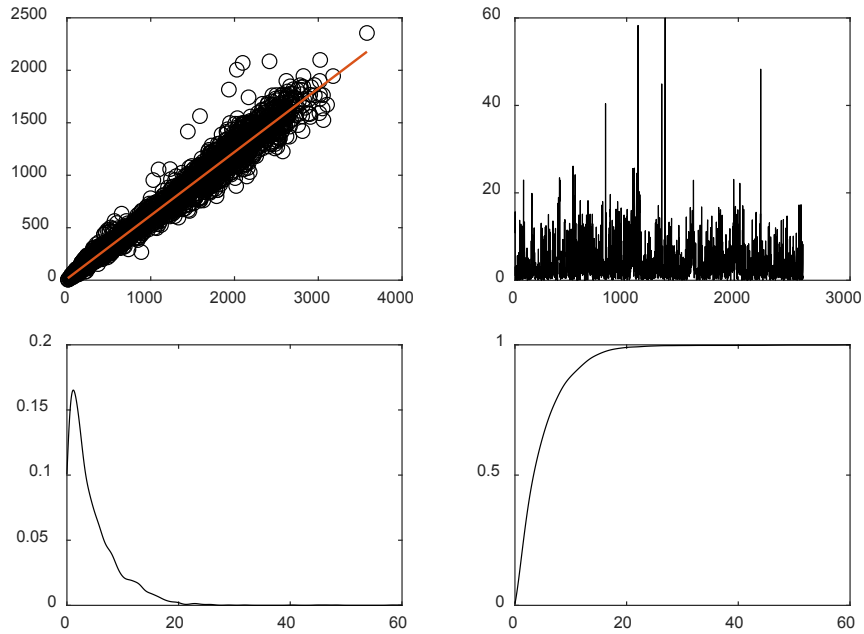


Рис. 2. К анализу особенностей зависимости *B=f (V)* (слева направо и сверху вниз): зависимость *B=f (V)*, зависимость расстояния от прямой

расстояния от прямой (1) до соответствующих точек:

$$d_i = \frac{|aV_i + b - B_i|}{\sqrt{a^2 + b^2}},\ i = \overline{1,2580}.$$

Последовательность $\{d_i\}$ представлена на рисунке 2 (вверху, справа). ПР и функция распределения (ФР) данной последовательности также представлены на рисунке 2 (снизу, слева и справа, соответственно). Из рисунка 2 (вверху, справа) видно, что члены последовательности $\{d_i\}$ являются случайными величинами с областью рассеяния [0.001; 60], среднее значение которой равняется 4.5399, а среднеквадратическое отклонение σ = 4.8438. Анализ ПР последовательности $\{d_i\}$ показывает, что значения 96% членов последовательности $\{d_i\}$ не

превосходят 3σ=14.5313, в связи с чем, с нашей точки зрения, нет оснований полагать, что на этих участках проводилась фальсификация результатов голосования. Значения 4% членов последовательности $\{d_i\}$ избирательных участка значения 4% превосходят 3σ.

Например, максимальные значения оказываются у членов последовательности $\{d_i\}$ с номерами i =811, 1102, 1314, 1345, 2200 (соответственно, порядковыми номерами УИК), которым соответствуют следующие пары точек на плоскости (V, B): (1443,1417); (1588, 1564); (2028,2006); (2098,2071); (1933,1817). Отмеченные электоральные результаты были опубликованы следующими УИК СО: УИК №1590 Ленинской ТИК г. Екатеринбурга; УИК №1782 Чкаловской ТИК г. Екатеринбурга; УИК №1905 Красно-Уральской городской ТИК; УИК №457 Камышловской городской ТИК; УИК №2595 Свободненской поселковой ТИК. При этом только в последней УИК 270 избирателей воспользовались правом досрочного голосования.

Эти результаты, с нашей точки зрения, обусловлены высокой в сравнении с другими избирательными участками явкой избирателей, которая, отнюдь, не является прямым доказательством фальсификации электоральных данных на этих участках, но поводом для анализа выявленных особенностей электорального поведения. Отметим, что подтвердить или опровергнуть достоверность аномальных результатов можно при наличии достоверных данных опросов избирателей, проводимых независимыми экспертами на выходе данных избирательных участков (экзит-поллов) (см., например, [20,21]).

В связи с отсутствием данной информации было проведено самостоятельное исследование распределения встречаемости цифр в последнем разряде значений явки избирателей на избирательные участки во время выборов Президента РФ в 2018 г. (отношений, вычисленных на каждом из избирательных участков числа избирательных бюллетеней, признанных действительных, к общему числу зарегистрированных избирателей, измеряемых с точностью до второго знака после запятой), а также распределения вероятности появления одинаковых цифр в первом и втором знаках после запятой выбранного показателя.

3. Основные идеи метода Бебера и Скакко

Использованный метод, называемый методом Бебера и Скакко [22], основан на анализе встречаемости цифр в данных электоральной статистики и сравнении с соответствующим распределением цифр в «нефальсифицированных» данных электоральной статистики.

Данный метод восходит к закону Бендорфа (закону первой цифры) [23], в соответствие с которым вероятность встретить в первом разряде численных характеристик некоторых процессов, к которым относятся стохастические процессы и процессы, являющиеся аддитивными суммами данных процессов, цифры d (d=0,1,…9)) $P(d)$ равняется

$$P(d)=\log_2(d+1)-\log_2(d)=\log_2\left(1+\frac{1}{d}\right).$$

Для электоральных данных закон Бендорфа непосредственно оказывается неприменимым, однако, есть основания полагать, что данному закону подчиняется не первая, но последняя цифры выбранного показателя электоральной статистики. В качестве таковых показателей ОЭС используют, например, целочисленные показатели: численность избирателей, численность проголосовавших избирателей, численность избирателей, проголосовавших за конкретного кандидата/конкретную партию и т.д. При этом полагается, что в условиях отсутствия фальсификаций частота встречаемости каждой из цифр, стоящих в последней позиции числа (отношения числа случаев, в которых выпала данная цифра к общему числу чисел, использованных в анализе), будет одинаковой.

Описанное свойство последней цифры целых случайных чисел иллюстрирует рисунок 3, на котором представлены ПР частоты встречаемости цифр «0», «3», «5», «9», вычисленные на основе анализа выборки целых случайных чисел, принадлежащих интервалу [11,3811].

Для вычисления зависимостей, представленных на рисунке 3, на каждом (i-ом) шаге метода Монте-Карло ($i=\overline{1,10^3}$) генерировалось $N = 10^3$ независимых случайных чисел, принадлежащих интервалу [11,3811], используя которые подсчитывались частоты встречаемости цифр «0», «1»,… «9» – n_j, $j=\overline{0,9}$, которые далее заносились в матрицу Z_{ij}, размером 10^3•10. Каждый столбец матрицы Z_{ij} представлял собой случайную выборку частот встречаемости соответствующей последней цифры. Далее были вычислены ПР каждой и цифр, а также их аппроксимации нормальными законами распределения $N(\mu_i, \sigma_i)$, $i=\overline{0,9}$, где в качестве параметров распределений использовались их оценки, вычисленные по соответствующим столбцам матрицы Z_{ij}.

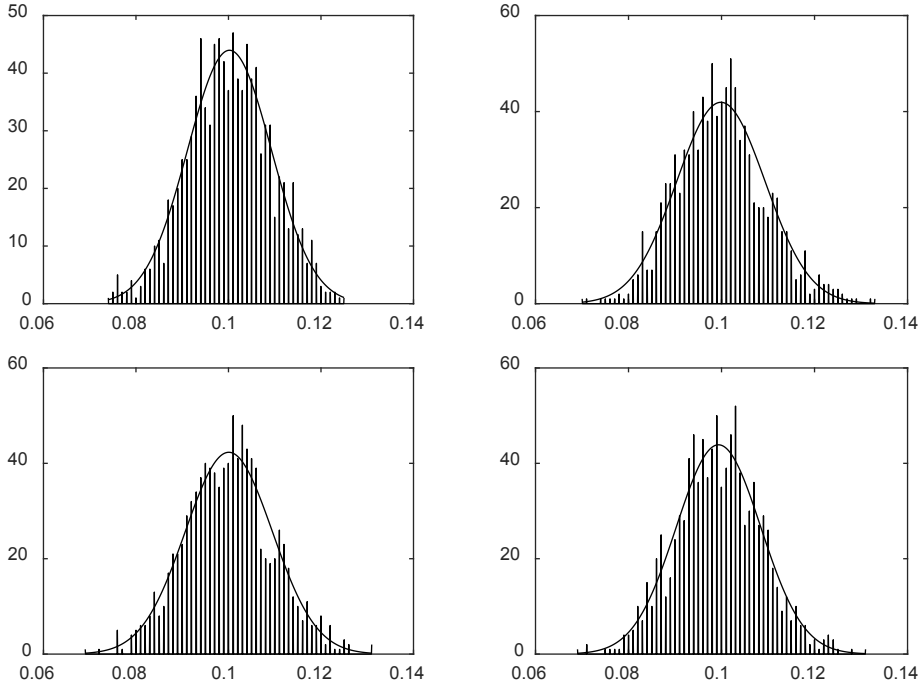


Рис. 3. ПР частот встречаемости цифр «0», «3», «5», «9» и их аппроксимации нормальным законом распределения $N(\mu_i, \sigma_i)$

$$\mu_i = \frac{1}{N_p}\sum_{j=0}^{N_p} Z_{ij}, \sigma_i = \left[\frac{1}{N_p - 1}\sum_{j=0}^{N_p}\left(Z_{ij} - \mu_i\right)^2\right]^{1/2} N_p = 10^3,$$

представленные в таблице 2.

Из таблицы 2 видно, что можно выдвинуть статистическую гипотезу о том, что частоты встречаемости цифр «0», «1»,… ,«9» в рассматриваемом случае являются случайной выборкой с равномерным законом распределения (плотность распределения $\mu_i^{\langle therory\rangle} = 0.1$, $i = \overline{0,9}$), которая подтверждается результатами сравнения статистики критерия x^2

Таблица 2

Параметры распределений $N(\mu_i, \sigma_i)$

i	0	1	2	3	4	5	6	7	8	9
μ_i	0.1002	0.1006	0.0996	0.0999	0.0999	0.1001	0.1005	0.0997	0.1001	0.0994
σ_i	0.0091	0.0096	0.0095	0.0095	0.0095	0.0094	0.0099	0.0094	0.0093	0.0091

$$\chi^2 = N_p \sum_{i=0}^{9} \frac{\left(\mu_i - \mu_i^{\langle theory\rangle}\right)^2}{\mu_i^{\langle theory\rangle}} = 0.0093 \qquad (2)$$

где N_p – объем выборки, по которой вычислена оценка частоты встречаемости μ_i с критическим значения квантиля x^2-распределения с 8 степенями свободы на уровне значимости $\alpha = 0.05$:

$$x^2_{1\text{-}a}(8)=15.5073.$$

Так как статистика $x^2 < x^2_{1\text{-}a}(8)$, значения частот встречаемости цифр «0», «1», …, «9» в последнем разряде изученной выборки целых случайных чисел μ_i можно считать одинаковыми и равными 0.1, соответственно, совокупность случайных чисел $\{\mu_i\}$ – выборкой из генеральной совокупности случайных чисел с дискретным равномерным законом распределения на интервале [0,9].

Данный результат положен в основу в метода Бебера и Скакко [22], в котором полагается, что внесение фальсификаций в те или иные целочисленные показатели выборов (численность избирателей N_b, число проголосовавших избирателей N_v и т.д.), с неизбежностью, приведет к изменению частот встречаемости последних цифр $\mu_i^{\langle exper\rangle}$, и, соответственно, изменению статистики критерия x^2 (2). В случае когда

$$x^2 \geq x^2_{0.95}(8)=15.5073, \qquad (3)$$

факт фальсификации электоральной статистики считается доказанным.

По мнению ОЭС наиболее часто встречающиеся фальсификации электоральных данных состоят в увеличении частот встречаемости цифр «0» и «5», μ_0, μ_5 за счет пропорционального уменьшения частот встречаемости цифр «1», «2», «3», «4», «6», «7», «8», «9». В этой связи закономерно возникает вопрос: На какую величину $\Delta/2$ следует увеличить частоты встречаемости цифр «0» $\left(\tilde{\mu}_0 = \mu_0 + \Delta/2\right)$, и «5» $\left(\tilde{\mu}_5 = \mu_5 + \Delta/2\right)$, пропорционально уменьшив при этом значения частот встречаемости каждой из цифр «1», «2», «3», «4», «6», «7», «8», «9» $\left(\tilde{\mu}_m = \mu_m - \Delta/8, m = \overline{1,4}, m = \overline{6,9}\right)$, чтобы гипотеза о равномерном распределении последовательности $\{n_i\}$ была отвергнута на уровне значимости 0.05? Для ответа на данный вопрос применительно к значениям частоты встречаемости, представленным в таблице 2, была вычислена зависимость статистики $\tilde{\chi}^2 = \tilde{\chi}^2(\Delta)$:

$$\tilde{\chi}^2(\Delta) = N_p \sum_{i=0}^{9} \frac{\left(\tilde{\mu}_i - 0.1\right)^2}{0.1} = N_p \left(\left(\mu_0 + \Delta/2\right)^2 + \left(\mu_5 + \Delta/2\right)^2 + \sum_{\substack{m=\overline{1,9}, \\ i \neq 5}}^{9} \left(\mu_m + \Delta/2\right)^2 \right),$$

представленная на рисунке 4.

Из рисунка 4 видно, что значение функции $\tilde{\chi}^2 = \tilde{\chi}^2(\Delta)$ превышает критическое значение критерия $x^2_{0.95}(8)$ при $\Delta \geq 0.1575$. Данный результат означает, что выявить внесенные изменения в данные, находящиеся в столбцах описанной выше матрицы *Z*, с помощью обсуждаемого критерия удастся если они таковы, что μ_0, $\mu_5 \geq 0.1788$, $\mu_1=\mu_2=\mu_3=\mu_4=\mu_6=\mu_7=\mu_8=\mu_9 \geq 0.1197$. Применительно к исходным данным это означает, что для достижения указанных значений частот встречаемости последних цифр следует изменить не менее чем на ≈8,0% количества простых чисел, оканчивающихся на число «0», «5», и уменьшения не менее чем на ≈2,0%, количество каждого из простых чисел, оканчивающихся цифрами «1», «2», «3», «4», «6», «7», «8», «9».

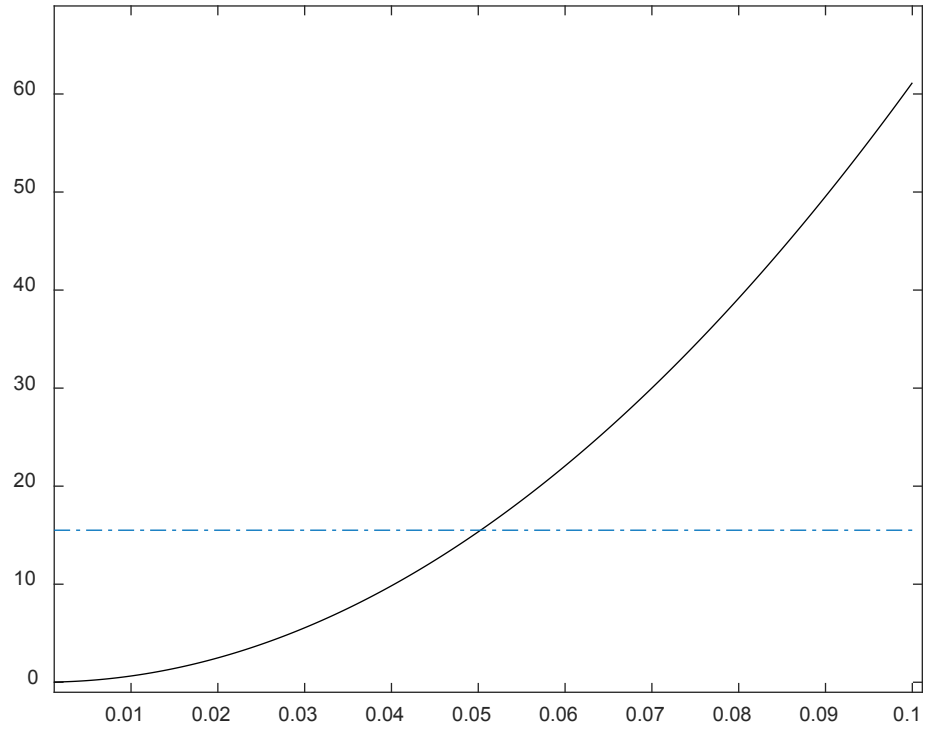


Рис. 4. График функции $\tilde{\chi}^2 = \tilde{\chi}^2(\Delta)$ (пунктир – прямая y=15.5073)

Аналогичные свойства, как показывает анализ результатов статистического моделирования, оказывается у распределения цифр, стоящих в предпоследней позиции целых случайных чисел – вероятность появления каждого из чисел «0», «1», …, «9» оказывается равна 0.1. Следовательно, вероятность появления двух одинаковых цифр в последней и предпоследней позициях целого случайного

числа равняется 0.1×0.1=0.01. В этой связи, факт отличия частот встречаемости одинаковых цифр в последнем и предпоследнем разрядах членов последовательности $V_i^{\langle r \rangle}$ рассматривается ОЭС, как один из индикаторов фальсификации электоральных результатов.

Отметим, что описанный выше подход, может быть использован при возникновении подозрений о возможных фальсификациях электоральных данных для оценки объемов, внесенных в них изменений.

3. Анализ распределений цифр в значениях явки избирателей на УИК СО во время выборов Президента РФ в 2018 г.

В нашем исследовании в качестве анализируемого показателя электоральной статистики было выбрано отношение числа выборщиков, принявших участие в голосовании на данном избирательном участке, к общему числу зарегистрированных избирателей, вычисляемому в процентах:

$$V_i^{\langle r \rangle} = \mathrm{round}\left(\frac{B_i}{V_i} \cdot 10^4 \right),$$

где round( ) – функция округления действительного числа до ближайшего целого. Выбор множителя 10^4 обеспечивает анализ распределения второй после запятой цифры в числе, равном отношению избирателей, принявших участие в голосовании, к количеству зарегистрированных избирателей, измеряемому в процентах. Данный показатель определяется активностью избирателей, на которую оказывают влияние большое число, в том числе, и случайных факторов, в то время как само число избирателей определяется большим числом «квазидетерминированных» процессов, например, экономическими и демографическими процессами.

Зависимость $V_i^{\langle r \rangle} / 100 = f(i),\ i = \overline{1,2580}$ – порядковый номер УИК, упорядоченных в алфавитном порядке и соответствующими образом пронумерованным, а также аппроксимация ее плотности распределения с помощью ядерной функции представлены на рисунке 5.

Из рисунка 5 видно, что последовательность $V_i^{\langle r \rangle} / 100$ представляет собой некоторую реализацию случайного процесса, область значений которого находится в интервале [30,100]%, среднее значение и дисперсия равняются 62.85%, 8.40%, соответственно. (Здесь высокий процент проголосовавших избирателей оказался на избирательных участках относительно небольшим числом зарегистрированных избирателей (не более 100), фальсификация электоральных данных на которых не имеет никакого смысла.)

Результаты подсчетов частот встречаемости последних цифр, выполненные по всем

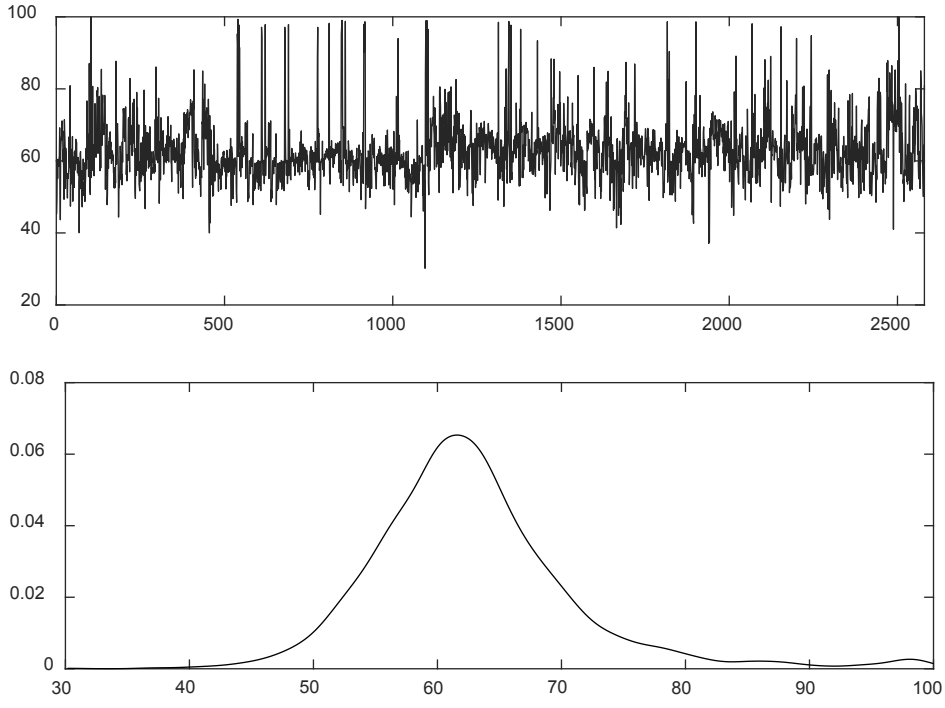


Рис. 5. Зависимость $V_i^{\langle r \rangle} / 100 = f(i), i = \overline{1,2580}$ (сверху) и ее ПР (снизу)

членам последовательности $V_i^{\langle r\rangle}$, а также частот встречаемости одинаковых цифр в последней и предпоследней позиции членов последовательности $V_i^{\langle r\rangle}$, представлены в таблице 3.

Значение статистики x^2, вычисленное в соответствие с (2), для данных, приведенных в таблице 3, оказывается равным $x^2 = 10.6589 < x^2_{0.95}(8)$. Уровень доверительной вероятности, соответствующего значению статистики x^2, оказывается равным 0.7782. Таким образом, следует есть все основания принять гипотезу о том, что последовательность $\{\mu_i\}$ случайной выборкой дискретного случайного процесса с равномерной плотностью распределения, равной 0.1, область рассеяния которого – отрезок [0,9].

Таблица 3

Частоты встречаемости цифр «0»–«9» в последнем разряде членов случайной последовательности $V_i^{\langle r\rangle}$

i	0	1	2	3	4	5	6	7	8	9
μ_i	0.1105	0.1000	0.0930	0.0984	0.0953	0.0884	0.1016	0.1012	0.1023	0.1093

Результаты подсчетов частот встречаемости одинаковых цифр в последней и предпоследней позиции членов последовательности $V_i^{\langle r\rangle}$ представлены в таблице 4.

Значение статистики x^2, вычисленное в соответствие с (2), для данных, приведенных в таблице 4, оказывается равным $x^2 = 12.8026 < x^2_{0.95}(8)$. Уровень доверительной вероятности, соответствующего значению статистики x^2, оказывается равным 0.8812. Таким образом, следует есть все основания принять гипотезу о том, что последовательность $\left\{\mu_i^{\langle 2\rangle}\right\}$ случайной выборкой дискретного случайного процесса с равномерной плотностью распределения, равной 0.1, область рассеяния которого – отрезок [0,9].

Таблица 4

Частоты встречаемости парных цифр в последнем и предпоследнем разрядах членов случайной последовательности $V_i^{\langle r\rangle}$

i	0	1	2	3	4	5	6	7	8	9
$\mu_i^{\langle 2\rangle}$	0.0159	0.0112	0.0105	0.0097	0.0105	0.0101	0.0108	0.0066	0.0097	0.0093

Описанные свойства распределения последних цифр последовательности $V_i^{\langle r\rangle}$ свидетельствую об отсутствии о фальсификации электоральных данных во время выбора Президента РФ, проведенных на территории СО в 2018 г.

Заключение

Проведен анализ электоральных данных, предоставленных УИК СО ЦИК РФ, размещенные на сайте ЦИК, цель которого состояла в проверке гипотезы об отсутствии фальсификаций электоральных данных во время выбора Президента РФ в 2018 г. в СО с помощью метода Бебера и Скакко.

На примере анализа распределения цифр, стоящих в последнем разряде целых чисел, синтезированных с помощью метода Монте-Карло целых чисел, находящихся в диапазоне [11,3581], получены оценки чувствительности метода Бебера и Скакко, свидетельствующие о возможности выявления потенциальных фальсификаций электоральных данных в случаях, когда количество чисел, заканчивающихся цифрами «0» и «5» не менее, чем на 8% превышает аналогичную величину в случае их отсутствия.

Получены оценки равномерности плотности распределения второй после запятой цифры в электоральном показателе «отношения числа проголосовавших избирателей на данном избирательном участке к общему числу зарегистрированных избирателей», свидетельствующие об отсутствии фальсификаций электоральных данных на этих выборах.

Литература

1. Российская политическая криминология: Словарь/Под общей ред. П.А. Кабанова. –Нижнекамск, 2003. С. 158.

2. Антонов О.Ю. Теория и практика выявления и расследования электоральных преступлений. Дисс….докт. юр. наук. М., 2008. 500 с.

3. Груздева А. П. Электоральная преступность: понятие и некоторые формы ее проявления в современной России// Вопросы национальной безопасности в исследованиях правоведов: Сборник научных трудов / Под ред. Г. Н. Горшенкова. –Сыктывкар, 2000. С. 95–102.

4. Кабанов П. А., Райков Г. И., Свигузова А. П., Чирков Д. К. Электоральная преступность в условиях формирования в России демократического правового государства (политико-криминологический анализ явления, его причин и эффективности мер противодействия): Монография/ Под науч. ред. д-ра юрид. наук П. А. Кабанова. –М.: Издательская группа «Граница», 2012. 92 с.

5. Кабанов П.А. Политическая криминология: основные этапы и некоторые перспективные направления её развития России // Вопросы национальной безопасности в исследованиях правоведов: Сборник научных трудов / Под ред. Г. Н. Горшенкова. –Сыктывкар, 2000. С. 93.

