

**УЧРЕДИТЕЛИ****ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ****ГОСУДАРСТВЕННЫЙ****УНИВЕРСИТЕТ (НИУ)»****ПРЕДСЕДАТЕЛЬ****РЕДАКЦИОННОГО СОВЕТА****ЧУВАРДИН О. П.,**

руководитель Управления
Федеральной службы
по техническому и экспортному
контролю России по Уральскому
федеральному округу

ГЛАВНЫЙ РЕДАКТОР**СОКОЛОВ А. Н.,**

к. т. н., доцент, зав. кафедрой
«Защита информации»,
Южно-Уральский государственный
университет (национальный
исследовательский университет)
(г. Челябинск)

ВЫПУСКАЮЩИЙ РЕДАКТОР**СОГРИН Е. К.****ОТВЕТСТВЕННЫЙ СЕКРЕТАРЬ****АНДРИАДИС Е. Ю.****ВЁРСТКА****ШРАЙБЕР А. Е.****КОРРЕКТОР****ФЁДОРОВ В. С.****РЕДАКЦИОННЫЙ
СОВЕТ:****БАРАНКОВА И. И.,**

д. т. н., профессор, зав. кафедрой
«Информатика и информацион-
ная безопасность», Магнитогор-
ский государственный техниче-
ский университет им. Г. И. Носова
(г. Магнитогорск);

ВАСИЛЬЕВ В. И.,

д. т. н., профессор, профессор
кафедры «Вычислительная
техника и защита информации»,
Уфимский государственный
авиационный технический
университет (г. Уфа);

ВОЙТОВИЧ Н. И.,

д. т. н., профессор кафедры
«Радиоэлектроника и системы
связи», Южно-Уральский
государственный университет
(национальный исследователь-
ский университет) (г. Челябинск);

ГАЙДАМАКИН Н. А.,

д.т.н., профессор, профессор
Учебно-научного центра «Инфор-
мационная безопасность»,
Уральский федеральный универ-
ситет им. первого президента
России Б.Н. Ельцина (г. Екатеринбу-
рг);

ДИК Д. И.,

к. т. н., доцент, зав. кафедрой
«Безопасность информацион-
ных и автоматизированных
систем», Курганский государ-
ственный университет
(г. Курган);

ЗАХАРОВ А. А.,

д.т.н., профессор, зав. базовой
кафедрой «Безопасность
информационных технологий
умного города», Тюменский
государственный университет
(г. Тюмень);

ЗЫРЯНОВА Т. Ю.,

к. т. н., доцент, зав. кафедрой
«Информационные технологии
и защита информации»,
Уральский государственный
университет путей сообщения
(г. Екатеринбург);

МЕЛЬНИКОВ А. В.,

д. т. н., профессор, директор
Югорского научно-исследова-
тельского института информа-
ционных технологий
(г. Ханты-Мансийск);

МИНБАЛЕЕВ А. В.,

д. ю. н., доцент, зав. кафедрой
«Информационное право и
цифровые технологии», Москов-
ский государственный юридиче-
ский университет им. О. Е.
Кутафина (МГЮА, г. Москва);

ПОРШНЕВ С. В.,

д.т.н., профессор, директор
Учебно-научного центра
«Информационная безопас-
ность», Уральский федеральный
университет им. первого
президента России
Б.Н. Ельцина (г. Екатеринбург);

РУЧАЙ А. Н.,

к. ф.-м. н., доцент, зав. кафедрой
«Компьютерная безопасность и
прикладная алгебра», Челябин-
ский государственный универ-
ситет
(г. Челябинск);

ХОРЕВ А. А.,

д. т. н., профессор, зав. кафе-
дрой «Информационная безопас-
ность», Национальный исследо-
вательский университет
«Московский институт
электронной техники»
(г. Москва, г. Зеленоград);

ШАБУНИН С. Н.,

д.т.н., профессор, зав. кафедрой
«Радиоэлектроника и телеком-
муникации», Уральский
федеральный университет
им. первого президента России
Б.Н. Ельцина (г. Екатеринбург).

**Подписной индекс 73852
в каталоге «Почта России»**

Журнал зарегистрирован Федераль-
ной 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**

Journal of the Ural Federal District.

Information security

№ 4(50) / 2023



ISSN 2225-5435

FOUNDER

**SOUTH URAL STATE
UNIVERSITY (NIU)**

CHAIRMAN OF THE EDITORIAL BOARD

CHUVARDIN O. P.,

Head of Department Federal Service
for Technical and Export Control of
Russia for the Urals Federal District

CHIEF EDITOR

SOKOLOV A.N.,

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

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SCHREIBER A. E.

PROOFREADING

FEDOROV V. S.

Subscription index 73852

in the «Russian Post» catalog

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

Certificate
PI No. 0C77-65765 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**

EDITORIAL COUNCIL:

BARANKOVA I. I.,

Doctor of Technical Sciences,
Professor, Head of Department
"Informatics and Information
Security", Magnitogorsk State
Technical University named after.
G.I. Nosova (Magnitogorsk city);

VASILYEV V. I.,

Doctor of Technical Sciences,
Professor, Professor of the
Department "Computer Science and
Information Protection", Ufa State
Aviation Technical University
(Ufa city);

VOITOVICH N. I.,

Doctor of Technical Sciences,
Professor, Professor of the
Department "Radioelectronics and
Communication Systems", South
Ural State University (National
Research University) (Chelyabinsk
city);

GAYDAMAKIN N. A.,

Doctor of Technical Sciences,
Professor, Professor of the
Information Security Training and
Research Center of the Ural Federal
University named after the first
President of Russia B.N.Yeltsin
(Ekaterinburg city);

DIK D. I.,

Ph.D., Associate Professor, Head of
Department "Security of information
and automated systems", Kurgan
State University (Kurgan city);

ZAHAROV A. A.,

Doctor of Technical Sciences,
Professor, Head Basic Department of
"Security information technologies
smart city", Tyumen State University
(Tyumen city);

ZYRYANOVA T. Y.,

Ph.D., Associate Professor, Head of
Department "Information
Technologies and Information
Protection", Ural State
University ways of communication
(Ekaterinburg city);

MELNIKOV A. V.,

Doctor of Technical Sciences,
Professor, Director Ugra Research
Institute of Information Technologies
(Khanty-Mansiysk city);

MINBALEEV A. V.,

Doctor of Law, Associate Professor,
Head of Department of "Information
Law and Digital Technologies",
Moscow State Law University. O. E.
Kutafina (Moscow city);

PORSHNEV S. V.,

Doctor of Technical Sciences,
Professor, Director of the Training
and Scientific Center "Information
Security", Ural Federal University
named after the first President of
Russia B.N.Yeltsin
(Ekaterinburg city);

RUCHAY A. N.,

Ph.D., Associate Professor, Head of
the Department "Computer Security
and Applied Algebra", Chelyabinsk
State University (Chelyabinsk city);

HOREV A. A.,

Doctor of Technical Sciences,
Professor, Head of Department of
"Information Security", National
Research University "Moscow
Institute of Electronic Technology"
(Moscow, the city of Zelenograd);

SHABUNIN S. N.,

Doctor of Technical Sciences,
Professor, Head of Department
"Radioelectronics and
Telecommunications", Ural Federal
University named after the first
President of Russia B.N.Yeltsin
(Ekaterinburg city).

16+

В НОМЕРЕ

РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ

**ПОРТНОВ А.В., НИКОЛАЕВ А.Н.,
НИКОЛАЕВА А.Р.**

Устройство и алгоритмы первичной
обработки видеоинформации для системы
машинного зрения на основе искусственных
фасеточных глаз 5

**ШВЫРЕВ Б.А., ПОЛИКАРПОВ Е.С.,
АНИСИМОВ С.Л.**

Особенность измерения побочных
электромагнитных излучений интерфейса
sata 13

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

ПОРШНЕВ С.В., РЯБКО Н.Ю.

Оценка адекватности некоторых методов
электоральной криминалистики на основе
анализа сгенерированных случайных
данных, статистические свойства которых
подобны реальным электоральным
данным 22

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ПАЛЮТИНА Г.Н.

О применении когнитивного моделирования
в адаптивной оценке рисков
информационной безопасности 43

**НЕКЛЮДОВ Д.Н., ЛЕБЕДЬ А.С.,
КУЗЬМИНА У.В.**

Исследование атак на бесконтактные
смарт-карты и rfid-метки 53

ПАЛЮТИНА Г.Н.

О применении нейронных сетей для оценки
весов связей между концептами нечеткой
когнитивной карты в адаптивной оценке
рисков информационной безопасности ... 60

ЧАСТИКОВА В.А., КОЗАЧЁК К.В.

Применение нейронных сетей в платформе
реагирования на инциденты как
эффективное средство управления
кибербезопасностью 70

ХОРЕВ А.А., ЧУМАКОВ А.А.

Анализ возможности реализации угроз
безопасности информации, обрабатываемой
средствами вычислительной техники, с
использованием радиомодулей 77

RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES

**PORTNOV A.V., NIKOLAEV A.N.,
NIKOLAEVA A.R.**

Device and algorithms for primary processing
of video information for a machine vision
system based on artificial compound eyes 5

**SHVYREV B.A., POLIKARPOV E.S.,
ANISIMOV S.L.**

The peculiarity of measuring the side
electromagnetic radiation of the sata
interface. 13

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

PORSHNEV S.V., RYABKO N.YU.

Assessment of the some electoral criminology
methods adequacy based on the analysis
of generated random data, the statistical
properties of which are similar to real electoral
data 22

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

PALYUTINA G.N.

On the application of cognitive modeling in
adaptive assessment of information security
risks 43

**NEKLYUDOV D.N., LEBED A.S.,
KUZMINA U.V.**

Research on attacks against contactless smart
cards and rfid tags 53

PALYUTINA G.N.

On the application of neural networks
for estimating the weights of connections
between the concepts of a fuzzy cognitive
map 60

CHASTIKOVA V.A., KOZACHOK K.V.

Using neural networks in an incident response
platform as an effective means of cybersecurity
management 70

HOREV A.A., CHUMAKOV A.A.

Analysis of the possibility of implementing
threats to the security of information processed
by computer technology using radio
modules 77



УСТРОЙСТВО И АЛГОРИТМЫ ПЕРВИЧНОЙ ОБРАБОТКИ ВИДЕОИНФОРМАЦИИ ДЛЯ СИСТЕМЫ МАШИННОГО ЗРЕНИЯ НА ОСНОВЕ ИСКУССТВЕННЫХ ФАСЕТОЧНЫХ ГЛАЗ

В статье обсуждаются задачи первичной обработки видеоинформации для систем бинокулярного машинного зрения на основе искусственных фасеточных глаз.

Проводится оценка необходимых вычислительных ресурсов для обработки потока видеоинформации в режиме реального времени.

Предлагается вариант реализации устройства на базе программируемой логической интегральной схемы и алгоритмы обработки информации в таком устройстве.

По результатам макетирования устройства и полученным экспериментальным данным ставятся задачи разработки алгоритмов определения границ движущихся объектов.

Ключевые слова: алгоритмы первичной обработки видеоинформации, искусственный фасеточный глаз, программируемая логическая интегральная схема, бинокулярное машинное зрение.

DEVICE AND ALGORITHMS FOR PRIMARY PROCESSING OF VIDEO INFORMATION FOR A MACHINE VISION SYSTEM BASED ON ARTIFICIAL COMPOUND EYES

The article discusses the tasks of primary processing of video information for binocular machine vision systems based on artificial compound eyes.

The assessment of the necessary computing resources for processing the stream of video information in real time is carried out.

A variant of implementing a device based on a programmable logic integrated circuit and algorithms for processing information in such a device is proposed.

Based on the results of the device layout and the experimental data obtained, the tasks of developing algorithms for determining the boundaries of moving objects are set.

Keywords: *algorithms of primary processing of video information, artificial compound eye, FPGA, binocular machine vision.*

Введение

Системы машинного зрения находят широкое применение в различных областях, в том числе обеспечения контроля и безопасности различных объектов. В качестве сенсоров в таких системах используются, как правило, видеокамеры высокого разрешения. Их основным недостатком является относительно узкий угол обзора. Поэтому в последнее время уделяется достаточно большое внимание сенсорам, построенным по принципу фасеточного глаза насекомых. Преимуществами системы машинного зрения на основе искусственных фасеточных глаз в сравнении со стандартными видеокамерами являются широкий угол обзора, компактная структура и чувствительность к движущимся объектам. В [1] приводится обзор возможных вариантов реализации искусственного фасеточного глаза, рассмотрены достоинства и недостатки каждого из вариантов. Выделяется 4 основных подхода к реализации фасеточного глаза:

1. Плоская ПЗС матрица со стандартной линзой.

2. Плоская ПЗС матрица с изогнутой линзой.

3. Изогнутая ПЗС матрица с изогнутыми линзами.

4. Многокамерная матрица.

Первый вариант соответствует стандартной видеокамере с относительно узким углом обзора. Второй и третий варианты являются сложными с точки зрения реализации оптической системы и нестандартных ПЗС матриц. Наиболее доступным в плане практической реализации вариантом является искусственный фасеточный глаз на основе нескольких видеокамер на плоских ПЗС матрицах. Однако в этом случае возникают проблемы, связанные с необходимостью обработки большого потока видеоинформации, поступающего от нескольких камер.

В настоящей статье рассмотрены алгоритмы первичной обработки видеоинформации для системы машинного зрения на основе многокамерных искусственных фасеточных глаз.

Обобщенная структурная схема интел-

лектуальной системы бинокулярного машинного зрения фасеточного типа приведена на рис. 1.

Основными структурными элементами системы являются: оптический модуль, аппаратно-программный контроллер и нейросеть.

Оптический модуль состоит из двух блоков многокамерных фасеточных глаз. Поток данных об изображении с ПЗС-матриц передается в аппаратно-программный контроллер на базе ПЛИС, где выполняется первичная обработка информации – разделение на отдельные сектора (омматидии). Полученные в результате данные по всем омматидиям поступают в две нейросети прямого распространения, которые решают задачу определения координат объекта в виде направления и дальности до объекта [2].

Задачи первичной обработки видеоинформации и оценка требуемых вычислительных ресурсов

В задачи первичной обработки информации входит:

- прием потока данных от ПЗС матриц, входящих в состав сенсора;

- формирование информации о яркости в отдельных фасетках (омматидиях) и сохранение в промежуточную буферную память;

- обработка двух соседних информационных кадров с целью обнаружения движущихся объектов.

Для оценки требуемой пропускной способности устройства приема информации от ПЗС-матриц были проведены расчеты на примере датчика изображения типа OV2640 (производства «OmniVision») Основные характеристики датчика:

- выходной информационный поток в формате RGB565/555 или YUV(422/420)/YCbCr422);

- разрешение: UXGA (1600x1200 пикселей), SVGA (800x600 пикселей), CIF (400x296 пикселей);

- частота кадров: при UXGA-разрешении

- 15 кадров в секунду, при SVGA-разрешении

- 30 кадров в секунду, при CIF-разрешении – 60 кадров в секунду;

- максимальная частота синхронизации 36 МГц.

Временные диаграммы передачи информации приведены на рис. 2.



Рис. 1. Обобщенная структурная схема системы машинного зрения на основе искусственных фасеточных глаз

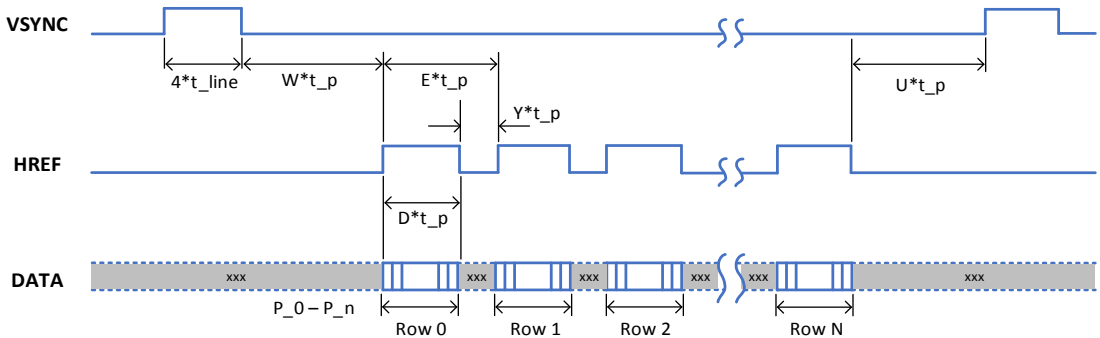


Рис. 2. Временные диаграммы синхронизации кадров

Назначение сигналов:

- VSYNC – сигнал кадровой синхронизации, указывает, на окончание текущего кадра (информация по всем пикселям изображения передана);

- HREF – строчная синхронизация, спад HREF свидетельствует об окончании передачи информации одной строки;

- D0-D7 – шина данных.

Параметр t_{line} рассчитывается по следующей формуле: $t_{\text{line}} = E \cdot t_p$. При дальнейших расчетах учтем, что время t_p берется минимально возможным, равным 27,78 нс (для максимальной частоты синхронизации 36 МГц).

В таблице 1 приведены временные пара-

Временные параметры синхронизации кадров

Разрешение	Параметр							
	W	E	Y	U	D	t_line, нс	P_n	Row N
UXGA	27193	1922	322	57697,0	1600	53393,16	1599	1199
SVGA	7415	1190	390	73895,0	800	33058,20	799	599
CIF	3707	595	195	17907,5	400	16529,10	399	295

метры под каждое возможное разрешение матрицы.

Общее время, затраченное на передачу одного кадра (T), рассчитывается по следующей формуле:

$$T = 4 \cdot t_{\text{line}} + t_p \cdot (W + E \cdot (\text{Row}_N + 1) + U)$$

Таким образом:

– с разрешением UXGA 1 кадр передается за 0,066644 секунды, следовательно, 15 кадров передаются за 0,9997 секунды;

– с разрешением SVGA 1 кадр передается за 0,022226 секунды, следовательно, 30 кадров передаются за 0,667 секунды;

– с разрешением CIF 1 кадр передается за 0,005559 секунды, следовательно, 60 кадров передаются за 0,334 секунды.

Максимальную пропускную способность, необходимую для обеспечения приема видеоинформации, рассчитаем по следующей формуле:

$$BW = \text{Row} \cdot \text{Col} \cdot C \cdot N_c,$$

где Row – количество строк в изображении, Col – количество столбцов в изображении, – количество бит, которые кодируют один пиксель, C – количество кадров в секунду.

В табл. 2 приведена рассчитанная пропускная способность для разного разрешения, при этом цвет каждого пикселя кодируют 16 бит информации.

Алгоритмы первичной обработки потока видеоинформации

В рассматриваемом варианте системы ма-

Таблица 2

Максимальная пропускная способность

Разрешение	Количество кадров	Информационный поток, Мбит/с
UXGA (1600x1200)	15	460,8
SVGA (800x600)	30	230,4
CIF (400x296)	60	113,7

шинного зрения определение координат движущихся объектов основано на использовании двумерной модели [2]. Для формирования яркостной информации в каждой фасетке (омматидии) пиксели ПЗС матрицы группируются в отдельные сектора. Сканирование пикселей происходит так, как показано на рис. 3.

Яркость каждого из омматидиев рассчитывается по следующей формуле:

$$Iom_k = \sum_{j=L}^R I_{\text{pixel}_{i,j}},$$

где Iom_k – яркость k-го омматидия, $I_{\text{pixel}_{i,j}}$ – яркость текущего пикселя изображения, L и R – номера левой и правой границ омматидия.

Схема, реализующая алгоритм формирования яркостной информации в отдельном омматидии приведена на рис. 4.

Объем памяти, требуемый для хранения одного преобразованного кадра, можно рассчитать по следующей формуле:

$$M = \left\lceil \log_2 \left(Cd \cdot \text{Row} \cdot \frac{\text{Col}}{N_{\text{omm}}} \right) \right\rceil \cdot N_{\text{omm}},$$

где Cd – глубина цвета пикселя, Row – количество строк в изображении, Col – количество столбцов в изображении, N_{omm} – количество омматидий.

Для примера с количеством строк изображения – 600, количеством столбцов изображения – 800, количеством омматидиев – 200 и глубиной цвета пикселей 255, необходимый объем памяти составляет 4000 бит. Таким образом, для хранения одного кадра, пришедших одновременно с двух камер, необходимо 7,82 Кбит памяти. Для сравнения, для хранения исходного кадра при данном разрешении необходимо примерно 469 Кб.