6. Mebane: A Layman's Guide to Statistical Election Forensics [Электронный ресурс]// URL: https://www.electionguide.org/digest/post/271/ (Дата обращения 19.02.2022).

7. Шалаев Н.Е. Электоральные аномалии в постсоциалистическом пространстве: опыт статистического анализа. Дисс…канд. политических наук. –Санкт-Петербург, 2016. –191 с.

8. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации».

9. URL: http://electoralpolitics.org/ru/ (дата обращения 19.02.2022).

10. URL:http://electoralpolitics.org/ru/articles/vozmozhnosti-matematicheskikh-metodov-povyiavleniiu-elektoralnykh-falsifikatsii/ (дата обращения 19.02.2022).

11. Подлазов А.В. Реконструкция фальсифицированных результатов выборов с помощью интегрального метода Шпилькина // Проектирование будущего. Проблемы цифровой реальности: труды 4-й Международной конференции (4–5 февраля 2021 г., Москва). –М.: ИПМ им. М.В. Келдыша, 2021. С. 193–208// URL: https://keldysh.ru/future/2021/18.pdf (дата обращения 19.02.2022).

12. Подлазов А.В. Формальные методы выявления масштабных электоральных фальсификаций на материале федеральных выборов1999-2018 гг. / Препринты ИПМ им. М.В. Келдыша. 2019. № 2. 28 с. doi:10.20948/prepr-2019-2 URL: http://library.keldysh.ru/preprint.asp?id=2019-2 (дата обращения 19.02.2022).

13. Шпилькин С. Поправки на 27 миллионов// URL: https://trv-science.ru/2020/07/popravki-na-27-millionov/ (дата обращения 19.02.2022).

14. Подлазов А.В. Исследование статистических методов выявления выдуманных результатов выборов: Часть 1. Круглые числа // Препринты ИПМ им. М.В.Келдыша. 2019. № 147. 28 с. http://doi.org/10.20948/prepr-2019-147 URL: http://library.keldysh.ru/preprint.asp?id=2019-147 (дата обращения19.02.2022).

15. Доклад Российского общественного института избирательного права (РОИИП) «Математические инструменты делигитимации выборов»//И.Б. Борисов, И.В Задорин, А.В. Игнатов, В.Н. Марачевский, В.И. Федоров/ –М.: РОИИП, 2020. 76 с. URL: http://www.roiip.ru/images/data/gallery/0_299_Matematicheskie_instrumenti_delegitimatsii_viborov.pdf (дата обращения 19.02.2022).

16. URL: https://www.electoral.graphics/ru-ru/ (дата обращения 20.02.2022).

17. Шень А. Как доклад РОИИП делегитимирует выборы URL: https://trv-science.ru/2020/09/kak-doklad-roiip-delegitimiruet-vybory/ (дата обращения 19.02.2022).

18. URL: http://www.vybory.izbirkom.ru/region/izbirkom?action=show&root=0&tvd=100100084849066&vrn=100100084849062&prver=0&pronetvd=null&region=0&sub_region=0&type=0&report_mode=null (дата обращения 19.02.2022).

Мирвода С.Г., Поршнев С.В., Рябко Н.Ю. Автоматизация процедуры доступа к электоральным данным, размещенным на сайте Центральной избирательной комиссии/ Вестник УрФО. Безопасность информационного пространства, 2022. Вып. 1 (43)/2022. 28-34 с. DOI: 10.14529/secur220104

19. Баскакова Ю.М. Экзит-полл и его задачи // Мониторинг общественного мнения: экономические и социальные перемены. 2011. № 4. С. 37–41.

20. Ротманд Д.Г., Правдивец В.В., Белов А.А. Электоральные социологические исследования: организация опросов в день выборов (экзит-полл)// Социология, 2015. № 3. С. 122–132.

21. Beber, B., Scacco, A., (2012) What the Number Say: A Digit-Based Test for Election Fraud, Political Analysis, , vol. 20, P. 211–234.

22. Benford, F. (1938) The Law of Anomalous Numbers. Proceedings of the American Philosophical Society, vol. 78, P. 551–572.

References

1. Rossiyskaya politicheskaya kriminologiya: Slovar'/Pod obshchey red. P.A. Kabanova. –Nizhnekamsk, 2003. S. 158.

2. Antonov O.YU. Teoriya i praktika vyyavleniya i rassledovaniya elektoral'nykh prestupleniy. Diss…. dokt. yur. nauk. M., 2008. 500 s.

3. Gruzdeva A. P. Elektoral'naya prestupnost': ponyatiye i nekotoryye formy yeye proyavleniya v sovremennoy Rossii// Voprosy natsional'noy bezopasnosti v issledovaniyakh pravovedov: Sbornik nauchnykh trudov / Pod red. G. N. Gorshenkova. –Syktyvkar, 2000. S. 95–102.

4. Kabanov P. A., Raykov G. I., Sviguzova A. P., Chirkov D. K. Elektoral'naya prestupnost' v usloviyakh formirovaniya v Rossii demokraticheskogo pravovogo gosudarstva (politiko-kriminologicheskiy analiz yavleniya, yego prichin i effektivnosti mer protivodeystviya): Monografiya/ Pod nauch. red. d-ra yurid. nauk P. A. Kabanova. –M.: Izdatel'skaya gruppa «Granitsa», 2012. 92 s.

5. Kabanov P.A. Politicheskaya kriminologiya: osnovnyye etapy i nekotoryye perspektivnyye napravleniya yeyo razvitiya Rossii // Voprosy natsional'noy bezopasnosti v issledovaniyakh pravovedov: Sbornik nauchnykh trudov / Pod red. G. N. Gorshenkova. –Syktyvkar, 2000. S. 93.

6. Mebane: A Layman's Guide to Statistical Election Forensics [Elektronnyy resurs]// URL: https://www.electionguide.org/digest/post/271/ (Data obrashcheniya 19.02.2022).

7. Shalayev N.Ye. Elektoral'nyye anomalii v postsotsialisticheskom prostranstve: opyt statisticheskogo analiza. Diss…kand. politicheskikh nauk. –Sankt-Peterburg, 2016. –191 s.

8. Federal'nyy zakon ot 27.07.2006 № 149-FZ (red. ot 02.07.2021) «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii».

9. URL: http://electoralpolitics.org/ru/ (data obrashcheniya 19.02.2022).

10. URL: http://electoralpolitics.org/ru/articles/vozmozhnosti-matematicheskikh-metodov-po-vyiavleniiu-elektoralnykh-falsifikatsii/ (data obrashcheniya 19.02.2022).

11. Podlazov A.V. Rekonstruktsiya fal'sifitsirovannykh rezul'tatov vyborov s pomoshch'yu integral'nogo metoda Shpil'kina // Proyektirovaniye budushchego. Problemy tsifrovoy real'nosti: trudy 4-y Mezhdunarodnoy konferentsii (4–5 fevralya 2021 g., Moskva). –M.: IPM im. M.V. Keldysha, 2021. S. 193–208 // URL: https://keldysh.ru/future/2021/18.pdf (data obrashcheniya 19.02.2022).

12. Podlazov A.V. Formal'nyye metody vyyavleniya masshtabnykh elektoral'nykh fal'sifikatsiy na materiale federal'nykh vyborov1999-2018 gg. / Preprinty IPM im. M.V. Keldysha. 2019. № 2. 28 s. doi:10.20948/prepr-2019-2 URL: http://library.keldysh.ru/preprint.asp?id=2019-2 (data obrashcheniya 19.02.2022).

13. Shpil'kin S. Popravki na 27 millionov// URL: https://trv-science.ru/2020/07/popravki-na-27-millionov/ (data obrashcheniya 19.02.2022).

14. Podlazov A.V. Issledovaniye statisticheskikh metodov vyyavleniya vydumannykh rezul'tatov vyborov: Chast' 1. Kruglyye chisla // Preprinty IPM im. M.V.Keldysha. 2019. № 147. 28 s. http://doi.org/10.20948/prepr-2019-147 URL: http://library.keldysh.ru/preprint.asp?id=2019-147 (data obrashcheniya19.02.2022)

15. Doklad Rossiyskogo obshchestvennogo instituta izbiratel'nogo prava (ROIIP) «Matematicheskiye instrumenty deligitimatsii vyborov»//I.B. Borisov, I.V Zadorin, A.V. Ignatov, V.N. Marachevskiy, V.I. Fedorov/ –M.: ROIIP, 2020. 76 s. URL: http://www.roiip.ru/images/data/gallery/0_299_Matematicheskie_instrumenti_delegitimatsii_viborov.pdf (data obrashcheniya 19.02.2022).

16. URL: https://www.electoral.graphics/ru-ru/ (data obrashcheniya 20.02.2022) 17. Shen' A. Kak doklad ROIIP delegitimiruyet vybory URL: https://trv-science.ru/2020/09/kak-doklad-roiip-delegitimiruet-vybory/ (data obrashcheniya 19.02.2022).

18. URL: http://www.vybory.izbirkom.ru/region/izbirkom?action=show&root=0&tvd=100100084849066&vrn=100100084849062&prver=0&pronetvd=null&region=0&sub_region=0&type=0&report_mode=null (data obrashcheniya 19.02.2022).

19. Mirvoda S.G., Porshnev S.V., Ryabko N.YU. Avtomatizatsiya protsedury dostupa k elektoral'nym dannym, razmeshchennym na sayte Tsentral'noy izbiratel'noy komissii/ Vestnik UrFO. Bezopasnost' informatsionnogo prostranstva, 2022. Vyp. 1 (43)/2022. 28-34 s. DOI: 10.14529/secur220104

20. Baskakova YU.M. Ekzit-poll i yego zadachi // Monitoring obshchestvennogo mneniya: ekonomicheskiye i sotsial'nyye peremeny. 2011. № 4. S. 37–41.

21. Rotmand D.G., Pravdivets V.V., Belov A.A. Elektoral'nyye sotsiologicheskiye issledovaniya: organizatsiya oprosov v den' vyborov (ekzit-poll)// Sotsiologiya, 2015. № 3. S. 122–132.

22. Beber, B., Scacco, A., (2012) What the Number Say: A Digit-Based Test for Election Fraud, Political Analysis, , vol. 20, pp. 211–234.

23. Benford, F. (1938) The Law of Anomalous Numbers. Proceedings of the American Philosophical Society, vol. 78, pp. 551–572.

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина», 620002, г. Екатеринбург, ул. Мира, 32, E-mail: s.v.porshnev@urfu.ru

РЯБКО Николай Юрьевич, аспирант федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина», 620002, г. Екатеринбург, ул. Мира, 32, E-mail: N.Yu.Ryabko@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin», 620002, Yekaterinburg, st. Mira, 32, E-mail: s.v.porshnev@urfu.ru

RYABKO Nikolay Yurievich, post-graduate student of the Federal State Autonomous Educational Institution of Higher Education "Ural Federal University named after the first President of Russia B.N. Yeltsin ", 620002, Yekaterinburg, st. Mira, 32, E-mail: N.Yu.Ryabko@urfu.ru

УДК 004.056 Вестник УрФО № 2(44) / 2022, с. 25–29

Маслова М.А.

DOI: 10.14529/secur220203

АНАЛИЗ, ПРИМЕНЕНИЕ И МОДИФИКАЦИЯ МЕТОДА ДЕЛЬФИ

При анализе и оценке рисков значимое место занимает выбор эффективности решений, который можно представить методом Дельфи. В работе будет проанализирован метод Дельфи и его модификации, выявлены слабые стороны. Будет приведено описание и рассмотрено применение метода Дельфи при оценке рисков информационной безопасности предприятий для разработанной программной реализации учитывающей не сходящиеся выходные данные основных методик оценки рисков информационной безопасности и адаптированной для современного дистанционного формата работы.

Ключевые слова: *риски информационной безопасности, метод Дельфи, Дельфийская процедура сходимость, входные данные, выходные данные.*

Maslova M.A.

ANALYSIS, APPLICATION AND MODIFICATION OF THE DELPHI METHOD

In the analysis and assessment of risks, a significant place is occupied by the choice of the effectiveness of solutions, which can be represented by the Delphi method. In the work, the Delphi method and its modifications will be analyzed, weaknesses identified. A description will be given and the application of the Delphi method in assessing the risks of information security of enterprises will be considered for the developed software implementation that takes into account the non–convergent output data of the main methods for assessing information security risks and adapted to the modern remote format of work.

Keywords: *information security risks, Delphi method, Delphi procedure convergence, input data, output data.*

Дельфийская процедура часто используется для различных профессиональных сфер жизнедеятельности человека, так как он достаточно лоялен, гибок и учитывает мнения всех людей, принимающих в данном вопросе решения.

Метод Дельфи или как часто его называют – дельфийский метод был разработан в исследовательском центре «RAND» после пятидесятых годов и назван был в честь Дельфийского Оракула. Метод давал возможность прогнозировать научные разработки будущего в военных целях. Разработан метод был О. Хэлмером, Н. Дэлки, Н. Ришером. и его основной идеей есть то, что групповые методы являются более точными и обоснованными, чем одиночные. Он предполагал, что каждый человек выскажет свое мнение о вероятно-

сти, частоте и интенсивности возможных атак противника и это улучшит ход войны и его результаты. В свою очередь другие эксперты должны были дать на предположения свои рассуждения до тех пор, пока они не приходили к консенсусу. Плюсами данного метода было то, что этот метод позволял всем задействованным в данный процесс лицам сосредотачиваться и рассматривать все вопросы, но обязательно компетентными в данном вопросе; так же все участники могли оставаться анонимными и это не могло повлиять на их решение за счет компетентности других экспертов, принимающих решение в данный момент, что очень важно, так как это дает возможность получить больше предложений, решений, рассуждений, не смотря на их новизну и неординарность [2, 3]. Минусами же есть то, что данный метод очень долгий и трудоемкий. В предлагаемом же методе существует возможность убрать рутинную ручную работу, автоматизировав ее, что кардинально уменьшит временные рамки. Так же он дает возможность выполнять данный процесс дистанционно в удобное для экспертов время без ограничения на принятие решения и привязанности к другим участникам экспертизы.

Данный метод будет применяться в разработанном программном модуле для оценки и ранжирования входных и выходных параметров рисков информационной безопасности (ИБ), который содержит проанализированную и структурированную базу данных сходящихся и расходящихся входных и выходных дата сетов по основным существующим методикам оценки рисков ИБ.

В данной статье будет рассмотрен метод Дельфи и его модификация, выделены положительные и отрицательные стороны и предложен дополненный, улучшенный метод Дельфи включающий объединение входных и выходных дата сетов общеизвестных методов оценки рисков ИБ с учетом данных временных изменений в жизни людей.

Метод Дельфи состоит из трех этапов: предварительного, основного и аналитического. Каждый из этапов экспертизы является важным, так как вовремя:

Предварительного этапа, где необходимо подобрать компетентных экспертов в рассматриваемой области, которых должно быть как можно больше, но желательно не меньше десяти.

Основного этапа, где необходима постановка проблемы и разделение ее на много мелких частей для удобства и возможности полной проработки каждой мелкой проблематики. Проводится анализ и выделение всех имеющихся активов предприятия и возможных рисков, которые тем или иным методом влияют на них, для дальнейшей их проработки. Составляется опросник для дальнейшей работы с ним экспертов. После работы экспертов и получения выходных данных по проблематике, информация прорабатывается, анализируется на сходимости и если она получается высокой, то принимается, если же нет, то составляется новый опросник и возвращается экспертам для работы заново. В новом опросном листе они должны обратить внимание на ответы других экспертов, мнения большинства которых сходится, и заново изложить свои способы решения проблемы.

При этом проведение экспертизы так же является независимой и без каких–либо навязывания мнений, т.е. им необходимо произвести оценку эффективности, наличия ресурсов учтя актуальность способов решения. Главная задача аналитиков заключается в том, чтобы выделить основные, более сходящиеся мнения экспертов. Те же мнения экспертов, которые имеют большую не сходимость, постараться как можно ближе их подобрать и сблизить. Если же все–таки мнения некоторых экспертов сильно расходятся, то тогда экспертов ознакамливают с более сходящимися данными и предлагают пересмотреть свои позиции к определенным, не сходящимся данным за счет новой экспертизы. Данный процесс повторяется до тех пор, пока мнения не будут иметь хорошую сходимость. Но данные действия не являются принудительными, а с помощью полученных данных, аналитики могут указать некоторым экспертам с сильно расходящимися данными на, например, незамеченные до этого нюансы какой–то проблемы. Когда экспертиза проведена и данные имеют хорошую сходимость, начинают формировать общую оценку и перечень актуальных рекомендаций для решения проблемы, которая была заявлена в экспертизе.

Аналитического этапа, где необходимо тщательно поработать все полученные данные, сгенерировать их, обработать и вынести грамотное решение для принятия, уменьшения или устранения рисков [4].

Существуют так же модифицированные методы Дельфийской процедуры.

С минимизацией временного ресурса называемый «Экспресс–Дельфи». Данный метод проводят в основном по тем же правилам, сохраняя все основные элементы методики, только проводится он быстро, за пару часов, но должна присутствовать специальная техническая база – интернет и компьютеры. Т.е. все участники со своего рабочего места в определенное время выходят в сеть, где эксперты предлагают свои мысли в решении проблемы, далее аналитики так же быстро проводят оценку и выносится конкретное решение. Но организация процесса должна быть заранее хорошо скоординирована и весь материал заранее обработан и систематизирован.

С помощью бесструктурного этапа, т.е. если решение проблемы четкая и направлена на что–либо конкретное и невозможно проблему форматировать в четко структурированные вопросы. Тогда первый и второй этап проходят одновременно, т.к. в постановке и разработке алгоритма приминают участие не только организаторы, но и эксперты.

Каждый метод имеет свои существенные недостатки. Например, недостаток метода «Экспресс–Дельфи» в том, что при ограниченном времени эксперты не могут подумать и взвесить все решения, а также оценить доводы других участников; так же необходимо чтобы у всех было оборудование и интернет в одно и то же время. Недостаток же бесструктурного метода в том, что несколько этапов объединяются в одно и есть вероятность того, что опуститься какой–либо важный элемент, а также то, что эксперты участвуют в обоих стадиях и это может повлиять на их мнение. Основной же метод Дельфи имеет недостатки в том, что организаторы имеют большие полномочия и могут манипулировать экспертной группой, аналитики часто отбрасывают креативные решения, занимает большое количество времени, эксперты могут принимать точку зрения других экспертов [4, 5].

Для работы был выбран метод Дельфи, но уже с устранением недостатков и актуальными на сегодня дистанционными форматами обработки данных, который будет применяться в созданной программе для оценки рисков информационной безопасности.

Идея заключается в том, что разрабатываемый программный модуль для расчета рисков информационной безопасности будет иметь базу клиентов и экспертов, которыми будет управлять один человек – модератор. Он отправляет приглашения клиентам и экспертам для работы, вносит их в базу данных для последующей работы. Они в свою очередь регистрируются на сервере с получением личного кабинета, где будет отображаться вся необходимая информация. При регистрации клиенты указывают личные данные, название фирмы, направление своей деятельности, краткое описание деятельности фирмы для того, чтоб модератор мог грамотно подобрать экспертов для дальнейшей экспертизы рисков. Далее им нужно заполнить окно с дополнительной информацией об активах предприятия и входных данных, так же можно в примечании указать пожелания.

Эксперты в свою очередь указывают при регистрации информацию о себе и деятельности для дальнейшего распределения по экспертизам в зависимости от компетентности эксперта.

Модератором формируется запрос фирмы, подбираются эксперты и далее ими проводится экспертиза путем определения критериев из сформированной уже базы данных раннее – сходящихся и не сходящихся параметров входных DataSet проанализированных и выбранных по основным существующим методикам определения рисков ИБ: ISO/IEC 27001, ГРИФ, OCTAVE, CORAS, CRAMM, FRAP, Risk IT, RiskWatch, MSAT, MOF, СТО БР ИББС, далее входные данные сопоставляются с выходной базой дата сетов данных, проанализированных методик. [1, 6, 7, 8].

После определения параметров важности выходных данных каждым экспертом применяется метод Дельфи. Для определенного предприятия, модератор выполняет обработку полученных данных с помощью формул 1–3:

$$\overline{X}_J = \frac{\sum_{i=1}^{m} X_{ij} K_i}{\sum_{i=1}^{m} K_i} \quad (1)$$

где: *Xij* – оценка относительной важности (в баллах), выставленная i–м экспертом j–му элементу;

Ki – коэффициент компетентности i –го эксперта, учитывающий степень знакомства с обсуждаемым вопросом – К3, а также коэффициент аргументированности ответа – Ка:

$$K_i = \frac{K_3 + K_a}{2} \quad (2)$$

где: i=1…m – номера экспертов; m – число экспертов; j=1…n – номера изучаемых элементов; n – число элементов древа целей.

Так же по формуле 3 потребуется опреде-

лить показатель степени надежности эксперта:

$$R = \frac{n}{N} \quad (3)$$

где: R – показатель степени надежности эксперта; N – общее количество оценок, обрабатываемых i–ым экспертом; n – количество правильных оценок.

Ответы имеют диапазон от 1 до 100 баллов и значение будет тем важнее, чем выше показатель $\overline{X_j}$. Далее используется дисперсия экспертных оценок, от которой будет зависеть результат – надежность, чем меньше значение она имеет, тем более точные будут ответы и надежнее результат. При большом расхождении мнений, экспертов знакомят с точками зрения других участников экспертизы и их обоснованием, оценку экспертизы проводят заново до получения средней оценки результатов сходимости, так чтоб она являлась надежной.

Далее проводится статистическая обработка полученной информации модератором, рассчитывается: среднее значение исследуемого параметра, средневзвешенное значение, медиана и область доверительности. В итоге получаем более точную групповую оценку [5].

Данные показатели будут влиять на принятое решение по рискам: принять, контролировать или устранить и выдаваться конкретное управленческое решение к действию.

Преимущество использования и применение метода Дельфи в комбинаторике в данной программной реализации в том, что устранены основные недостатки метода, расширена база данных, улучшена работа при проведении экспертных оценок, а именно:

– программная реализация имеет редактируемую базу данных модератором;

– большой диапазон базы данных входных и выходных параметров;

– экспертиза проводится дистанционно;

– эксперт имеет конкретно установленный диапазон времени по дням на проведение экспертизы;

– время экспертизы не ограниченно, что влияет на более обдуманное и взвешенное решение;

– нет необходимости выходить в чат в определенное время – эксперт может работать удаленно с любой точки страны и даже мира, в удобное для него время;

– нет взаимодействия между собой экспертов, что повлияет на индивидуальность принятых решений и, следовательно, более точность их;

– зависимости от интернета одновременно всех участников.

Выводы

Метод Дельфи применим практически в любой ситуации, требующей прогнозирования, в том числе если для принятия решения недостаточно информации и имеет множество преимуществ по сравнению с обычными методами, основанными на статистической обработке результатов индивидуальных опросников.

В данной работе было показано, как можно соединить существующие модифицированные методы Дельфийской процедуры для устранения всех негативных факторов, превратив их в плюсы. На основе существующих методов, их анализа, выделения сходящихся и не сходящихся входных и выходных данных, объединенных в базу появилась возможность более детального и качественного анализа, получения рекомендаций и точного принятия решения. В нынешней ситуации с постоянными дистанционными форматами и локдаунами – данный метод является очень продуктивным, актуальным и удобным, так как полностью независим от внешних факторов и имеет множество преимуществ использования при оценке рисков информационной безопасности.

Литература

1. Кузнецов А.А., Маслова М.А. Управление рисками информационной безопасности на примере современных методик: Городская научно–практическая конференция с международным участием «Молодежная инициатива – 2019», Сборник материалов конференции г. Ростов–на–Дону 6.12.2019 г. – С.189–190.

2. Черноусова М.В. Метод экспертных оценок. Метод Дельфи. Международная научно–техническая конференция молодых ученых БГТУ им. В.Г. Шухова. Белгород, 01–20 мая 2017 г. – С. 65–75.

3. Никитеева Ю.А., Святкина Л.И. Метод «Дельфи»/ Метод мозгового штурма. В сборнике: Оценка качества и безопасность потребительских товаров. Материалы XI региональной научно–практической конференции молодых ученых. Печатается по решению Совета НИР МИЭЛ ИГУ 2017. – С. 83– 88.

4. Стончюте К.Э., Гурбо А.А., Пузыревская А.А. Методы экспертных оценок: Метод Дельфи. Научное знание современности. – 2021. – № 5 (53). – С. 16– 19.

5. Метод Дельфи. [Электронный ресурс] база данных:– Режим доступа: https://max–k–studio.com/delphi–method/.

6. Средство оценки безопасности Microsoft Security Assessment Tool (MSAT): понимание рисков, процесс MSAT, загрузка и установка | Microsoft Docs [Электронный ресурс] : база данных. – Режим доступа: https://www.microsoft.com/ru–ru/download/details.aspx?id=12273.

7. Обзор методик и анализ рисков информационной безопасности, информационных систем предприятия [Электронный ресурс]: база данных. – Режим доступа: https://cyberleninka.ru/article/v/obzor–metodik–analiza–riskov–informatsionnoy–bezopasnosti–informatsionnoy–sistemy–predpriyatiya.

8. Microsoft Security Assessment Tool 4.0 [Электронный ресурс]: база данных. – Режим доступа: anti–malware.ru

9. Али–Заде. Дельфийский метод в контексте методологического самоопределения общественных наук. [Электронный ресурс]: база данных. – Режим доступа: https://cyberleninka.ru/article/n/delfiyskiy–orakul–na–sluzhbe–nauke.

References

1. Kuznetsov A.A., Maslova M.A. Upravleniye riskami informatsionnoy bezopasnosti na primere sovremennykh metodik: Gorodskaya nauchno–prakticheskaya konferentsiya s mezhdunarodnym uchastiyem «Molodezhnaya initsiativa – 2019», Sbornik materialov konferentsii g. Rostov–na–Donu 6.12.2019 g. – S. 189–190.

2. Chernousova M.V. Metod ekspertnykh otsenok. Metod Del'fi. Mezhdunarodnaya nauchno–tekhnicheskaya konferentsiya molodykh uchenykh BGTU im. V.G. Shukhova. Belgorod, 01–20 maya 2017 g. – S. 65–75.