На рис. 5 приведен результат деления изображения на отдельные омматидии в системе, состоящей из двух камер.

В традиционных системах видеонаблюдения для обнаружения движения объектов в

кадре широко используется метод вычитания фона [3,4]. Одним из алгоритмов реализации такого метода является вычисление разности

соседних кадров изображения. Такой подход может быть применен для обнаружения движения объектов в системе машинного зрения

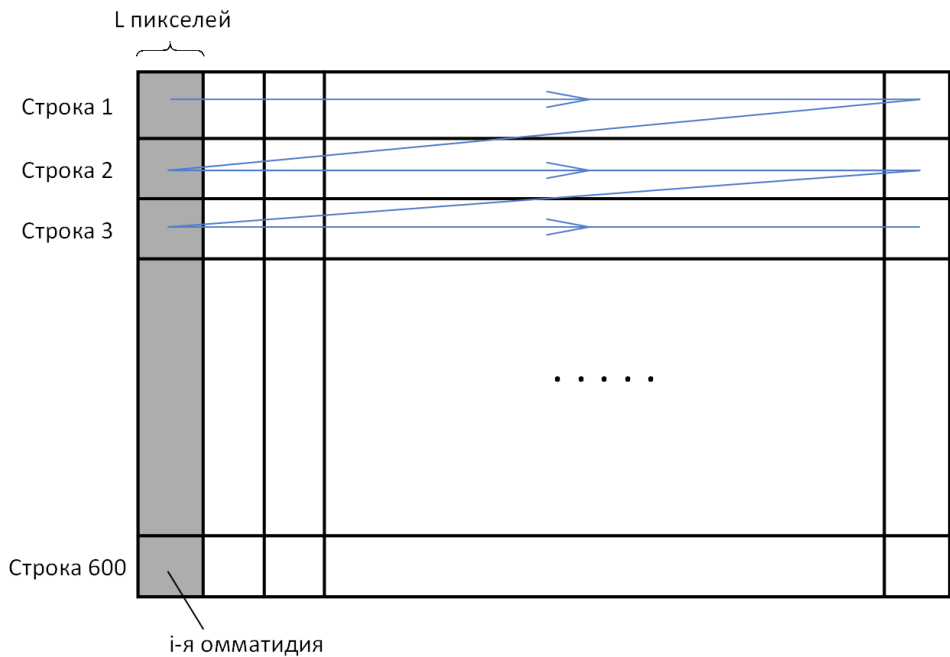


Рис. 3. Сканирование пикселей и формирование омматициев

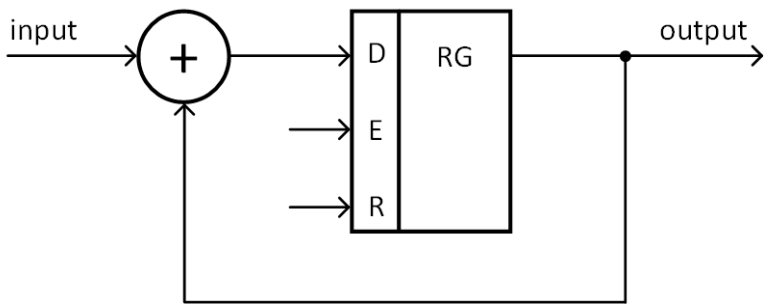


Рис. 4. Алгоритм первичной обработки информации в отдельном омматиции

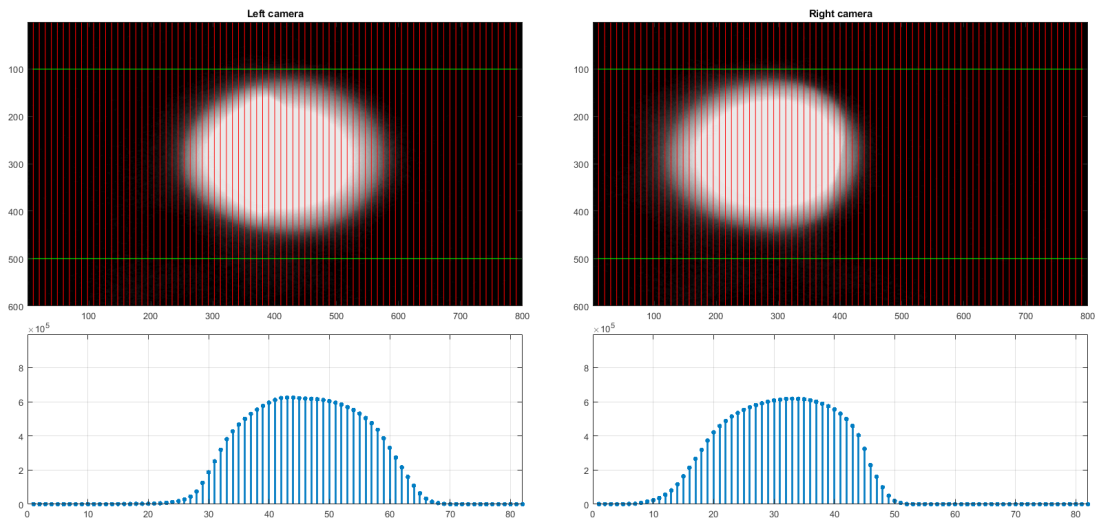


Рис. 5. Результат первичной обработки информации в омматициях

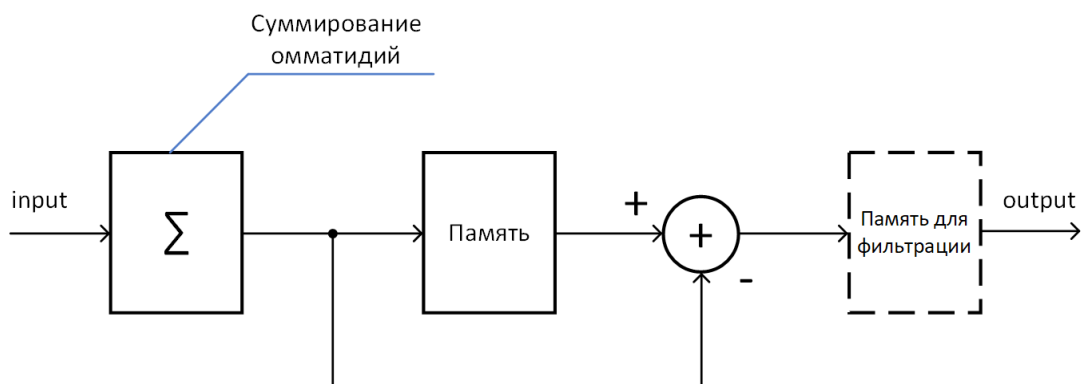


Рис. 6. Алгоритм разностной обработки яркостной информации в омматидиях

на основе искусственных фасеточных глаз. На рис. 6 показан алгоритм получения разностной информации о яркости в соседних кадрах изображения для отдельных омматидиев.

Результаты эксперимента

Для проведения экспериментов был создан макетный образец аппаратно-программного контроллера системы бинокулярного машинного зрения. Основой контроллера является программируемая логическая интегральная схема (ПЛИС) семейства CycloneV

(ф. Intel). В качестве датчиков изображения применялись модули на основе ПЗС матриц OV2640 с объективами. Визуализация результатов проводилась на ПЭВМ. Системе демонстрировались движущиеся объекты различной формы, выводимые на широкоформатный дисплей. Результаты работы алгоритмов первичной обработки информации, включая вычисление разности яркости в омматидиях для соседних кадров изображения, приведены на рис. 7.

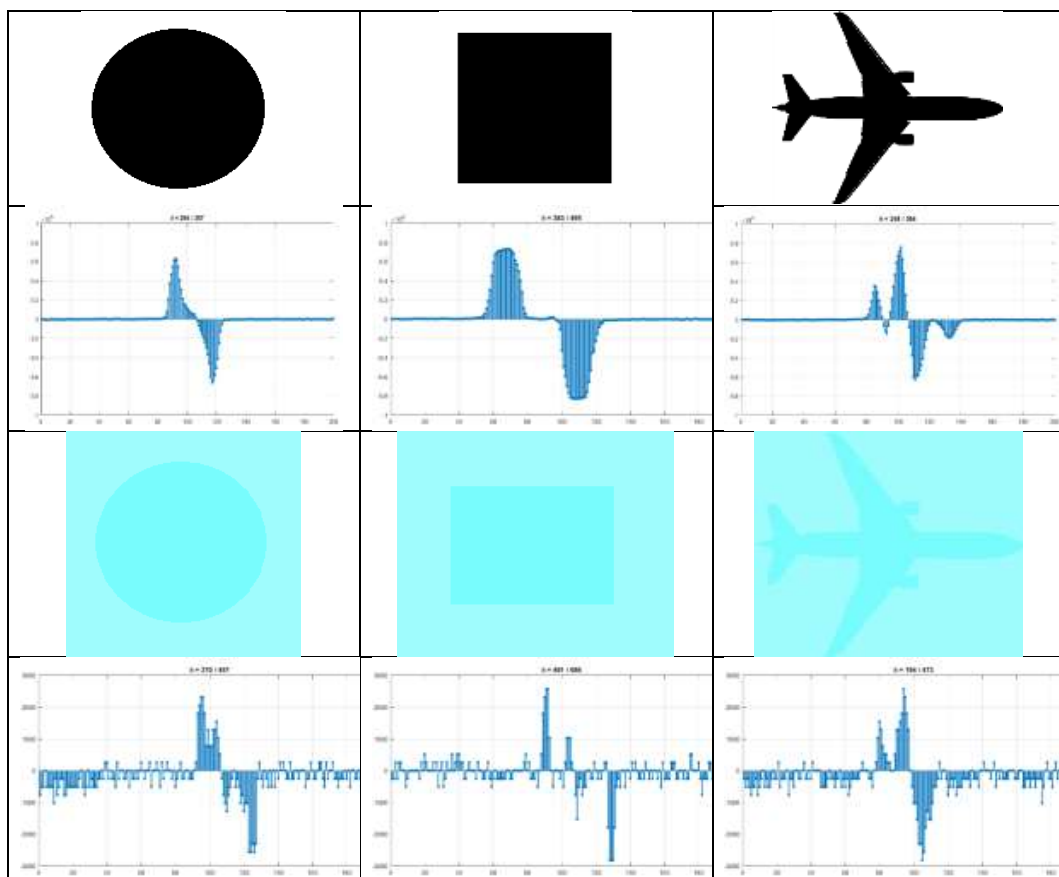


Рис. 7. Результаты первичной обработки видеоинформации

Анализ полученных результатов показывает, что вычисление разности яркостной информации по отдельным омматидиям позволяет обнаружить границы движущихся объектов, и направление их движения. Наиболее благоприятными условиями для работы алгоритма является простая форма объекта, его равномерное освещение (затенение) и контрастность на общем фоне. В случае малоконтрастных объектов, а также объектов сложной формы требуется дополнительная обработка полученной информации. Одним из мощных инструментов для такой обработки может послужить вейвлет-анализ [5].

Заключение

Алгоритмы первичной обработки видеoinформации для системы бинокулярного ма-

шинного зрения на основе искусственных фасеточных глаз позволяют выделить движущийся объект на общем фоне изображения. Обработка информации от датчиков изображения в режиме реального времени дает существенную экономию памяти, требуемой для хранения промежуточных результатов обработки видеoinформации.

Важным условием корректной работы нейросетей, определяющих координаты движущихся объектов, является точное определение их границ. Поэтому требуется разработка алгоритмов фильтрации информации, полученной в результате первичной обработки изображения.

Литература

1. Yang Cheng, Jie Cao, Yangkun Zhang, Qun Hao. Review of state-of-the-art artificial compound eye imaging systems // *Bioinspiration & Biomimetics*. 2019. Volume 14. № 3.
2. Starkov A. E., Sokolinsky L. B. Building 2D Model of Compound Eye Vision for Machine Learning // *Mathematics*. 2022. № 2 (10).
3. Баймухаметова А.И. Методы вычитания фона для обнаружения объекта в видеопотоке // *Международный журнал гуманитарных и естественных наук*. 2022. №7-1.
4. Берников В.В. Преображенский А.П. Чопоров О.Н. Анализ алгоритмов обнаружения движущихся объектов на видеоизображении. Моделирование, оптимизация и информационные технологии. 2013;1(1).
5. Безуглов Д.А., Кузин А.П., Швидченко С.А. Алгоритмические методы вейвлет-анализа изображений в условиях априорной неопределенности на случайном фоне // *Научное обозрение. Технические науки*. – 2015. – № 1. – С. 71-72.

References

1. Yang Cheng, Jie Cao, Yangkun Zhang, Qun Hao. Review of state-of-the-art artificial compound eye imaging systems // *Bioinspiration & Biomimetics*. 2019. Volume 14. № 3.
2. Starkov A. E., Sokolinsky L. B. Building 2D Model of Compound Eye Vision for Machine Learning // *Mathematics*. 2022. № 2 (10).
3. Baymukhametova A.I. Metody vychitaniya fona dlya obnaruzheniya obyektov v videopotoke // *Mezhdunarodnyy zhurnal gumanitarnykh i estestvennykh nauk*. 2022. №7-1.
4. Bernikov V.V. Preobrazhenskiy A.P. Choporov O.N. Analiz algoritmov obnaruzheniya dvizhushchikhsya obyektov na videoizobrazhenii. Modelirovaniye. optimizatsiya i informatsionnyye tekhnologii. 2013;1(1).
5. Bezuglov D.A., Kuzin A.P., Shvidchenko S.A. Algoritmicheskiye metody veyvlet-analiza izobrazheniy v usloviyakh apriornoy neopredelennosti na sluchaynom fone // *Nauchnoye obozreniye. Tekhnicheskiye nauki*. – 2015. – № 1. – С. 71-72.

ПОРТНОВ Андрей Владимирович, аспирант федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, просп. В.И. Ленина, д. 76. E-mail: portnovav@susu.ru

PORTNOV Andrey Vladimirovich, post-graduate student of the Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Chelyabinsk, st. Lenina, 76. E-mail: portnovav@susu.ru

НИКОЛАЕВ Андрей Николаевич, доцент федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, просп. В.И. Ленина, д. 76. E-mail: nikolaevan@susu.ru

NIKOLAEV Andrey Nikolaevich, docent of the Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Chelyabinsk, st. Lenina, 76. E-mail: nikolaevan@susu.ru

НИКОЛАЕВА Алиса Робертовна, инженер федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, просп. В.И. Ленина, д. 76. E-mail: nikolaevaar@susu.ru

NIKOLAEVA Alisa Robertovna, engineer of the Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Chelyabinsk, st. Lenina, 76. E-mail: nikolaevaar@susu.ru

ОСОБЕННОСТЬ ИЗМЕРЕНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ИНТЕРФЕЙСА SATA

Развитие высокоскоростных интерфейсов взаимодействия периферийного оборудования вычислительной техники не только увеличивает пропускную способность, но и увеличивает риск несанкционированного доступа путем перехвата побочных электромагнитных высокочастотных излучений информационных интерфейсов. В настоящее время наиболее распространёнными являются следующие интерфейсы SATA1, SATA2 и SATA 3. В целом, развитие версий SATA и кабелей в значительной степени способствовало развитию возможностей хранения и передачи данных. Излучение кабеля SATA на частоте 1,5 ГГц и выше можно представить как излучение антенны «длинный провод», учитывая длину кабеля от 0.3 до 1 м. С целью повышения селективности излучения от интерфейса SATA в системном блоке компьютера рассматривались две антенны: петлевой вибратор Пистолькорса и круглая рамочная антенна сформированные из кабеля SATA без нарушения его целостности. Проведенные расчеты установили оптимальное значение диаметра круглой рамочной антенны. А исследования спектрального состава электромагнитного излучения интерфейса SATA 1, позволили обнаружить первую гармонику на частоте 1.5 ГГц и последующие вторую, третью и четвертую кратные гармоники. Проведенные исследования показали реальность угрозы утечки информации через побочные электромагнитные излучения интерфейса SATA.

Ключевые слова: побочные электромагнитные излучения, интерфейс, SATA, рамочная антенна, полуволновый вибратор.

Shvyrev B.A., Polikarpov E.S., Anisimov S.L.

THE PECULIARITY OF MEASURING THE SIDE ELECTROMAGNETIC RADIATION OF THE SATA INTERFACE

The development of high-speed interfaces for the interaction of peripheral computer equipment not only increases throughput, but also increases the risk of unauthorized access by intercepting side electromagnetic high-frequency radiation of information interfaces. Currently, the most common interfaces are SATA1, SATA2 and SATA 3. In general, the development of SATA and

cable versions has greatly contributed to the development of data storage and transmission capabilities. The radiation of a SATA cable at a frequency of 1.5 GHz and above can be represented as the radiation of a "long wire" antenna, given the cable length from 0.3 to 1 m. In order to increase the selection of radiation from the SATA interface, two antennas were considered in the computer system unit: a Pistolcors loop vibrator and a round frame antenna formed from a SATA cable without violating its integrity. The calculations carried out have established the optimal value of the diameter of the circular frame antenna. The conducted studies of the spectral composition of the electromagnetic radiation of the SATA 1 interface made it possible to detect the first harmonic at a frequency of 1.5 GHz and the subsequent second, third and fourth multiple harmonics. The conducted research has shown the reality of the threat of information leakage through the side electromagnetic radiation of the SATA interface.

Keywords: side electromagnetic radiation, interface, SATA, frame antenna, half-wave vibrator.

Развитие высокоскоростных интерфейсов взаимодействия периферийного оборудования вычислительной техники не только увеличивает пропускную способность, но и увеличивает риск несанкционированного доступа путем перехвата побочных электромагнитных высокочастотных излучений информационных интерфейсов. Одним из высокоскоростных интерфейсов вычислительной техники является SATA. Данный интерфейс достаточно новый и обладает особенностями. В открытых источниках вопросы исследования побочных электромагнитных излучений интерфейсов накопителей на жестких дисках представлены в источнике [1]. Анализ исследований скрытых технических каналов утечки информации рассматривается в источнике [2], анализ терминологии в источнике [3]. Утечка информации по техническим каналам за счет побочных электромагнитных излучений интерфейсов передачи данных обсуждается в источниках [3, 4], методы радиомониторинга в источнике [5].

Обнаружение и исследование излучения

от достаточно нового высокоскоростного интерфейса SATA является актуальной задачей.

SATA — это командно-транспортный протокол, который определяет способ передачи данных между материнской платой компьютера и устройствами массового хранения, такими как жесткие магнитные диски (HDD), оптические приводы и твердотельные накопители (SSD). Как следует из названия, SATA основан на технологии последовательной передачи сигналов, при которой данные передаются в виде последовательности отдельных битов.

Рассматривать классический параллельный IDE интерфейс уже нет смысла. Во-первых, параллельный (следовательно, менее «опасный»), во-вторых уже всё реже и реже встречающийся. Его место в дисковых интерфейсах безраздельно занимает интерфейс SATA в различных своих вариантах.

В настоящее время наиболее распространенными являются следующие интерфейсы SATA1, SATA2 и SATA3 с параметрами, приведенными в табл. 1.

Таблица 1

Скорости передачи данных интерфейса SATA

Стандарт	Пропускная способность	Скорость передачи данных
SATA I	1.5 Гбит/сек	150 Мбит/сек
SATA II	3 Гбит/сек	300 Мбит/сек
SATA III	6 Гбит/сек	600 Мбит/сек

Первая версия SATA, представленная в 2003 году, имела пропускную способность 1,5 Гбит/с и скорость передачи данных 150 Мбит/с. В 2004 году был выпущен SATA 2.0 с удвоенной пропускной способностью и скоростью передачи данных, достигнув 3,0 Гбит/с и 300 Мбит/с соответственно. Четыре

года спустя, в 2008 году, был представлен интерфейс SATA 3.0 с еще более высокими характеристиками, обеспечивающий пропускную способность 6,0 Гбит/с и скорость передачи данных 600 Мбит/с. Эти улучшения в технологии SATA позволили ускорить и повысить эффективность передачи данных между

устройствами. В целом, развитие версий SATA и кабелей в значительной степени способствовало развитию возможностей хранения и передачи данных.

Кабели SATA представляют собой 7-кон-

тактный кабель, состоящий из заземления (контакты 1,4,7), передачи (контакты 2,3) и приема (контакты 5,6), изображенный на рис.1.

Дифференциальная пара в кабеле SATA

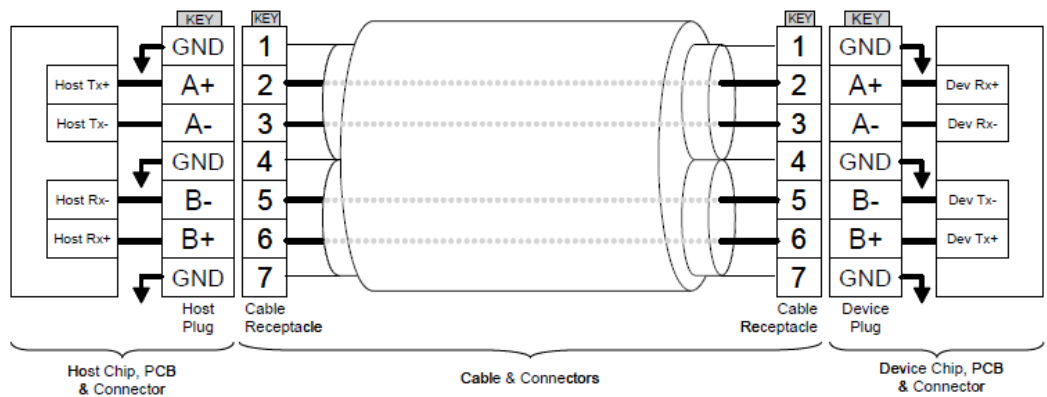


Рис. 1. Схема подключения кабеля / разъема SATA [6].

уменьшает излучающую способность, то есть конструктивно кабель должен меньше излучал побочные электромагнитные излучения.

Из анализа публикаций [7,8,9] следует, что передача данных осуществляется на ча-

стотах СВЧ диапазона начиная с 1,5 ГГц. Для таких высоких частот характерен волновой характер распространения сигнала и кабель SATA можно рассматривать как длинную линию (табл. 2).

Таблица 2

Длина несущей частоты интерфейса SATA

Стандарт	Частота, ГГц	Длина волны, м
SATA I	1,5	0,1998
SATA II	3	0,09993
SATA III	6	0,04996

Наличие дифференциальных пар проводников в кабеле SATA уменьшает побочные электромагнитные излучения, что на ряду с значительным электромагнитным зашумлением от элементов материнской платы компьютера, блока питания и контроллеров затрудняет обнаружение излучения именно кабеля SATA. Излучение кабеля SATA на частоте 1,5 ГГц и выше можно представить как излучение антенны «длинный провод», учитывая длину кабеля от 0.3 до 1 м. Такой тип антенн с увеличением ее длины сжимает диаграмму направленности вдоль проводника. С целью повышения коэффициента направленного действия рассматривались две антенны: петлевой вибратор Пистолькорса и рамочная антенна. Петлевой вибратор Пистолькорса достаточно просто реализуется путем формовки кабеля SATA в размере равном пол длине волны. Параметры петлевого вибратора аналогичны разрезному. Коэффициент

усиления полуволнового вибратора равен 0 дБ, однако диаграмма направленности имеет вид восьмерки, что позволяет излучать электромагнитную волну в более определенном направлении. (Рис.2)

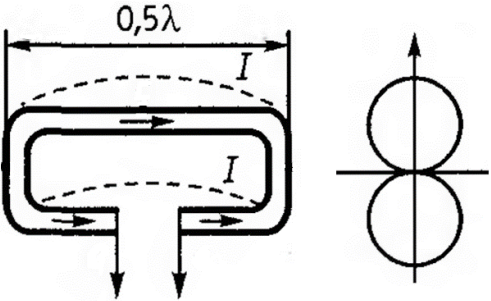


Рис.2. Петлевой вибратор Пистолькорса и его диаграмма направленности [10].

С целью получения большего коэффициента усиления при излучении кабеля SATA без нарушения его целостности построили кру-

глуую рамочную антенну соизмеримую с длиной волны. Рамка создает максимальное излучение с КНД $D_{\max}=1,5$ в своей плоскости и не излучает электромагнитную энергию вдоль оси, и обладает диаграммой направленности в виде восьмерки. Такая антенна обладает кроме селективности по частоте, еще и селективностью по азимуту. Как известно, радиосигнал состоит из электрических и магнитных колебаний. Прием магнитной составляющей радиосигнала обусловлен специальной конструкцией рамочной антенны. Полуволновый диполь, в отличие от рамочной антенны, реагирует на электрическое переменное поле высокочастотного сигнала. У магнитных рамочных антенн есть значительное преимущество они менее чувствительны к бытовым случайным помехам (компьютер, блок питания и т. д.). Другое преимущество магнитной антенны обусловлено её конструкцией: это колебательный контур с довольно высокой добротностью.

Для расчёта воспользовались выражением [10] в полярных координатах рис.3.

$$A_{\varphi\infty}^3 = \frac{2\exp(-ikR)}{4\pi R} \int_0^\pi I_p^3 \cos \phi \exp(jka \sin \theta \cos \phi) d\phi \quad (1)$$
 где a – диаметр рамки, $k = 2\pi/\lambda$, I_p^3 – постоянный ток в рамке

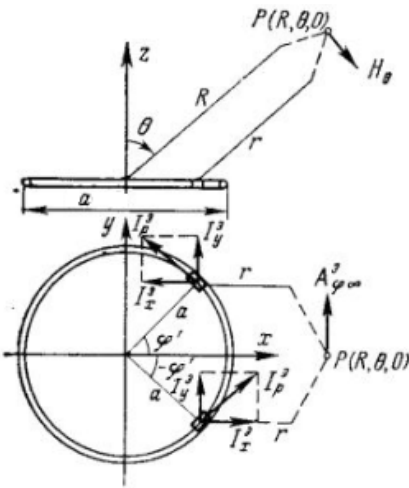


Рис.3. К вычислению поля электрической рамки [4]

Для определения радиуса рамки выражение 1 упростили положив угол $\theta=\pi/2$ и выполнив нормировку на максимальное значением получим

$$D_{\max} = \int_0^\pi \cos \phi \exp(jka \cos \phi) d\phi$$

По результатам численного интегрирования получен график рис.4. Из рис.4 видно, что наибольший КПД рамочной круглой антенны будет при диаметре $a=0.293\lambda$.

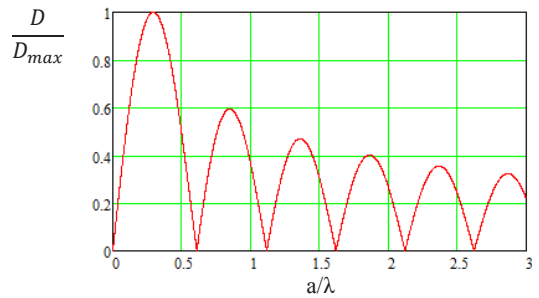


Рис.4. К расчету диаметра рамочной антенны на 6ГГц

Для частоты 1.5 ГГц интерфейса SATA I длина волны 0,1998 м, тогда диаметр антенны будет равен $0.293 \cdot 0.1998 = 0.059$ (м), что соответствует длине окружности немногим меньше длины волны. В зависимости от длины кабеля SATA удавалось реализовать один или два витка вокруг пластиковой формы соответствующего диаметра.

С целью проверки предложенного способа получения большего коэффициента усиления при излучении кабеля SATA, путем использования рамочной антенны с заданными параметрами, в работе проведены исследования на примере излучения, образующегося при передаче информации на жесткий магнитный диск. Исследование других периферийных устройств подключаемых по SATA I, II, III в работе не приводятся и будут опубликованы позже.

Все последующие измерения проводились с кабелем SATA I, сформированным в одно петлевую круглую рамочную антенну, используемый для подключения накопителя на жестком магнитном диске.

Путем исследования спектрального состава излучаемого электромагнитного поля интерфейса SATA с помощью спектроанализатора, установлено, что интерфейс транслирует электромагнитное излучение в диапазонах с центральными частотами 1,5 ГГц, 3 ГГц, 4,5 ГГц и 6 ГГц.

Порядок проведения измерений ПЭМИ интерфейса SATA:

1. Установить измерительный приемник. Подключить к измерительному приемнику электрическую антенну. Установить требуемые для измерения настройки приемника.
2. Включить СВТ, запустить тестовую программу (тест-сигнал).
3. Перестраивая измерительный приемник в диапазоне частот от 1 ГГц до 9 ГГц произвести поиск сигналов (при необходимости производится смена измерительной антенны).

4. При обнаружении сигнала провести его идентификацию.

Наблюдение за изменением характера и формы сигналов производится визуально на дисплее измерительного приемника.

5. Измерить напряжение сигнала на частоте идентифицированного информативного сигнала при включенном (U_и) и выключенном (U_ш) тесте, дБ (мкВ).

В состав лабораторного стенда, используемого для исследования спектров ПЭМИ накопителя на жёстких магнитных дисках, вхо-

дят: средство вычислительной техники, анализатор спектра R&S FSH13, комплект антенны П6-223, комплект антенны АИР 3-2, сборник тестовых программ «Сигурд-Тест».

Установив необходимые параметры, анализатор спектра выводит ПЭМИ интерфейса SATA на частоте 1,5 ГГц. Пример спектра сигнала представлен на рис. 5.

Далее выключим тестовый режим записи «Сигурд-Тест» и посмотрим, изменится ли спектр. Изменения спектра представлены на рис. 6.

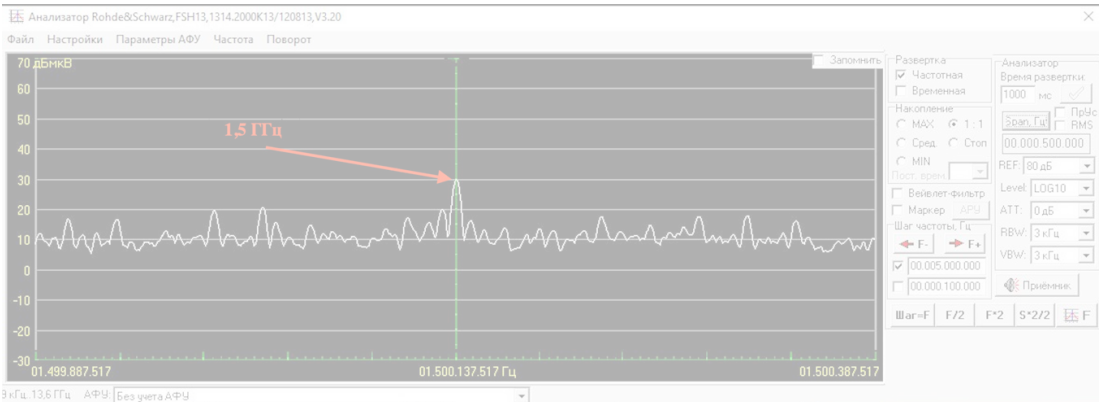


Рис. 5. Спектр сигнала на частоте 1,5 ГГц, SPAN 500 кГц

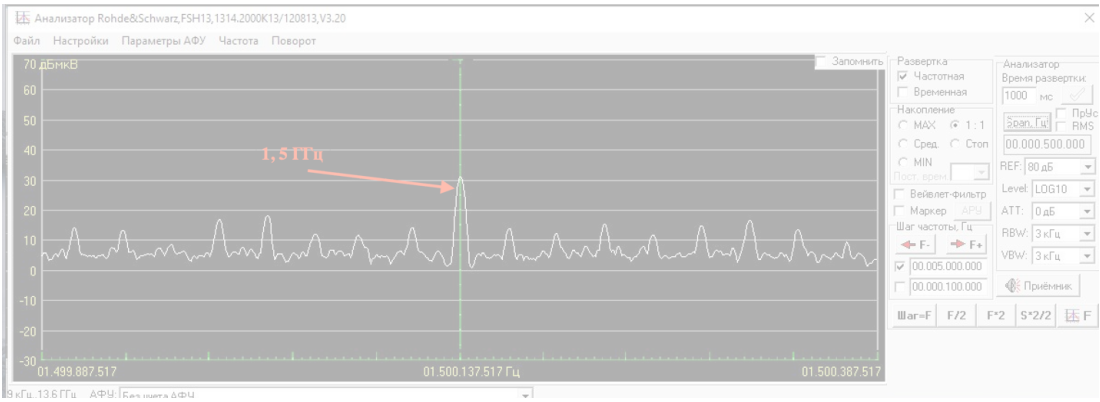


Рис. 6. Спектр сигнала при выключенном режиме записи

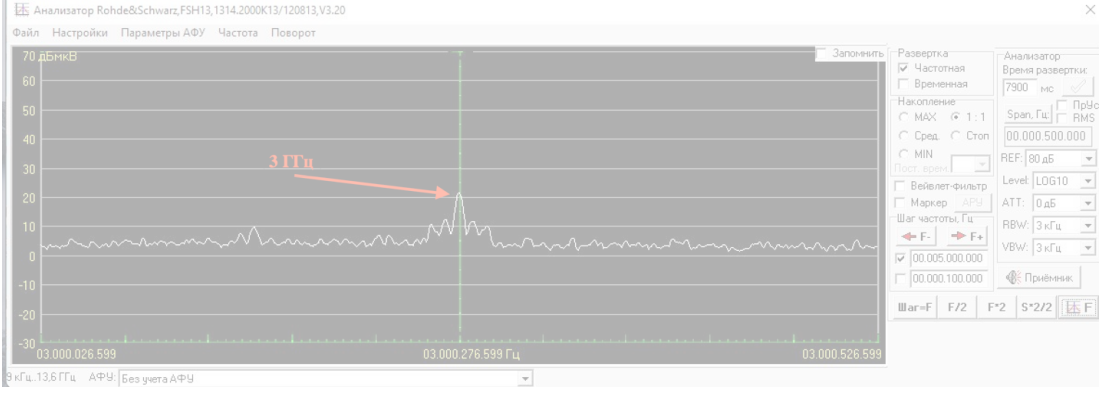


Рис. 7. Вторая гармоника

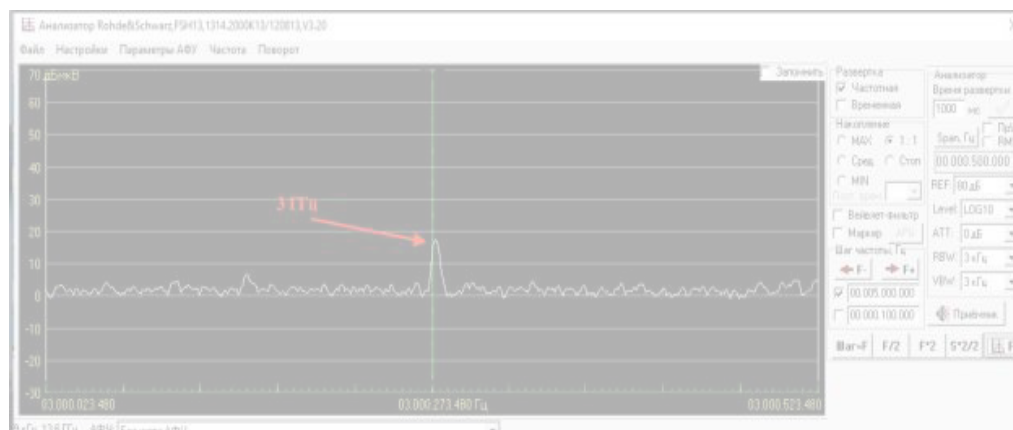


Рис. 8. Спектр сигнала при выключенном режиме

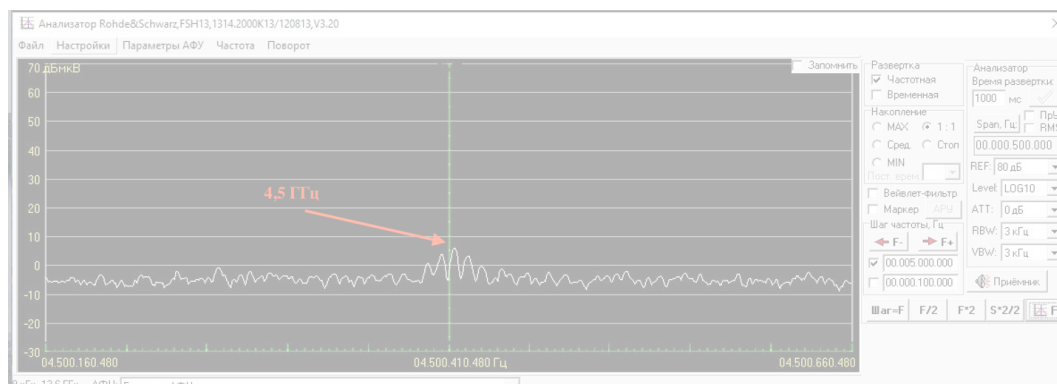


Рис. 9. Третья гармоника

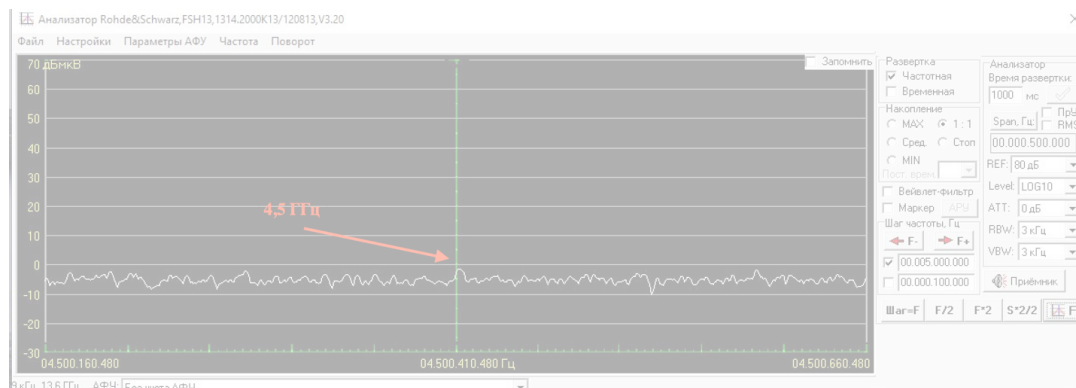


Рис. 10. Спектр сигнала при выключенном режиме



Рис. 11. Четвертая гармоника



Рис. 12. Спектр сигнала при выключенном режиме

Путем сравнения спектрограмм можно заметить, что спектр сигнала при включении/выключении теста действительно изменяется.

Следующая гармоника находится около 3 ГГц, поэтому необходимо включить тестовую программу в режим «Чтения» и выставить центральную частоту 3 ГГц и искать вторую гармонику рядом. Вторая гармоника представлена на рис. 7.

Чтобы убедиться, что это наша вторая гармоника выключаем режим «Чтения». Результат представлен на рис. 8.

Следующая гармоника находится около 4,5 ГГц, поэтому выставляем центральную частоту 4,5 ГГц и ищем сигнал. Третья гармоника представлена на рис. 9.

Чтобы убедиться, что это наша третья гармоника выключаем режим «Чтения». Результат представлен на рис. 10.

Четвертая гармоника, выставляем центральную частоту 6 ГГц и ищем спектр. Четвертая гармоника представлена на рис. 11.

Чтобы убедиться, что это наша четвертая гармоника выключаем режим «Чтения». Результат представлен на рис. 12.

Таким образом можно сделать вывод, что утечка информации через побочные электромагнитные излучения интерфейса SATA является реальной угрозой для безопасности данных, передаваемых периферийными устройства, например, HDD, SSD, DVD-Rom. Для всестороннего исследования рассматриваемого канала утечки актуально продолжить исследование различных модификаций интерфейса SATA в сочетании с разнообразными периферийными устройствами. Для предотвращения утечки необходимо использовать специальные средства измерения и проводить соответствующие мероприятия по защите данных. Важным шагом в этом направлении является проведение измерений побочных электромагнитных излучений средств вычислительной техники, что позволяет выявить уязвимые места и принять меры по их устранению.