3. Nikiteyeva YU.A., Svyatkina L.I. Metod "Del'fi"/ Metod mozgovogo shturma. V sbornike: Otsenka kachestva i bezopasnost' potrebitel'skikh tovarov. Materialy XI regional'noy nauchno–prakticheskoy konferentsii molodykh uchenykh. Pechatayetsya po resheniyu Soveta NIR MIEL IGU 2017. – S. 83– 88.

4. Stonchyute K.E., Gurbo A.A., Puzyrevskaya A.A. Metody ekspertnykh otsenok: Metod Del'fi. Nauchnoye znaniye sovremennosti. – 2021. – № 5 (53). – S. 16– 19.

5. Metod Del'fi. [Elektronnyy resurs] baza dannykh: – Rezhim dostupa: https://max–k–studio.com/delphi–method/.

6. Sredstvo otsenki bezopasnosti Microsoft Security Assessment Tool (MSAT): ponimaniye riskov, protsess MSAT, zagruzka i ustanovka | Microsoft Docs [Elektronnyy resurs]: baza dannykh. – Rezhim dostupa: https://www.microsoft.com/ru–ru/download/details.aspx?id=12273.

7. Obzor metodik i analiz riskov informatsionnoy bezopasnosti, informatsionnykh sistem predpriyatiya [Elektronnyy resurs]: baza dannykh. – Rezhim dostupa: https://cyberleninka.ru/article/v/obzor–metodik–analiza–riskov–informatsionnoy–bezopasnosti–informatsionnoy–sistemy–predpriyatiya.

8. Microsoft Security Assessment Tool 4.0 [Elektronnyy resurs]: baza dannykh. – Rezhim dostupa: anti–malware.ru

9. Ali–Zade. Del'fiyskiy metod v kontekste metodologicheskogo samoopredeleniya obshchestvennykh nauk. [Elektronnyy resurs]: baza dannykh. – Rezhim dostupa: https://cyberleninka.ru/article/n/delfiyskiy–orakul–na–sluzhbe–nauke.

МАСЛОВА Мария Александровна, аспирант, старший преподаватель кафедры «Информационная безопасность» Федеральное государственное автономное образовательное учреждение высшего образования Севастопольский государственный университет. Университетская улица, дом 33, город Севастополь, 299053, РФ. E–mail: sevsu.ru, mashechka–81@mail.ru

MASLOVA Maria Alexandrovna, postgraduate student, Senior lecturer of the Department "Information Security" Federal State Autonomous Educational Institution of Higher Education Sevastopol State University. 33 Universitetskaya Street, Sevastopol, 299053, RF. E-mail: sevsu.ru, mashechka-81@mail.ru

УДК 004.056 Вестник УрФО № 2(44) / 2022, с. 30–36

Герасимова К.С., Михайлова У.В., Баранкова И.И. DOI: 10.14529/secur220204

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОПТИМИЗАЦИИ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье рассмотрен подход к оптимизации процесса категорирования объектов критической информационной инфраструктуры (далее – КИИ). Оптимизация процесса реализована за счет разработки программного обеспечения для категорирования объектов КИИ, которое позволит существенно снизить временные затраты на осуществление процесса категорирования. Категорирование выполняется на основании Постановления Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». В статье рассматривается функционал и принцип работы разработанного приложения.

Разработанное программное обеспечение позволяет выполнять оценку категории значимости объекта КИИ на основании исходных данных в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ. В приложении реализована возможность присвоения объекту КИИ одной из категорий значимости или принятие решения об отсутствии необходимости присвоения ему одной из категорий значимости. Результаты категорирования в разработанном приложении оформляются актом, который содержит исходные сведения об объекте КИИ, сведения о присвоенной объекту КИИ категории значимости и необходимый состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости.

Ключевые слова: *информационная безопасность, критическая информационная инфраструктура, объекты критической информационной инфраструктуры, категорирование объектов, разработка программного обеспечения.*

DEVELOPMENT OF SOFTWARE TO OPTIMIZE THE CATEGORIZATION OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

The purpose of this research work is to optimize the process of categorizing objects of critical information infrastructure (hereinafter referred to as CII). To achieve this goal, it was decided to develop software for categorizing CII objects. Categorization is carried out on the basis of Decree of the Government of the Russian Federation of February 8, 2018 No. 127 «On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values». The article discusses the principle of operation of the developed application.

The developed software makes it possible to evaluate the category of significance of the CII object based on the initial data in accordance with the list of indicators of criteria for the significance of the scale of possible consequences in the event of computer incidents at the CII objects. It is possible to assign a CII object to one of the categories of significance, or a decision is made that there is no need to assign one of the categories of significance to it. The categorization results are documented in an act that contains the initial information about the CII object, information about the significance category assigned to the CII object and the necessary set of security measures for a significant object of the corresponding significance category.

Keywords: *information security, critical information infrastructure, critical information infrastructure objects, categorization of objects, software development.*

Категорирование объектов критической информационной инфраструктуры (далее – КИИ) является обязательным с 1 января 2018, когда вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1], регулирующий отношения в области обеспечения безопасности КИИ РФ. Так, субъекты КИИ должны определить категорию значимости для каждого из принадлежащих им объектов КИИ или принять решение об отсутствии необходимости присвоения объекту одной из категорий значимости и предоставить данные во ФСТЭК Россия.

Категорирование – ресурсоемкая работа, предполагающая инвентаризацию всех информационных систем, автоматизированных систем управления и сетей, используемых субъектом КИИ, а также определение категории значимости для каждого такого объекта на основании утвержденных Постановлением Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [2] правил категорирования. У одного субъекта КИИ могут быть сотни таких систем, поэтому категорирование – очень сложный и длительный процесс.

Использование автоматизированной системы значительно упрощает и ускоряет процедуру категорирования, что особенно важ-

но в случаях, когда под контролем субъекта КИИ находится множество объектов КИИ.

Для ускорения и облегчения процесса категорирования разработано программное обеспечение, позволяющее оптимизировать этот процесс. Результатом категорирования является отчет, оформленный согласно требованиям приказа ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» [3].

Среди существующих программных продуктов можно выделить платформу «R-Vision SGRC», разработанную компанией R-Vision, и программный комплекс «Security Vision КИИ», созданный компанией «Интеллектуальная безопасность».

R-Vision SGRC обеспечивает решение следующих задач:

• Ведение реестра активов организации;

• Проведение категоризации объектов КИИ (ведение перечней объектов КИИ и связанных критических процессов, автоматический расчет категории значимости на основе опроса экспертов, формирование пакета документов по результатам категорирования);

• Проведение оценки соответствия активов нормативным и законодательным требованиям;

• Проведение оценки рисков информационной безопасности;

• Ведение базы внутренней документации по информационной безопасности;

• Автоматизация функций по формированию отчетности.

Security Vision КИИ позволяет субъектам КИИ:

• собирать и структурировать всю информацию по объектам КИИ на единой платформе;

• категорировать объекты КИИ согласно законодательству;

• осуществлять непрерывный контроль соответствия защищенности объектов КИИ нормативным требованиям;

• автоматизировать формирование отчетности по форме регулятора.

Преимуществом разработанного приложения перед уже существующими является простота и удобство интерфейса. Так же категорирование можно выполнять либо в ручном режиме, где специалист будет определять значения показателей защищенности, либо в автоматическом, где приложение будет рассчитывать рекомендованные значения показателей защищенности на основе исходных данных. В приложении можно открыть Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» для ознакомления с правилами категорирования объектов КИИ.

Рассмотрим работу разработанной программы «Категорирование объектов КИИ».

При запуске программы открывается главная форма (рис.1).

Перед выполнением категорирования на форме необходимо в верхней половине заполнить все обязательные исходные данные: Наименование объекта, Адрес размещения объекта, Назначение объекта, Сфера деятельности, Архитектура объекта, Площадь и Тип объекта. Также следует заполнить сведения о программных, программно-аппаратных средствах, используемых на объекте КИИ (рис.2).

Следующим шагом необходимо добавить все критические процессы, связанные с объектом КИИ, которые необходимо прокатегорировать [4].

Для автоматического расчета рекомендованных значений показателей значимости необходимо указать будет дополнительные сведения. В случае, если специалист проводит расчет категорий значимости самостоятельно, то для удобства он может воспользоваться «Справочной информацией» и ознакомиться с полным содержанием Постановления Правительства №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изменениями от 24 декабря 2021 г.).

После всей выполненной работы формируются «Акт категорирования объекта критической информационной инфраструктуры», оформленный по требованиям Приказа ФСТЭК и необходимый состав мер по обеспе-

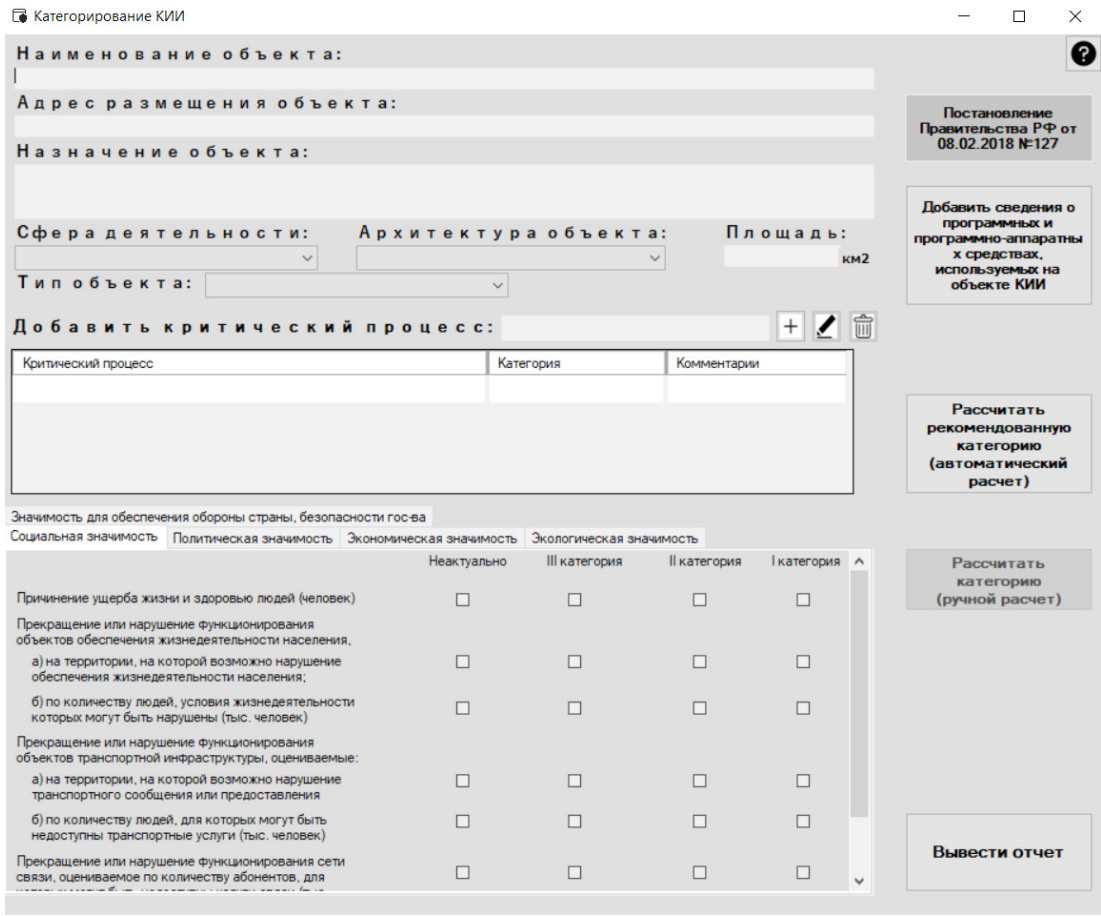


Рис. 1. Главная форма приложения

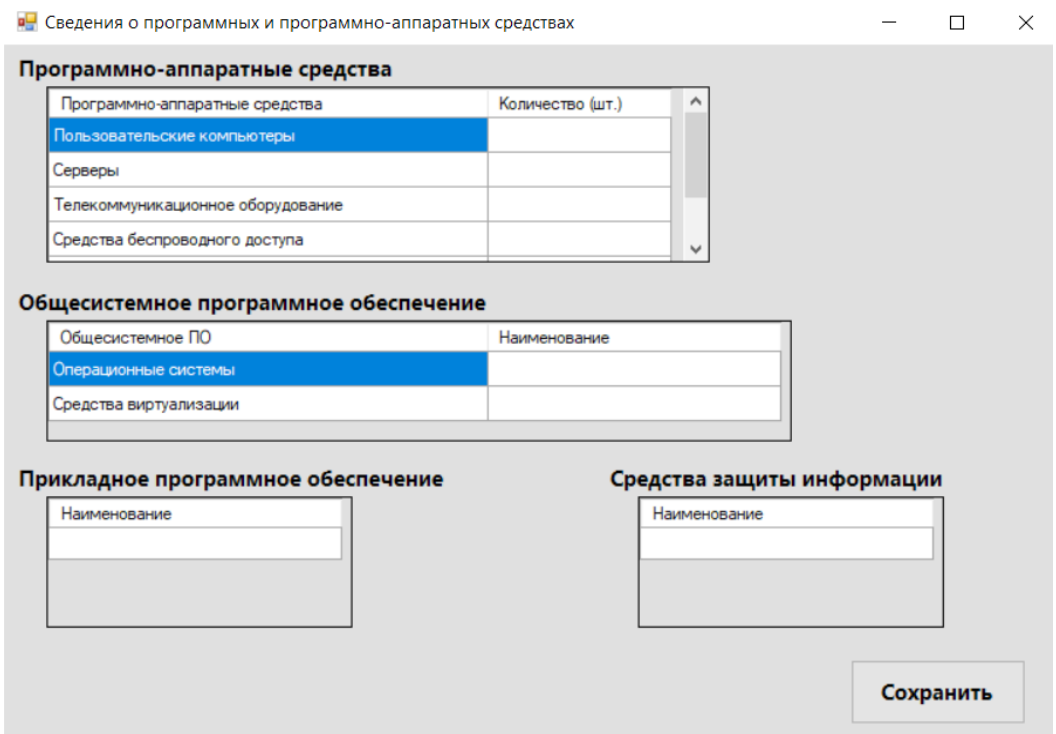


Рис. 2. Форма «Сведения о программных и программно-аппаратных средствах»

чению безопасности для значимого объекта соответствующей категории значимости, сформированный согласно Приказу ФСТЭК России №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [5] (рис.3).

Акт категорирования объекта критической информационной инфраструктуры

УТВЕРЖДАЮ

_____
(руководитель организации)

_____
(подпись, инициалы, фамилия)

«___»_____20___г.

А К Т
категорирования объекта критической информационной инфраструктуры
<NAME>
_____
(наименование объекта)

На основании приказа от «___»_____20___г. №_____комиссия в составе:

председатель комиссии: _____
(роль, должность, фамилия, инициалы)

члены комиссии: _____
(роль, должность, фамилия, инициалы)

_____
(роль, должность, фамилия, инициалы)

_____
(роль, должность, фамилия, инициалы)

в соответствии с требованиями Федерального закона от 26.07.2017 №187, постановления Правительства РФ от 08.02.2018г. №127 провела категорирование объекта критической информационной инфраструктуры <NAME>.
В ходе работы комиссия по категорированию определила:

1. Сведения об объекте критической информационной инфраструктуры (далее – КИИ), представленные в Приложении 1.
2. Сведения об угрозах безопасности информации объекта КИИ, представленные в Приложении 2.
3. Реализованные на объекте КИИ меры по обеспечению безопасности, представленные в Приложении 3.
4. Масштаб возможных последствий в случае возникновения компьютерных инцидентов в соответствии с перечнем показателей критериев значимости, представленный в Приложении 4.

На основании результата анализа значений показателей критериев значимости объекта КИИ в соответствии с постановлением Правительства РФ от 08.02.2018г. №127 объекту <NAME>
_____
(наименование объекта)
присвоена категория<CATEGORY>

Состав необходимых мер по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, утвержденными приказом ФСТЭК от 25.12.2017 № 239, представлен в Приложении 5.

Председатель комиссии: _____
(ФИО, подпись)

Члены комиссии: _____
(ФИО, подпись)

_____
(ФИО, подпись)

_____
(ФИО, подпись)

Приложение 1

Сведения об объекте КИИ:

Наименование объекта	<NAME>
Адреса размещения объекта	<ADDRESS>
Сфера (область) деятельности, в которой функционирует объект	<SCOPE>
Назначение объекта	<APPOINTMENT>
Критические процессы, которые обеспечиваются объектом	<PROCESSES>
Архитектура объекта	<ARCHITECTURE>

Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ:

Программно-аппаратные средства	Пользовательские компьютеры - шт. Серверы - шт. Телекоммуникационное оборудование - шт. Средства беспроводного доступа - шт. Производственное оборудование - шт. Иные программно-аппаратные средства - шт.
Общесистемное программное обеспечение	Наименования операционных систем: Средства виртуализации:
Прикладное программное обеспечение	
Средства защиты информации	

Сведения о взаимодействии объекта КИИ и сетей электросвязи.

Категория сети электросвязи	
Наименование оператора связи	
Цель взаимодействия с сетью электросвязи	
Способ взаимодействия с сетью электросвязи	

Рис. 3. Шаблон Акта категорирования объекта КИИ

Таким образом, было разработано программное обеспечение «Категорирование КИИ» для оптимизации и ускорения процесса категорирования объектов КИИ. Результатом работы и категорирования является отчет «Акт категорирования объекта критической информационной инфраструктуры», содержащий в себе все исходные данные об объекте (Наименование объекта, Адрес размещения объекта, Назначение объекта, Сфера деятельности, Архитектура объекта, Площадь и Тип объекта, Критические процессы, Сведения о программных средствах, программно-аппаратных и средствах защиты информации), перечень показателей критериев значимости и их значения, а так же состав мер по обеспечению безопасности для объекта соответствующей категории значимости.

Литература

1. Федеральный закон №187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Текст], Принят Государственной Думой 12 июля 2017 г., Одобрен Советом Федерации 19 июля 2017 г. – 2017. – 21 с.

2. Постановление Правительства РФ № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Текст], Принят 8 февраля 2018 г. – 2018. – 20 с.

3. Приказ ФСТЭК России №236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий», Принят 22 декабря 2017 г. – 2017. – 7 с.

4. Баранкова, И.И. О.В. Пермякова. Определение перечня защищаемых ресурсов и их критичности. Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова, 2016. – 14 с.

5. Приказ ФСТЭК России №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Текст], Утвержден ФСТЭК России 25 декабря 2017 г. – 2017. – 37 с.

References

1. Federal'nyy zakon №187 «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» [Tekst], Prinyat Gosudarstvennoy Dumoy 12 iyulya 2017 g., Odobren Sovetom Federatsii 19 iyulya 2017 g. – 2017. – 21 p.

2. Postanovlenie Pravitel'stva RF № 127 «Ob utverzhdenii Pravil kategorirovaniya ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe perechnya pokazateley kriteriev znachimosti ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy» [Tekst], Prinyat 8 fevralya 2018 g. – 2018. – 20 p.

3. Prikaz FSTEK Rossii №236 «Ob utverzhdenii formy napravleniya svedeniy o rezul'tatakh prisvoeniya ob"ektu kriticheskoy informatsionnoy infrastruktury odnoy iz kategoriy znachimosti libo ob otsutstvii neobkhodimosti prisvoeniya emu odnoy iz takikh kategoriy», Prinyat 22 dekabrya 2017 g. – 2017. – 7 p.

4. Barankova, I.I. O.V. Permyakova. Opredelenie perechnya zashchishchaemykh resursov i ikh kritichnosti. Magnitogorsk: Magnitogorskiy gosudarstvennyy tekhnicheskiy universitet im. G.I. Nosova, 2016. – 14 p.

5. Prikaz FSTEK Rossii №239 «Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» [Tekst], Utverzhden FSTEK Rossii 25 dekabrya 2017 g. – 2017. – 37 p.

ГЕРАСИМОВА Ксения Сергеевна, студент 5 курса, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: gierasimovak@mail.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: u.mihaylova@magtu.ru

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

GERASIMOVA Ksenia Sergeevna, student, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: gierasimovak@mail.ru

MIKHAILOVA Uliana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: u.mihaylova@magtu.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Informatics and Information Security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru

УДК 004.31:681.513.6+ 004.891.3 Вестник УрФО № 2(44) / 2022, с. 37–42

Егорова А.О., Тищенко Е.Н.

DOI: 10.14529/secur220205

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

В статье приводится математическая модель системы защиты информации от утечки по техническим каналам с адаптивным управлением. Модель представляет собой комбинацию моделей нескольких подсистем. Предложенная модель описывает принципы функционирования подсистем генерирования псевдослучайных последовательностей для задач системы, машинного обучения, защиты от утечки информации, оценки защищенности информации. Приведённая математическая модель в дальнейшем может быть использована для построения аппаратно-программного комплекса для защиты информации от утечки по техническим каналам.

Ключевые слова: *технические каналы утечки информации, математическая модель, машинное обучение, защита информации, маскирующий сигнал, речеподобный шумовой сигнал.*

Egorova A.O., Tishchenko E.N.

MATHEMATICAL MODEL OF ADAPTIVE SYSTEM OF INFORMATION SECURITY FROM LEAKAGE THROUGH TECHNICAL CHANNELS

The article presents a mathematical model of the information security system against leakage through technical channels with adaptive control. The model is a combination of models of several subsystems. The proposed model describes the principles of functioning of subsystems for generating pseudo-random sequences for system tasks, machine learning,

information leakage protection, and information security assessment. The above mathematical model can be used later to build a hardware-software complex for the security of information from leakage through technical channels.

Keywords: *technical channels of information leakage, mathematical model, machine learning, information security, masking signal, speech-like noise signal.*

Целью данной работы является разработка математической модели адаптивной системы защиты информации от утечки по техническим каналам. Разрабатываемая модель представляет собой основу для проектирования систем защиты информации от утечки по техническим каналам с адаптивным управлением.

Защита информации от утечки по техническим каналам с помощью средств активной технической защиты производится путем блокирования электромагнитных, электрических и акустических сигналов, препятствуя распространению информативного сигнала за пределы помещений, в которых циркулирует информация. Построение математической модели адаптивной системы защиты информации от утечки по техническим каналам начинается описания структуры. Компоненты модели:

1. Модель генератора случайных чисел – генерирует выделенную частоту из диапазона, определяемого исходя из выбранного канала утечки информации.

2. Модель блокирования канала утечки информации – определяет требования к задаваемой мощности шумового сигнала.

3. Модель машинного обучения – задаёт алгоритм и параметры обучения.

4. Модель системы оценки эффективности защиты информации – проводит анализ функционирования системы защиты информации на соответствие критериям защищенности.

Следует рассмотреть вышеуказанные модели более детально.

Для обучения разрабатываемой системы следует использовать множества X объектов и Y ответов. Тогда следует предположить, что существует функциональная зависимость:

$$F : X \to Y \qquad (1)$$

Зависимость между объектами и ответами неизвестны, но известна обучающая выборка:

$$S = \{(x_i, y_{xi} = F(x_i) \in X \times Y) | i=1, \ldots, l\} \qquad (2)$$

Задача обучения — найти аппроксимирующую функцию $a_S : X \to Y$ такой, что

$$\forall x \in X \quad a_S(x) \approx F(x) \qquad (3)$$

Для решения задачи построения функции $a_S : X \to Y$ по обучающей выборке S выбирается некоторая модель обучения. Структура модели представлена как взаимосвязь двух компонент:

1. Предсказательная модель:

$$a : X \times W \to Y \qquad (4)$$

где W – множество параметров.

Для нахождения искомой функции a_S используется следующая зависимость:

$$a_S(x) = a(x,w) \qquad (5)$$

Проектируемая модель должна решать задачи регрессии, поскольку она позволяет прогнозировать значения множества ответов Y. Для этого следует использовать линейную предсказательную модель. В линейной предсказательной модели множество W параметров имеет вид R^n, где n – число признаков объектов, т.е. каждый параметр w представляет собой вектор действительных чисел $w = (w_1, w_2, \ldots, w_n)$, и $Y = R$, и

$$a(x, w) = \langle x, w \rangle \stackrel{\text{def}}{=} \sum_{i=1}^{n} x^i w_i \qquad (6)$$

где $\langle x, w \rangle$ - скалярное произведение x и w.

2. Алгоритм обучения – алгоритм поиска такого значения w, для которого функция a_S, определяемая соотношением (5), обладает некоторыми свойствами оптимальности. Для точного описания свойств оптимальности алгоритмов обучения используется понятие функции потерь, которая сопоставляет паре (a_S, x), где $x \in X$, число $\mathcal{L}(a_S, x)$, выражающее величину ошибки аппроксимации a_S на объекте $x \in X$. Задач регрессии функция потерь имеет вид:

$$\mathcal{L}(a_S, x) = (a_S(x) - f(x))^2 \qquad (7)$$

Функционал эмпирического риска аппроксимации a_S, используемый в описаниях свойств оптимальности алгоритмов обучения вычисляется следующим образом:

$$Q(a_S) = \frac{1}{l} \sum_i^l \mathcal{L}(a_S, S) \qquad (8)$$

Таким образом, одно из свойств оптимальности алгоритма обучения по обучающей выборке S заключается в том, что значение параметра $w \in W$, определяющее наилучшую аппроксимацию a_S, должно удовлетворять соотношению

$$w = \arg\min_{w \in W} Q(a_S) \qquad (9)$$

Исходя из вышеизложенного, решение

задачи машинного обучения сводится к нахождению такого параметра $w \in W$, который минимизирует риск $Q(a_s)$.

Первой задачей при построении модели генератора случайных чисел стоит выбор типа генератора. Разновидности генераторов случайных чисел по способу получения чисел приведён на рисунке 1.

Рис.1. Классификация генераторов случайных чисел

Оптимальным выбором для разрабатываемой системы являются алгоритмические генераторы случайных чисел, поскольку они отличаются малой ресурсоемкостью и быстродействием. Однако, при оценке эффективности системы защиты информации следует учитывать тот факт, что алгоритмические генераторы позволяют получить только псевдослучайные числа [1].