Литература

1. Субботин С. Д., Поршнев С. В., Пономарева О. А. Исследование поведения информативных сигналов от накопителя на жестких магнитных дисках при обработке информации в разных областях диска // Вестник УрФО. Безопасность в информационной сфере. – 2020. – №. 1 (35). – С. 5-11.
2. Поршнев С. В., Беляев Д. О. Скрытые технические каналы утечки информации, обрабатываемой средствами вычислительной техники: анализ результатов исследований // Вестник УрФО. Безопасность в информационной сфере. – 2020. – №. 4 (38). – С. 5-21.
3. Поршнев С. В., Беляев Д. О. Скрытые технические каналы утечки информации, обрабатываемой в средствах вычислительной техники: анализ действующей нормативно-методической базы, терминология // Вестник УрФО. Безопасность в информационной сфере. – 2021. – №. 1 (39). – С. 5-13.
4. Бузов Г.А, Калинин С.В, Кондратьев А.В. Защита от утечки информации по техническим каналам. М.: Горячая линия – Телеком, 2005.
5. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Радиомониторинг задачи, методы, средства. М.: Горячая линия – Телеком, 2006.
6. Serial ATA International Organization: Serial ATA Revision 3.1. 18-July-2011 Gold Revision https://sata-io.org/system/files/specifications/SerialATA_Revision_3_1_Gold.pdf

7. Испытательная лаборатория к вопросу оценки ПЭМИН цифровых сигналов. Жёсткие диски (HDD), оптические диски (CD, DVD) Автор: Кондратьев А.В. <https://www.mascom.ru/library/statyi/isyatelnaya-laboratoriya-k-voprosu-otsenki-pemin-tsifrovyykh-signalov-zhyestkie-diski-hdd-optichesk.php>
8. Mordechai Guri. SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables. <https://doi.org/10.48550/arXiv.2207.07413>
9. HDMI Forum. HDMI Forum. <https://web.archive.org/web/20180222200543/https://www.hdmi.org/learningcenter/faq.aspx#1>
10. Марков Г.Т., Сазонов Д.М. Антенны. – М.: Энергия, 1975. – 528 с.

References

1. Subbotin S. D., Porshnev S. V., Ponomareva O. A. Issledovaniye povedeniya informativnykh signalov ot nakopitelya na zhestkikh magnitnykh diskakh pri obrabotke informatsii v raznykh oblastiakh diska // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2020. – №. 1 (35). – S. 5-11.
2. Porshnev S. V., Belyayev D. O. Skrytyye tekhnicheskiye kanaly utechki informatsii, obrabatyvayemoy sredstvami vychislitel'noy tekhniki: analiz rezul'tatov issledovaniy // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2020. – №. 4 (38). – S. 5-21.
3. Porshnev S. V., Belyayev D. O. Skrytyye tekhnicheskiye kanaly utechki informatsii, obrabatyvayemoy v sredstvakh vychislitel'noy tekhniki: analiz deystvuyushchey normativno-metodicheskoy bazy, terminologiya // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2021. – №. 1 (39). – S. 5-13.
4. Buzov G.A, Kalinin S.V, Kondrat'yev A.V. Zashchita ot utechki informatsii po tekhnicheskim kanalam. M.: Goryachaya liniya –Telekom, 2005.
5. Rembovskiy A.M., Ashikhmin A.V., Koz'min V.A. Radiomonitoring zadachi, metody, sredstva. M.: Goryachaya liniya –Telekom, 2006.
6. Serial ATA International Organization: Serial ATA Revision 3.1. 18-July-2011 Gold Revision https://sata-io.org/system/files/specifications/SerialATA_Revision_3_1_Gold.pdf
7. Ispytatel'naya laboratoriya k voprosu otsenki PEMIN tsifrovyykh signalov. Zhostkiye diski (HDD), opticheskiye diski (CD, DVD) Avtor: Kondrat'yev A.V. <https://www.mascom.ru/library/statyi/isyatelnaya-laboratoriya-k-voprosu-otsenki-pemin-tsifrovyykh-signalov-zhyestkie-diski-hdd-optichesk.php>
8. Mordechai Guri. SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables. <https://doi.org/10.48550/arXiv.2207.07413>
9. HDMI Forum. HDMI Forum. <https://web.archive.org/web/20180222200543/https://www.hdmi.org/learningcenter/faq.aspx#1>
10. Markov G.T., Sazonov D.M. Antenny. – M.: Energiya, 1975. – 528 s.

ШВЫРЕВ Борис Анатольевич, кандидат физико-математических наук, доцент, доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий. Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет МВД России имени В. Я. Кикотя». 117997, Москва, ул. Академика Волгина, д.12. E-mail: bor2275@yandex.ru

SHVYREV Boris Anatolyevich, Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Special Information Technologies of the educational and scientific complex of information Technologies. Federal State Public Educational Establishment of Higher Education "Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Y. Kikot". 117997, Moscow, Akademika Volgina str., 12. E-mail: bor2275@yandex.ru

ПОЛИКАРПОВ Евгений Сергеевич, кандидат технических наук, доцент, начальник кафедры специальных информационных технологий учебно-научного комплекса информационных технологий. Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет МВД России имени В. Я. Кикотя». 117997, Москва, ул. Академика Волгина, д.12. E-mail: binox@mail.ru

POLIKARPOV Evgeny Sergeevich, Candidate of Technical Sciences, Associate Professor, Head of the Department of Special Information Technologies of the educational and scientific complex of

information Technologies. Federal State Public Educational Establishment of Higher Education "Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Y. Kikot". 117997, Moscow, Akademika Volgina str., 12. E-mail: binox@mail.ru

АНИСИМОВ Сергей Леонидович, кандидат технических наук, доцент кафедры физики и радиоэлектроники. Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт МВД России». 394065, Воронеж, проспект Патриотов, д. 53. E-mail: anisimov12@mail.ru

ANISIMOV Sergey Leonidovich, Candidate of Technical Sciences, Associate Professor of the Department of Physics and Radioelectronics. Federal State-owned educational institution of higher Education "Voronezh Institute of the Ministry of Internal Affairs of Russia". 394065, Voronezh, Patriots Avenue, 53. E-mail: anisimov12@mail.ru



ОЦЕНКА АДЕКВАТНОСТИ НЕКОТОРЫХ МЕТОДОВ ЭЛЕКТОРАЛЬНОЙ КРИМИНАЛИСТИКИ НА ОСНОВЕ АНАЛИЗА СГЕНЕРИРОВАННЫХ СЛУЧАЙНЫХ ДАННЫХ, СТАТИСТИЧЕСКИЕ СВОЙСТВА КОТОРЫХ ПОДОБНЫ РЕАЛЬНЫМ ЭЛЕКТОРАЛЬНЫМ ДАННЫМ

В статье описаны алгоритм генерации случайных данных, статистические свойства которых подобны статистическим свойствам реальных электоральных, представленных в Центральную избирательную комиссию (ЦИК) Российской Федерации (РФ) в ходе выборов в 2018 г. Президента России избирательными комиссиями нижних уровней (участковыми избирательными комиссиями (УИК), территориальными избирательными комиссиями (ТИК), избирательными комиссиями (ИК) уровня субъектов РФ и приравненных к ним ИК «Город Байконур (Республика Казахстан)», ИК «Территории за пределами РФ») и, собственно, статистические характеристики этих данных.

Обсуждаются результаты применения к сгенерированным данным выбранных методов электоральной криминалистики, обеспечивающих по утверждениям электоральных статистиков, оппозиционных власти, действующей в РФ, электоральных оппозиционных статистиков (ЭОС), выявление возможных фальсификаций результатов выборов, в том числе: метод анализа распределений первой цифры после запятой в показателе явка избирателей на выборы, метод Бебера и Скакко, метод Шпилькина, модифицированный метод Шпилькина. Продемонстрировано, что изученные методы электоральной криминалистики обнаруживают индикаторы фальсификаций в модельных заведомо не сфальсифицированных электоральных данных.

В этой связи, сделан обоснованный вывод о том, что обвинения в масштабных

фальсификациях результатов выборов и референдумов, проводимых в России в конце XX – первой четверти XXI вв., предъявляемые избирательной системе России ЭОС на основе результатов анализа электоральных данных с помощью методов электоральной криминалистики, отвергаются результатами проведенного исследования.

Ключевые слова: выборы, электоральные данные, электоральная криминалистика, делигитимация выборов, метод Бебера и Скакко, метод Шпилкина.

Porshnev S.V., Ryabko N.Yu.

ASSESSMENT OF THE SOME ELECTORAL CRIMINOLOGY METHODS ADEQUACY BASED ON THE ANALYSIS OF GENERATED RANDOM DATA, THE STATISTICAL PROPERTIES OF WHICH ARE SIMILAR TO REAL ELECTORAL DATA

The article describes the algorithm for generating random data whose statistical properties are similar to the statistical properties of real electoral data submitted to the Central Election Commission (CEC) of the Russian Federation (RF) during the 2018 presidential elections by lower-level election commissions (precinct election commissions (PEC), territorial election commissions (TEC), election commissions (EC) at the level of the subjects of the Russian Federation and equivalent EC «The Baikonur city (Republic of Kazakhstan)», EC «Territories outside the Russian Federation») and in fact the statistical characteristics of these data.

The results of applying the selected electoral criminalistics methods generated data are discussed, which, according to the statements of electoral statisticians, the opposition authorities operating in the Russian Federation, electoral opposition statisticians (EOS), identify possible falsifications of election results, including: the analyzing the distributions of the first digit after the decimal point in the voter turnout indicator method, the Beber and Scacco method, the Shpilkin method, the modified Shpilkin method.

It is demonstrated that the studied electoral criminalistics methods detect indicators of falsifications in model deliberately not falsified electoral data.

In this regard, a reasonable conclusion is made that the accusations of large-scale falsifications of the results of elections and referendums held in Russia at the end of the XX – first quarter of the XXI century, presented to the electoral system of Russia by the EOS based on the results of the analysis of electoral data using methods of electoral criminology, are rejected by the results of the study.

Keywords: elections, electoral data, election commission, electoral forensics, Shpilkin method, modified Shpilkin method.

Введение

Результаты многомерного статистического анализа электоральных данных, представленных УИК в ЦИК РФ по итогам выборов Президента России в 2018 г., проведенного в [1], позволили сделать обоснованный вывод об отсутствии признаков масштабных фальсификаций результатов выборов в пользу их победителя – В.В. Путина, одержавшего, априори, ожидаемую победу с явным преимуществом над остальными кандидатами: по данным ЦИК РФ за победителя выборов проголосовало 76.69 % (56 430 712 избирателей) от общего числа избирателей, принявших участие в выборах (73 578 992) при явке 67.5 % от общего числа зарегистрированных избирателей, равного 109 008 428 избирателей.

При этом, понятно, что изложенные в [1] результаты являются косвенным, но не прямым доказательством отсутствия масштабных фальсификаций электоральных данных в ходе проведения в 2018 г. выборов Президента России. В этой ситуации, очевидна необходимость прямой проверки адекватности методов выявления фальсификаций электоральных данных, популяризируемых электоральными статистиками, находящимися в оппозиции к действующей власти в РФ – электоральные оппозиционные статистики (ЭОС). Для проведения подобной проверки, как очевидно, требуются использовать электоральные данные, в которые, заведомо, не вносилось каких-либо фальсификаций. Принимая во внимание, что сегодня не существует механизмов проведения и контроля за выборами, обеспечивающих проведение «абсолютно честных» выборов, как с точки зрения сторонников победителя выборов, так и с точки зрения сторонников, проигравших выборы, представляется целесообразным синтезировать «абсолютно честные» электоральные данные, провести их анализ с помощью наиболее часто используемых методов электоральной криминалистики и оценить адекватность получаемых при этом результатов.

В статье описан алгоритм генерации случайных данных статистические характеристики, которых подобны статистическим характеристикам реальных электоральных данных, а также результаты применения выбранных методов электоральной криминалистики (метод анализа распределений первой цифры после запятой в показателе явка избирателей на выборы, метод Бебера и Скакко, метод Шпилькина, модифицированный метод Шпилькина) для их анализа.

2. Алгоритм генерация случайных данных, статистические характеристики которых подобны аналогичным характеристикам реальных электоральных данных

Априори понятно, что структура генерируемых электоральных данных, в самом общем случае, должна быть аналогичной структуре выбранных реальных электоральных данных, в качестве которых были использованы электоральные данные, представленные УИК, ТИК и ИК субъектов РФ в ЦИК РФ в ходе проведения выборов в 2018 г. Президента Российской Федерации. Их структура определяется следующей древовидной структурой системы избирательных комиссий, созданных для проведения в 2018 г. выборов Президента РФ:

- вершина дерева – ЦИК РФ,
- вершины второго уровня – 85 ИК субъектов РФ, а также две приравненные к ним ИК «г. Байконур (Республика Казахстан)» и ИК «Территория за пределами РФ» (итого 87 ИК);
- вершины третьего уровня – 2887 территориальных избирательных комиссий (ТИК), созданных ИК субъектов РФ (ТИК ИК «г. Байконур (Республика Казахстан)» и ИК «Территория за пределами РФ» не создавались);
- вершины четвертого уровня – 97314 участковых избирательных комиссии (УИК), созданных соответствующими ТИК субъектов РФ, а также 7 УИК, созданных ИК «г. Байконур (Республика Казахстан)» и 393 УИК, созданных в ЦИК в ИК «Территория за пределами РФ» (итого 97695 УИК, без учета 21 УИК, не приступивших к передаче данных в ЦИК РФ).

Однако результаты анализа электоральных данных, обсуждавшиеся в [1], подтвердили их согласованность на всех уровнях избирательной системы РФ: уровнях ЦИК РФ, ТИК РФ и приравненных к ним ИК «Город Байконур (республика Казахстан)» и ИК «Территория за пределами Российской Федерации», уровне УИК, созданных данными ТИК. В этой связи для синтеза электоральных данных, используемых далее для проверки работоспособности методов, используемых ЭОС, достаточно генерировать данные на уровне УИК.

Результаты выборов на уровне УИК характеризуются следующим набором показателей (эквивалентно, электоральные данные).

1. Число зарегистрированных УИК $N_{\text{УИК}}$ (целое число).
2. Число кандидатов, участвующих в выборах N_c (целое число).

3. Число избирателей, зарегистрированных в i -ой УИК $[N_{уик}^{ER}]_i, i = 1, N_{уик}$ (целое число).

4. Число избирателей, принявших участие в выборах в i -ой УИК $[N_{уик}^V]_i, i = 1, N_{уик}$ (целое число).

5. Явка на выборы избирателей, зарегистрированных в i -ой УИК (десятичное число, выраженное в процентах):

$$[\alpha_{уик}^{\%}]_i = \frac{[N_{уик}^V]_i}{[N_{уик}^{ER}]_i} \cdot 100\%,$$

где $i = \overline{1, N_{уик}}$.

6. Число голосов избирателей, проголосовавших в i -ой УИК за j -го кандидата (целое число):

$$[N_{уик}^V]_i^{(j)}$$

где $i = \overline{1, N_{уик}}, j = \overline{1, N_c}$.

7. Доля избирателей, проголосовавших в i -ой УИК за j -го кандидата (десятичное число, выраженное в процентах):

$$[\alpha_{уик}^{\%}]_i^{(j)} = \frac{[N_{уик}^V]_i^{(j)}}{[N_{уик}^{ER}]_i} \cdot 100\%,$$

где $i = \overline{1, N_{уик}}, j = \overline{1, N_c}$.

8. Общее количество зарегистрированных избирателей (целое число):

$$N_{уик}^{ER} = \sum_{i=1}^{N_{уик}} [N_{уик}^{ER}]_i.$$

9. Общее количество избирателей, принявших участие в выборах (целое число):

$$N_{уик}^V = \sum_{i=1}^{N_{уик}} [N_{уик}^V]_i.$$

10. Относительная явка избирателей на выборы на уровне УИК (десятичное число, выраженное в процентах):

$$\alpha_{уик}^{\%} = \frac{N_{уик}^V}{N_{уик}^{ER}} \cdot 100\%.$$

11. Общее число избирателей, проголосовавших за j -го кандидата:

$$[N_{уик}^V]_{all}^{(j)} = \sum_{i=1}^{N_{уик}} [N_{уик}^V]_i^{(j)}.$$

12. Доля избирателей, проголосовавших за j -го кандидата, вычисляемая по всем УИК (десятичное число, выраженное в процентах):

$$\alpha_{уик}^{\%} \Big|_{all}^{(j)} = \frac{[N_{уик}^V]_{all}^{(j)}}{N_{уик}^{ER}} \cdot 100\% = \frac{[N_{уик}^V]_{all}^{(j)}}{\sum_{i=1}^{N_{уик}} [N_{уик}^{ER}]_i} \cdot 100\%.$$

Из приведенного выше списка показателей видно, что они относятся к одной из следующих групп:

1. Константы ($N_{уик}, N_c$).

2. Целые случайные числа ($[N_{уик}^{ER}]_i, [N_{уик}^V]_i, [N_{уик}^V]_i^{(j)}, N_{уик}^{ER}, N_{уик}^V, [N_{уик}^V]_{all}^{(j)}$).

3. Действительные случайные числа ($[\alpha_{уик}^{\%}]_i, [\alpha_{уик}^{\%}]_i^{(j)}, \alpha_{уик}^{\%}, [\alpha_{уик}^{\%}]_{all}^{(j)}$).

При этом показатели, отнесенные ко второй и третьей группам, как показали результаты анализа электоральных данных, представленные в [1], являются некоторыми случайными выборками из соответствующих генеральных совокупностей с ограниченными областями рассеяния. Таким образом, синтез модельных электоральных данных сводится к заданию: числа участковых избирательных комиссий $N_{уик}$; заданию числа кандидатов (партий), участвующих в выборах, N_c ; генерации целочисленных СП: $[N_{уик}^{ER}]_i$, составленной из числа избирателей зарегистрированных в i -ой УИК; $[N_{уик}^V]_i$ составленной из числа избирателей, принявших участие в выборах в i -ой УИК; $[N_{уик}^V]_i^{(j)}$, составленной из числа избирателей, проголосовавших в i -ой УИК, за j -го кандидата; и далее вычислении остальных показателей, характеризующих «волеизъявление избирателей».

В связи с необходимостью генерации целочисленных СП с заданным законом распределения были проанализированы соответствующие функции пакета MATLAB ($\text{randi}(a,b)$) и языка Python ($\text{randint}(a,b)$, $\text{randrange}(a,b,s)$). Результаты проведенного анализа показали [2], что данные функции, возвращают целые случайные числа $a \leq n \leq b$ в соответствии равномерным законом распределения на отрезке $[a, b]$. Аналогичные функции, возвращающие целые случайные числа в соответствии с законом распределения, отличным от равномерного, в указанных выше программных инструментах отсутствуют. В то время как анализ электоральных данных, проведенный в [1], показал, что функции распределений у каждого из целочисленных показателей оказываются отличными от равномерного закона, поэтому для генерации целых случайных чисел проводилась в два этапа: на первом этапе в соответствии с выбранным законом распределения генерировалось целое случайное число, которое далее округлялось до ближайшего целого. (Далее, для более краткого описания алгоритма, данная двухэтапная процедура генерации целочисленных СП $[N_{уик}^{ER}]_i, [N_{уик}^V]_i$ называется генерацией целых случайных чисел.)

Кроме того, с вычислительной точки зрения оказывается более удобным сначала генерировать СП $[\alpha_{уик}^{\%}]_i$, составленную из значений относительной явки избирателей на выборы в i -ой УИК, а затем рассчитывать число избирателей, принявших участие в голосовании. Аналогично, сначала генерируется СП

$[\alpha_{\text{УИК}}]_i^{(j)}$ составленная из значений доли голов избирателей, проголосовавших в i -ой УИК за j -го кандидата, вычисляются значения СП $[N_{\text{УИК}}^V]_i^{(j)}$, а затем рассчитывается соответствующее число избирателей.

Соответственно, алгоритм генерации электоральных данных (АГЭД), реализуется выполнением следующей последовательности действий.

1. Задать число зарегистрированных УИК $N_{\text{УИК}}$ и число кандидатов, участвующих в выборах N_C .

2. Выбрать закон распределения и область рассеяния случайной величины $[N_{\text{УИК}}^{ER}]$.

3. Сгенерировать $N_{\text{УИК}}$ целых случайных чисел в соответствие с выбранными в п. 2 законом распределения и областью рассеяния – СП $\{[N_{\text{УИК}}^{ER}]_i\}, i=1, N_{\text{УИК}}$.

4. Выбрать законы распределения и области рассеяния случайных величин $[\alpha_{\text{УИК}}]_i^{(j)}$ – СП $\{[\alpha_{\text{УИК}}]_i^{(j)}\}, i=1, N_{\text{УИК}}, j=1, N_C$ так, что бы $\sum_{j=1}^{N_C} [\alpha_{\text{УИК}}]_i^{(j)} \leq 1$.

5. В соответствие с выбранными в п. 4 законами распределения и областью рассеяния сгенерировать действительные СП $\{[\alpha_{\text{УИК}}]_i^{(j)}\} i=1, N_{\text{УИК}}, j=1, N_C$.

6. Вычислить значения числа избирателей, проголосовавших за j -го кандидата в i -ой избирательной комиссии – СП $\{[N_{\text{УИК}}^V]_i^{(j)}\}, i=1, N_{\text{УИК}}, j=1, N_C$:

$$[N_{\text{УИК}}^V]_i^{(j)} = \text{round}([\alpha_{\text{УИК}}^{\%}]_i^{(j)} [N_{\text{УИК}}^{ER}]_i).$$

Наличие синтезированных электоральных данных позволяет далее последовательно вычислить следующие показатели:

– число зарегистрированных избирателей

$$N_{\text{УИК}}^{ER} = \sum_{i=1}^{N_{\text{УИК}}} [N_{\text{УИК}}^{ER}]_i;$$

– число избирателей, принявших участие

$$\text{в выборах в } i\text{-ой УИК } [N_{\text{УИК}}^V]_i = \sum_{j=1}^{N_C} [N_{\text{УИК}}^V]_i^{(j)};$$

– число избирателей, принявших участие

$$\text{в выборах, } N_{\text{УИК}}^V = \sum_{i=1}^{N_{\text{УИК}}} [N_{\text{УИК}}^V]_i = \sum_{i=1}^{N_{\text{УИК}}} \sum_{j=1}^{N_C} [N_{\text{УИК}}^V]_i^{(j)};$$

– относительную явку на выборы $[\alpha_{\text{УИК}}^{\%}]_{\text{all}}$:

$$[\alpha_{\text{УИК}}^{\%}]_{\text{all}} = \text{round}([N_{\text{УИК}}^V] / [N_{\text{УИК}}^{ER}] \cdot 10^4) / 100;$$

далее провести статистический анализ СП $\{[N_{\text{УИК}}^{ER}]_i\}, \{[N_{\text{УИК}}^V]_i\}, \{[N_{\text{УИК}}^{ER}]_i^{(j)}\}, \{[N_{\text{УИК}}^V]_i^{(j)}\}$, анализ распределений цифр в показателях $\{[\alpha_{\text{УИК}}^{\%}]_i\}, \{[\alpha_{\text{УИК}}^{\%}]_i^{(j)}\}, i=1, N_{\text{УИК}}, j=1, N_C$, а также анализ зависимостей $[\alpha_{\text{УИК}}]_i^{(j)} = f([\alpha_{\text{УИК}}]_i)$.

3. Анализ статистических свойств синтезированных электоральных данных

Из описания АГЭД, приведенного в предыдущем разделе, видно, что необходимым

условием его использования является выбор вида функций распределения СП $[N_{\text{УИК}}^{ER}]_i, [N_{\text{УИК}}^V]_i, [\alpha_{\text{УИК}}]_i, [\alpha_{\text{УИК}}]_i^{(j)}$, имеющих ограниченную область рассеяния, который определяется следующими обстоятельствами.

1. В связи с невозможностью получить прямые доказательства, свидетельствующие об отсутствии фальсификаций электоральных данных, полученных в ходе проведения конкретных выборов, использование для синтеза электоральных данных оценок функций распределений, выбранных первичных электоральных данных, возникает закономерный вопрос о достоверности с точки зрения электоральной криминалистики, собственно, синтезированных данных.

2. Де-факто, большинство методов, используемых ЭОС, основаны на предположении о том, что перечисленные в разделе 2. показатели электорального процесса имеют нормальный закон распределения, поэтому обнаруживаемые отличия от нормального закона распределения принимаются в качестве доказательств фальсификаций.

3. Любое статистическое распределение соответствует некоторому случайному процессу без последствия. В частности, нормальный закон распределения, как было показано А. Эйнштейном [3], соответствует конечному состоянию броуновского процесса в неограниченной области, математическая модель которого рассматривается, например, в [4].

4. Статистические распределения случайной величины с ограниченной областью рассеяния, как показано М. Смолуховским [5–7], соответствуют распределению координат случайного броуновского процесса в ограниченной области. Программные инструменты для компьютерного моделирования случайных блужданий в ограниченной области рассеяния, созданные в пакете MATLAB, описаны в [8]. Алгоритмы оценки параметров плотностей распределений и функций распределений случайных величин, построенных на основе моделей М. Смолуховского, рассматривались в [9, 10]. Алгоритмическое обеспечение для оценивания плотностей вероятностей и функций распределений случайных последовательностей с ограниченной областью рассеяния, а также их генерации, описаны в [10]. Существует программная реализация данного алгоритмического обеспечения – программная библиотека ES&RP [11].

Следует отметить, принципиальные отличия

чия между усеченным нормальным распределением и случайной величины с ограниченной областью рассеяния.

Усеченное нормальное распределение (УНР) традиционно используется в задачах оценки надежности технических систем и точности производства [12–18]. Напомним, следуя [10], что УНР $N'(\mu, \sigma)$ имеет случайная подпоследовательность $\{x'\}$, извлеченная из

случайной последовательности $\{x\}$, имеющей ПР $N(\mu, \sigma)$ каждый элемент которой удовлетворяет следующим условиям:

$$x_{\min} \leq x'_k \leq x_{\max},$$

где $x_{\min}, x_{\max}$ – точки усечения.

Основные характеристики УНР и соответствующие формулы для их вычисления представлены в таблице 1.

Распределение случайной величины с

Таблица 1

Характеристики УНР [3.48]

Название характеристики	Формула или числовое значение характеристики
Обозначение	$N'(\mu, \sigma, x_{\min}, x_{\max})$
Параметры	$\mu, \sigma, x_{\min}, x_{\max}$
Плотность распределения	$f_{LIM}(x; \mu, \sigma, x_{\min}, x_{\max}) = \frac{1}{\sigma} \frac{\varphi\left(\frac{x-\mu}{\sigma}\right)}{F\left(\frac{x_{\max}-\mu}{\sigma}\right) - F\left(\frac{x_{\min}-\mu}{\sigma}\right)},$ где $\varphi(x)$ – плотность стандартного нормального распределения $N(0,1)$, $F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{\xi^2}{2}} d\xi$ – функция Лапласа, μ, σ – параметры исходного нормального распределения, $x_{\min} < x_{\max}$ – точки усечения
Функция распределения	$F_{LIM}(x; \mu, \sigma, x_{\min}, x_{\max}) = \int_{a_1}^x f_{LIM}(\xi; \mu, \sigma, x_{\min}, x_{\max}) d\xi =$ $\frac{1}{\sigma} \frac{1}{F\left(\frac{x_{\max}-\mu}{\sigma}\right) - F\left(\frac{x_{\min}-\mu}{\sigma}\right)} \int_{a_1}^x \varphi\left(\frac{\xi-\mu}{\sigma}\right) d\xi =$ $\frac{F\left(\frac{x-\mu}{\sigma}\right) - F\left(\frac{a_1-\mu}{\sigma}\right)}{F\left(\frac{x_{\max}-\mu}{\sigma}\right) - F\left(\frac{x_{\min}-\mu}{\sigma}\right)}$
Среднее значение	$M[x] = \mu - (\lambda_2 - \lambda_1)\sigma,$ где $\lambda_1 = \frac{\varphi(\xi_1)}{F(\xi_2) - F(\xi_1)}$, $\lambda_2 = \frac{\varphi(\xi_2)}{F(\xi_2) - F(\xi_1)}$, $\xi_1 = \frac{x_{\min} - \mu}{\sigma}$, $\xi_2 = \frac{x_{\max} - \mu}{\sigma}$
Дисперсия	$D[x] = (1 + \lambda_1 \xi_1 - \lambda_2 \xi_2 + (\lambda_1 + \lambda_2)^2) \sigma^2$

ограниченной областью рассеяния, как показано в [10], вычисляется по формуле:

$$f_{LAD}(x; x_0, \sigma, l) = A \left[\varphi(x; x_0, \sigma, l) + \sum_{g=0}^{\infty} \varphi_{2g+1}^{\pm}(x; x_0, \sigma, l) + \sum_{g=1}^{\infty} \varphi_{2g}^{\pm}(x; x_0, \sigma, l) \right],$$

где A – нормировочный коэффициент, определяемый из условия:

$$\int_a^b f_{LAD}(\xi; x_0, \sigma, l) d\xi = 1,$$

$$\varphi(x; x_0, \sigma, l) = \exp\left[-(x - x_0)^2 / 2\sigma^2\right],$$

$$\varphi_{2g+1}^{\pm}(x; x_0, \sigma, l) = \exp\left[-(x - x_{2g+1}^{\pm})^2 / 2\sigma^2\right],$$

$$\varphi_{2g}^{\pm}(x; x_0, \sigma, l) = \exp\left[-(x - x_{2g}^{\pm})^2 / 2\sigma^2\right],$$

здесь x_0 – координата точки, в которой нахо-

дится порождающий источник с плотностью распределения $\varphi(x; x_0, \sigma, l)$, $l = x_{\max} - x_{\min}$, $x_{2g+1}^{\pm}, x_{2g}^{\pm}$ вычисляются по формулам:
 $x_{2g}^{\pm} = \pm 4gl + x_0, x_{2g+1}^{\pm} = \pm (4g + 2)l - x_0$,
 где $g = 0, 1, \dots$

Характеристики рассматриваемого распределения и соответствующие формулы для их вычисления представлены в таблице 2.
 В [10] доказано, что при вычислении плотности распределения и функции распре-

Таблица 2

Характеристики плотности распределения и функции распределения случайной величины с ограниченной областью рассеяния

Название характеристики	Формула или числовое значение характеристики
Обозначение	$LAD(x_0, \sigma, x_{\min}, x_{\max})$
Параметры	$\mu, \sigma, x_{\min}, x_{\max}$
Плотность распределения	$f_{LAD}(x; x_0, \sigma, x_{\min}, x_{\max}) = A \left[\varphi(x; x_0, \sigma, x_{\min}, x_{\max}) + \sum_{g=0}^{\infty} \varphi_{2g+1}^{\pm}(x; x_0, \sigma, x_{\min}, x_{\max}) + \sum_{g=1}^{\infty} \varphi_{2g}^{\pm}(x; x_0, \sigma, x_{\min}, x_{\max}) \right],$ где A – нормировочный коэффициент, определяемый из условия $\int_{x_{\min}}^{x_{\max}} f_{LAD}(\xi; x_0, \sigma, x_{\min}, x_{\max}) d\xi = 1,$ $\varphi(x; x_0, \sigma, x_{\min}, x_{\max}) = \exp\left[-(x - x_0)^2 / 2\sigma^2\right],$ $\varphi_{2g+1}^{\pm}(x; x_0, \sigma, x_{\min}, x_{\max}) = \exp\left[-(x - x_{2g+1}^{\pm})^2 / 2\sigma^2\right],$ $\varphi_{2g}^{\pm}(x; x_0, \sigma, x_{\min}, x_{\max}) = \exp\left[-(x - x_{2g}^{\pm})^2 / 2\sigma^2\right],$ $x_{2g}^{\pm} = \pm 4g(x_{\max} - x_{\min}) + x_0, \quad x_{2g+1}^{\pm} = \pm (4g + 2)(x_{\max} - x_{\min}) - x_0,$ $x_{\min}, x_{\max}$ – границы области рассеяния
Функция распределения	$F_{LAD}(x; x_0, \sigma, x_{\min}, x_{\max}) = \int_{x_{\min}}^x f_{LAD}(\xi; x_0, \sigma, x_{\min}, x_{\max}) d\xi$

деления на компьютере достаточно использовать $g \leq 5$.

Для генерации реализаций случайных процессов была использована функция `GenerateBoundData(Mu, Sigma, a1, a2, NumElements)`, где μ, σ – параметры порождающего нормального распределения; $a1, a2$ – левая и правая границы области рассеяния, соответственно, NumElements – число членов генерируемой последовательности, которая входит в состав программной библиотеки ES&RP [11].

Рассмотрим результаты многомерного статистического анализа типичных электро-альных данных, сгенерированных в соответствии с АГЭД, описанным в разделе 2, в предположении, что в выборах принимали участие два кандидата, со следующими значени-

ями параметров, представленными в таблице 3.

Визуализация синтезированной СП $\left\{ \left[N_{УИК}^{ER} \right]_i \right\}, i = 1, N_{УИК}$, составленной из значений числа избирателей, зарегистрированных в данной УИК, и аппроксимация Парзена-Розенблатта ее плотности распределения представлены на рис. 1.

При этом «минимальное число зарегистрированных в соответствующей УИК избирателей» $\min\left(\left\{ \left[N_{УИК}^{ER} \right]_i \right\}\right) = 11$, «максимальное число зарегистрированных в соответствующей УИК избирателей» $\max\left(\left\{ \left[N_{УИК}^{ER} \right]_i \right\}\right) = 3179$, «общее число зарегистрированных избирателей» $N_{all}^{ER} = 92\,088\,068$, что сравнимо с числом избирателей, принявших участие в 2018 г. в выборах Президента РФ, общее число которых оказалось равным 73 955 927, «явка избирателей на выборы» составила 80.31 % (ре-

Параметры имитационной модели, использованные для генерации электоральных данных

Название параметра	Обозначение параметра	Значение параметра
Параметры, используемые для генерации числа избирателей, зарегистрированных в данных УИК		
Число участковых избирательных комиссий	$N_{\text{УИК}}$	$9 \cdot 10^4$
Математическое ожидание порождающего нормального распределения	μ	1017
Дисперсия порождающего нормального распределения	σ	502
Левая граница области рассеяния	a_1	6
Правая граница области рассеяния	a_2	10000
Параметры, используемые для генерации доли избирателей, проголосовавших в данной УИК за победившего на выборах кандидата		
Математическое ожидание порождающего нормального распределения	μ	0.6
Дисперсия порождающего нормального распределения	σ	0.07
Левая граница области рассеяния	a_1	0.51
Правая граница области рассеяния	a_2	1.0
Параметры, используемые для генерации доли избирателей, проголосовавших в данной УИК за проигравшего на выборах кандидата		
Математическое ожидание порождающего нормального распределения	μ	0.11
Дисперсия порождающего нормального распределения	σ	0.015
Левая граница области рассеяния	a_1	0.1
Правая граница области рассеяния	a_2	0.2

альная явка на выборы 2018 г. Президента РФ – 67,54 % от общего количества избирателей, включенных в списки).

Визуализация сгенерированной СП $\{\alpha_{\text{УИК}}^{(i)}\}, i = \overline{1, N_{\text{УИК}}}$, составленной из значений «доли числа избирателей, проголосовавших в i -ой УИК за кандидата № 1», и аппроксимация Розенблатта-Парзена [17–20] ее плот-

ности распределения представлены на рис. 2.

Из рис. 2 видно, что минимальное значение «доли голосов избирателей, проголосовавших за кандидата № 1» (победителя выборов), $\min\left(\{\alpha_{\text{УИК}}^{(i)}\}\right) = 0.5102$ (51.02% от «числа избирателей, принявших участие в выборах в данной УИК»), максимальное значение

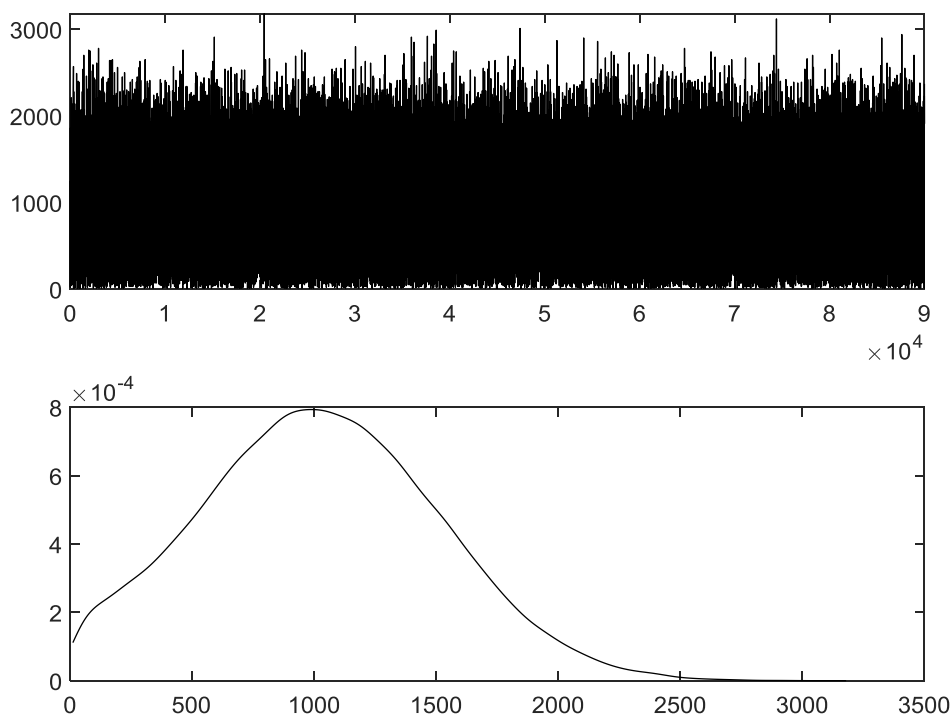


Рис. 1. Визуализация СП $\left\{ \left[N_{УИК}^{ER} \right]_i \right\}, i = \overline{1, N_{УИК}}$ (сверху) и аппроксимация Розенблатта-Парзена (нормальное ядро, $h^* = 54.497$) ее ПР (снизу)

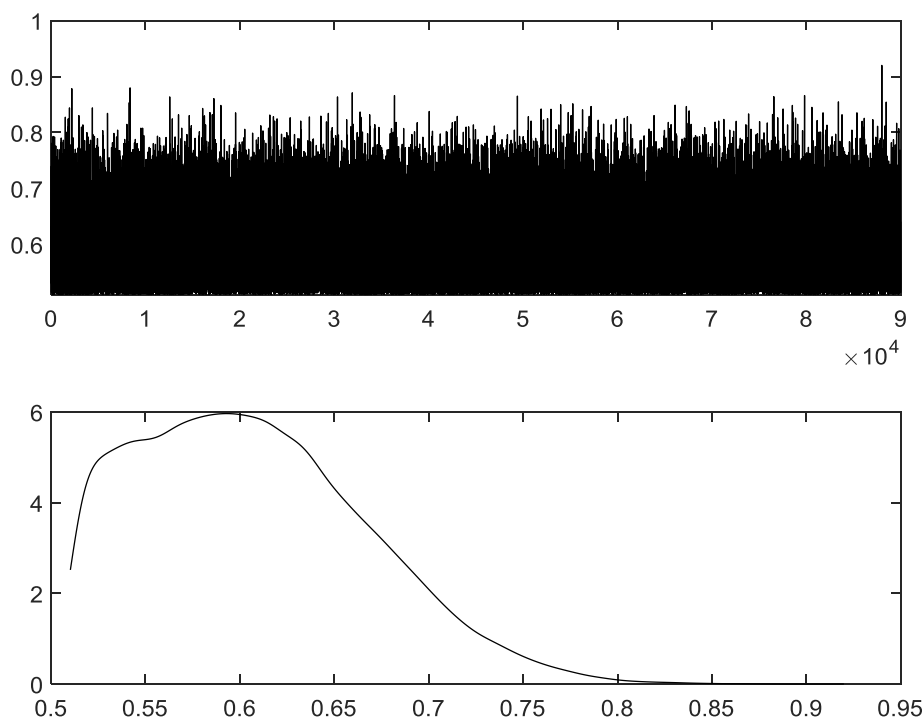


Рис. 2. Визуализация СП $\left\{ \left[\alpha_{УИК}^{(2)} \right]_i \right\}, i = \overline{1, N_{УИК}}$ (сверху) и аппроксимация Розенблатта-Парзена (нормальное ядро, $h^* = 0.0071$) ее ПР (снизу)

данного показателя $\max \left\{ \left[\alpha_{УИК}^{(1)} \right]_i \right\} = 0.8844$ (88.44% от «числа избирателей, принявших участие в выборах в данной УИК»).

Визуализация сгенерированной СП $\left\{ \left[\alpha_{УИК}^{(2)} \right]_i \right\}, i = \overline{1, N_{УИК}}$ составленной из значений

«доли числа избирателей, проголосовавших в i -ой УИК за кандидата № 2», и аппроксимация Розенблатта-Парзена ее плотности распределения представлены на рис. 3.