Наиболее часто используемым алгоритмическим методом генерации псевдослучайных чисел является линейный конгруэнтный метод. Его базовое преимущество заключается в простоте реализации, что позволяет минимизировать затраты вычислительных ресурсов. Вычисление последовательности производится по формуле:

$$r_{i+1} = \mathrm{mod}(k \cdot r_i + b, M) \qquad (10)$$

В формуле (10) k – множитель, b – приращение, M – модуль, r_i – предшествующий элемент последовательности, где $k \in [0; M)$, $b \in [0; M)$ $r_i \in [0; M)$ и $M \in (0; +\infty)$. При этом b и M взаимно простые. Оптимальным выбором значения модуля является $M = 2^N - 1$ при использовании алгоритма в двоичных вычислительных системах [2].

Моделирование активной защиты информации от утечки по техническим каналам производится на основании схемы, приведённой на рисунке 2 [3, С. 168-175].

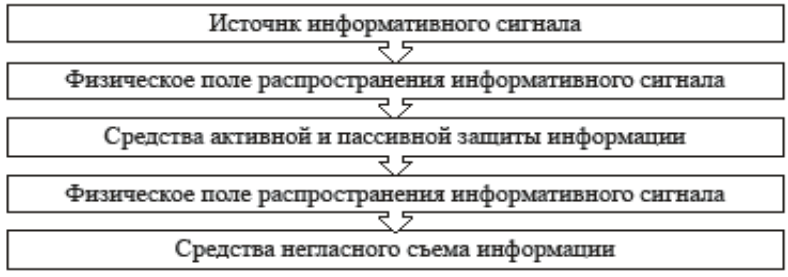


Рис. 2. Структура технического канала утечки информации

Технические каналы утечки информации по физической природе носителя делятся на:

– оптические;
– радиоэлектронные;
– акустические;
– материально-вещественные [4].

Из вышеприведённых каналов средства активной защиты применяются для акустических и радиоэлектронных каналов. Следовательно, алгоритм вычисления мощности должен учитывать модели указанных каналов.

Акустические каналы утечки информации представляют собой технические каналы, в которых полезный сигнал представляет собой акустический сигнал. Акустический сигнал представляет собой возмущения упругой среды, проявляющиеся в возникновении акустических колебаний различной формы и длительности, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины [5]. Классификация акустических каналов по физической природе приведена на рисунке 3.

Для блокирования приведённых выше каналов утечки информации используют средства активной акустической маскировки, которая снижает отношение сигнал/шум на входе технического средства разведки за счет увеличения уровня шума (помехи). Виброакустическая маскировка эффективно используется для защиты речевой информации от утечки по прямому акустическому, виброа-

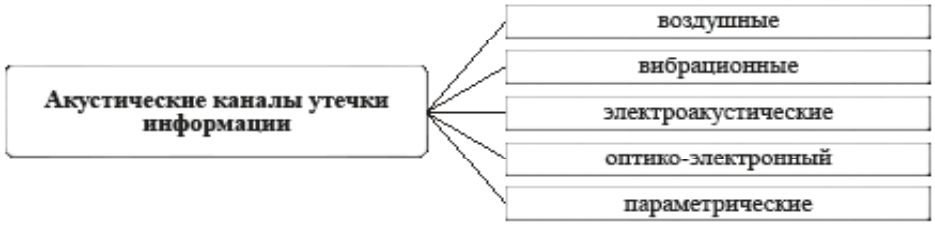


Рис. 3. Классификация акустических каналов утечки информации

кустическому и оптико-электронному каналам утечки информации. Для формирования акустических помех применяются специальные генераторы, к выходам которых подключены звуковые колонки (громкоговорители) или вибрационные излучатели (вибродатчики) Большую группу генераторов шума составляют устройства, принцип действия которых основан на усилении колебаний первичных источников шумов. В качестве источников шумовых колебаний используются электровакуумные, газоразрядные, полупроводниковые и другие электронные приборы, и элементы. Временной случайный процесс, близкий по своим свойствам к шумовым колебаниям, может быть получен и с помощью цифровых генераторов шума, формирующих последовательности двоичных символов, называемые псевдослучайными.

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС - линейное зашумление [6].

Механизм действия устройств зашумления в основе схожий для всех каналов утечки информации, где используются подобные средства. Сформированный генератором шумовой сигнал направляется на устройства вывода (динамики, антенны и т.д.). При достаточной мощности излучения и соответствия блокируемому полезному сигналу (частотные диапазоны разных каналов передачи информации различаются) за пределами контролируемой зоны на техническое средство разведки поступает шумовой сигнал, в котором становится невозможно выделить полезный сигнал.

Так, для защиты от утечки информации озвучиваемой на объекте информатизации, в качестве маскирующего шума может быть использован речеподобный шумовой сигнал. Речеподобный шум создают из исходного речевого сигнала путем его фазовой модуляции шумовым сигналом, что приводит к разрушению формантной структуры исходного речевого сигнала. Формальная запись представлена ниже.

$$S(t) = \sum_{p=1}^{N} U_p(t) \sin\left[2\pi\rho \int_0^1 F_0(\tau)\, d\tau + \right.$$
$$\left. + \Phi_\rho(t)\right] + r(t),\ S_{\text{РПП}}(t) = \sum_{j=1}^{6} \sum_{p=1}^{N} U_{pj}(t)$$
$$\sin\left[2\pi\rho \int_0^{t-t_j} F_0(\tau)\, d\tau + \Phi_{\rho j}(t)\right] +$$
$$+ \sum_{j=1}^{6} r_j(t) \qquad (11)$$

где $S(t)$ – речевой сигнал, $S_{\text{РПП}}(t)$ – речеподобный шумовой сигнал, $F_0(\tau)$ – мгновенная частота основного тона звука, $U_p(t)$ – амплитуда p-ой гармонической составляющей звука, N – фаза -ой гармонической составляющей звука, $r(t)$– число энергетически значимых гармонических составляющих звука, $t \in [0; T]$, $\tau \in [0; t]$, T – шумовая составляющая звука, j – время анализа звука; t_j – количество каналов в генераторе речеподобной помехи; – интервалы задержки исходного сигнала в каналах генератора [7].

В системах зашумления в электрическом и магнитном полях используются помехи типа «белый шум» – стационарный шум, спектральные составляющие которого равномерно распределены по всему диапазону задействованных частот.

Базовым методом оценки эффективности защиты информации от утечки по техническим каналам является определение уровня сигнал/шум для рассматриваемого объекта информатизации. Уровень сигнала/шум в месте размещения датчика в i-го частотного интервала:

$$\Delta = L_{ci} - L_{ши} \qquad (12)$$

Для дополнительной оценки защищенности речевой информации от утечки по техническим каналам применяется метод оценки разборчивости речи [8], которая заключается в следующем:

1. Разделение частотного диапазона на определенное число смежных полос (октавных полос).

2. Определение формантного параметра

спектра речевого сигнала в октавной полосе ΔA_i

$$\Delta A_i = \begin{cases} 200f^{0,43} - 0,37, \text{если } f \le 1000 \text{ Гц} \\ 1,37 - \frac{1000}{f^{0,69}}, \text{если } f > 1000 \text{ Гц} \end{cases} \quad (13)$$

3. Определение эффективного уровня ощущений формант Q_i для каждой средней частоты f_i каждой полосы.

$$Q_i = \Delta - \Delta A_i \quad (14)$$

4. Расчет коэффициента восприятия формант для каждой октавной полосы

$$P_i = \begin{cases} \frac{0,78+5,46 \cdot e^{\left[-4,3 \cdot 10^{-3} \cdot (27,3-|Q_i|)^2\right]}}{1+10^{0,1 \cdot |Q_i|}}, \text{если } Q_i \le 0 \\ 1 - \frac{0,78+5,46 \cdot e^{\left[-4,3 \cdot 10^{-3} \cdot (27,3-|Q_i|)^2\right]}}{1+10^{0,1 \cdot |Q_i|}}, \text{если } Q_i > 0 \end{cases} \quad (15)$$

5. Расчет формантной разборчивости

$$R = \sum_{i=1}^{n} P_i k_i \quad (16)$$

где $k_i = \begin{cases} 2,57 \cdot 10^{-8} \cdot f^{2,4}, \text{если } 100 < \\ 1 - 1,047 \cdot e^{-10^{-4} \cdot f^{1,18}}, \text{если } 400 < \end{cases}$

$< f \le 400$ Гц
$< f \le 10000$ Гц – весовой коэффициент.

6. Вычисление словесной разборчивости

$$W = \begin{cases} 1,54 \cdot R^{0,25} \cdot [1 - e^{-11R}], \text{если } \langle R \rangle < 0,15 \\ 1 - e^{-\frac{11R}{1+0,7R}}, \text{если } \langle R \rangle \ge 0,15 \end{cases} \quad (17)$$

Рассмотрим элементарный электрический излучатель (диполь Герца) в сферической системе координат (рисунок 3)

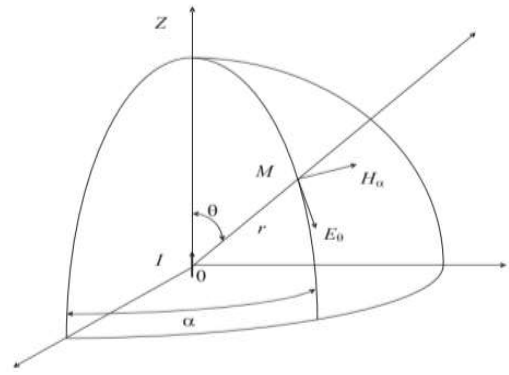


Рис. 3. Элементарный электрический диполь в сферической системе координат

Амплитуда напряжённости электрической E_m и магнитной H_m составляющих электромагнитного поля, которые измеряются с использованием электрических и магнитных антенн имеют вид:

$$E_m = \frac{klI_m}{4\pi\omega\varepsilon r} \sqrt{\left(\frac{3}{k^2r^2} + \frac{5}{r^2}\right)\cos^2(\vartheta) + k^2\sin^2(\vartheta) + \frac{1}{k^2r^2} - \frac{1}{r^2}} \quad (18)$$

$$H_m = \frac{klI_m}{4\pi r} \sqrt{\frac{1}{k^2r^2} + 1} \cdot \sin(\vartheta) \quad (19)$$

Параметры электрического диполя, стоящие перед корнем в уравнениях для E_m и H_m, могут быть определены из измерений электрической и магнитной составляющей электромагнитного поля. Следовательно, оценка защищённости может быть сведена к численному решению уравнений вида $E_m = E_n$ и $H_m = H_n$, где величины E_n и H_n определяются нормативно-методическими документами [9].

Таким образом, в данной работе описана модель обучения адаптивной системы на основе базовой модели машинного обучения. В качестве алгоритма обучения выбран метод восстановления регрессии – метод наименьших квадратов. Также для решения поставленных задач линейный конгруэнтный метод генерации псевдослучайной последовательности выбран как оптимальный. Защита информации от утечки по техническим каналам в части касающейся разрабатываемой модели в общем виде представляет собой применение устройств пространственного и линейного зашумления, шумовой сигнал для которых будет сформирован в виде речеподобного шума для акустических сигналов и в виде белого шума – для электрических и магнитных сигналов.

Литература

1. Генераторы случайных чисел [Электронный ресурс]. — Режим доступа: https://intellect.icu/generatory-sluchajnykh-chisel-5256.

2. Генераторы случайных чисел [Электронный ресурс]. — Режим доступа: http://stratum.ac.ru/education/textbooks/modelir/lection22.html.

3. Реализация ESG-принципов в стратегии устойчивого развития экономики России: монография / Н.Г. Вовченко и др.; под. ред. д.э.н., проф. Е.Н. Макаренко, д.геогр.н., проф. С.В. Бердникова. – Ростов-на-Дону: Издательскополиграфический комплекс Рост. гос. экон. ун-та (РИНХ), 2022. – 508 с.

4. Общие вопросы технической защиты информации [Электронный ресурс]. — Режим доступа: https://intuit.ru/studies/courses/2291/591/lecture/12696?page=1.

5. Технические каналы утечки акустической (речевой) информации Хорев А.А. Специальная техника. 1998. № 1. С. 50.

6. Хорев А.А. Способы и средства зашиты информации. - М.: МО РФ, 2000. – 316 с.

7. Моисеева, М. В. Система защиты информации от утечки по акустическим каналам на основе речеподобной помехи / М. В. Моисеева, А. В. Фурсова // Инновационные процессы в научной среде: Материалы Международной (заочной) научно-практической конференции, Прага, 16 июня 2021 года / под общей редакцией А.И. Вострецова. – Нефтекамск: Научно-издательский центр «Мир науки» (ИП Вострецов Александр Ильич), 2021. – С. 78–84.

8. Рева, И. Л. Реализация оптимальной помехи при защите речевой информации от утечки по акустическому и виброакустическому каналам / И. Л. Рева, В. А. Трушин, А. В. Иванов // Научный вестник Новосибирского государственного технического университета. – 2011. – № 4(45). – С. 140–145.

9. Носов, Л. С. Оценка защищённости СВТ путём моделирования канала ПЭМИН / Л. С. Носов // Математические структуры и моделирование. – 2014. – № 4(32). – С. 254–257.

References

1. Generatory sluchajnyh chisel [Jelektronnyj resurs]. — Rezhim dostupa: https://intellect.icu/generatory-sluchajnykh-chisel-5256.

2. Generatory sluchajnyh chisel [Jelektronnyj resurs]. — Rezhim dostupa: http://stratum.ac.ru/education/textbooks/modelir/lection22.html.

3. Realizacija ESG-principov v strategii ustojchivogo razvitija jekonomiki Rossii: monografija / N.G. Vovchenko i dr.; pod. red. d.je.n., prof. E.N. Makarenko, d.geogr.n., prof. S.V. Berdnikova. – Rostov-na-Donu: Izdatel'sko poligraficheskij kompleks Rost. gos. jekon. un-ta (RINH), 2022. – 508 s.

4. Obshhie voprosy tehnicheskoj zashhity informacii [Jelektronnyj resurs]. — Rezhim dostupa: https://intuit.ru/studies/courses/2291/591/lecture/12696?page=1.

5. Tehnicheskie kanaly utechki akusticheskoj (rechevoj) informacii Horev A.A. Special'naja tehnika. 1998. № 1. S. 50.

6. Horev A.A. Sposoby i sredstva zashity informacii. - M.: MO RF, 2000. – 316 s.

7. Moiseeva, M. V. Sistema zashhity informacii ot utechki po akusticheskim kanalam na osnove rechepodobnoj pomehi / M. V. Moiseeva, A. V. Fursova // Innovacionnye processy v nauchnoj srede: Materialy Mezhdunarodnoj (zaochnoj) nauchno-prakticheskoj konferencii, Praga, 16 ijunja 2021 goda / pod obshhej redakciej A.I. Vostrecova. – Neftekamsk: Nauchno-izdatel'skij centr "Mir nauki" (IP Vostrecov Aleksandr Il'ich), 2021. – S. 78–84.

8. Reva, I. L. Realizacija optimal'noj pomehi pri zashhite rechevoj informacii ot utechki po akusticheskomu i vibroakusticheskomu kanalam / I. L. Reva, V. A. Trushin, A. V. Ivanov // Nauchnyj vestnik Novosibirskogo gosudarstvennogo tehnicheskogo universiteta. – 2011. – № 4(45). – S. 140–145.

9. Nosov, L. S. Ocenka zashhishhjonnosti SVT putjom modelirovanija kanala PJeMIN / L. S. Nosov // Matematicheskie struktury i modelirovanie. – 2014. – № 4(32). – S. 254–257.

ЕГОРОВА Анастасия Олеговна, аспирант кафедры Информационных технологий и защиты информации, Ростовский государственный экономический университет (РИНХ). 344002, г. Ростов-на-Дону, ул. Б. Садовая, 69. E-mail: anastasya-olegovna.kalita@yandex.ru.

ТИЩЕНКО Евгений Николаевич, доктор экономический наук, профессор, декан факультета Компьютерных технологий и информационной безопасности, Ростовский государственный экономический университет (РИНХ). 344002, г. Ростов-на-Дону, ул. Б. Садовая, 69. E-mail: celt@inbox.ru.

EGOROVA Anastasia Olegovna, Postgraduate Student, Department of Information Technologies and Information Protection, Rostov State University of Economics. 344002, Rostov-on-Don, st. B. Sadovaya, 69. E-mail: anastasya-olegovna.kalita@yandex.ru.

TISCHENKO Evgeny Nikolaevich, Doctor of Economics, Professor, Dean of the Faculty of Computer Technologies and Information Security, Rostov State University of Economics. 344002, Rostov-on-Don, st. B. Sadovaya, 69. E-mail: celt@inbox.ru.

УДК 004.058 Вестник УрФО № 2(44) / 2022, с. 43–48

Костюченко К.Л., Хабаров И.А.

DOI: 10.14529/secur220206

РАЗРАБОТКА ОБУЧАЮЩЕЙ ПРОГРАММЫ – ВИРТУАЛЬНОГО ТРЕНАЖЕРА «ПОИСК ЗАКЛАДОЧНЫХ УСТРОЙСТВ»

Статья посвящена разработке компьютерной программы, предназначенной для обучения поиску скрытых закладочных устройств – специальных технических средств, предназначенных для негласного получения информации. Показана актуальность повышения профессиональной подготовленности в вопросах технической защиты информации, особенно в условиях различных ограничений. Описана структура программы – виртуального тренажера, а также различные сценарии работы с ней. Рассмотрены основные возможности, режимы и уровни сложности разрабатываемой программы. Представлены особенности, преимущества и перспективы применения программы.

Ключевые слова: *закладочные устройства, специальные технические средства негласного получения информации, утечка информации, техническая защита информации, поисковая техника, поисковые мероприятия, обучающая программа.*

Kostyuchenko K.L., Khabarov I.A.

CREATION OF A TRAINING PROGRAM – VIRTUAL TRAINER «SEARCH FOR EAVESDROPPING DEVICE»

The article is devoted to the development of a computer program designed to teach the search for hidden eavesdropping devices – special technical means designed to secretly obtain information. The relevance of improving professional preparedness in matters of technical protection of information, especially in conditions of various restrictions, is shown. The structure of the virtual simulator program is described, as well as various scenarios for working with it. The main features, modes and levels of complexity of the developed program are considered. The features, advantages and prospects of the application of the program are presented.

Keywords: *eavesdropping devices, special technical means of secretly obtaining information, information leakage, technical protection of information, search equipment, search activities, training program.*

Вопросы защиты информации актуальны всегда. Каждый год из-за различного рода утечек информации, а также из-за незаконного доступа к носителям и средствам обработки информации у предприятий, компаний и фирм возникают множественные проблемы: материальные, финансовые, организационные, репутационные, политические.

Даже утеря (например, уход к конкуренту) 5 % всего объема конфиденциальных данных компании приводит к серьезным последствиям. Эксперты отмечают, что такого количества достаточно для утраты лидирующих позиций на рынке [1].

Примерно такая же оценка существует в отношении закладочных устройств (радиопередатчики, радиомикрофоны, диктофоны), подключаемых к телефонной линии офиса: «полгода прослушивания достаточно для того, чтобы обанкротить фирму-конкурента». Причем подобные утверждения справедливы и в век «тотальной цифровизации».

Поскольку арсенал специальных технических средств для негласного получения информации достаточно широк, а спрятаны и закамуфлированы они могут самыми неожиданными способы и в любое время, проблема борьбы с закладочными устройствами является постоянной [2–5].

Решить данную проблему позволит повышение качества обучения специалистов по защите информации, а также сотрудников смежных сфер (безопасности, охраны, управления). Для этого необходимо расширять объем знаний по технической защите информации и практических навыков по поиску закладочных устройств и каналов утечки информации.

Традиционные методы обучения, не всегда соответствуют современным требованиям. Как правило, акценты расставляются на теоретической части изучаемого материала, а для практической составляющей остается недостаточно времени. Кроме того, чисто лекционная («сухая») подача материала приводит к его неполноценному усвоению и даже к потере интереса у обучаемых. Также есть множество примеров, когда существующая учебная материальная база не позволяет рассмотреть и проанализировать весь спектр ситуаций, возникающих в реальности. Это становится особенно очевидно в нынешних условиях эпидемиологических ограничений.

В данном случае в качестве современной эффективного метода обучения можно использовать игровой метод, реализуемый в виде обучающей компьютерной программы. Суть такой обучающей программы заключается в получении обучающей среды по тематике поиска и идентификации скрытых закладочных устройств (ЗУ) – специальных технических средств для негласного получения информации.

Разрабатываемая программа «Поиск закладочных устройств» – по сути, виртуальный тренажер – позволит изучить основы поиска ЗУ и технических каналов утечки информации (ТКУИ); освоить методику проведения поисковых мероприятий; рассмотреть особенности применения всего арсенала приемов и средств поиска в различных ситуациях.

Структура программы включает в себя несколько блоков (режимов): «Теория», «Закладка ЗУ», «Поиск ЗУ» и «Поиск ТКУИ» (рис. 1).

Режим «Теория» содержит информацию по видам, конструкциям, характеристикам и вариантам установки ЗУ; по физическим основам появления ТКУИ; по теоретическим основам защиты информации; по принципам, способам и алгоритмам поисковых мероприятий; по локации нелинейностей, нелинейным локаторам (НЛ); по поисковой технике [2–5]. Завершением этого режима является тест по изученному теоретическому материалу. Успешное прохождение теста может давать право перехода к остальным режимам.

Режим «Закладка ЗУ» реализует принцип «для создания средств защиты необходимо знать средства нападения». В этом режиме обучающемуся дается возможность побыть в роли виртуального злоумышленника, который может прятать ЗУ в различных помещениях. Предполагается несколько уровней сложности, в которых варьируется конфигурация и назначение помещений, количество и характеристики ЗУ, способы и качество установки ЗУ, а также время, отводимое на установку ЗУ. Возможно создание различных условий: выбор и размещение ЗУ другим обучающимся или самой компьютерной программой (случайным образом из пополняемой библиотеки элементов); имитация окружающих помех; ограничение времени на поиск; включение встроенных контекстных подсказок и др.

Режим «Поиск ЗУ» (антипод режима «Закладка ЗУ») предназначен для обучения нахождению и нейтрализации ЗУ. В этом режиме предусматривается выбор нелинейного локатора (по тактико-техническим характе-

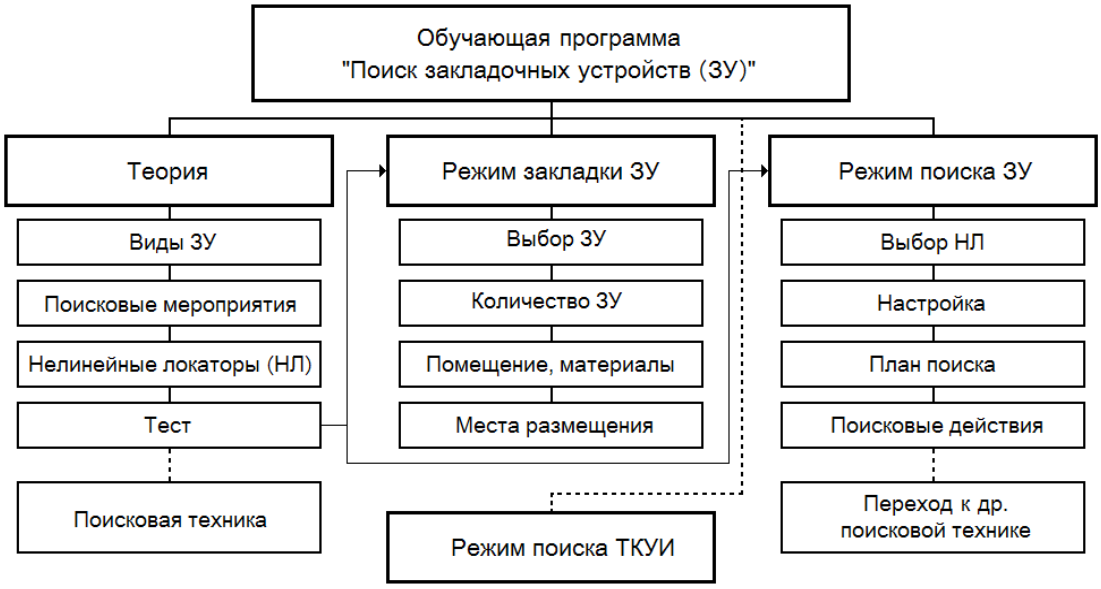


Рис. 1. Структура обучающей программы

ристикам); настройка (калибровка поисковой аппаратуры); выбор иной поисковой техники из имеющегося арсенала. Всё это можно сделать на нескольких уровнях сложности, определяемыми параметрами помещений, способами установки ЗУ, их количеством и др.

Режим «Поиск ТКУИ» включает в себя блоки программы, связанные с поиском и ликвидацией технических каналов утечки информации. Данный режим из-за достаточно большого объема предполагается реализовывать на завершающих этапах.

Основой для создания программы является межплатформенная среда разработки компьютерных игр – платформа разработки 3D-контента реального времени Unity [6]. Крупными разработчиками и независимыми студиями на «платформе Unity» написано большое множество программ: игр, приложений и визуализаций математических моделей. Выбранная среда обладает рядом имеющихся преимуществ: возможность визуализации процесса разработки, межплатформенная поддержки, модульная система компонентов и т.п. Указанные особенности отличают представляемую разработку от уже существующих аналогичных виртуальных тренажеров, например [7].

В данный момент программа находится на этапе активной разработки: вырабатывается стиль и дизайн программы (скриншоты на рис. 2–5), определяется соотношение между элементами двухмерной и трёхмерной графики, апробируются варианты представления помещений, отрабатывается перевод приемов работы с поисковой техникой (прежде всего, нелинейным локатором) в цифровую форму, пополняется теоретический раздел и база характеристик используемых устройств, создается генератор уровней (сценариев) сложности.

На рис. 2 представлено основное меню выбора режима. Ознакомление с техническими характеристиками поисковой аппаратуры в режиме «Теория» иллюстрируется на примере нелинейного локатора «Лорнет» (рис. 3). В загрузочном меню выбранного уровня сложности в режиме «Поиск» (рис. 4) выдается поисковая задача с кратким ее описанием и схемой помещения. На рис. 5 изображен скриншот панели управления нелинейным локатором «ORION» во время поиска ЗУ в помещении учебного класса.