Из рис. 3 видно, что минимальное значе-

ние «доли голосов избирателей, проголосовавших за кандидата № 1» (победителя выборов), $\min\left\{\left\{\alpha_{уик}^{(2)}\right\}\right\}=0.1001$ (10.01% от «числа избирателей, принявших участие в выборах в данной УИК»), максимальное значение данного показателя $\max\left\{\left\{\alpha_{уик}^{(2)}\right\}\right\}=0.1713$ (17.13% от числа избирателей, принявших участие в выборах в данной УИК).

Визуализация сгенерированной СП

$\left\{\left[N_{уик}^V\right]_i^{(1)}\right\}, i=1, \overline{N_{уик}}$ составленной из значений «числа избирателей, проголосовавших в i-ой УИК за кандидата № 1», и аппроксимация Розенблатта-Парзена ее плотности распределения представлены на рис. 4.

Из рис. 4 видно, что минимальное значение показателя «число голосов избирателей, проголосовавших за кандидата № 1» (победителя выборов), $\min\left\{\left\{N_{уик}^V\right\}\right\}=6$,

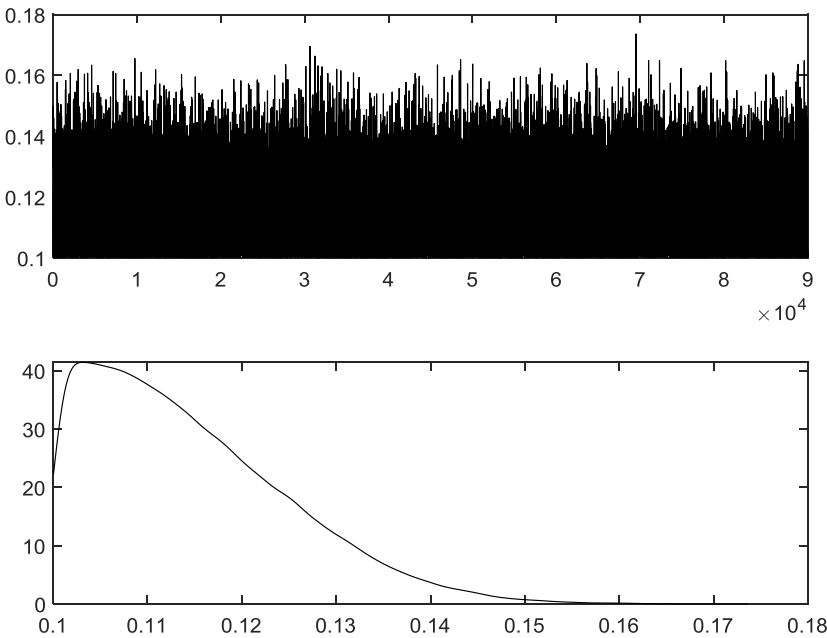


Рис. 3. Визуализация СП $\left\{\left[\alpha_{уик}^{(2)}\right]_i\right\}, i=1, \overline{N_{уик}}$ (сверху) и аппроксимация Розенблатта-Парзена (нормальное ядро, $h^*=0.0012$) ее ПР (снизу)

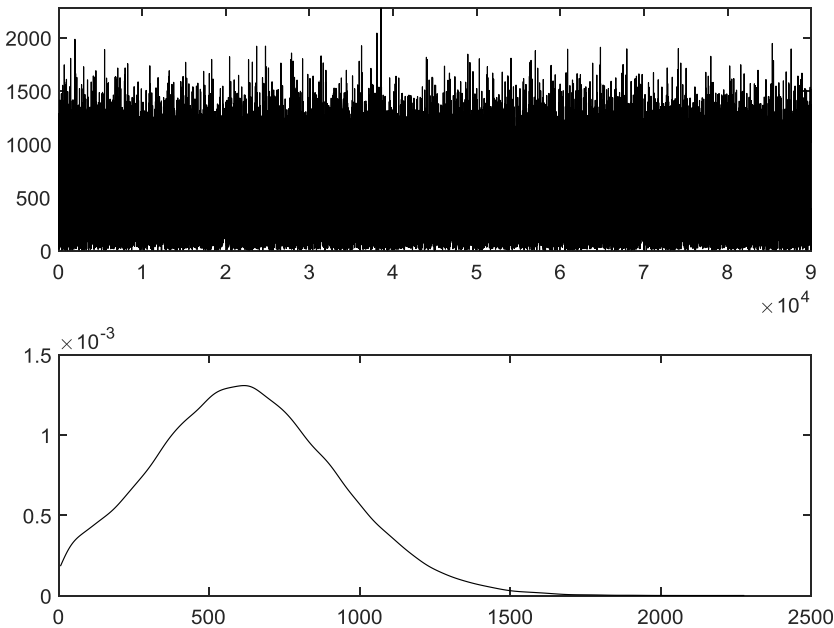


Рис. 4. Визуализация СП $\left\{\left[N_{уик}^V\right]_i\right\}, i=1, \overline{N_{уик}}$ (сверху) и аппроксимация Розенблатта-Парзена (нормальное ядро, $h^*=33.199$) ее ПР (снизу)

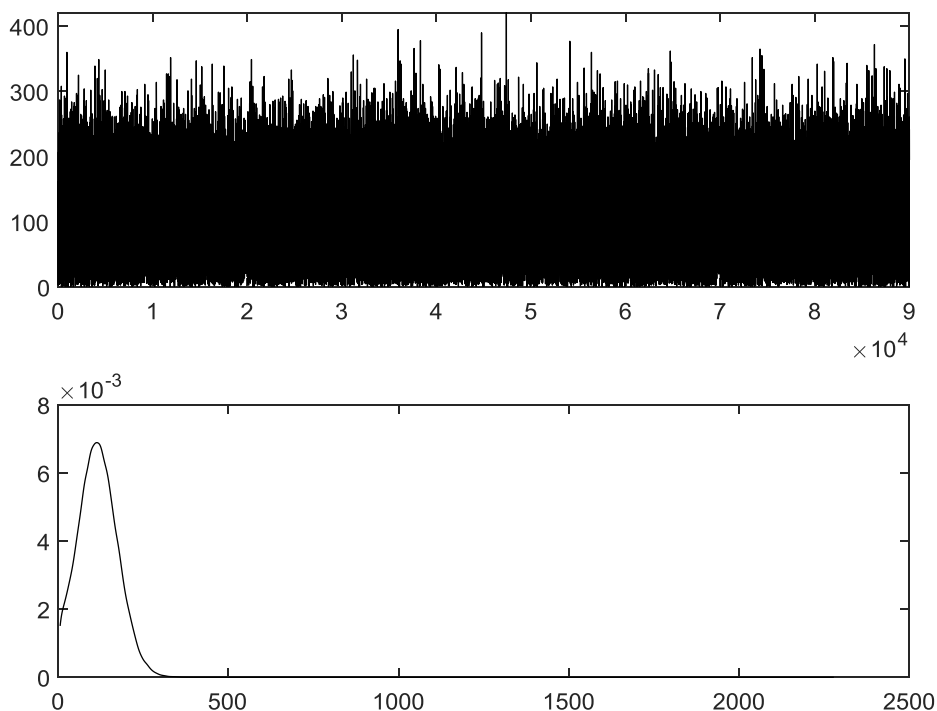


Рис. 5. Визуализация СП $\left\{ \left[N_{УИК}^V \right]_i^{(2)} \right\}, i = \overline{1, N_{УИК}}$ (сверху) и аппроксимация Розенблатта-Парзена (нормальное ядро, $h^* = 6.255$) ее ПР (снизу)

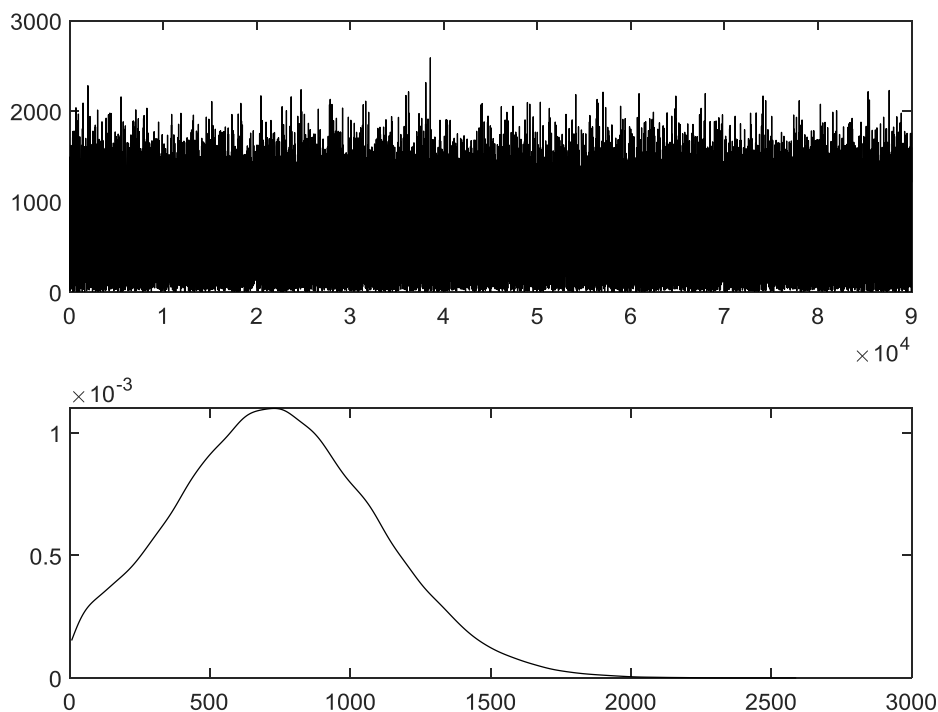


Рис. 6. Визуализация СП $\left\{ \left[N_{УИК}^V \right]_i \right\}, i = \overline{1, N_{УИК}}$ (сверху) и аппроксимация Розенблатта-Парзена (нормальное ядро, $h^* = 39.294$) ее ПР (снизу)

максимальное значение данного показателя $\max \left\{ \left\{ \left[N_{УИК}^V \right]_i^{(1)} \right\} \right\} = 2278$.

Визуализация сгенерированной СП составленной из значений «числа избирателей, проголосовавших в

i -ой УИК за кандидата № 1», и аппроксимация Розенблатта-Парзена ее плотности распределения представлены на рис. 5.

Из рис. 5 видно, что минимальное значение голосов избирателей, проголосовавших

ших за кандидата № 1 (победителя выборов), $\min\left(\left\{\left[N_{УИК}^V\right]_i^{(2)}\right\}\right)=1$, максимальное значение данного показателя $\max\left(\left\{\left[N_{УИК}^V\right]_i^{(2)}\right\}\right)=421$.

Визуализация синтезированной случайной последовательности $\left\{\left[N_{УИК}^V\right]_i\right\}, i=\overline{1, N_{УИК}}$, составленной из значений числа избирателей, проголосовавших в i-ой УИК, и аппроксимация Розенблатта-Парзена ее плотности распределения представлены на рис. 6.

Из рис. 6 видно, что минимальное значение «голосов избирателей, проголосовавших на выборах» $\min\left(\left\{\left[N_{УИК}^V\right]_i\right\}\right)=7$, максимальное значение данного показателя $\max\left(\left\{\left[N_{УИК}^V\right]_i\right\}\right)=2589$.

Визуализация сгенерированной СП $\left\{\left[\alpha_{УИК}\right]_i\right\}, i=\overline{1, N_{УИК}}$, составленной из значений «числа избирателей, проголосовавших в i-ой УИК», и аппроксимация Розенблатта-Парзена ее плотности распределения представлены на рис. 7.

Из рис. 7 видно, что минимальное значение «доли голосов избирателей, проголосовавших на выборах» $\min\left(\left\{\left[N_{УИК}^V\right]_i\right\}\right)=0.6060$ максимальное значение данного показателя $\max\left(\left\{\left[N_{УИК}^V\right]_i\right\}\right)=0.9958$.

Для удобства дальнейшего анализа зна-

чения левой и правой границ интервалов изменения описанных выше показателей приведены в табл. 4.

Из табл. 4. видно, что приведенные в данной таблице оценки значений электоральных показателей, вычисленные на основе анализа модельных электоральных данных, согласуются с аналогичными показателями электоральных данных, изученных в [1]. Следовательно, сгенерированные электоральные данные (заведомо, **нефальсифицированные**) можно использовать для оценки адекватности методов, популярных среди ЭОС.

4. Результаты анализа показателей, синтезированных электоральных данных с помощью методов электоральной статистики

Рассмотрим типичные результаты анализа показателей, сгенерированных данных с помощью выбранных методов электоральной статистики.

1. Анализ распределений первой после запятой цифры

В ходе проведенных исследований были использованы следующие показатели:

– «доля избирателей в процентах, прого-

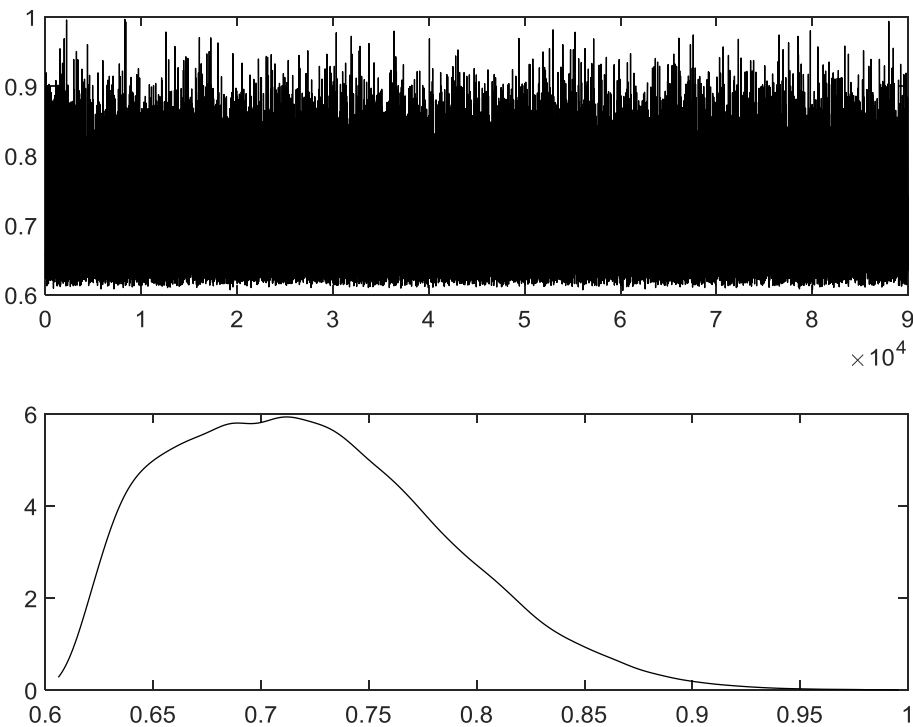


Рис. 7. Визуализация СП $\left\{\left[\alpha_{УИК}\right]_i\right\}, i=\overline{1, N_{УИК}}$ (сверху) и аппроксимация Розенблатта-Парзена (нормальное ядро, $h^*=0.7145 \cdot 19^{-2}$) ее ПР (снизу)

Оценки минимального, среднего и максимального «значений электоральных показателей»

Название электорального показателя	Минимальное значение электорального показателя	Среднее значение электорального показателя*	Максимальное значение электорального показателя
Число зарегистрированных избирателей в данной УИК	11	1023	3179
Доля избирателей, проголосовавших в данной УИК за победителя выборов	0.5102	0.5995	0.8844
Доля избирателей, проголосовавших в данной УИК за кандидата, проигравшего выборы	0.1001	0.1124	0.1703
Число избирателей, проголосовавших в данной УИК за победителя выборов	11	621	2278
Число избирателей, проголосовавших в данной УИК за кандидата, проигравшего выборы	1	117	421
Число избирателей, принявших участие в выборах в данной УИК	7	738	2589
Доля избирателей, принявших участие в выборах, от числа избирателей, зарегистрированных в данной УИК	0.6060	0.7205	0.9958

* Здесь средние значения показателей вычислялись по формуле:

$$\bar{x} = \int_{x_{\min}}^{x_{\max}} \xi \hat{p}(\xi) d\xi, \text{ где } \hat{p}(\xi) - \text{ аппроксимация Розенблатта-Парзена соответствующей слу-}$$

чайной последовательности.

лосовавших в данной УИК за победителя выборов» $\left[\alpha_{УИК} \right]_i^{(1)}$ (показатель № 1);
– «доля избирателей в процентах, проголосовавших в данной УИК за кандидата, проигравшего на выборах» $\left[\alpha_{УИК} \right]_i^{(2)}$ (показатель № 2);
– «относительная явка избирателей на выборы в данной УИК в процентах» $\left[\alpha_{УИК} \right]_i$ (показатель № 3),
округленные до второй цифры после запятой с помощью преобразований:

$$\begin{aligned} & \text{round}\left(\left[\alpha_{УИК}\right]_i^{(1)} \cdot 10^4\right) / 10^2; \\ & \text{round}\left(\left[\alpha_{УИК}\right]_i^{(2)} \cdot 10^4\right) / 10^2; \\ & \text{round}\left(\left[\alpha_{УИК}\right]_i \cdot 10^4\right) / 10^2. \end{aligned}$$

Далее в округленных до второй цифры после запятой подсчитывалась количество случаев, в которых была обнаружена каждая из цифр 0, 1, ..., 9. Результаты подсчетов представлены в таблице 5.

Из табл. 5 видно, что встречаемости цифр

Результаты анализа распределений первой после десятичной запятой цифры

Цифра	Показатель № 1	Показатель № 2	Показатель № 3
0	9038	8926	9086
1	9312	9579	9070
2	9440	8999	8755
3	8612	8983	9181
4	8659	8937	8609
5	8892	9089	9095
6	9324	9197	8901
7	9384	8738	9687
8	8591	8727	8799
9	8749	8826	8818

являются случайными числами, значения которых находятся в диапазонах: [8591,9440] (показатель № 1); [8727,9579] (показатель № 2); [8755,9687] (показатель № 3). (Напомним, что в предположении о равномерном законе распределения последней цифры в выбранных показателях встречаемость каждой из цифр должна равняться 9000.) В этой связи с помощью критерия χ^2 – квадрат были проверены гипотезы о равномерном распределении последней цифры выбранных показателей. Значения критериев, вычисленных для показателей № 1, 2, 3, χ_1^2 , χ_2^2 , χ_3^2 оказались равными 117.067, 62.08, 91.35, соответственно. В то время как, граничные значения критерия $\chi_{теор}^2(9) = 15.51$. Таким образом, $\chi_{1.2.3}^2 > \chi_{теор}^2(9)$, поэтому гипотезы о равномерном законе распределения последней цифры в выбранных показателях, округленных до второй цифры после запятой, должна быть отвергнута.

Полученный результат позволяет сделать вывод о том, что метод анализа распределения последней цифры электоральных показателей, обнаруживает отличие от равномер-

ного закона распределения даже в случае подтвержденного отсутствия преднамеренных фальсификаций электоральных данных. Следовательно, данный метод не может применяться для выявления преднамеренных фальсификаций электоральных данных.

2. Метод Бебера и Скакко [21]

В соответствие с методом Бебера и Скакко для указанных выше электоральных показателей, округленных до двух значащих цифр после запятой, были вычислены числа встречаемости пар, составленных из одинаковых цифр 0, 1, ..., 9, находящихся в первом и втором разрядах после запятой, представленные в табл. 6.

Из табл. 6 видно, что встречаемости пар цифр являются случайными числами, значения которых находятся в диапазонах: [705,1066] (показатель № 1); [682,1069] (показатель № 2); [850,1048] (показатель № 3). (Напомним, что в предположении о равномерном законе распределения пар, составленных из одинаковых цифр в первом и втором разрядах после запятой, встречаемость каждой из пар цифр в выбранных показателях

Таблица 6

Результаты анализа распределений пар одинаковых цифр, в первом и втором разрядах после запятой

Цифра	Показатель № 1	Показатель № 2	Показатель № 3
0	920	721	920
1	935	1030	885
2	912	1069	850
3	1039	897	950
4	705	899	895
5	797	835	1048
6	1066	847	910
7	774	798	1041
8	884	784	943
9	803	682	912

должна равняться 900.) В этой связи с помощью критерия χ^2 – квадрат были проверены гипотезы о равномерном распределении последней цифры выбранных показателей. Значения критериев, вычисленных для показателей № 1, 2, 3, χ_1^2 , χ_2^2 , χ_3^2 оказались равными 136.4878, 173.2552, 55.0311, соответственно. В то время как, граничные значения критерия $\chi_{теор}^2(9) = 15.51$. Так как $\chi_{1,2,3}^2 > \chi_{теор}^2(9)$ гипотезы о равномерном законе распределения пар, составленных из первой и второй цифр после запятой, в выбранных показателях, округленных до второй цифры после запятой, должна быть отвергнута.

Полученный результат позволяет сделать вывод о том, что метод анализа распределения пар цифр, составленных из первой и второй цифр после запятой, обнаруживает отличие от равномерного закона распределения даже в случае подтвержденного отсутствия преднамеренных фальсификаций электоральных данных. Следовательно, метод, основанный на анализе распределений цифр в электоральных показателях, не могут применяться для выявления преднамеренных фальсификаций электоральных данных.

Отметим, что аналогичные результаты были получены авторами при изучении распределений первой и второй цифр после запятой в ансамбле чисел $\text{round}((n_2/n_1) \cdot$

$\cdot 10^4)/10^2$, где $\text{round}(\)$ – функция округления до ближайшего целого числа, $n_1 \in [N_{\min}, N_{\max}]$, $n_2 \in [0, n_1]$ – целые числа, извлекаемые из генеральных совокупностей с равномерным законом распределения с областями рассеяния $[N_{\min}, N_{\max}]$, $[0, n_1]$, которые, как очевидно, являются аналогом явки избирателей на выборы в данной УИК (здесь n_1 число избирателей, зарегистрированных в данной УИК, $n_2 \leq n_1$ – число избирателей, принявших участие в выборах в данной УИК) [22].

Таким образом, изложенные в данном разделе результаты отвергают методы электорально криминалистики, активно пропагандируемых А.В. Подлазовым [23,24], которые обнаруживают признаки масштабных фальсификаций, в том числе, в заведомом не фальсифицированных данных.

3. Метод Шпилькина [25–28]

Рассмотрим типичные зависимости доли числа голосов избирателей, проголосовавших за победителя выборов и кандидата, проигравших на выборах, от доли числа избирателей, принявших участие в выборах в данной УИК, вычисляемой как отношение числа избирателей, принявших участие в выборах к числу избирателей, зарегистрированных в данной УИК, представленные на рис. 8, а также приведенные ниже количественные характеристики линейных аппроксимаций данных зависимостей.

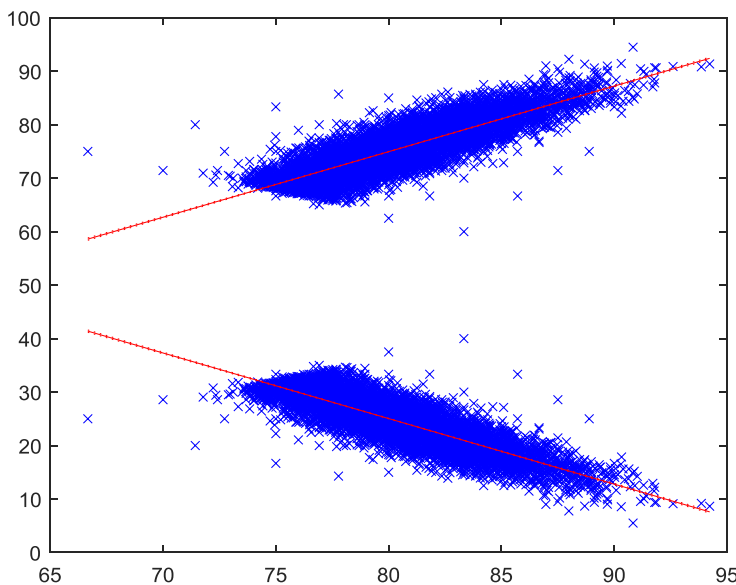


Рис. 8. Визуализация зависимостей $[\alpha_{уик}]_i^{(1)} = f([\alpha_{уик}]_i)$ (вверху), $[\alpha_{уик}]_i^{(2)} = f([\alpha_{уик}]_i)$ (снизу), вычисленные на основе анализа синтезированных электоральных данных, и их линейных аппроксимаций

Количественные характеристики линейной аппроксимации зависимости

$$[\alpha_{\text{УИК}}]_i^{(1)} = f([\alpha_{\text{УИК}}]_i)$$

Linear regression model:

$y \sim 1 + x_1$

Estimated Coefficients:

	Estimate	SE	tStat	pValue
(Intercept)	-23.159	0.63502	-36.47	1.6295e-273
x1	1.2264	0.0079009	155.23	0

Number of observations: 90000,

Error degrees of freedom: 89998

Root Mean Squared Error: 2.55

R-squared: 0.707, Adjusted R-Squared: 0.707

F-statistic vs. constant model: 2.41e+04, p-value = 0

Количественные характеристики линейной аппроксимации зависимости

$$[\alpha_{\text{УИК}}]_i^{(2)} = f([\alpha_{\text{УИК}}]_i)$$

Linear regression model:

$y \sim 1 + x_1$

Estimated Coefficients:

	Estimate	SE	tStat	pValue
(Intercept)	123.16	0.63502	193.94	0
x1	-1.2264	0.0079009	-155.23	0

Number of observations: 90000,

Error degrees of freedom: 89998

Root Mean Squared Error: 2.55

R-squared: 0.707, Adjusted R-Squared: 0.707

F-statistic vs. constant model: 2.41e+04, p-value = 0

Анализ зависимостей, представленных на рис. 9 и оценок статистических показателей линейных аппроксимаций данных зависимостей позволяет сделать вывод о том, и свойства оказываются схожими со свойствами аналогичных зависимостей, вычисленных в [1], на основе анализа электоральных данных, представленных УИК в ЦИК РФ по итогам проведенных в 2018 г. выборов Президента РФ. Действительно, аналогично зависимостям, изученным [1]:

– угловые коэффициенты прямых, аппроксимирующие зависимости $[\alpha_{\text{УИК}}]_i^1 = f([\alpha_{\text{УИК}}]_i)$, $[\alpha_{\text{УИК}}]_i^2 = f([\alpha_{\text{УИК}}]_i)$, статистических значимо отличаются от нуля, что свидетельствует о наличии линейной связи между анализируемыми показателями электорального процесса;

– доля голосов избирателей, проголосовавших за победителя выборов, при увеличении доли избирателей, принявших участие в выборах в данной УИК, линейно возрастает, в то время как доля избирателей, проголосовавших за кандидата, проигравшего выборы, линейно уменьшается. (Объяснение данной особенности анализируемых зависимостей приведено в разделе 2.4.4.)

Таким образом, метод Шпилькина, будучи примененным для анализа синтезированных электоральных данных, в которых, гарантировано, не вносилось каких-либо изменений, обнаружил в них фальсификации. Это, с нашей точки зрения, свидетельствует о невозможности его использования для анализа электоральных данных и требует критического пересмотра многочисленных выводов ЭОС, де-факто, обвиняющих избирательные органы РФ в электоральных преступлениях на основе, полученных с его помощью результатов.

4. Модифицированный метод Шпилькина [29]

Напомним, что модифицированный метод Шпилькина, де-факто, основан на анализе зависимости $N_i^{(1)}([\alpha_{\text{УИК}}]_i) = f(N_i^{(2)}([\alpha_{\text{УИК}}]_i))$. При этом, в соответствие с гипотезой А.В. Подлазова, при отсутствии фальсификаций электоральных данных функция $f(N_i^{(2)}([\alpha_{\text{УИК}}]_i))$ должна быть линейной:

$$N_i^{(1)}([\alpha_{\text{УИК}}]_i) = k \cdot N_i^{(2)}([\alpha_{\text{УИК}}]_i)$$

где $k = \text{const}$, а факт отклонения обсуждаемой зависимости от линейной свидетельствует об искусственном увеличении числа голосов избирателей, проголосовавших за победителя

выборов, и, соответственно, пропорциональном уменьшении голосов избирателей, проголосовавших за проигравшего кандидата, реализованном УИК с высокой явкой избирателей.

В этой связи модифицированный метод

Шпилькина был применен к синтезированному электоральным данным, в которые, заведомо, не вносились описанные выше фальсификации. Полученные при этом результаты представлены на рис. 9.

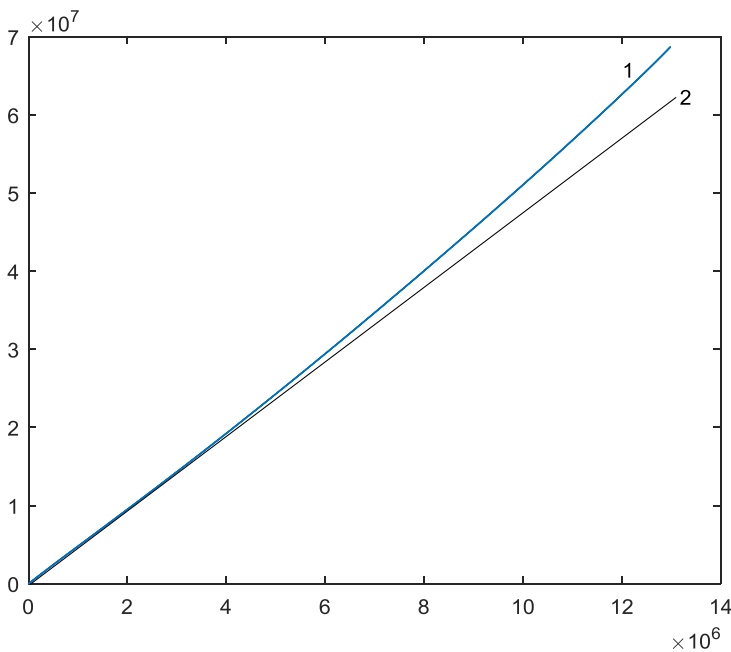


Рис. 9. Визуализации зависимости показателя «число голосов избирателей, проголосовавших за победителя выборов» от показателя «число голосов избирателей, проголосовавших за кандидата, проигравшего на выборах» (1) и зависимости в случае прямой пропорциональности данных показателей (2)

Из рис. 9 видно, что зависимость оказывается отличной от линейной, что с точки зрения модифицированного метода Шпилькина является подтверждением фальсификации анализируемых электоральных данных, которая, заведомо, не совершалась. Следовательно, обсуждаемый метод анализа электоральных данных, дающий ложный результат для синтезированного набора данных, не может применяться для выявления фальсификаций реальных электоральных данных, а выводы ЭОС, сделанные на его основе, должны быть пересмотрены.

Также необходимо отметить, что выводы, сделанные в данном разделе выше, также подтвердились результатами анализа электоральных данных, синтезированных в процессе 20 независимых испытаний, которые оказались аналогичными в каждом из независимых испытаний. Таким образом, опыт применения популярных у ЭОС методов, предназначенных для выявления фальсификаций электоральных данных, для анализа синтезированных электоральных данных свидетельствует о том, что в каждом независимом слу-

чае исследователь, с неизбежностью, должен был совершить ошибку второго рода (принять неверную гипотезу о фальсификации электоральных данных и отвергнуть верную гипотезу об отсутствии фальсификаций).

Анализ опыта использования и других известных формальных методов выявления электоральных аномалий, также позволил обнаружить, что ни один из данных методов не проходил тестирование на достоверность получаемых его помощью результатов, например, на основе использования синтезированных в соответствии с описанным в разделе 3.2 алгоритме. При этом, данные результаты ЭОС многократно использовали для делегитимации результатов выборов в органы государственной власти РФ различных уровней а, в ряде случаев дестабилизации общественно-политической ситуации в РФ (например, массовые политические выступления в РФ, начавшиеся после выборов в Государственную думу VI созыва 4 декабря 2011 г., которые продолжались во время кампании по выборам Президента РФ и после президентских выборов, состоявшихся 4 марта 2012 г.,

на которых В.В. Путин победил в первом туре).

В этой связи требуется проведение целенаправленных исследований с целью проверки адекватности результатов анализа электоральных данных, получаемых каждым из использованных ЭОС методов, которые выходят из рамки нашей работы, а также повышение ответственности (в том числе, на законодательном уровне) за использование методов анализа электоральных данных, работоспособность которых не была подтверждена научно, с целью целенаправленной делигитимации в выборах, проводимых в РФ, на основе полученных с их помощью результатов.

В условиях, когда достоверность формальных методов выявления электоральных аномалий оказывается не доказанной, с нашей точки зрения, единственным методом, обеспечивающим подтверждение легитимности выборов в органы государственной власти РФ, оказывает метод, основанный на опросах избирателей, проводимых на выходе с УИК (экзит-поллов). Подтверждением правомерности их использования является согласованность данных экзит-поллов, проведенных ВЦИОМ, в ходе выборов в 2018 г. Президента РФ, и официальных результатов выборов (см. раздел 2.5), а также результаты опросов экспертов, мониторинга общественного мнения накануне выборов в 2018 г. Президента РФ и результатов экзит-поллов, проведенных сотрудниками социологических подразделений уполномоченных органов государственной власти

Заключение

1. Предложен алгоритм статистического синтеза электоральных данных, в котором входными параметрами являются: число избирательных участков, области рассеяния целочисленной случайной последовательности, образованной значениями числа избирателей, зарегистрированных в данной УИК; доли избирателей, проголосовавших в данной УИК за победителя выборов; доли избирателей, проголосовавших в данной УИК, за

кандидата, проигравшего выборы, и используется математическая модель плотности распределений данных случайных чисел, основанная на решении задачи о случайных блужданиях броуновской частицы в ограниченной области рассеяния, полученного М. Смолуховским; выходными параметрами – электоральные данные представляемые в ЦИК РФ УИК, созданных в субъектах РФ.

2. Проведен анализ статистических характеристик, синтезированных электоральных данных, значения которых оказались сравнимыми с аналогичными характеристиками, вычисленными на основе анализа электоральных данных о выборах в 2018 г. Президента РФ.

3. Проведен анализ свойств электоральных показателей, вычисленных на основе синтезированных электоральных данных, результаты которого показали:

- законы распределения второй цифры после запятой в показателях «относительная явка избирателей на выборы (в процентах)», «доля голосов избирателей, проголосовавших за победителя выборов (в процентах)», «доля голосов избирателей, проголосовавших за кандидата, проигравшего выборы (в процентах)», а также пар одинаковых цифр, стоящих в первом и во втором разрядах после запятой, не являются равномерными;

- метод Шпилькина и модифицированный метод Шпилькина обнаруживают фальсификации в синтезированных электоральных данных, в которых они заведомо отсутствовали.

В этой связи изученные методы электоральной криминалистики, наиболее часто используемые ЭОС для делигитимации результатов выборов в органы государственной власти РФ различных уровней и референдумов, результаты которых оказываются недостоверными, а также иные методы, основанные на предположении о нормальном законе распределения электоральных показателей, должны быть исключены из арсенала методов электоральной статистики.

Литература

1. Поршнев С.В., Рябко Н.Ю. Оценка адекватности одного метода выявления предполагаемых фальсификаций электоральных данных// С.В. Поршнев, Н.Ю. Рябко// Вестник УрФО. Безопасность в информационной сфере, 2023, № 3 (49), С. 5-20.
2. Gilmiyarov R.V., L.I. Galimzyanova, Porshnev S.V., Chernova O.E. Comparative Quality Analysis of Random Number Generators in MATLAB and NumPy packages// Proceedings 2023 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russian Federation, 2023, pp. 293-297, doi: 10.1109/USBEREIT58508.2023.10158838.

3. Эйнштейн А. О движении взвешенных в покоящейся жидкости частиц, требуемом молекулярно-кинетической теорией теплоты // Броуновское движение. – М.: ОНТИ-НКТП-СССР, 1936. С. 13–25.
4. Гнеденко Б.В. Курс теории вероятностей. – М.: Физматгиз, 1961. 407 с.
5. Смолюховский М. Броуновское молекулярное движение под действием внешних сил и его связь с обобщенным уравнением диффузии // Броуновское движение. – М.: ОНТИ-НКТП-СССР, 1936. С. 319–331.
6. Смолюховский М. Несколько примеров броуновского молекулярного движения под действием внешних сил // Броуновское движение. – М.: ОНТИ-НКТП-СССР, 1936. С. 205–225.
7. Смолюховский М. Три доклада о диффузии, броуновском молекулярном движении и коагуляции коллоидных частиц // Броуновское движение. – М.: ОНТИ-НКТП-СССР, 1936. С. 332–416.
8. Поршнев С.В. Компьютерное моделирование физических процессов и систем в пакете MATLAB. – М.: Горячая линия-Телеком, 2020. – 808 с.
9. Поршнев С.В., Овечкина Е.В., Каплан В.Е. Теория и алгоритмы аппроксимации эмпирических зависимостей и распределений. – Екатеринбург: УрО РАН, 2006. – 166 с.
10. Копосов А.С., Поршнев С.В. Случайные величины с ограниченной областью рассеяния: математическое и алгоритмическое обеспечение для оценивания плотностей вероятностей и функций распределений. – М.: Горячая линия-Телеком, 2019 г. 184 с.
11. Поршнев С.В., Копосов А.С. Программная библиотека ES&RP // Свидетельство о государственной регистрации программы для ЭВМ № 2016614275 (Заявка № 2016611747. Дата поступления 2 марта 2016 г. Дата государственной регистрации в Реестре программ для ЭВМ 20 апреля 2016 г.)
12. Барлоу Р., Прошан Ф. Статистическая теория надежности и испытания на безотказность. – М.: Наука, 1984. – 328 с.
13. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. – М.: Наука, 1965. – 524 с.
14. Матвиевский В.Р. Надежность технических систем. – М.: Московский государственный институт электроники и математики, 2002. 113 с.
15. Острейковский В.А. Теория надёжности. 2-е изд., испр. – М.: Высшая школа, 2008. – 464 с.
16. Половко А.М., Гуров С.В. Основы теории надёжности. – СПб.: БХВ-Петербург, 2006. – 702 с.
17. Rosenblatt M. Remarks on Some Nonparametric Estimates of a Density Function // The Annals of Mathematical Statistics, 1956. – Т. 27. Vol. 3. – P. 832–837.
18. Parzen E. On the estimation of probability density function and the mode // Ann. Math. Stat., 1962. – Vol. 33. – P. 1065–1076.
19. Сызранцев В.Н. Расчет прочностной надежности изделий на основе методов непараметрической статистики / В.Н. Сызранцев, Я.Н. Невелев, С.Л. Голофаст // Новосибирск: Наука, 2008. – 128 с.
20. Симахин В.А. Робастные непараметрические оценки: адаптивные оценки взвешенного максимального правдоподобия в условиях статистической априорной неопределенности / В.А. Симахин // –Saarbrücken, Germany: LAP LAMBERT Academic Publishing GmbH & Co. KG, 2011. – 292 с.
21. Beber B., Scacco A. What the Numbers Say: A Digit-Based Test for Election Fraud // Political Analysis, 2012. Vol. 20. P. 211–234.
22. Поршнев С.В., Рябко Н.Ю. Анализ распределений цифр в частных от деления двух целых случайных чисел / С.В. Поршнев, Н.Ю. Рябко // Научно-технический вестник Поволжья. 2023. № 8. С. 93–96.
23. Формальные методы выявления масштабных электоральных фальсификаций на материале федеральных выборов 1999–2018 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).
24. Подлазов А.В. Формальное выявление вымышленных результатов выборов // Проектирование будущего. Проблемы цифровой реальности: труды 3-й Международной конференции (6-7 февраля 2020 г., Москва). — М.: ИПМ им. М.В.Келдыша, 2020.С. 176-190. URL: <https://keldysh.ru/future/2020/15.pdf> (Дата обращения: 29.01.2023)
25. Шпилькин С. Статистическое исследование результатов российских выборов 2007–2009 гг. // Троицкий вариант – наука, 2009. 21(40), 2–4. URL: <http://trv-science.ru/2009/10/statisticheskoe-issledovanie-rezultatov-rossijskix-vyborov-2007-2009-gg/> (Дата обращения: 28.02.2023).
26. Шпилькин С. Математика выборов – 2011 // Троицкий вариант – наука, 2011. 25(94), 2–4. URL: <https://troiskmsk.bezformata.com/listnews/troitckij-variant-nauka-25-94-20-12-2011/2246645/> (Дата обращения: 28.02.2023).
27. Шпилькин С. Двугорбая Россия // Троицкий вариант – наука, 2016. 20(214), 1–3. URL: <http://trv-science.ru/2016/10/dvugorbaya-rossiya/> <http://trv-science.ru/2016/10/dvugorbaya-rossiya/> (Дата обращения: 28.02.2023).