Заключение

Использование в учебном процессе предлагаемой обучающей программы «Поиск закладочных устройств» позволит:

– усилить интерес обучающихся к тематике отдельных направлений информационной безопасности;

– за счет теоретической составляющей программы расширить кругозор обучающихся и базу их знаний в сфере технический защиты информации;

– иметь возможность изучать учебный материал по обнаружению каналов утечки информации как в очном, так и в дистанционном варианте (например, в условиях сложной эпидемиологической обстановки);

Рис. 2. Скриншот меню выбора режима

Рис. 3. Скриншот страницы в режиме «Теория»

Рис. 4. Загрузочное меню режима «Поиск»

Рис. 5. Скриншот работы с нелинейным локатором (с индикацией уровней мощности передачи и принятых сигналов 2-й и 3-й гармоник)

– благодаря игровому методу набрать определенный опыт проведения поисковых мероприятий за счет рассмотрения («проигрывания» в виртуальном пространстве) большого количества самых разнообразных ситуаций, в т.ч. с учетом появления новой техники;

– снизить определенным образом затраты на процесс обучения;

– повысить общую эффективность подготовки и тренажа специалистов в сере защиты информации;

– приобрести необходимые компетенции по тематике технической защиты информации специалисты смежных специальностей (IT, связь, безопасность, охрана и др.).

Литература

1. ПАО «Ростелеком-Солар». Финансовые и репутационные потери от утечек информации [Электронный ресурс] режим доступа: https://rt-solar.ru/products/solar_dozor/blog/2163/ (дата обращения: 12.01.2022).

2. Защита информации: устройства несанкционированного съема информации и борьба с ними: учебно-практическое пособие. / С.Н. Козлов – М.: Академический проспект, 2018.

3. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов – М.: Горячая линия – Телеком, 2018.

4. Выявление специальных технических средств несанкционированного получения информации / Г.А. Бузов – М.: Горячая линия – Телеком, 2019.

5. Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков; под ред. А.П. Зайцева и А.А. Шелупанова – М.: Горячая линия – Телеком, 2020.

6. Платформа Unity. [Электронный ресурс] режим доступа: https://unity.com/ru/products/unity-platform (дата обращения: 05.11.2021).

7. Шпак В.А., Кремлев Е.С., Михайлова У.В. Разработка виртуального тренажера для оценки защищенности акустической информации в контролируемом помещении / Вестник УрФО. Безопасность в информационной сфере. № 2(36) / 2020, с. 10–16.

References

1. PAO «Rostelekom-Solar». Finansovye i reputacionnye poteri ot utechek informacii [Financial and Reputational Losses from Information Leaks]. Available at: https://rt-solar.ru/products/solar_dozor/blog/2163/ (accessed 12 January 2022).

2. Kozlov S.N. Zashhita informacii: ustrojstva nesankcionirovannogo s'ema informacii i bor'ba s nimi:

Uchebno-prakticheskoe posobie. [Information Protection: Devices for Unauthorized Removal of Information and Combating Them: An Educational and Practical Guide]. Moscow, Akademicheskij prospekt, 2018.

3. Buzov G.A. Zashhita informacii ogranichennogo dostupa ot utechki po tehnicheskim kanalam /– [Protection of Restricted Access Information from Leakage Through Technical Channels]. Moscow, Gorjachaja linija – Telekom, 2018.

4. Buzov G.A. Vyjavlenie special'nyh tehnicheskih sredstv nesankcionirovannogo poluchenija informacii [Finding Special Technical Means of Unauthorized Receipt of Information]. Moscow, Gorjachaja linija – Telekom, 2019.

5. Zajcev A.P., Shelupanov A.A., Meshherjakov R.V. Tehnicheskie sredstva i metody zashhity informacii. Uchebnik dlja vuzov / [Technical Means and Methods of Information Protection. Textbook for Universities]. Moscow, Gorjachaja linija – Telekom, 2020.

6. Platforma Unity. [Platform Unity]. Available at: https://unity.com/ru/products/unity-platform (accessed 5 May 2021).

7. Shpak V.A., Kremlev E.S., Mihajlova U.V. Razrabotka virtual'nogo trenazhera dlja ocenki zashhishhennosti akusticheskoj informacii v kontroliruemom pomeshhenii [Development of a Virtual Trainer for Assessing the Protection of Acoustic Information in a Controlled Room]. Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. № 2(36) / 2020, p. 10–16.

КОСТЮЧЕНКО Константин Леонидович, кандидат технических наук, доцент, доцент кафедры Информационных технологий и защиты информации, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: KKostyuchenko@usurt.ru.

ХАБАРОВ Игорь Андреевич, студент, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: WonderChief@mail.ru.

KOSTYUCHENKO Konstantin Leonidovich, Candidate of Engineering Sciences, Docent, Associate Professor of the Department of Information Technology and Information Security, Ural State University of Railway Transport. 66 Kolmogorov str., Yekaterinburg, 620034. E-mail: KKostyuchenko@usurt.ru.

KHABAROV Igor Andreevich, Student, Ural State University of Railway Transport. 66 Kolmogorov str., Yekaterinburg, 620034. E-mail: WonderChief@mail.ru.

УДК 004.056 Вестник УрФО № 2(44) / 2022, с. 49–56

Манжосов А.В., Болодурина И.П.

DOI: 10.14529/secur220207

МЕТОД АВТОМАТИЗИРОВАННОГО ПОСТРОЕНИЯ ГРАФА ЗНАНИЙ СВЯЗНОСТИ ФОРМАЛЬНЫХ МОДЕЛЕЙ НОРМ И ТРЕБОВАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В последние десятилетия объем накопленной человечеством информации увеличился невероятно. Люди придумывают всё более оптимальные способы для систематизации, совместного использования и анализа большого объема данных с помощью традиционных алгоритмов и структур данных, но при этом они не предусматривают анализ естественного языка и зачастую не используют семантические связи.

Исходя из этого, назрела необходимость в таком анализе и представлении информации, которые позволяли бы с одной стороны хранить огромное количество объектов и отношений между ними, а с другой – предоставляло высокоскоростной доступ большому количеству пользователей к хранящимся данным, и, кроме того, сохраняло семантику. Одной из самых эффективных структур данных, позволяющей решать подобные задачи, являются графы и базы знаний, которые относительно недавно появились и стали предметом исследований в последние годы.

Ключевые слова: *граф знаний, онтология, анализ, нормативно-правовой акт, информационная безопасность.*

AUTOMATED CONSTRUCTION OF THE KNOWLEDGE GRAPH OF REFERENCE TO FORMAL MODELS OF NORMS AND TREATMENTS IN THE FIELD OF INFORMATION SECURITY METHOD

The amount of information accumulated by mankind has increased incredibly in recent decades. People are coming up with ever better ways to organize, share, and analyze large amounts of data using algorithms and data structures.

There is a need for such an analysis and presentation of information that would on the one hand, allow to store a huge number of objects and relationships between them, and on the other hand, provide high-speed access to a large number of users to the stored data, and, in addition, preserve the semantics. One of the most effective data structures that allows to solve such problems are graphs and knowledge bases, which have appeared relatively recently and have become the subject of research in recent years.

Keywords: *knowledge graph, ontology, analysis, normative act, information security.*

Введение

В этой статье рассматриваются все этапы реализации графа знаний, а также проблемы, с которыми, возможно, придется столкнуться при создании собственного экземпляра данной абстракции. Помимо этого, рассмотрены методы создания интерактивного визуального представления информации для ее эффективного хранения в графе, а также практические шаги по его реализации и использованию.

Разработку метода автоматизированного построения графа знаний связности формальных моделей норм и требований в области информационной безопасности предлагается разделить на четыре основных этапа.

Во-первых, анализ разработок в области визуализации нормативно-правовой базы, а также использования графовой модели в сфере информационной безопасности.

Во-вторых, исследование способов формального представления норм права и требований стандартов для использования компьютерных технологий в области права.

В-третьих, анализ норм права на предмет возможности создания их машиночитаемого представления и автоматизированного способа пополнения базы знаний.

В-четвертых, разработка инструментов для работы экспертов в области информационной безопасности над формальными моделями норм и требований.

Анализ исследований по способам визуализации нормативно-правовой базы, а также использованию графовой модели в сфере информационной безопасности

Авторы статьи [1] предлагают анализ существующих подходов представления знаний в виде графов. Исследование включает в себя извлечение отношений из текста, методы встраивания отношений для создания ссылок, обзор существующих графов знаний,

сравнение хранилищ графов знаний, импорт графов знаний. Статья полезна для первичного анализа работы с графами знаний, определения концепции построения, хранения и импорта графов знаний. При этом отмечается, что подходы, предложенные в статье, применимы для любой области знаний, т.е. универсальны.

Основная работа в статье [2] разделена на части. Обсуждается создание базы знаний по кибербезопасности в соответствии с трехэтапной процедурой и предлагается структура для создания базы знаний:

– во-первых, извлечение информации путем сбора и анализа структурированных и неструктурированных данных;

– во-вторых, построение онтологии в соответствии с полученной информацией компьютерных атак;

– в-третьих, метод машинного обучения для извлечения объектов, связанных с компьютерной атакой.

Данное исследование [3] описывает создание онтологии по информационной безопасности в рамках прецедентного подхода к описанию компьютерных угроз. Разрабатываемая онтология достаточно полно описывает предметную область компьютерных угроз и является концептуальной. Авторы предложили способ создания на основе онтологии базы данных основных известных прецедентов компьютерных атак и нарушений информационной безопасности, с их описанием, методами идентификации и способами устранения последствий.

В статье [4] авторы предлагают новую общую структуру защиты промышленной управляющей сети на основе данных. С целью повышения качества анализа отношения сущностей в данных о кибербезопасности, авторами предлагается прототип новой модели извлечения отношений кибербезопасности ResPCNN-ATT.

Авторами [5] разработана модель информационной безопасности баз знаний, включающая следующие составляющие: функции защиты информации в базах знаний; методы защиты баз знаний, технико-экономические показатели методов защиты информации в базах знаний.

По сравнению с представленными работами, в статье предлагается решение нескольких задач:

– исследование способов формального представления норм права и требований стандартов для использования компьютерных технологий в области права;

– разработка формального представления предметной области;

– анализ норм права, на предмет возможности создания их машиночитаемого представления и автоматизированного способа пополнения базы знаний;

– разработка инструментов для работы экспертов в области информационной безопасности над формальными моделями норм и требований.

Описание способа формального представления норм права и требований стандартов для использования компьютерных технологий в области права

Наиболее часто применяемым инструментом при визуализации реляционных типов данных является графовая модель, которая также применяется и в других направлениях визуализации. Модель представляет не только данные, но и отношения между данными. Графовая модель является структурой данных, состоящей из связанных сущностей. Представление информации в виде графа знаний не ново, но в последнее время оно приобрело популярность благодаря его использованию в приложениях искусственного интеллекта. Ниже представлены основные термины и определения, использующиеся в статье.

Граф знаний – это семантическая сеть, в которой хранятся сущности и отношения между сущностями в виде графа. Преимущество использования графа знаний – это возможность обработки большего количества запросов, чем у традиционных методов хранения. Граф знаний – гибкая форма хранения и визуализации данных, которые легко обновить.

Ключевое слово — особо важное, общепонятное, емкое и показательное слово в тексте, набор которых может дать высокоуровневое описание его содержания.

Нормативно-правовой акт – концепт, соответствующий официальному документу, изданному в установленном порядке органом государственной власти, органом местного самоуправления или должностным лицом, и содержащий правовые нормы.

Онтология – классы, свойства классов, правила, которые в совокупности отражают формальную концепцию предметной области; попытка всеобъемлющей и подробной формализации некоторой области знаний с помощью концептуальной схемы.

Отношение – связь между сущностями, являющаяся ребром графа знаний.

Ссылка – связь, ведущая от фрагмента текста одного нормативно-правового акта к другому нормативно-правовому акту.

Сущность – нормы права, являющиеся узлами (вершинами) графа знаний.

Тип отношения – способ указать, что означает отношение между сущностями, семантику соответствующего отношения.

Сегодня термины, применяемые при построении баз и графов знаний, употребляются в различных контекстах. Моделирование и формальное представление схемы данных в виде баз и графов знаний обеспечивают гораздо большие возможности, чем традиционные базы данных или объектно-ориентированный подход.

Разработка формального представления предметной области

В этом разделе представлено формальное представление онтологии графа знаний нормативно-правовой базы в сфере информационной безопасности.

Согласно определению, формализация онтологии – процесс выражения концептуализации предметной области в соответствии с парадигмой представления знаний, предлагаемой языком моделирования.

Формализация онтологии проведена в соответствии с условиями:

– онтология является одним из инструментов, необходимых для моделирования предметной области;

– онтология содержит перечень ключевых слов данной предметной области;

– знание о смысле ключевых слов, представленное онтологией, должно быть очевидным для любого эксперта в данной предметной области.

Цель онтологии – повысить количество и качество описываемых общих свойств предметной области, не зависящих от ее конкретных реализаций.

Формальной онтологией предметной области *EA* называется пара <*e, a*>, где *e* – множество ключевых слов предметной области, а *a* – множество аналитических предложений, отношений, ссылок, описывающее смысл данных ключевых понятий.

Онтология предметной области включает в себя:

– словарь ключевых понятий, использующихся в данной предметной области;

– совокупность отношений, обеспечивающих корректную интерпретацию понятий и их правильное использование.

Представление знаний в виде онтологий применяется ради семантической интеграции информационных ресурсов, корректной интерпретации содержания или названия текстовых документов, представленных с помощью естественного языка. На основе онтологий разрабатываются базы знаний и графы знаний.

Поэтому всё множество *S* предложений, которые являются верными в предметной области *EA*, будем называть теорией предметной области *EA*.

Тогда, если *E*, *A* – формальная онтология предметной области *EA*, а *S* – теория предметной области *EA*. Тогда каждый элемент *E* является элементом *S*.

Примем во внимание, что если некоторое утверждение базы данных не является истинным, то утверждение принимается ложным. В то время, как для базы знаний в этом случае такое утверждение является ни истинным, ни ложным. Это свойство существенно влияет на то, какие факты считаются логически следующими из заданной базы знаний, и на понятие логического следования в эти факты базы знаний.

Анализ норм права, на предмет возможности создания их машиночитаемого представления и автоматизированного способа пополнения базы знаний

Законодательная база Российской Федерации содержит множество нормативно-правовых актов в сфере информационной безопасности. Анализ нормативно-правовых актов свободного доступа позволит сформировать базу знаний. Алгоритм анализа нормативно-правового акта представлен в виде алгоритма на рисунке 1.

Описание основных этапов алгоритма представлены ниже.

1. Добавление нормативно-правовых актов.

На данном этапе происходит добавление пользователем нормативно-правовых актов, которые в дальнейшем будут считаться нормативно-правовой базой, и на основании которых предлагается строить граф знаний. Добавление НПА происходит посредством выбора директории с необходимым набором документов текстового формата.

2. Обработка заголовков НПА.

В загруженных документах определяются их заголовки и выносятся в отдельный мас-

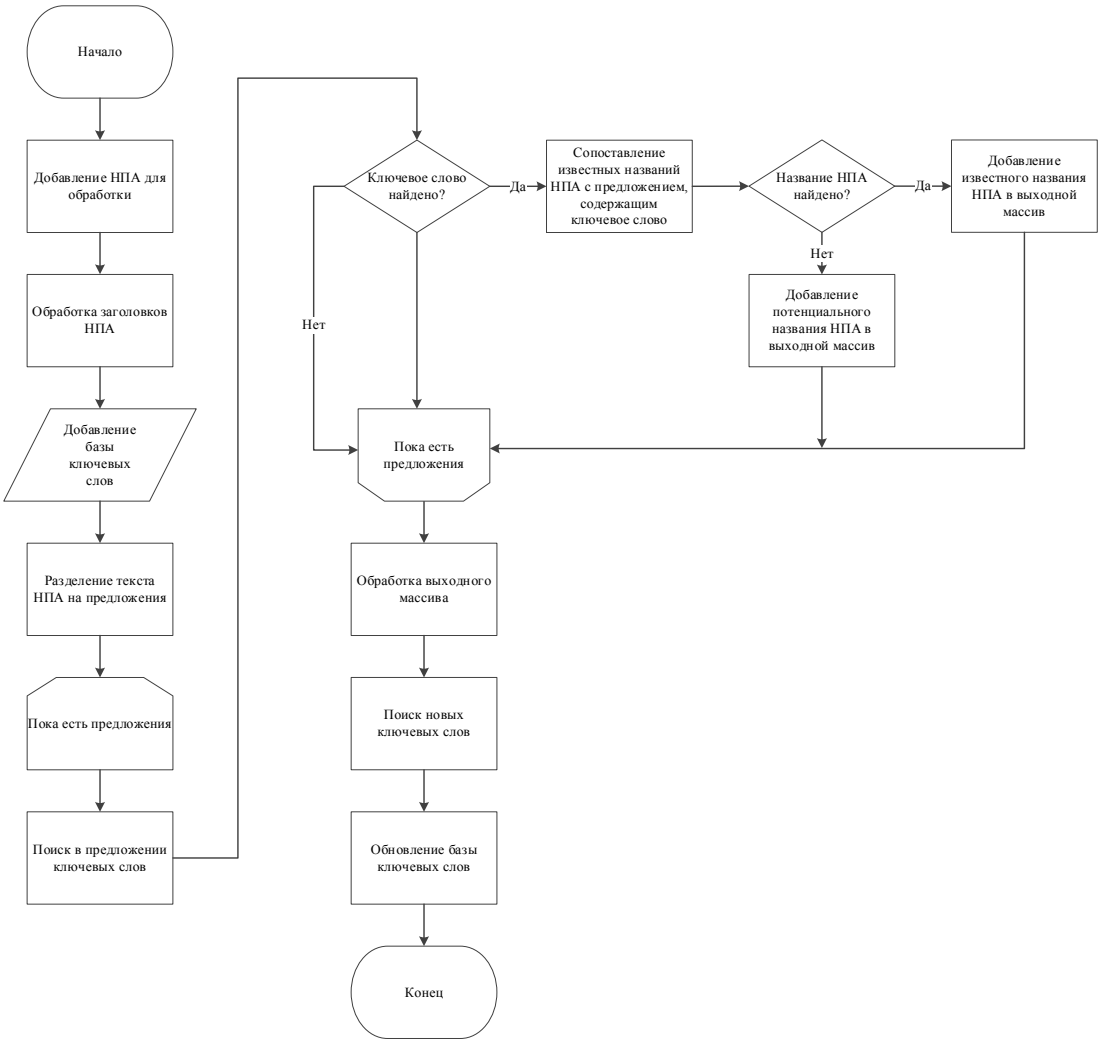


Рис. 1. Алгоритм анализа нормативно-правового акта

сив. При этом подразумевается, что файлы, найденные в каталоге, могут иметь, а могут не иметь соответствующие шаблону наименования норм законодательства названия (%тип документа% %издатель% от %дата% %номер% %название%). Набор ключевых слов определяется исходя из шаблонов наименования норм законодательства в полуавтоматическом режиме.

3. Разделение текста НПА на предложения.

В данном цикле осуществляется основная работа по определению связей между НПА следующим образом: осуществляется поиск по всем предложениям на предмет явного содержания в предложении или предложений, потенциально содержащих ключевые слова заголовков НПА.

4. Обработка выходного массива.

Массив полученных из предложений названий НПА (ссылок на документы) соотносится с заголовками из текущего множества загруженных НПА. Следующим шагом выявляются совпадения между полученной ссылкой и заголовком с помощью ключевых слов. Найденные ключевые слова или потенциальные ключевые слова добавляются в массив, который в последствии редактируется.

5. Поиск новых ключевых слов.

Пользователю предлагается анализировать потенциальные ключевые слова на предмет добавления их в базу ключевых слов для последующего использования при обработке НПА. Результатом анализа пользователя на этом этапе является Обновленная база ключевых слов.

На практике извлечение сущностей заключается в извлечении из текста нормативно-правового акта ссылок на другие нормативно-правовые акты. Процесс построения

графа знаний состоит из извлечения сущностей и их взаимоувязки отношениями с базой нормативно-правовых актов через онтологию. Это сформирует граф знаний и предоставит возможность экспертам в области ИБ проводить рассуждения о связности документов. Разработанную онтологию также можно связать с внешними знаниями и онтологиями.

Основной подход к извлечению отношений основан на техниках обработки естественного языка, включая тегирование части речи, синтаксический анализ, распознавание именованных сущностей.

Онтологии представляются в виде в графов знаний, чтобы визуализировать взаимосвязанные отношения между сущностями области знания. Графы знаний – наилучшие средства представления сущностей и отношений между ними. Онтология же состоит из набора классов с атрибутами и отношениями.

База знаний представляет собой семантический граф знаний, описывающий семантику источников информации. Таким образом, получившаяся онтология предлагает для аналитиков и профессионалов в данной области инструмент для анализа. Граф знаний является результатом связывания области знания и модели представления данных, а именно онтологии. В нашем случае граф знаний является связностью нормативно-правовых актов, извлеченных в специальную онтологию.

Разработка инструментов для работы экспертов в области информационной безопасности над формальными моделями норм и требований

Реализацией предложенных алгоритмов и формализованных представлений является разработанная программа для ЭВМ [6]. Программа является инструментом для работы экспертов в области информационной безопасности над формальными моделями норм и требований в области законодательства РФ. На рисунке 2 представлен интерфейс программы для ЭВМ.

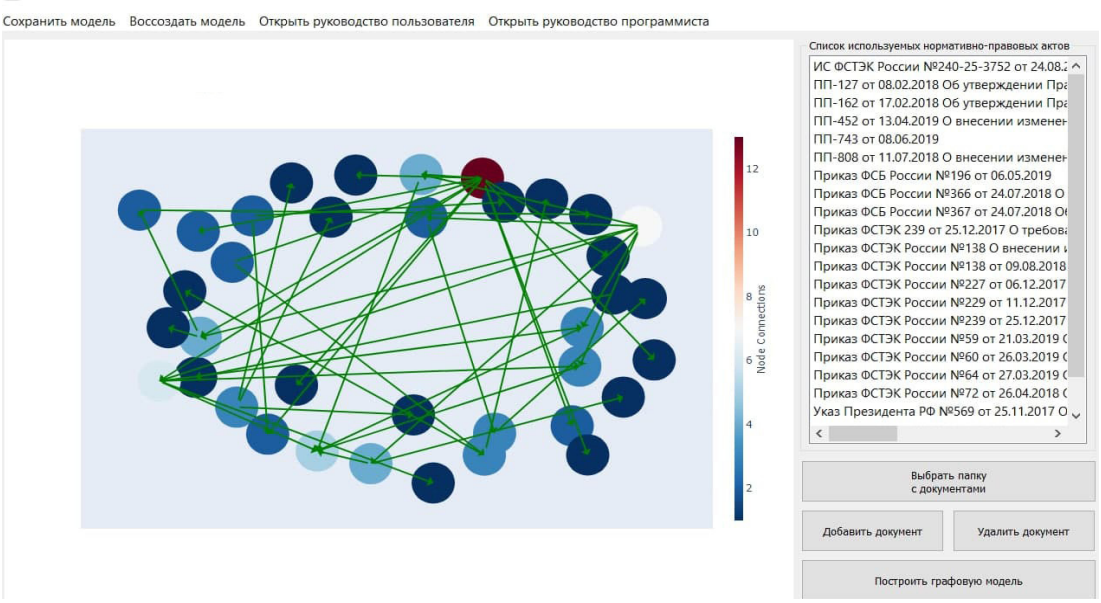


Рис. 2. Интерфейс программы для ЭВМ

Интерфейс состоит из:

– элементов управления;

– зоны управления загруженными нормативно-правовыми актами;

– области визуализации отношений сущностей нормативно-правовой базы.

Элементы управления позволяют пользователю определить входные данные для работы программы, корректировать состав НПА, ознакомиться с руководствами пользователя и администратора, сохранить или восстановить граф знаний.

Зона управления загруженными НПА отражает состав документов, выбранных пользователем в качестве входных данных. Перечень документов, отображаемых в этой зоне, имеет функционал интерактивного взаимодействия с областью визуализации отношений сущностей нормативно-правовой базы.

Область визуализации отношений сущ-

ностей нормативно-правовой базы является основным полем работы пользователя с программой для ЭВМ. Область визуализации отношений отражает связь всех обрабатываемых пользователем НПА. Визуализация отношений реализована в виде графа знаний и является интерактивной. Пользователю доступен функционал перемещения вершин графа, взаимодействия с вершинами и ребрами графа для получения дополнительной информации. Визуально количество упоминаний документа в других НПА отличается цветом. В области визуализации отношений представлена шкала, демонстрирующая соотношение количества упоминаний документа в других НПА (число связных ребер графа знаний с конкретной вершиной) и цветового оттенка.

Целью применения средства автоматизированного построения нормативно-правовой базы является снижение трудоемкости задачи анализа требований нормативно-правовой базы. Анализ требований нормативно-правовой базы проводится аналитиками информационной безопасности периодически.

Заключение

Представленные разработки предлагают метод автоматизированной визуализации отношений между нормативно-правовыми актами посредством построения графа знаний, что позволяет ускорить анализ информации специалистом в сфере ИБ. Основным преимуществом предложенного метода является автоматизированный способ пополнения базы ключевых слов, а также скорость анализа данных, поскольку автоматизированная реализация способна в десятки раз сократить время, затрачиваемое на ручной поиск, анализ и систематизацию информации, изложенной в нормативно-правовой базе. Программная реализация предложенного метода зарегистрирована в государственном фонде электронных ресурсов. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-07-01065, а также гранта Президента Российской Федерации для государственной поддержки ведущих научных школ Российской Федерации (НШ-2502.2020.9).

Литература

1. Гурин В. С., Костров Е. В., Гавриленко Ю. Ю., Саада Д. Ф., Ильюшин Е. А., Чижов И. В. Представление знаний в виде графа: основные технологии и подходы // Современные информационные технологии и ИТ-образование. 2019. Т. 15, № 4. С. 932-944. DOI: 10.25559/SITITO.15.201904.932-944.

2. A Practical Approach to Constructing a Knowledge Graph for Cybersecurity Yan Jia, Yulu Qi, Huaijun Shang, Rong Jiang, Aiping Li https://doi.org/10.1016/j.eng.2018.01.004.

3. Мирзагитов А. А., Пальчунов Д. Е. Методы разработки онтологии по информационной безопасности, основанные на прецедентном подходе // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11, вып. 3. С. 37–46.

4. Guowei Shen, Wanling Wang, Qilin Mu, Yanhong Pu, Ya Qin, and Miao Yu Data-Driven Cybersecurity Knowledge Graph Construction for Industrial Control System Security doi.org/10.1155/2020/8883696.

5. Рихтер Т.В., Абрамова И.В. Разработка модели информационной безопасности баз знаний. Физико-математическое образование. 2020. Выпуск 1(23). С. 106-110. DOI 10.31110/2413-1571-2020-023-1-017.

6. Свидетельство 2021666949 «Автоматизированное построение графовой модели нормативно-правовой базы»: программа для ЭВМ / А.В. Манжосов, И.П. Болодурина, В.Д. Родионов, М.С. Гнамм (RU); правообладатель А.В. Манжосов. заявл. от 13.09.2021. опуб. 21.10.2021.

References

1. Gurin V. S., Kostrov Ye. V., Gavrilenko YU. YU., Saada D. F., Il'yushin Ye. A., Chizhov I. V. Predstavleniye znaniy v vide grafa: osnovnyye tekhnologii i podkhody // Sovremennyye informatsionnyye tekhnologii i IT-obrazovaniye. 2019. T. 15, № 4. S. 932-944. DOI: 10.25559/SITITO.15.201904.932-944.

2. A Practical Approach to Constructing a Knowledge Graph for Cybersecurity Yan Jia, Yulu Qi, Huaijun Shang, Rong Jiang, Aiping Li https://doi.org/10.1016/j.eng.2018.01.004.

3. Mirzagitov A. A., Pal'chunov D. Ye. Metody razrabotki ontologii po informatsionnoy bezopasnosti, osnovannyye na pretsedentnom podkhode // Vestn. Novosib. gos. un-ta. Seriya: Informatsionnyye tekhnologii. 2013. T. 11, vyp. 3. S. 37–46.

4. Guowei Shen, Wanling Wang, Qilin Mu, Yanhong Pu, Ya Qin, and Miao Yu Data-Driven Cybersecurity Knowledge Graph Construction for Industrial Control System Security doi.org/10.1155/2020/8883696.

5. Rikhter T.V., Abramova I.V. Razrabotka modeli informatsionnoy bezopasnosti baz znaniy. Fiziko-matematicheskoye obrazovaniye. 2020. Vypusk 1(23). S. 106-110. DOI 10.31110/2413-1571-2020-023-1-017.

6. Svidetel'stvo 2021666949 «Avtomatizirovannoye postroyeniye grafovoy modeli normativno-pravovoy bazy»: programma dlya EVM / A.V. Manzhosov, I.P. Bolodurina, V.D. Rodionov, M.S. Gnamm (RU); pravoobladatel' A.V. Manzhosov. zayavl. ot 13.09.2021. opub. 21.10.2021.

МАНЖОСОВ Артём Владимирович, аспирант кафедры прикладной математики Факультета математики и информационных технологий Федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет». 460018, Оренбург, пр. Победы, 13. E-mail: a.v.manzhosov@gmail.com

БОЛОДУРИНА Ирина Павловна, профессор, доктор технических наук, заведующий кафедрой прикладной математики Факультета математики и информационных технологий Федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет». 460018, Оренбург, пр. Победы, 13. E-mail: ipbolodurina@yandex.ru

MANZHOSOV Artyom Vladimirovich, post-graduate student of the Department of Applied Mathematics, Faculty of Mathematics and Information Technologies, Federal State Budgetary Educational Institution of Higher Education "Orenburg State University". 460018, Orenburg, Pobedy Ave., 13. E-mail: a.v.manzhosov@gmail.com, +79228133818.

BOLODURINA Irina Pavlovna, Professor, Doctor of Technical Sciences, Head of the Department of Applied Mathematics, Faculty of Mathematics and Information Technologies, Federal State Budgetary Educational Institution of Higher Education "Orenburg State University". 460018, Orenburg, Pobeda ave., 13. E-mail: ipbolodurina@yandex.ru

УДК 004.056.53 Вестник УрФО № 2(44) / 2022, с. 57–62

Баранкова И.И., Афанасьева М.В., Дегтярева А.В. DOI: 10.14529/secur220208

ПОСТРОЕНИЕ МОДЕЛИ ЗРЕЛОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ АСУ ТП ЦППН

В статье произведена адаптация методики построения модели зрелости безопасности интернета вещей под нужды и требования защиты объекта критической информационной инфраструктуры – цеха подготовки и перекачки нефти. В процессе работы былисмоделированы целевой и текущий профили.В статье приведены самые значимые практики по каждому из профилей, а также выведены диаграммы уровней полноты и специфики. Итогом работы стало приведенное в статье сравнение профилей с выявленными разрывами в обеспечении информационной защиты.

Ключевые слова: *информационная безопасность (ИБ), модель зрелости безопасности, критическая информационная инфраструктура (КИИ), автоматизированная система управления технологическим процессом (АСУ ТП), цех подготовки и перекачки нефти (ЦППН).*

Barankova I.I., Afanasyeva M.V., Degtyareva A.V.

BUILDING AN INFORMATION SECURITY MATURITY MODEL FOR THE APCS OF THE OIL TREATMENT AND PUMPING SHOP

The article adapts the methodology for building a security maturity model for the Internet of Things to the needs and requirements of protecting a critical information infrastructure object - an oil treatment and pumping shop. In the process of work, the target and current profiles were modeled. The article presents the most significant practices for each of the profiles, as well as diagrams of the levels of completeness and specificity. The result of the work was the comparison of profiles given in the article with the identification of gaps in information security.

Keywords: *information security (IS), security maturity model, critical information infrastructure (CII), automated process control system (APCS), oil treatment and pumping shop.*

На сегодняшний день прослеживается тенденция увеличения числа кибератак на организации всех типов, а нестабильная геополитическая ситуация обязывает еще пристальней обращать внимание на киберугрозы в критической инфраструктуре. Для того

чтобы выстроить адекватную программу информационной безопасности (ИБ), организации стали смотреть в сторону моделей зрелости. Модель зрелости призвана:

• Предоставлять организациям возможность эффективно оценивать и сравнивать показатели информационной безопасности.

• Определять пути развития и усовершенствования ИБ.

• Делиться знаниями и передовым опытом со смежными предприятиями, для усиления национальной безопасности.

Цель данной статьи – применить опыт построения модели зрелости для объекта КИИ – АСУ ТП ЦППН, который в дальнейшем поможет другим предприятиям выстроить или улучшить свою систему защиты ИБ.

Практически все современные модели зрелости основаны на модели CMM (CapabilityMaturityModel), разработанной и опубликованной в начале 1990-х гг. Институтом программной инженерии Карнеги – Мелона[1].

В 2019 году Kaspersky ICS CERT опубликовал руководство по применению модели IoTSecurityMaturityModel: Practitioner'sGuide. Эта модель направлена на интернет вещей, но в данной статье она была адаптирована под нужды и требования защиты КИИ (модель зрелости была разработана с учетом, что рассматриваемый объект имеет третью категорию значимости).

Модель зрелости ИБ строится путем сравнения целевого и текущего профилей безопасности. Целевой профиль зрелости представляет собой описание стопроцентной зрелости безопасности для системы, к достижению которой следует стремиться при ее развитии[2]. В текущем профиле зрелости безопасности определяется состояние защиты информации на предприятии в данный момент. Данные профили создаются путем определения набора пар «полнота+специфика» по всем практикам безопасности. Домены - это высокоуровневые представления, которые отражают ключевые аспекты зрелости безопасности: управление, внедрение и укрепление. Каждый из доменов имеет разные ключевые аспекты, называемые поддоменами. Например, домен усиления безопасности включает в себя поддомены уязвимости и обновления, ситуационная осведомленность и реагирование на события и инциденты. Далее каждый поддомен углубляется в две практики безопасности. Каждый домен может использовать различные методы, как технические, так и организационные, для достижения результатов в этой области. Такой иерархический подход позволяет рассматривать анализ зрелости на разных уровнях детализации - от различных областей в целом до отдельных практик [3].Иерархия доменов, поддоменов и практик в модели зрелости безопасности представлена в [4].

В рамках данной работы в первую очередь был смоделирован целевой профиль. Углубление осуществлялось до самого нижнего уровня – уровня практик. Следовательно, в работе были рассмотрены все восемнадцать практик, самые значимые приведены в статье.

В домене «Управление» особое внимание заслуживают практики «Руководство программой безопасности» и «Обеспечение соответствия внешним требованиям», так как они составляют базу защиты информации.

Для значимого объекта КИИ необходимо регулярно вести контроль, принимать стратегические решения относительно обеспечения безопасности, отслеживать технологические новинки, поэтому целевой уровень практики «Руководство программой безопасности» был определен как третий. Также данной практике был присвоен второй уровень специфики, так как внутренние документы, регулирующие вопросы, связанные с обеспечением ИБ, должны быть адаптированы под нужды и специфику производственного предприятия.

Всем значимым объектам КИИ предъявляются конкретные требования от регуляторов в зависимости от их категории значимости, в частности выполнение требований Приказа ФСТЭК России от 25 декабря 2017 г. N 239, следовательно, практика «Обеспечение соответствия внешним требованиям» имеет второй уровень, как у полноты, так и у специфики.

Далее были рассмотрены практики домена «Внедрение». Целевой уровень практики «Управление учетными записями» был определен как третий, так как согласно Приказу ФСТЭК №239 для данной системы необходимо организовать управление доступом с разделением полномочий пользователей, назначением минимально необходимых прав и привилегий и т.д. Используемое средство должно быть выбрано на основе анализа рынка передовых технологических решений. При этом специфике был присвоен первый уровень, так как процесс управления учетны-

ми записями может осуществляться через универсальные для любой другой типичной сферы программные продукты.

Для обеспечения защиты объекта должны быть отобраны лучшие, прошедшие сертификацию, средства защиты. Должен производиться мониторинг новинок. Это образует третий целевой уровень полноты практики «Реализация механизмов защиты данных». Необходимо учитывать совместимость средств защиты с системой, следовательно, специфика имеет третий уровень.

При инцидентах на значимом объекте КИИ необходимо: во первых, незамедлительно информировать о компьютерных инцидентах ФСБ России (НКЦКИ); во вторых, оказывать содействие должностным лицам ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов. Это образует второй целевой уровень полноты для практики «План реагирования на инциденты информационной безопасности» домена «Укрепление». Данные процессы будут иметь специфичный для индустрии характер, то есть второй уровень.

Для промышленного производства непрерывная работа является одним из ключевых приоритетов. В рамках практики «Поддержание непрерывной работы и восстановление» необходимо проводить организационные мероприятия по вопросам обеспечения НРВ, должны применяться различные способы резервирования аппаратных ресурсов, эталонного копирования программных и страхового копирования информационных ресурсов системы, а также проведение постоянного анализа эффективности принятых мер, разработка и реализация предложений по их совершенствованию[5]. Данные меры образуют третий целевой уровень полноты. Поддержание непрерывной работы должно учитывать особенности производственного процесса, следовательно, иметь второй уровень специфики.

Для наглядности получившийся целевой профиль был представлен графически (рис. 1). Цветом выделены уровни специфики, а высота графиков отражает уровни полноты.

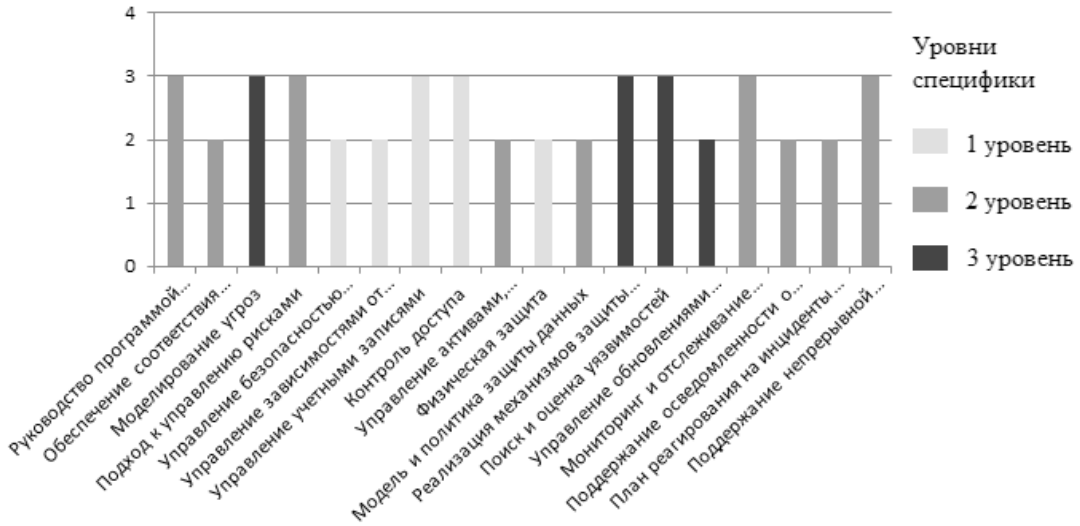


Рис. 1. Целевой профиль

На следующем этапе был смоделирован текущий профиль. Он создавался по тому же плану, что и целевой. Вначале были рассмотрены практики домена «Управление».В рамках данной работы было установлено, что практика «Руководство программой безопасности» на предприятии реализована на втором уровне полноты: руководством сформирован отдел по защите информации. В отделе выстроена иерархия, каждому сотруднику отведена зона ответственности (прописывание политик и контроль их соблюдения, настройка СЗИ и т.д.), начальник отдела контролирует все процессы, связанные с ИБ и отчитывается перед руководством. Все отмеченные процессы имеют специфичный для индустрии характер, то есть второй уровень.

На АСУ ТП ЦППН проведено категорирование объекта КИИ, результаты переданы во ФСТЭК, подготовлены все обязательные до-

кументы (модель угроз, политики) данные мероприятия определяют текущий уровень полноты и специфики как второй для практики «Обеспечение соответствия внешним требованиям».

Далее был рассмотрен домен «Внедрение». На предприятии реализуется управление учетными записями пользователей, в том числе внешних пользователей (возлагается на администратора ИБ): определение типа учетной записи; объединение учетных записей в группы; верификация пользователя; заведение, активация, блокирование и уничтожение учетных записей пользователей; пересмотр и, при необходимости, корректировка учетных записей не реже одного раза в три месяца; предоставление пользователям прав доступа к объектам доступа, основываясь на задачах, решаемых пользователями на предприятии. Все это образует второй текущий уровень полноты для практики «Управление учетными записями», при этом данные меры являются стандартными и применимы для любой типичной среды, поэтому присвоен первый уровень специфики.

На предприятии введены в действие сертифицированные ФСТЭК программные и технические продукты по защите информации, но их недостаточно для покрытия всех актуальных угроз, также есть средства с истекшими сертификатами.На основе этих данных, практике «Реализация механизмов защиты данных» был присвоен первый текущий уровень полноты. При подборе средств, специалисты учитывалисовместимость средств защиты с системой, следовательно, специфика имеет третий уровень.

На последнем этапе рассматривался домен «Укрепление». Практика «План реагирования на инциденты информационной безопасности» реализован на втором уровне полноты, так как план реагирования задокументирован, при возникновении инцидентов обеспечивается незамедлительное информирование ФСБ России (НКЦКИ); оказывается содействие должностным лицам ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов. Данные процессы имеют специфичный для индустрии характер, то есть второй уровень.

На АСУ ТП ЦППН проводятся организационные мероприятия по вопросам обеспечения НРВ, применяется система горячего резервирования SCADA TRACE MODE. Данные меры образуют второй текущий уровень полноты для практики «Поддержание непрерывной работы и восстановление». Поддержание непрерывной работы учитывает особенности производственного процесса, следовательно, имеет второй уровень специфики.

Для наглядности получившийся текущий профиль был представлен графически (рис. 2).

Завершающим этапом работы стало построение графика сравнения двух профилей (рис. 3), это и есть модель зрелости.

Из построенной модели зрелости видно,

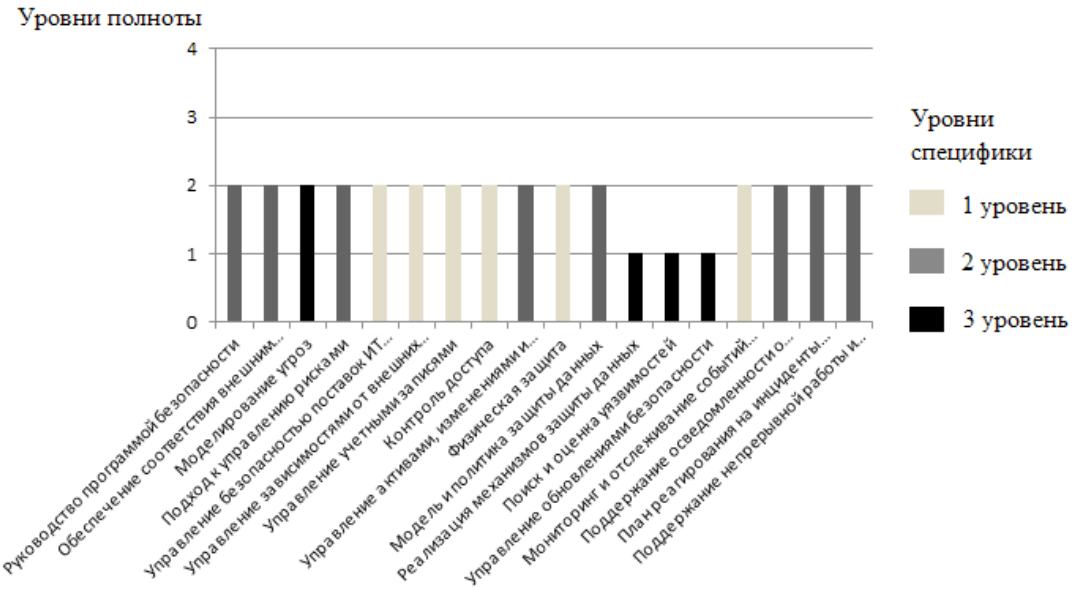


Рис. 2. Текущий профиль

Рис. 3. Модель зрелости

что критические разрывы имеют практики «Реализация механизмов защиты данных» и «Поиск и оценка уязвимостей», что свидетельствует о необходимости принятия кардинальных мер по модернизации данных направлений. Остальные восемнадцать практик разделились поровну: либо текущий уровень соответствует целевому, и от предприятия требуется лишь поддерживать защиту в ее текущем состоянии, либо имеется разрыв в один уровень и предприятию необходимо увеличить степень защиты в данном направлении. Если грамотно воспользоваться данной моделью, то она может стать эффективным инструментом в создании качественной системы защиты.

На основе модели зрелости любая компания может увидеть пробелы в своей системе защиты и эффективно закрыть подавляющее число уязвимостей. Данная работа может стать базой для проведения работ в сфере обеспечения информационной защиты на промышленных предприятиях, а также может быть легко адаптированадля обеспечения корпоративной защиты.

Литература

1. Борисов И.С. Обзор уровня зрелости процессов ИБ: о трендах и методологиях. Information Seecurity, 2019. – Режимдоступа: https://www.itsec.ru/articles/obzor-urovnya-zrelosti-protsessov-ib-o-trendakh-i-metodologiyakh.

2. Рудина Е.А., Гончаров Е.В. Модель зрелости безопасности интернета вещей: толчок к развитию безопасных систем. Kaspersky ICS CERT, 2019. – Режим доступа: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity/.

3. Рудина Е.А. Модель зрелости и безопасности IoT. Connect-WIT, 2019. – Режим доступа: https://www.connect-wit.ru/model-zrelosti-i-bezopasnosti-iot.html.

4. Баранкова И.И., Афанасьева М.В., Федорова А.Р. Модель зрелости безопасности АСУ ТП доменной печи №10 ПАО «ММК». Актуальные проблемы кибербезопасности, Вестник УрФО № 3(41), 2021, С. 57–64.

5. Баранкова И.И., Михайлова У.В., Афанасьева М.В., Афанасьев М.Ю. Принципы построения модели надежности системы защиты информации АСУ ТП доменной печи. Актуальные проблемы современной науки, техники и образования. Тезисы докладов 77-й Междун. Науч.-Технич. Конф. 2019. С. 424.

References

1. Borisov I.S. Obzor urovnja zrelosti processov IB: o trendah i metodologijah. Information Seecurity, 2019. – Rezhimdostupa: https://www.itsec.ru/articles/obzor-urovnya-zrelosti-protsessov-ib-o-trendakh-i-metodologiyakh.

2. Rudina E.A., Goncharov E.V. Model' zrelosti bezopasnosti interneta veshhej: tolchok k razvitiju

bezopasnyh sistem. Kaspersky ICS CERT, 2019. – Rezhim dostupa: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity/.

3. Rudina E.A. Model' zrelosti i bezopasnosti IoT. Connect-WIT, 2019. – Rezhim dostupa: https://www.connect-wit.ru/model-zrelosti-i-bezopasnosti-iot.html.

4. Barankova I.I., Afanas'eva M.V., Fedorova A.R. Model' zrelosti bezopasnosti ASU TP domennoj pechi №10 PAO «MMK». Aktual'nye problemy kiberbezopasnosti, Vestnik UrFO № 3(41), 2021, S. 57–64.

5. Barankova I.I., Mihajlova U.V., Afanas'eva M.V., Afanas'ev M.Ju. Principy postroenija modeli nadezhnosti sistemy zashhity informacii ASU TP domennoj pechi. Aktual'nye problemy sovremennoj nauki, tehniki i obrazovanija. Tezisy dokladov 77-j Mezhdun. Nauch.-Tehnich. Konf. 2019. S. 424.

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

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

ДЕГТЯРЕВА Алена Владимировна, студент кафедры информатики и информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: alenastudy5@yandex.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Associate Professor, Head of the Department of computer science and information security, Nosov Magnitogorsk State Technical University.455000, Magnitogorsk, LeninAve., 38. E-mail: inna_barankova@mail.ru

AFANASYEVA Margarita Vladimirovna, Assistant Professor of the Department of computer science and information security, Nosov Magnitogorsk State Technical University.455000, Magnitogorsk, Lenin Ave., 38. E-mail: nansy_stokli@mail.ru

DEGTYAREVA Alena Vladimirovna, student of the Department of computer science and information security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: alenastudy5@yandex.ru

Вестник УрФО № 2(44) / 2022, с. 63–69

DOI: 10.14529/secur220209

Ghadeer Darwesh, Jaafar Hammoud, Vorobeva A.A.

SECURITY IN KUBERNETES: BEST PRACTICES AND SECURITY ANALYSIS

Kubernetes emerged as docker containers' most popular orchestration, it is widely used for developing microservices and deploying applications. Because of advancements in containerization technology, information technology organizations use Kubernetes to manage their systems and report benefits in the deployment process. However, security concerns have been highlighted as challenges in Kubernetes deployment, The hackers can exploit the security vulnerabilities to cause damage to company assets. This work will shed the light on the Kubernetes orchestration platform and how attacks can be contacted against subevents manifest. we also demonstrate 10 security best practices in the Kubernetes cluster based on practitioners' reports, which we should follow to help protect our infrastructure.

Keywords: *Kubernetes, security, security policies, security practices, container security.*

Introduction

In recent years, microservices architecture has become more important and helped increase the software agility, containers emerged as the standard to deploy applications and microservices to the cloud. Nowadays this architecture is used by a big number of organizations to deliver their software such as Amazon, Netflix, Twitter, and other [1]. Kubernetes is an open-source software system used in microservices architecture such as cloud computing, the Internet of Things (IoT), and AI workflow. It has emerged as the most popular platform to manage the docker container life cycle and automate the management of computerized services.

From the viewpoint of cybersecurity, the Kubernetes system still has its own security challenges, and the users reported their concerns related to Kubernetes security. This work aims to explain potential exploits in the Kubernetes cluster and help users in securing their Kubernetes installation and deployment platform related to Kubernetes security best practices.

Section 2 states the background of this work and some important explanations related to it. Section 3 explains the threats and most recent security challenges in the Kubernetes system. In the last section, we present the Kubernetes security best practices for securing the Kubernetes deployment environment.

Backend

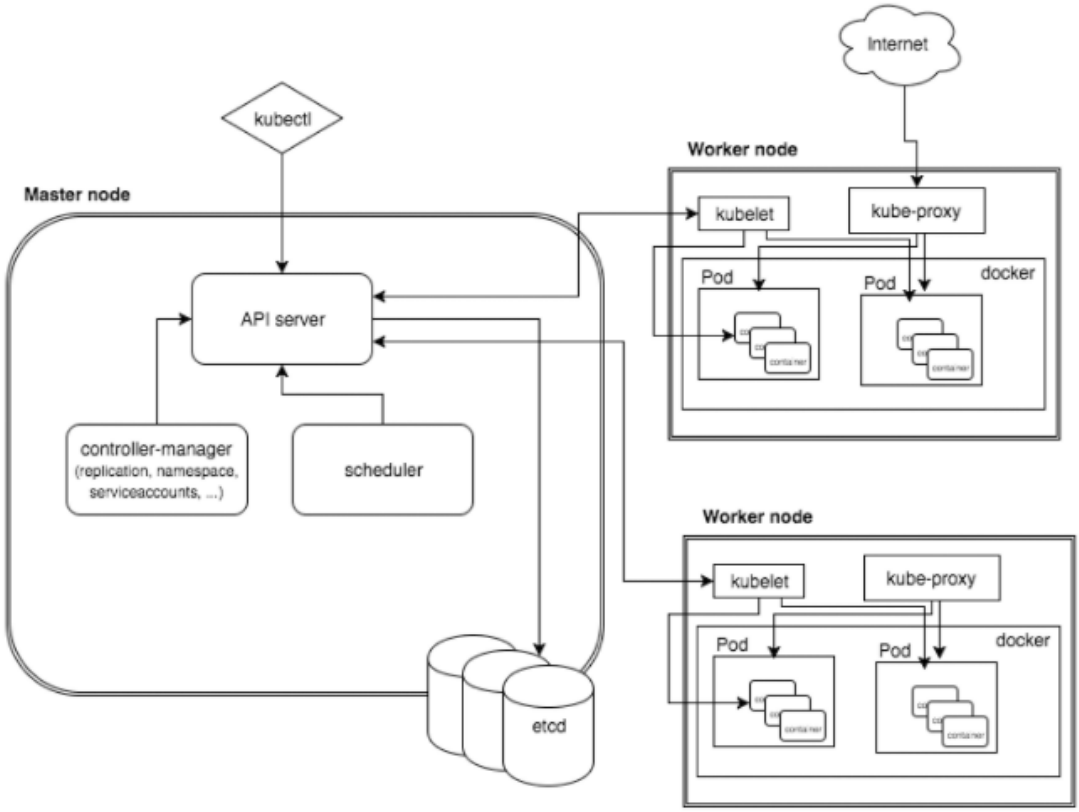
Kubernetes, at its fundamental level, maybe a framework for running and planning containerized applications over a cluster of machines. It disposes of most of the existing manual forms, which include the scaling, deploying, and managing of containerized applications [2]. Furthermore, based on utilization Kubernetes can scale the services up or down, ensuring we're only running what we would, like after we require it, wherever we need it. Like containers, Kubernetes permits us to oversee clusters, empowering the setup to be form controlled and replicated.

For a certain working scale, it gets to be fundamental to design our applications as a distributed system. Kubernetes is planned to supply the infrastructural layer for such desired systems, yielding clean applications to construct applications on top of a cluster [3]. More particularly, Kubernetes gives an interface to connect and manage this cluster such simply without needing to communicate individually with each machine.

Kubernetes follows the architecture of client-server architecture. It's conceivable to have a multi-master setup, but by default, there's a single master which acts as a controller and

point of contact [4]. The master server comprises different components counting a Kube-apiserver, an etcd, a Kube-controller-manager, a cloud-controller-manager, a kube-scheduler, and a DNS server for Kubernetes services. Node components incorporate kubelet and kube-proxy on top of Docker.

The Kubernetes master controls and



facilitates all nodes within the cluster with the assistance of three components that run on one or more master nodes within the cluster. Each Kubernetes master in our cluster runs these three processes:

1. Kube-apiserver: the single point of administration for the whole cluster. The API server implements a RESTful interface to communicate with tools and libraries. The kubectl command interacts directly with the API server.

2. Kube-controller-manager: controls the state of the cluster by managing all different kinds of controllers.

3. Kube-scheduler: schedules and plans the workloads across the nodes available in the cluster.

The entities state within the system is presented by Kubernetes Objects at any given point in time. Kubernetes Objects too act as an extra layer of abstraction over the container interface. We will presently specifically connect with instances of Kubernetes Objects rather than connection with containers. The fundamental Kubernetes objects are as follows:

Pod is the littlest deployable unit on the nodes. It's a bunch of containers that must run together. Very regularly, but not fundamentally, the pod contains one container.

Service is used to characterize a logical set of Pods and related policies utilized to access them.

Volume is basically a directory accessible to all containers running in a Pod. Namespaces are virtual clusters supported by the physical cluster.

Kubernetes security

Kubernetes workloads are vulnerable to several types of security threats, including:

• Compromise of the control plane—basic components like the API Server and etcd are not enough secured by default. The attacker gaining access to a Kubernetes master node can get control of the entire cluster.

• Compromise of pods and nodes—an attacker can get access to a physical host running Kubernetes pods, or to the individual

pods, enabling exfiltration of data within the pods.

• Compromise of network connections—pods and containers may be able to freely connect to each other and could be exposed to the public Internet. Any such open connections are an entry point for the attacker.

• Compromise of containers—containers can become vulnerable, due to a vulnerability or misconfiguration, or a backdoor in the container image. Containers with excess privileges can allow attackers access to the physical host.

Kubernetes security is imperative throughout the container lifecycle due to the dispersed, dynamic nature of a Kubernetes cluster. Distinctive security approaches are required for each of the three stages of an application lifecycle: build, deploy, and runtime. Kubernetes gives intrinsic security advantages. For case, application containers are regularly not fixed or updated — instead, container images are replaced totally with new versions. This enables strict version control and grants fast rollbacks in case a vulnerability is revealed in new code.

Despite the detailed benefits, recent studies show that security is one of the essential concerns for practitioners[5]. The study result from the StackRox [9] suggests that more than 44% of organizations delay their deployment for security concerns. The result moreover illustrates that 94% of the organizations have confronted at least one security occurrence within the final 12 months, among which 69% of security issues are misconfiguration-related [6]. The Cloud Computing (CNCF) study [6] result appears that 32% of practitioners among 1,324 overview members consider that security is their essential challenge in Kubernetes. Recent occurrences of security breaches give the authenticity of the professionals' concern.

According to the security risks characterized in NIST SP-800-190, most of the security solutions are appropriate for image pretest and also for operating system and network layer discovery within the host [7]. For protection against network attacks, we can introduce IPS, IDS, and web application firewalls within the network layer. In the operating system layer, we can install an antivirus program and host IDS for assurance against malware attacks. As there are numerous services on a single host in the runtime container environment, inner activities or anomalous behavior for each container cannot be followed by previous security solutions; only external communication attacks may be identified. This limits the ability to recognize containers that are subject to hacking attacks.

Related work

To collect our Internet artifacts. We use the Google search engine with 3 search strings: "Kubernetes security" 'Kubernetes security best practices, 'Kubernetes security policies".

[8] explored the availability of Kubernetes using a set of tests, and detailed that service outages can happen frequently. Shah and Dubaria [9] compared management features of Kubernetes, Docker Swarm, and Google Cloud Platform, and watched Kubernetes provide features, such as monitoring, deployment, and easy scalability. Takahashi etal Burns et al. [10] described the advancement of container management systems at Google and described how two internal systems called Omega and Borg evolved into Kubernetes.

Container security: SANS12 presented several tools for container security. For example, AppArmor13 was introduced as a policy-based Linux kernel security module that helps system administrators restrict process capabilities, such as file read/write permissions or network access, through their own security profiles[7].

[11] proposed a Kubernetes portable load balancer and detailed improved portability without sacrificing performance. Song et al. [12] constructed an auto-scaling system for API gateways using Kubernetes. The authors [12] reported that their constructed system could improve the utilization of system resources and ensure high availability. Muralidharan et al. [12] presented a Kubernetes-based system to manage and monitor Internet of Things (IoT) applications for smart cities.

reviewer [13]introduced a case study on Kubernetes and talked about how key concepts of Kubernetes can be utilized to streamline the scaling of containers. Medel et al. [14] collected real data from Kubernetes and used it to apply formal modeling to characterize resource management in Kubernetes. Chang et al. [15] presented a monitoring platform that uses Kubernetes to dynamically provision cloud resources.

KUBERNETES SECURITY PRACTICES

In this section we describe 10 Kubernetes security best practices reported by practitioners that can take enterprise security to the next level:

Authentication and Authorization Role-Based Access Control (RBAC) [9]

Authentication in Kubernetes alludes to the

verification of API requests through authentication plugins [16]. Authorization refers to the assessment of each authenticated API request against all policies to permit or deny the request [16].

One of these available plugins is the role-based access control (RBAC) plugin which allows the customer to control who can access the Kubernetes API and what permissions they have [17].

Practitioners have detailed a set of tasks to actualize the practice of authentication and authorization:

• In case we upgraded from a very old Kubernetes release and had not enabled RBAC earlier, RBAC settings should be checked to make sure they are enabled.

• Anonymous access to the Kubernetes server ought to be disabled. By default, Kubernetes permits anonymous get to the Kubernetes API server. [16] For case, a malicious user can figure out the default configuration of an insecure admission, gain access to the admission controller, and execute malicious commands.

• We should moreover manage the authorization approaches and utilize them properly. We use RBAC to limit groups and clients to just the activities and tasks they may need.

• Admission controller is a tool that intercepts requests to the Kubernetes API after the request is authorized, and before a volume is made persistent. Admission controllers have to be enabled and default authorization modes have to be disabled.

• We also should continuously follow the principle of least privilege to guarantee that users and Kubernetes service accounts have the minimal set of privileges required and make sure to not provide clusterwide authorizations, and don't deliver anybody cluster admin privileges unless completely necessary.

Private Kubernetes API Endpoint

Kubernetes cluster admins and operators can configure the Kubernetes API endpoint of a cluster as part of a public or private subnet. In the private cluster, the API server (endpoint) inside the control plane has a private IP address that makes the master blocked off from the public internet. In expansion to private worker nodes, we should make sure to configure the Kubernetes API endpoint as a private endpoint.

Kubernetes-specific Security Policies

Network policies Containerized applications generally make utilize cluster networks. We watch active network activity and compare it to the traffic permitted by Kubernetes network policy, to recognize how our application interacts and identify anomalous communications. By default, all Kubernetes pods have the ability to communicate with other pods. Practitioners suggest approaches to reduce network exposure, restrict traffic between pods, and restrict API server access to secure the network. In case firewalls are not set and network policies are not defined, at that point anybody may attack the API server from any IP address.

Pod-specific policies: It's recommended to apply security context to pods and containers. Pod policies define how the workloads should run in the Kubernetes cluster. Implementing workloads without defining a secure context for pods can make the Kubernetes cluster vulnerable, where a container can run with root privilege and write permission into the root file system. Practitioners also recommend that containers inside a pod must run as a non-root user with enabling Linux security modules and read-only permission.

Audit Logging Monitor Network Traffic to Limit Communications

It is recommended to enable audit logging and save audit logs to a secure repository to analyze the event of a compromise. Kubernetes moreover gives cluster-based logging to record container activity into a central logging subsystem. The standard output and error output of each container in a Kubernetes cluster can be ingested using an agent like Fluentd running on each node into tools like Elasticsearch and seen with Kibana. And at last, monitor pods, containers, services, and other components of our cluster using tools such as Prometheus and Grafana for monitoring, visibility, and following our cluster's state.

Namespace separation

A 'namespace' in Kubernetes is a logically isolated virtual cluster inside the physical cluster. [16] The creation of namespaces enables resources to be isolated between namespaces. Practitioners suggest that each group in a company should have a separate namespace for better manageability and running its production and development and environments.

Isolate Kubernetes Nodes

In addition to OS security, it is recommended that nodes are on a private network and not accessible from outside. A gateway may be

configured to get other services outside the cluster network, if required network ports to access nodes should be controlled via access lists. It is additionally recommended to restrict Secure Shell (SSH) access to the nodes.

Keep Kubernetes Version Up to Date

We should always update our cluster and run the most recent version of Kubernetes. This helps us to keep updated with all new security patches and Kubernetes updates. Upgrading Kubernetes can be a complex process case we're using a hosted Kubernetes provider.

Encrypt and restrict access to etcd

Etcd stores the state of the cluster and its secrets, so it is a sensitive asset and an attractive target for attackers. If unauthorized users could access the etcd, they can take over the whole cluster. Read access is additionally dangerous since malicious users can utilize it to elevate privileges.

The security practice is to encrypt the etcd storage. Encryption is important for securing etcd, and it's not enabled by default. We can enable it via kube-apiserver process, bypassing the argument "–encryption-provider-config" within the configuration, we need to select a provider to perform encryption and define our secret keys. [17]. Practitioners recommend restricting access to 'etcd', to only be available from the API servers, and isolated behind a firewall.

Limit CPU and memory quota

If a malicious user begins a denial of service (DOS) attack within a pod inside the Kubernetes cluster at that point, due to a high volume of requests, Kube-scheduler will create a new pod and an instance of the container will begin inside the new pod. This process proceeds until it consumes all available CPU resources and memory leaving all the applications in starvation. Practitioners recommend defining the number of resources by defining the maximum amount of memory for a namespace or a pod, the number of CPU shares for an application to consume, and the maximum number of instances for a container.

Enable SSL/TLS support

Practitioners suggest enabling TLS and SSL certificates for Kubernetes components. Enabling transport layer security (TLS) or secure sockets layer (SSL) protocol to ensure secure and encrypted communication between Kubernetes components.

Conclusion and future work

Over the years, containerization has steadily appeared its potential edges in the market. Developers use container innovation and serverless computing to solve various real-world challenges, such as VM's auto-scaling, performance loss issues, optimizing fetched, stack adjusting, and numerous others. Kubernetes is getting to be an attractive choice for keeping up containers for practitioners and organizations. Securing the Kubernetes system requires more consideration as default configurations of Kubernetes are frequently unreliable and insecure. Our paper appears that secure and effective utilization of Kubernetes requires the implementation of security practices applicable for numerous components inside the Kubernetes establishments: pods, containers, 'etcd' database, etc. This work helps practitioners to secure their Kubernetes installations system. Further, our current findings can lay the basis for conducting research in Kubernetes security.

References

1. Sultan S., Ahmad I., Dimitriou T. Container security: Issues, challenges, and the road ahead // IEEE Access. 2019. T. 7. C. 52976–52996.

2. Hightower K., Burns B., Beda J. Kubernetes: Up and running: Dive into the future of Infrastructure. Beijing, China: O'reilly, 2017.

3. Mondal S.K. и др. Kubernetes in it administration and Serverless Computing: An empirical study and research challenges // The Journal of Supercomputing. 2021. T. 78. № 2. C. 2937–2987.

4. Zhu H., Gehrmann C. Kub-SEC, an automatic Kubernetes Cluster APPARMOR Profile Generation Engine // 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS). 2022. C. 129–137.

5. Shamim S.I. Mitigating security attacks in Kubernetes manifests for security best practices violation // Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2021. C. 1689–1690.

6. 94% of organizations have suffered insider data breaches, egress research reveals [Электронный

ресурс]. URL: https://www.businesswire.com/news/home/20210713005123/en/94-Of-Organizations-Have-Suffered-Insider-Data-Breaches-Egress-Research-Reveals (дата обращения: 05.06.2022).

7. Tien C.W. и др. Kubanomaly: Anomaly Detection for the Docker orchestration platform with neural network approaches // Engineering Reports. 2019. Т. 1. № 5.

8. Abdollahi Vayghan L. и др. Deploying microservice based applications with Kubernetes: Experiments and Lessons Learned // 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). 2018. С. 970–973.

9. Shah J., Dubaria D. Building modern clouds: Using Docker, Kubernetes & Google Cloud Platform // 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). 2019. С. 184–189.

10. Burns B. и др. Borg, Omega, and kubernetes // Queue. 2016. Т. 14. № 1. С. 70–93.

11. Aida K., Tanjo T., Sun J. A portable load balancer for kubernetes cluster // Proceedings of the International Conference on High Performance Computing in Asia-Pacific Region. 2018. С. 222–231.

12. Song M., Zhang C., Haihong E. An auto scaling system for API gateway based on Kubernetes // 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS). 2018. С. 109–112.

13. Brewer E.A. Kubernetes and the path to cloud native // Proceedings of the Sixth ACM Symposium on Cloud Computing. 2015. С. 167–167.

14. Medel V. и др. Modelling Performance & Resource Management in Kubernetes // Proceedings of the 9th International Conference on Utility and Cloud Computing. 2016. С. 257–262.

15. Chang C.-C. и др. A Kubernetes-based monitoring platform for Dynamic Cloud Resource Provisioning // GLOBECOM 2017 - 2017 IEEE Global Communications Conference. 2017. С. 1–6.

16. Kubernetes Documentation [Электронный ресурс]. URL: https://kubernetes.io/docs/home/ (дата обращения: 05.06.2022).

17. Islam Shamim M.S., Ahamed Bhuiyan F., Rahman A. Xi commandments of Kubernetes Security: A systematization of knowledge related to Kubernetes Security Practices // 2020 IEEE Secure Development (SecDev). 2020. С. 58–64.

Ghadeer Darwesh, Ph.D. Student ITMO. Kronverksky pr., 49, St. Petersburg, Russia,197101. E-mail: ghadeerdarwesh32@gmail.com

Jaafar Hammoud, Ph.D. Student ITMO. St. Petersburg, Kronverksky pr., 49, St. Petersburg, Russia, 197101. E-mail: hammoudgj@gmail.com

VOROBEVA Alisa Andreevna, Associate professor ITMO. Kronverksky pr., 49, St. Petersburg, Russia, 197101. E-mail: alice_w@mail.ru

УДК 004.42 + 004.49 + 004.056

Гадир Дарвеш, Джафар Хаммуд, Воробьева А.А.

БЕЗОПАСНОСТЬ В ПЛАТФОРМЕ KUBERNETES: РЕКОМЕНДАЦИИ И АНАЛИЗ БЕЗОПАСНОСТИ

Платформа Kubernetes появилась как самая популярная оркестровка контейнеров Docker и широко используется для разработки микросервисов и развертывания приложений. Благодаря усовершенствованию технологии контейнеризации, организации в сфере информационных технологий применяют платформу Kubernetes для управления своими системами и создания отчетов о положительных эффектах в процессе развертывания. Однако специалисты обращают внимание на возможные проблемы обеспечения безопасности при развертывании с использованием платформы Kubernetes. Хакеры могут воспользоваться уязвимыми местами системы безопасности, чтобы нанести вред активам компании. Данная работа прольет свет на платформу оркестровки Kubernetes и на то, как проявляются атаки на подсобытия и как справляться с ними. Мы также приводим основанные на отчетах практикующих специалистов 10 рекомендаций по безопасности для кластера платформы Kubernetes, которые следует соблюдать для обеспечения защиты инфраструктуры.

Ключевые слова: *платформа Kubernetes, безопасность, правила разграничения доступа, рекомендации по безопасности, безопасность контейнера.*

Гадир Дарвеш, аспирант Университета ИТМО. Кронверкский пр., 49, Санкт-Петербург, Россия, 197101. Электронная почта: ghadeerdarwesh32@gmail.com

Джафар Хаммуд, аспирант Университета ИТМО. Санкт-Петербург, Кронверкский пр., 49, Санкт-Петербург, Россия, 197101. Электронная почта: hammoudgj@gmail.com

ВОРОБЬЕВА Алиса Андреевна, доцент Университета ИТМО. Кронверкский пр., 49, Санкт-Петербург, Россия, 197101. Электронная почта: alice_w@mail.ru

УДК 004.588 Вестник УрФО № 2(44) / 2022, с. 70–79

Астахова Л.В., Волегов Н.В.

DOI: 10.14529/secur220210

ДИНАМИКА ПОРТРЕТА ВНУТРЕННЕГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Инциденты информационной безопасности по вине внутреннего нарушителя обладают мощным разрушительным потенциалом. Последствия случайных ошибок или злонамеренных действий персонала могут проявляться не только в имущественных или репутационных потерях, но и в приостановке или ликвидации бизнеса как такового. Внутренний нарушитель не остается неизменным, вектор его действий меняется в связи с социокультурными трансформациями, развитием технологий организации информационных систем компаний, изменением локальных проблем объекта. Цель статьи – выявить изменения характеристик внутреннего нарушителя информационной безопасности организации за последние годы, их обусловленность. С помощью сравнительного анализа экспертных оценок за 2016-2021 годы в статье выявлены некоторые тенденции, которые наиболее ярко отражают динамику характеристик внутреннего нарушителя безопасности информационной системы: снижение утечек по вине внутреннего нарушителя в связи с распространением заболевания COVID-19; рост числа умышленных внутренних утечек защищаемой информации; стабильное доминирование случайных утечек персональных данных, по сравнению с умышленными, их медленное снижение; рост числа утечек по вине подрядчиков. Показаны возможные причины возникновения названных тенденций и некоторые пути решения проблем. Обоснована необходимость расширения критериев оценки внутренних нарушителей за счет мотивационных факторов, что позволит существенно повысить прагматическую ценность статистических экспертно-аналитических отчетов для практики защиты информации в организациях.

Ключевые слова: *внутренний нарушитель, информационная безопасность, организация, человеческие риски, критерии оценки, осведомленность, вовлеченность.*

DYNAMICS OF INTERNAL INTERVENTOR PORTRAIT INFORMATION SECURITY OF THE ORGANIZATION

Information security incidents due to the fault of an insider have a powerful destructive potential. The consequences of accidental errors or malicious actions of personnel can manifest themselves not only in property or reputational losses, but also in the suspension or liquidation of the business as such. An insider does not remain unchanged, the vector of his actions changes in connection with socio-cultural transformations, the development of technologies for organizing information systems of companies, and changes in the local problems of the object. The purpose of the article is to identify changes in the characteristics of an internal violator of the information security of an organization in recent years, their conditionality. Using a comparative analysis of expert assessments for 2016-2021, the article reveals some trends that most clearly reflect the dynamics of the characteristics of an internal violator of information system security: a decrease in leaks due to the fault of an internal violator due to the spread of COVID-19 disease; an increase in the number of intentional internal leaks of protected information; stable dominance of accidental leaks of personal data, compared with intentional ones, their slow decline; an increase in the number of accidental leaks of state secrets; an increase in the number of leaks caused by contractors. Possible causes of these trends and some ways to solve problems are shown. The necessity of expanding the criteria for assessing insiders due to motivational factors is substantiated, which will significantly increase the pragmatic value of statistical expert-analytical reports for the practice of information security in organizations.

Keywords: *insider, information security, organization, human risks, evaluation criteria, awareness, involvement.*

Введение. На протяжении длительного периода наблюдений в корпоративных информационных системах обнаруживается множество опасных уязвимостей, связанных с внутренними нарушителями информационной безопасности (ИБ). Их реализация приводит к существенным финансовым и репутационным потерям организации. Большое влияние на портрет внутреннего нарушителя не могут не оказывать социально-культурные трансформации общества, изменения в отрасли ИБ. Этим обусловлена цель статьи – выявить изменения характеристик внутреннего нарушителя информационной безопасности организации в условиях социально-культурной эволюции последнего времени, обосновать их причины и показать императивы управления организационным поведением сотрудников для предотвращения инцидентов ИБ по их вине.

Современные тенденции изменений характеристик внутреннего нарушителя. Нарушитель информационной безопасности организации (нарушитель)– физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации [1, п. 3.3.5]. Внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей [2, п.5.1.6]. При оценке возможностей внутренних нарушителей необходимо учитывать принимаемые оператором орга-

низационные меры по допуску субъектов к работе в информационной системе. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационной системе и ее компонентам, а также мер по контролю за доступом и работой этих лиц. Внутренний нарушитель может действовать как умышленно (преднамеренно), так и нет (неумышленно, непреднамеренно).

Результаты анализа ежегодных исследований российских и зарубежных аналитических центров свидетельствуют о том, что количество инцидентов ИБ по вине внутренних нарушителей не является неизменным. Так, мониторинг ежегодных отчетов Экспертно-аналитического центра компании InfoWatch за 2016-2021 годы позволил нам выявить динамику внутренних утечек, которую мы представили в графическом виде на рис. 1.

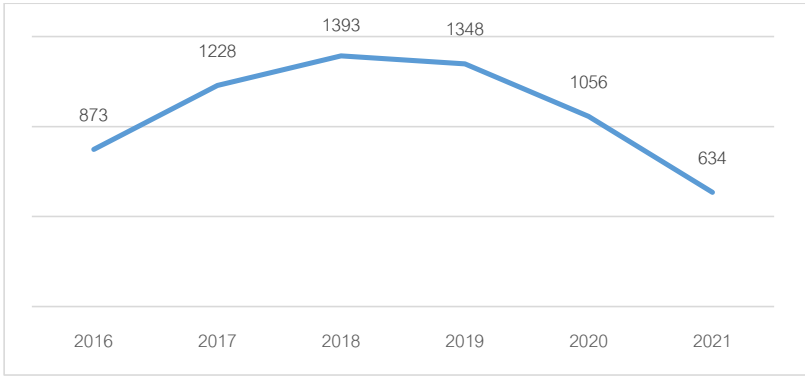


Рис. 1. Динамика утечек информации по вине внутреннего нарушителя информационной безопасности за 2016-2021 гг

Как видим, рост числа внутренних утечек, зафиксированный в 2016-2018 годах, в 2019 году сменился снижением. В 2020-2021 годах мы наблюдаем дальнейшее снижение числа утечек, т.к. в 2021 году утечки снизились на 53% по сравнению с 2019. В результате умышленных и случайных действий внутренних нарушителей произошло 36,8% утечек в 2021 г. и 47,1% в 2020 г. Если в 2018 г. на долю внутренних нарушителей пришлось примерно 2/3 случаев, то по итогам 2021 г. картина получилась практически зеркальной – почти в 2/3 всех внесенных опубликованных (ставших известными) утечек информации ограниченного доступа в качестве виновников указаны внешние нарушители. По мнению экспертов, большую роль сыграло распространение удаленной работы в период пандемии, когда контроль за сотрудниками оказался сильно затруднен. Недобросовестные работники могли незаметно похищать информацию, большой пласт случайных нарушений также мог остаться незамеченным [3]. Неуклонный рост доли числа внешних утечек, по сравнению с внутренними, эксперты связывают также: со становлением широкого спектра хакерских группировок; повышением доступности вредоносного ПО; вступлением сотрудников в сговор с хакерами; ошибками сотрудников, которые привели к раскрытию аутентификационной информации, которой воспользовались внешние нарушители; сокрытием информации о внутренних нарушителях и пробелах в организации безопасной удалённой работы и защитой своего имиджа и невозможностью перепроверить результаты их отчётов.

Интересен вопрос отношения количества умышленных утечек к случайным. В 2020 и 2021 году доля умышленных нарушений среди утечек внутреннего характера (по вине персонала) составляет более 51%. При этом доля умышленных нарушений внутреннего характера в мире растет: если в 2018 году это было 35,3%, то в 2021 – уже 51,8%. Ликвидность конфиденциальной информации становится все выше, что позволяет внутренним злоумышленникам ее монетизировать.

Главным объектом внимания внутренних нарушителей в течение 2016-2021 гг. стабильно являются персональные данные, о чем свидетельствует построенная диаграмма (Рис.2).

Очевидно, что ежегодно с 2016 года утечки персональных данных весьма сильно доминируют над утечками других видов данных. Интерес к платежной информации становится меньше, но тенденция роста наблюдается к коммерческой тайне.

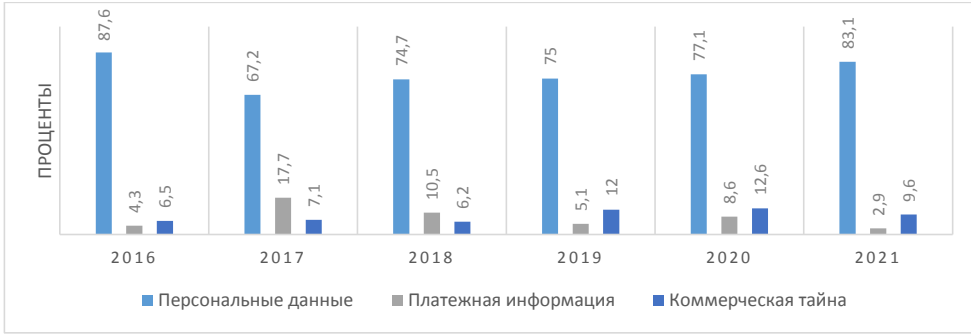


Рис. 2. Распределение внутренних утечек по типу данных за 2016-2021 гг

Проведя сравнительный анализ экспертных исследований за разные годы [3], [4] и [5], мы пришли к выводу, что причины утечек разных видов данных существенно разнятся. Так, если в 2017-208 годах наблюдалось больше случайных утечек платежной информации, то с 2019 года доминируют умышленные утечки (рис. 3).

Полагаем, что внимание к повышению осведомленности сотрудников финансовых подразделений организаций принесло определенные плоды.

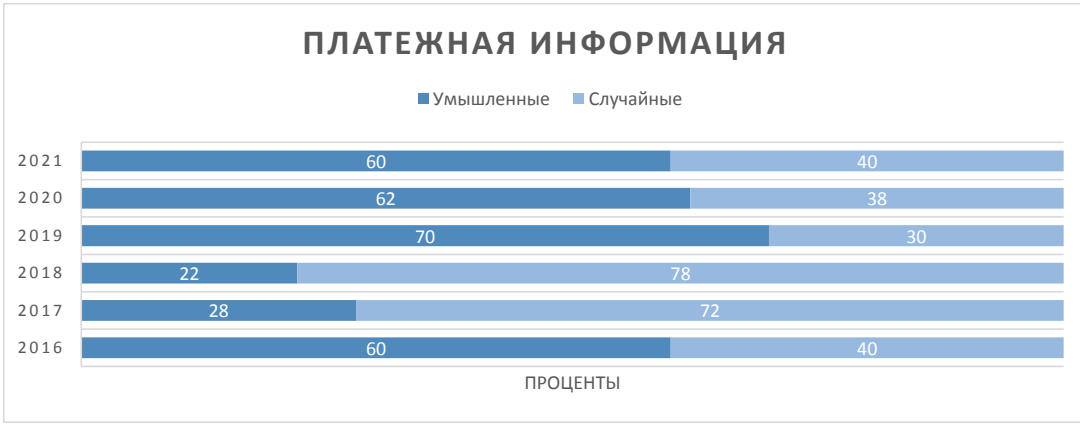


Рис. 3. Распределение утечек платежной информации по умышленным и случайным

Этого нельзя сказать о персональных данных, их случайные утечки стабильно доминируют с 2016 года (рис. 4).

Это говорит о том, что далеко не все сотрудники организации, допущенные к обработке персональных данных в организации, столь же осведомлены о правилах ИБ и ответственны в процессе выполнения своих долж-

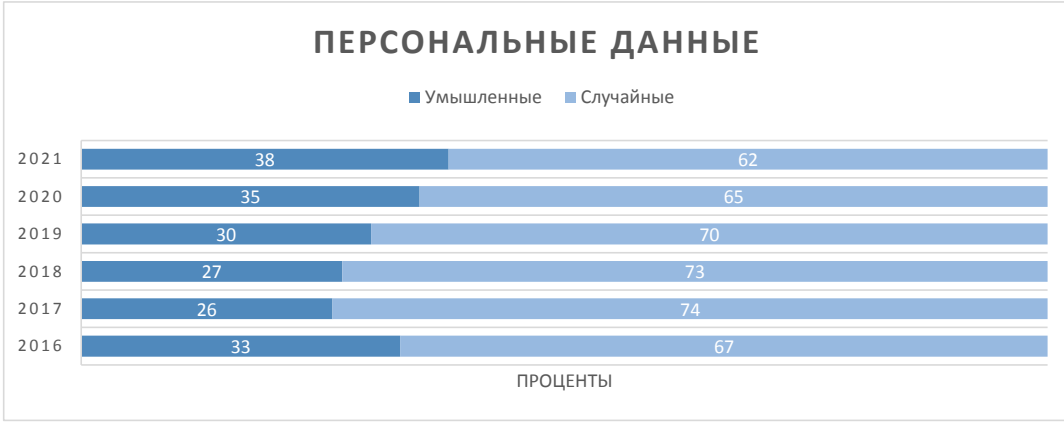


Рис. 4. Распределение утечек персональных данных по умышленным и случайным

ностных обязанностей. Процесс повышения осведомленности идет медленно, хотя при этом и наблюдается небольшое плавное снижение случайных утечек.

Анализ отчетов InfoWatch [3], [4] и [5] позволил нам конкретизировать типы внутреннего нарушителя. Результаты анализа приведены на рис. 5.

Рис. 5. Распределение внутренних утечек по виновнику

Из диаграммы видно, что лидером по нарушениям является рядовой сотрудник, поэтому из года в год актуальным остается проблема осведомленности и инструктаж персонала. К сожалению, по-прежнему во многих компаниях у руководства не находится времени или желания повышать осведомленность сотрудника или делать выбор сотрудников более тщательным на этапе их приема на работу. На втором месте по инцидентам ИБ из числа внутренних нарушителей находятся лица из числа персонала подрядных организаций, осуществляющих обработку информации ограниченного доступа по заданию коммерческой компании или государственной организации и допустивших утечку такой информации (в период действия контракта). Мало кто говорит про действия подрядных организаций, в основном внимание уходит на рядовых сотрудников и хакеров. Уделять внимание выбору подрядчика и его осведомленности об ИБ в процессе деятельности на объекте также важно, как и работа с рядовым сотрудником. С 2017 года усиливается тенденция роста утечек по вине руководителя, а также уменьшения числа утечек по вине системного администратора.

К сожалению, экспертные отчеты участников мирового аналитического рынка не содержат оценки характеристик внутренних нарушителей по социально-демографическим и психологическим критериям, без которых невозможно понять динамику их портрета под воздействием тех или иных мотивационных факторов.

Поэтому статистическая информация может быть дополняться результатами исследований, проводимых с помощью DLP-систем. Так, исследование «Ростелеком-Солар», направленное на создание типичного портрета сотрудника-нарушителя, проводилось с помощью DLP-системы SolarDozor и модуля анализа поведения с 2018 по 2020 год в 150 российских организациях в 20 отраслях и направлениях деятельности с различной численностью сотрудников [6, 7].

Результаты исследования по ряду аспектов характеристики внутренних нарушителей представим в виде круговых диаграмм (рис. 6 и 7). 55% всех нарушителей – это мужчины, 58% – до 40 лет (рис. 6), 46% имеют стаж выше 5 лет (рис. 6).

При этом нарушители мужского пола молодого возраста подрабатывают в основное рабочее время, женского – рассылают резюме, публикуют их на сервисах по поиску работы. 26% нарушений приходится на сотрудников в возрасте 40–50 лет. Мужчины этого возраста используют много рабочего времени для посещения развлекательных ресурсов, а женщины - так же занимаются поиском новой работы. Кроме того, нарушители-женщины пересылают данные (в том числе личные и данные об оплате труда в организации) на внешние почтовые адреса. Эту особенность эксперты объясняют тем, что в бухгалтериях и отделах кадров (т.е. в подразделениях, где хранится эта информация), в России традиционно работают в основном женщины.

К сожалению, эксперты не предпринима-

Рис. 6. Распределение увольнений в связи с инцидентами по возрасту

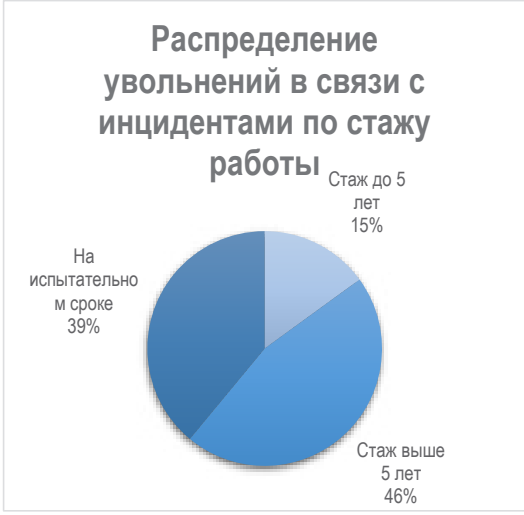


Рис. 7. Распределение увольнений в связи с инцидентами по стажу работы

ют более детального статистического анализа - мотивации внутреннего нарушителя ИБ организации, что существенно тормозит процессы мониторинга динамики его характеристик. Между тем, мотивы неправомерного поведения играют жизненно важную роль в области внутренних угроз информационной безопасности, и выявление мотивационных факторов и их классификация могут помочь руководству контролировать и уменьшить внутренние угрозы в организациях. На это обращают внимание зарубежные и российские эксперты.

Согласно классической структуре угроз защищаемой информации причинами, вызывающими преднамеренное дестабилизирующее воздействие, могут быть: стремление получить материальную выгоду (подработать), нанести вред (отомстить) руководству или коллеге по работе, а иногда и государству, оказать бескорыстную услугу приятелю из конкурирующей фирмы, продвинуться по службе, обезопасить себя, родных и близких от угроз, шантажа, насилия или показать свою значимость. А предпосылками, способствующими появлению этих причин, как правило, бывают: тяжелое материальное положение, финансовые затруднения; корыстолюбие, алчность; склонность к развлечениям, пьянству, наркотикам; зависть, обида; политическое или научное инакомыслие; личные связи с представителями конкурента; недовольство служебным положением, карьеризм; трусость, страх; тщеславие, хвастовство и др. [8]. Иные предпосылки – отсутствие интереса к работе, недооценка своих возможностей и способностей, плохое отношение со стороны администрации и др. - у причин непреднамеренных воздействий сотрудников на защищаемую информацию, к которым относятся безответственность, недисциплинированность, болезнь, переутомление и т.д. Исследования зарубежных экспертов [9] и [10] также связаны с анализом общих признаков и предпосылок неправомерных воздействий внутренних нарушителей на защищаемую информацию.

На основе приведенных результатов анализа статистической информации и экспертных мнений мы можем очертить штрихи к примерному портрету современного внутреннего нарушителя ИБ. Им является мужчина до 40 лет, со стажем более 5 лет или же он находится на испытательном сроке. Его социальные связи внутри коллектива слабы, а плохая привязанность к компании подталкивает его к поиску новой работы или нецелесообразному использованию времени на рабочем месте, у него нет достижений, плохая репутация, а его личностные нормы не соответствуют общепринятым в компании. Его должность относится к той, которая не подразумевает ответственности за обеспечение безопасности объекта, а значит – потенциальный нарушитель не заинтересован в противодействии утечкам, его заработная плата не зависит от количества утечек в организации. Это увеличивает вероятность как умышленных, так и неумышленных воздействий на защищаемую информацию. Названные характеристики внутреннего нарушителя под-

тверждаются приведенными выше статистическими данными: слабая привязанность сотрудника к компании-работодателю и нахождение сотрудника на должности, которая не предполагает заинтересованности в информационной безопасности объекта. К числу таких сотрудников-нарушителей относятся: новый работник в компании, работник, собирающийся увольняться, или работник из подрядной организации. Все эти типы входят в тройку тех сотрудников, из-за которых чаще всего возникают утечки. Должности такого типа сотрудников не предполагают вовлеченности в обеспечение безопасности информационных систем.

Как видим, гуманитарная оценка портрета внутреннего нарушителя и выводы, полученные в процессе авторского статистического анализа утечек по его вине, совпадают. Данный вывод позволяет заключить, что руководство организации не может не обращать внимание на факторы внутренней и внешней среды, которые побуждают сотрудников к неправомерному поведению в области информационной безопасности. Поэтому все большее значение для снижения числа инцидентов ИБ организации по вине внутреннего нарушителя приобретает расширение критериев оценки анализа субъектов инцидентов ИБ за счет их гуманитарных характеристик. Тем более, что стремительное развитие российских и зарубежных DLP-систем дает возможность расширить количество этих критериев, формализовать их и включить в качестве объектов исследования экспертно-аналитических подразделений. Так, задачей, которую можно решить с помощью DLP-системы, является выявление групп риска — т. е. работников, имеющих склонности, увлечения, которые использованы для ведения или привлечения к незаконной деятельности, к деятельности в ущерб компании, её руководству или работникам [11]. Выявление признаков конфликта интересов также входит в перечень задач DLP-систем. По сути степень совпадения ценностей сотрудников с ценностями компании – это вовлеченность персонала. В это понятие входит позитивное психологическое состояние работника: энергичность, готовность приложить усилия при возникновении трудностей, преданность делу, вдохновение, гордость, полная концентрация на обязанностях [12]. Поскольку термин «вовлеченность» обладает «большей описательной силой и очевидной валидностью», именно его используют вместо таких терминов, как «удовлетворенность работой», «приверженность» и «мотивация» [13]. Вовлеченность сотрудника в работу организации является трендом современной практики работы с персоналом во всех отраслях деятельности и важнейшим фактором повышения осведомленности сотрудников об ИБ организации [14]. Кроме того, уже накоплен определенный опыт работы с данными ИБ-систем для оценки вовлеченности сотрудников [15]. Все это обусловливает необходимость в изменении подходов к статистическим аналитическим исследованиям в области информационной безопасности. Полагаем, что использование интегративной концепции внутренней угрозы (как возможности нарушения правил ИБ и мотивации внутреннего нарушителя в организации) позволит углубить содержание экспертно-аналитических отчетов по инцидентам ИБ в организациях различных типов и видов и усилить их эвристический и прогностический потенциал для практики защиты информации.

Вывод. Внутренние утечки обладают мощным разрушительным потенциалом. Последствия ошибок или злонамеренных действий персонала могут проявляться не только в имущественных или репутационных потерях, но и в приостановке или ликвидации бизнеса как такового. В определенные периоды наблюдаются изменения тенденций утечек по вине внутреннего нарушителя. Вектор его действий меняется в связи с внедрением новых технологий организации информационных систем компаний, динамикой локальных проблем объекта и др.

Анализ экспертных оценок за 2016-2021 годы позволил нам выявить несколько тенденций, которые наиболее ярко отражают динамику характеристик внутреннего нарушителя безопасности информационной системы. Снижение утечек по вине внутреннего нарушителя вызвано распространением заболевания COVID-19, переводом персонала в дистанционный режим работы, ограничением доступности физических каналов утечки (кража или утеря документов, взлом сейфов) и является временным явлением. Рост числа умышленных внутренних утечек защищаемой информации, вызванных взаимной неудовлетворенностью друг другом работодателя и работника, требует усиления самореализации и вовлеченности последнего в процесс реализации бизнес-целей организации. Ста-

бильное доминирование случайных утечек персональных данных, по сравнению с умышленными, их медленное снижение свидетельствует о необходимости повышения эффективности повышения осведомленности сотрудников об ИБ организации и культуры ее ИБ. Рост числа утечек по вине подрядчиков должен стимулировать работодателя тратить больше сил на повышение осведомленности этих категорий работников и правовые аспекты взаимодействия с ними.

Сам процесс выявления динамических характеристик внутреннего нарушителя – это процесс, требующий сегодня инновационных подходов. Развитие теоретических аспектов исследований внутреннего нарушителя, углубление факторного анализа его поведения, а также развитие инструментальных информационных технологий его мониторинга в организации – все это свидетельствует о необходимости изменения методологии создания статистических аналитических исследований в области информационной безопасности. Расширение критериев оценки внутренних нарушителей за счет мотивационных факторов позволит существенно повысить прагматическую ценность использования аналитических отчетов в практике защиты информации.

Литература

1. ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 N 532-ст). – URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 11.04.2022).

2. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 года. – URL: https://docs.cntd.ru/document/607699443?section=text (дата обращения: 11.04.2022).

3. Отчёт об исследовании утечек информации ограниченного доступа в 2021 году / Экспертно-аналитический центр InfoWatch. – 2022. – 32. с. – URL: https://www.infowatch.ru/analytics/analitika/v-2021-stalo-bolshe-umyshlennykh-utechek (дата обращения: 12.04.2022).

4. Исследование утечек информации ограниченного доступа в 2020 году / Экспертно-аналитический центр InfoWatch. – 2021. – 30. с. – URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2020-godu (дата обращения: 12.04.2022).

5. Утечки данных организаций по вине или неосторожности внутреннего нарушителя. Сравнительное исследование. 2013-2019 гг. / Экспертно-аналитический центр InfoWatch. – 2020 – 32. с. – URL: https://www.infowatch.ru/analytics/analitika/utechki-dannykh-po-vine-vnutrennego-narushitelya-2013-2019-gg (дата обращения: 12.04.2022).

6. Ростелеком-Солар. Кто он – типовой нарушитель в российской организации? 2018-2020 / Ростелеком-Солар. – 2021. – 12 с. – URL:https://rt-solar.ru/analytics/reports/2212/ (дата обращения: 12.04.2022).

7. Дарья Чебакова. Портрет типичного нарушителя служебной дисциплины. / Компания РБК. – 2021. – URL: https://www.rbc.ru/technology_and_media/26/05/2021/60aceff59a7947750b54bec7 (дата обращения: 24.03.2022).

8. Алексенцев, А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. – 2000. – № 3. – С. 10–17.

9. Safa N. S., Maple C., Watson T., Von Solms R. Motivation and opportunity based model to reduce information security insider threats in organizations // Journal of Information Security and Applications. – 2018. – Vol. 40. – P. 247-257. – ISSN 2214-2126. – URL: https://www.sciencedirect.com/science/article/pii/S2214212617302600 (дата обращения: 12.04.2022).

10. Defining organisational information security culture-Perspectives from academia and industry / A. Da Veiga, L. V. Astakhova, A. Botha, M. Herselman // Computers & Security. – 2020. – Vol. 92. – P. 101713. – DOI 10.1016/j.cose.2020.101713. – EDN QHJBSK.

11. DLP И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ Отчёт по результатам исследования / Экспертно-аналитический центр InfoWatch. 2021. – 24 с. – URL:https://www.infowatch.ru/analytics/analitika/dlp-i-ekonomicheskaya-bezopasnost-otchyot-po-rezultatam-issledovaniya (дата обращения: 12.04.2022).

12. Schaufeli, W.B. Defining and Measuring Work Engagement: Bringing Clarity to the Concept / W.B. Schaufeli, A.B. Bakker // Work Engagement: A Handbook of Essential Theory and Research. – New York: Psychology Press. – 2010. – P. 5–24. – URL: https://psycnet.apa.org/record/2010-06187-002 (дата обращения: 10.04.2022).

13. Reilly, P. Employee Engagement: Future Focus or Fashionable Fad for Reward Management? / P. Reilly, D. Brown // World at Work Journal. – 2008. – № 17 (4). – P. 37–49.

14. Астахова, Л. В. Развитие готовности будущего выпускника вуза к организационной вовлеченности как императив современного высшего образования / Л. В. Астахова // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. – 2021. – Т. 13. – № 4. – С. 19–29. – DOI 10.14529/ped210402. – EDN EJEKBZ

15. Работа с данными ИБ систем для оценки вовлеченности сотрудников. – URL: https://www.infowatch.ru/resources/webinar/video-38245?utm_source=terrasoft&utm_medium=email&utm_campaign=email041021&bulk_email_rid=406&bpmtrackid=2&bpmreplica=0&contactId=84826d85-1296-4ae7-9269-46fd7edcde36&bulkEmailRecipientId=33e54ad0-14ba-440f-9694-5dc044eb1863 (дата обращения: 12.04.2022).

References

1. GOST R 53114-2008. Natsional'nyy standart Rossiyskoy Federatsii. Zashchita informatsii. Obespecheniye informatsionnoy bezopasnosti v organizatsii. Osnovnyye terminy i opredeleniya (utv. i vveden v deystviye Prikazom Rostekhregulirovaniya ot 18.12.2008 N 532-st). – URL: https://docs.cntd.ru/document/1200075565 (data obrashcheniya: 11.04.2022).

2. Metodicheskiy dokument. Metodika otsenki ugroz bezopasnosti informatsii. Utverzhden FSTEK Rossii 5 fevralya 2021 goda. – URL: https://docs.cntd.ru/document/607699443?section=text (data obrashcheniya: 11.04.2022).

3. Otchot ob issledovanii utechek informatsii ogranichennogo dostupa v 2021 godu / Ekspertno-analiticheskiy tsentr InfoWatch. – 2022. – 32. s. – URL: https://www.infowatch.ru/analytics/analitika/v-2021-stalo-bolshe-umyshlennykh-utechek (data obrashcheniya: 12.04.2022).

4. Issledovaniye utechek informatsii ogranichennogo dostupa v 2020 godu / Ekspertno-analiticheskiy tsentr InfoWatch. – 2021. – 30. c. – URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2020-godu (data obrashcheniya: 12.04.2022).

5. Utechki dannykh organizatsiy po vine ili neostorozhnosti vnutrennego narushitelya. Sravnitel'noye issledovaniye. 2013-2019 gg. / Ekspertno-analiticheskiy tsentr InfoWatch. – 2020 – 32. c. – URL: https://www.infowatch.ru/analytics/analitika/utechki-dannykh-po-vine-vnutrennego-narushitelya-2013-2019-gg (data obrashcheniya: 12.04.2022).

6. Rostelekom-Solar. Kto on – tipovoy narushitel' v rossiyskoy organizatsii? 2018-2020 / Rostelekom-Solar. – 2021. – 12 c. – URL:https://rt-solar.ru/analytics/reports/2212/ (data obrashcheniya: 12.04.2022).

7. Dar'ya Chebakova. Portret tipichnogo narushitelya sluzhebnoy distsipliny. / Kompaniya RBK. – 2021. – URL: https://www.rbc.ru/technology_and_media/26/05/2021/60aceff59a7947750b54bec7 (data obrashcheniya: 24.03.2022).

8. Aleksentsev, A.I. Ponyatiye i struktura ugroz zashchishchayemoy informatsii // Bezopasnost' informatsionnykh tekhnologiy. – 2000. – № 3. – S. 10–17.

9. Safa N. S., Maple C., Watson T., Von Solms R. Motivation and opportunity based model to reduce information security insider threats in organizations // Journal of Information Security and Applications. – 2018. – Vol. 40. – P. 247-257. – ISSN 2214-2126. – URL: https://www.sciencedirect.com/science/article/pii/S2214212617302600 (дата обращения: 12.04.2022).

10. Defining organisational information security culture-Perspectives from academia and industry / A. Da Veiga, L. V. Astakhova, A. Botha, M. Herselman // Computers & Security. – 2020. – Vol. 92. – P. 101713. – DOI 10.1016/j.cose.2020.101713. – EDN QHJBSK.

11. DLP I EKONOMICHESKAYA BEZOPASNOST' Otchot po rezul'tatam issledovaniya / Ekspertno-analiticheskiy tsentr InfoWatch. 2021. – 24 c. – URL:https://www.infowatch.ru/analytics/analitika/dlp-i-ekonomicheskaya-bezopasnost-otchyot-po-rezultatam-issledovaniya (data obrashcheniya: 12.04.2022).

12. Schaufeli, W.B. Defining and Measuring Work Engagement: Bringing Clarity to the Concept / W.B. Schaufeli, A.B. Bakker // Work Engagement: A Handbook of Essential Theory and Research. – New York: Psychology Press. – 2010. – P. 5–24. – URL: https://psycnet.apa.org/record/2010-06187-002 (дата обращения: 10.04.2022).

13. Reilly, P. Employee Engagement: Future Focus or Fashionable Fad for Reward Management? / P. Reilly, D. Brown // World at Work Journal. – 2008. – № 17 (4). – P. 37–49.

14. Astakhova, L. V. Razvitiye gotovnosti budushchego vypusknika vuza k organizatsionnoy vovlechennosti kak imperativ sovremennogo vysshego obrazovaniya / L. V. Astakhova // Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Obrazovaniye. Pedagogicheskiye nauki. – 2021. – T. 13. – № 4. – S. 19–29. – DOI 10.14529/ped210402. – EDN EJEKBZ

15. Rabota s dannymi IB sistem dlya otsenki vovlechennosti sotrudnikov. – URL: https://www.infowatch.ru/resources/webinar/video-38245?utm_source=terrasoft&utm_medium=email&utm_

campaign=email041021&bulk_email_rid=406&bpmtrackid=2&bpmreplica=0&contactId=84826d85-1296-4ae7-9269-46fd7edcde36&bulkEmailRecipientId=33e54ad0-14ba-440f-9694-5dc044eb1863 (data obrashcheniya: 12.04.2022).

АСТАХОВА Людмила Викторовна, доктор педагогических наук, профессор, профессор кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: astakhovalv@susu.ru

ВОЛЕГОВ Никита Вячеславович, студент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: volegov.2323@gmail.com

ASTAKHOVA Liudmila Victorovna, Doctor of Pedagogy, Professor, Professor of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, LeninAvenue, 76. E-mail: astakhovalv@susu.ru

VOLEGOV Nikita Vyacheslavovich, student of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: volegov.2323@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(44) / 2022
Подписано в печать 23.06.2022. Дата выхода в свет 27.06.2022.
Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 7. Тираж 50 экз.
Заказ 227/204.
Цена свободная.

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

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 2(44) / 2022
Signed to print June 23, 2022. Date of publication of the 27.06.2022.
Format 70×108 1/16. Screen printing. Conventional printed sheet 7. Circulation – 50 issues.
Order 227/204.
Open price.

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