28. Шпилькин С. Выборы 2018 года: Фактор Х и «пила Чурова» // Троицкий вариант – наука, 2018. 8(252), 8–10. URL: <http://trv-science.ru/2018/04/vybory-2018-faktor-x-i-pila-churova/> (Дата обращения: 28.02.2023).

29. Подлазов А.В. Реконструкция фальсифицированных результатов выборов с помощью интегрального метода Шпилькина// Проектирование будущего. Проблемы цифровой реальности: труды 4-ой Международной конференции (4–5 февраля 2021 г., Мос4ква_ –М.: ИПМ им. М.В. Келдыша, 2021. –С. 193–208. <https://keldysh.ru/future/2021/18.pdf> <https://doi.org/10/20948/future-2021-18> (Дата обращения: 08.10.2023).

References

1. Porshnev S.V., Ryabko N.YU. Otsenka adekvatnosti odnogo metoda vyiavleniya predpolagaemykh falsifikatsiy elektoralnykh dannykh// S.V. Porshnev, N.YU. Ryabko// Vestnik UrFO. Bezopasnost v informatsionnoy sfere, 2023, № 3 (49), s. 5–20.
2. Gilmiyarov R.V., L.I. Galimzyanova, Porshnev S.V., Chernova O.E. Comparative Quality Analysis of Random Number Generators in MATLAB and NumPy packages// Proceedings 2023 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russian Federation, 2023, pp. 293–297, doi: 10.1109/USBEREIT58508.2023.10158838.
3. Eynshteyn A. O dvizhenii vzveshennykh v pokoyascheysya jidkosti chastits, trebuemom molekulyarno-kineticheskoy teoriiy teploty// Brounovskoe dvizhenie. – М.: ONTI-NKTP-SSSR, 1936. S. 13–25.
4. Gnedenko B.V. Kurs teorii veroyatnostey. – М.: Fizmatgiz, 1961. 407 s.
5. Smoluhovskiy M. Brounovskoe molekulyarnoe dvizhenie pod deystviem vneshnih sil i ego svyaz s obobshchennym uravneniem diffuzii// Brounovskoe dvizhenie. – М.: ONTI-NKTP-SSSR, 1936. S. 319–331.
6. Smoluhovskiy M. Neskolko primerov brounovskogo molekulyarnogo dvizheniya pod deystviem vneshnih sil// Brounovskoe dvizhenie. – М.: ONTI-NKTP-SSSR, 1936. S. 205–225
7. Smoluhovskiy M. Tri doklada o diffuzii, brounovskom molekulyarnom dvizhenii i koagulyatsii kolloidnykh chastits//Brounovskoe dvizhenie. – М.: ONTI-NKTP-SSSR, 1936. S. 332–416.
8. Porshnev S.V. Kompyuternoe modelirovanie fizicheskikh protsessov i sistem v pakete MATLAB. – М.: Goryachaya liniya-Telekom, 2020. – 808 s.
9. Porshnev S.V., Ovechkina E.V., Kaplan V.E. Teoriya i algoritmyi approksimatsii empiricheskikh zavisimostey i raspredeleniy. – Ekaterinburg: UrO RAN, 2006. – 166 s.
10. Koposov A.S., Porshnev S.V. Sluchaynyie velichinyi s ogranichennoy oblastyu rasseyaniya: matematicheskoe i algoritmicheskoe obespechenie dlya otsenivaniya plotnostey veroyatnostey i funktsiy raspredeleniy. – М.: Goryachaya liniya-Telekom, 3019 g. 184 s.
11. Porshnev S.V., Koposov A.S. Programmnyaya biblioteka ES&RP// Svidetelstvo o gosudarstvennoy registratsii programmy dlya EVM № 2016614275 (Zayavka № 2016611747. Data postupleniya 2 marta 2016 g. Data gosudarstvennoy registratsii v Reestre programm dlya EVM 20 aprelya 2016 g.)
12. Barlou R., Proshan F. Statisticheskaya teoriya nadejnosti i ispyitaniya na bezotkaznost. – М.: Nauka, 1984. – 328 s.
13. Gnedenko B.V., Belyaev YU.K., Solovov A.D. Matematicheskie metodyi v teorii nadejnosti. – М.: Nauka, 1965. – 524 s.
14. Matvievskiy V.R. Nadejnost tehnikeskikh sistem. –М: Moskovskiy gosudarstvennyiy institut elektroniki i matematiki, 2002. 113 s.
15. Ostreykovskiy V.A. Teoriya nadëjnosti. 2-e izd., ispr. – М.: Vysshaya shkola, 2008. – 464 s.
16. Polovko A.M., Gurov S.V. Osnovy teorii nadëjnosti. – SPb.:BHV-Peterburg, 2006. – 702 s.
17. Rosenblatt M. Remarks on Some Nonparametric Estimates of a Density Function // The Annals of Mathematical Statistics., 1956. – T. 27. Vol. 3. – P. 832–837.
18. Parzen E. On the estimation of probability density function and the mode // Ann. Math. Stat., 1962. – Vol. 33. – P. 1065–1076.
19. Syzrantsev V.N. Raschet prochnostnoy nadejnosti izdeliy na osnove metodov neparametricheskoy statistiki/V.N. Syzrantsev, YA.N. Nevelev, S.L. Golofast// – Novosibirsk: Nauka, 2008. – 128 s.
20. Simahin V.A. Robastnyie neparametricheskie otsenki: adaptivnyie otsenki vzveshennogo maksimalnogo pravdopodobiya v usloviyakh statisticheskoy apriornoy neopredelennosti/ V.A. Simahin // –Saarbrücken, Germany: LAP LAMBERT Academic Publishing GmbH & Co. KG, 2011. – 292 s.
21. Beber B., Scacco A. What the Numbers Say: A Digit-Based Test for Election Fraud//Political Analysis, 2012. Vol. 20. P. 211–234.
22. Porshnev S.V., Ryabko N.YU. Analiz raspredeleniy tsifr v chastnykh ot deleniya dvuh tselykh

sluchaynykh chisel /S.V. Porshnev, N.YU. Ryabko// Nauchno-tehnicheskiiy vestnik Povol'jya. 2023. № 8. S. 93–96.

23. Formalnyie metodyi vyyavleniya masshtabnykh elektoralnykh falsifikatsiy na materiale federalnykh vyiborov 1999–2018 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 obrascheniya 19.02.2022).

24. Podlazov A.V. Formalnoe vyyavlenie vyidumannyykh rezul'tatov vyiborov // Proektirovanie buduschego. Problemyi tsifrovoy realnosti: trudyi 3-y Mejdunarodnoy konferentsii (6–7 fevralya 2020 g., Moskva). — M.: IPM im. M.V.Keldysha, 2020.S. 176–190. URL: <https://keldysh.ru/future/2020/15.pdf> (Data obrascheniya: 29.01.2023)

25. SHpilkin S. Statisticheskoe issledovanie rezul'tatov rossiyskikh vyiborov 2007–2009 gg. // Troitskiy variant – nauka, 2009. 21(40), 2–4. URL: <http://trv-science.ru/2009/10/statisticheskoe-issledovanie-rezul'tatov-rossiyskix-vyiborov-2007-2009-gg/> (Data obrascheniya: 28.02.2023).

26. SHpilkin S. Matematika vyiborov – 2011 // Troitskiy variant – nauka, 2011. 25(94), 2–4. URL: <https://troitskmsk.bezformata.com/listnews/troitckij-variant-nauka-25-94-20-12-2011/2246645/> (Data obrascheniya: 28.02.2023).

27. SHpilkin S. Dvugorbaya Rossiya // Troitskiy variant – nauka, 2016. 20(214), 1–3. URL: <http://trv-science.ru/2016/10/dvugorbaya-rossiya/> <http://trv-science.ru/2016/10/dvugorbaya-rossiya/> (Data obrascheniya: 28.02.2023).

28. SHpilkin S. Vyiboryi 2018 goda: Faktor H i «pila CHurova» // Troitskiy variant – nauka, 2018. 8(252), 8–10. URL: <http://trv-science.ru/2018/04/vyibory-2018-faktor-x-i-pila-churova/> (Data obrascheniya: 28.02.2023).

29. Podlazov A.V. Rekonstruktsiya falsifitsirovannykh rezul'tatov vyiborov s pomoschyu integralnogo metoda SHpilkina // Proektirovanie buduschego. Problemyi tsifrovoy realnosti: trudyi 4-oy Mejdunarodnoy konferentsii (4–5 fevralya 2021 g., Mos4kva_ –M.: IPM im. M.V. Keldysha, 2021. – S. 193–208. <https://keldysh.ru/future/2021/18.pdf> <https://doi.org/10/20948/future-2021-18> (Data obrascheniya: 08.10.2023).

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

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

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

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



О ПРИМЕНЕНИИ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ В АДАПТИВНОЙ ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ¹

В статье обсуждаются результаты анализа возможности применения технологий когнитивного моделирования (КМ), а именно нечетких когнитивных карт (НKK) в различных этапах оценки рисков информационной безопасности (РИБ).

Были проанализированы ГОСТы, международные стандарты, различные научные публикации в области оценки РИБ, и была сформирована функциональная модель процесса оценки РИБ.

Продemonстрировано внедрение в один из этапов данной функциональной модели элементов КМ. Предложено на этапе «Идентификации угроз» использовать НKK для анализа необходимых исключительно для текущей ситуации факторов угроз, выраженных в виде концептов НKK.

Ключевые слова: информационная безопасность, оценка информационных рисков, адаптивная оценка рисков информационной безопасности, когнитивное моделирование, нейронные сети, нечеткие когнитивные карты.

¹ В рамках исполнения гранта ИБ МТУСИ № 40469-23/2022-к 15.06.2022г. протокол №2

ON THE APPLICATION OF COGNITIVE MODELING IN ADAPTIVE ASSESSMENT OF INFORMATION SECURITY RISKS

The article discusses the results of an analysis of the possibility of using cognitive modeling (CM) technologies, namely fuzzy cognitive maps (FCMs) in various stages of information security risk assessment (ISS).

GOSTs, international standards, various scientific publications in the field of RIB assessment were analyzed, and a functional model of the RIB assessment process was formed.

The implementation of CM elements into one of the stages of this functional model is demonstrated. It is proposed to use the NCC at the stage of "Threat Identification" to analyze the threat factors necessary exclusively for the current situation, expressed in the form of NCC concepts.

Keywords: *information security, information risk assessment, adaptive information security risk assessment, cognitive modeling, neural networks, fuzzy cognitive maps.*

Введение

В современном информационном обществе обеспечение защищённости информации становится все более важной и актуальной задачей. Угрозы кибербезопасности постоянно эволюционируют, традиционные статичные методы оценки рисков ИБ и противодействия им оказываются недостаточными. Отсюда вытекает актуальность поиска новых подходов и методов, позволяющих адаптивно оценивать риски ИБ и эффективно предотвращать их реализацию.

Одним из перспективных направлений в данном вопросе является применение КМ, которое позволяет учитывать неопределенность, сложность и динамичность информационной среды, а также факторы человеческого поведения и принятия решений.

Напомним, что процесс оценки рисков ИБ включает несколько этапов [1-4]. Сперва осуществляется идентификация и анализ уязвимостей информационной системы, а также оценка вероятности их возникновения. Затем проводится анализ потенциальных последствий этих уязвимостей, включая потерю конфиденциальности, целостности и доступно-

сти данных. Далее происходит определение уровня рисков и разработка мер по управлению рисками, включая рекомендации по применению комплекса мероприятий по защите информации.

Цель данной работы в исследовании применения технологий КМ в вышеупомянутых этапах оценки рисков ИБ с целью придания ему свойств адаптивности.

В статье проведен анализ ГОСТов, международных стандартов, научных публикаций по оценке рисков ИБ и КМ, сформирована функциональная модель оценки рисков ИБ, построена НКК, применимая на одном из этапов оценки рисков ИБ.

Формирование функциональной модели процесса оценки рисков ИБ и особенности внедрения в модель технологий КМ

Понятие управления и оценки рисков ИБ, подходы к организации этих процессов, методы, которые могут быть применены, общие рекомендации к проведению оценки рисков описываются в ГОСТах, международных стандартах, руководящих и прочих документах [1-3]. Опираясь на определения оценки риска, определим этот процесс как процесс, состоя-

щий из идентификации риска, анализа и оценки опасности риска, также можно использовать подход PDCA, который отмечает следующие этапы [4-5]:

- 1) идентификация контекста;
- 2) оценка рисков;
- 3) разработка плана обработки рисков;
- 4) принятие рисков;

- 5) ввод сформированного перечня действий по обработке рисков;
- 6) мониторинг и обновление рисков;
- 7) модернизация процесса риск-менеджмента.

Подробное описание данных этапов приведено в таблице 1 [5].

Опираясь на вышеперечисленные опре-

Таблица 1

Этапы оценки рисков информационной безопасности

№	Этапы	Характеристики
1	Идентификация риска	Классификация методов: – основанные на документальных свидетельствах: анализ контрольных листов, анализ экспериментальных данных, а также данных и событий, произошедших в прошлом; – посредством структурированного множества подсказок или вопросов; – индуктивные методы
2	Анализ риска	– Оценка методов управления; – анализ последствий реализации риска; – анализ и оценка вероятности; – предварительный анализ; – определение неопределенности и чувствительности. Классификация методов: качественные, количественные, смешанные.
3	Сравнительная оценка риска	Сопоставление уровня риска с критериями риска, установленными при определении области применения менеджмента риска, для определения типа риска и его значимости.

деления управления и оценки рисков ИБ, была сформирована функциональная модель данного процесса. В качестве основных этапов были определены следующие: идентификация активов; идентификация угроз; оценка уязвимостей; оценка вероятностей и воздействия; определение уровня рисков; формирование мер по снижению рисков; мониторинг и обновление.

Сформированная модель в нотации IDEF0 отображена на рисунке 1. В качестве управления используются приказы и методические документы ФСТЭК России. Остальные данные для входа, выхода и механизмы управления отражены в таблице 2.

Настоящая модель представляет собой стандартный статический подход к оценке рисков ИБ. Усовершенствование модели технологиями КМ позволит добавить ей свойства адаптивности. Эти вопросы рассмотрены авторами работ [6-8]. Отмечены основные проблемы оценки рисков ИБ: из-за недостаточности и противоречивости статистической информации об угрозах и уязвимостях, достоверная оценка рисков информационной безопасности затрудняется. Успешность

такой оценки значительно зависит от качества экспертных оценок, полученных в ходе аудита информационной безопасности.

В [9] приведен сравнительный анализ методов КМ: сети Байеса; НКК; серые НКК. НКК выделен как ключевой метод КМ, однако у них есть недостатки. Эти недостатки включают необходимость ввода экспертной оценки вероятности активации входного концепта и невозможность комплексной оценки влияния нескольких факторов на один узел. Для решения этих проблем предложено использование серых НКК, которые позволяют более точно отражать вероятность реализации атаки на данный узел. В [10] рассмотрены алгоритмы построения и оптимизации структуры НКК. Нечеткость НКК позволяет включать в модель большое количество переменных с нечеткими значениями. НКК моделируют системы, в которых объем точной информации ограничен, но доступны экспертные знания о причинно-следственных связях концептов. Авторы отмечают, что НКК можно охарактеризовать как интерпретируемые рекуррентные НС, включающие элементы нечеткой логики. В отличие от классических НС, НКК не содержат

Элементы функциональной модели оценки рисков ИБ

№	Этап	Вход	Выход	Механизм
1	Идентификация активов	Документация на системы и сети	Результаты анализа документации на системы и сети	Эксперты и специалисты по ИБ
2	Идентификация угроз	1.БДУ ФСТЭК России; 2.Открытые базы угроз; 3.Результаты анализа документации на системы и сети	Модель угроз безопасности информации, модель нарушителя	Эксперты и специалисты по ИБ
3	Оценка уязвимостей	пункты; 4.Информация об имеющихся угрозах, модель нарушителя	Информация по уязвимостям	Программное обеспечение по поддержке принятия решения
4	Оценка вероятностей и воздействия	пункты; 5.Информация по уязвимостям	Информация о рисках	Программное обеспечение по поддержке принятия решения
5	Определения уровня рисков	1-5 пункты; 6.Информация о рисках	Информация об уровне рисков	Программное обеспечение по поддержке принятия решения
6	Формирование мер по снижению рисков	6 пункт; 7.Информация об уровне рисков	План по снижению рисков	Эксперты и специалисты по ИБ
7	Мониторинг и обновление	6, 7 пункты; 8.План по снижению рисков	–	Эксперты и специалисты по ИБ

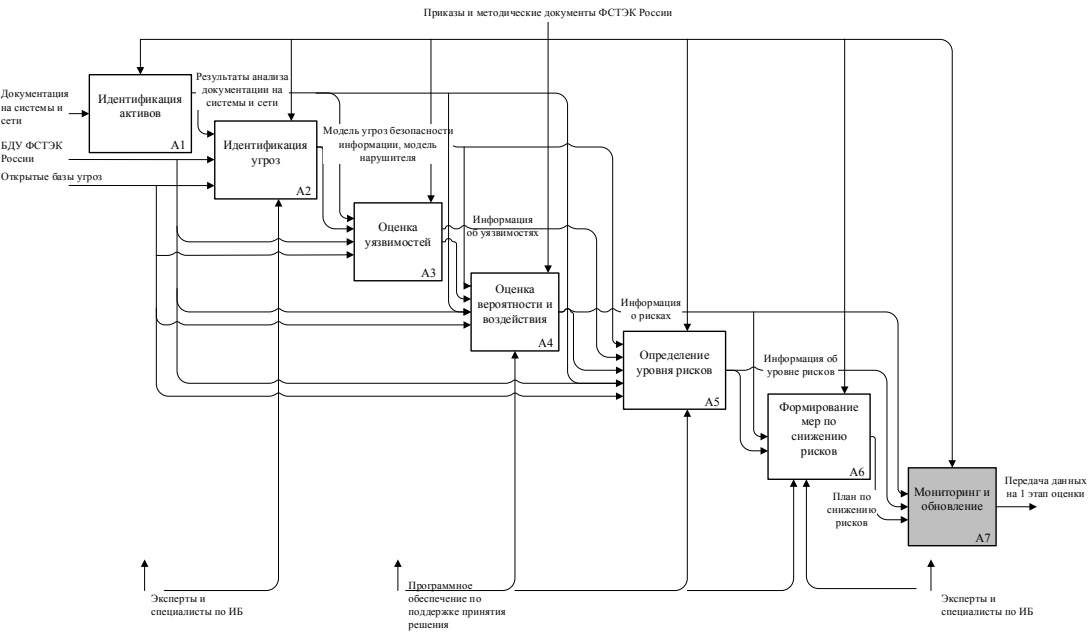


Рис. 1. Функциональная модель оценки рисков ИБ

скрытых нейронов, что позволяет им быть более интерпретируемыми. Однако, существуют проблемы, такие как выбор функции активации и правила обновления, а также сложности с обобщением и интерпретацией НКК. Авторы выделяют несколько актуальных на-

правлений исследований: учет задержки распространения влияния и динамического изменения структуры НКК; создание методов, которые учитывают экспертные знания и ретроспективные данные, а также обнаружение предвзятости в экспертном мнении.

В [11] представлены результаты анализа рисков кибербезопасности с использованием НКК, построенных на основе знаний и опыта экспертов-специалистов. Упомянуты различные типы НКК, связанных с представлением силы связей в виде интервальных оценок: серые, интервально-значные и интуиционистские НКК. Для оценки силы связей между концептами в НКК с учетом возникающей неопределенности во мнениях экспертов при оценке локального риска рассматриваются различные подходы к формализации знаний экспертов, в том числе применение ансамбля НКК. В [12] представлена методика оценки актуальных угроз и уязвимостей, основанная на применении комбинации технологий КМ и Text-Mining. В работе подчеркивается важность автоматизации моделирования сценариев эксплуатации уязвимостей и реализации угроз на основе описания шаблонов компьютерных атак из различных БД и открытых источников. Одним из главных недостатков текущих текстовых описаний безопасности программного и аппаратного обеспечения информационной инфраструктуры является их недостаточная структурированность и фрагментированность. Анализ таких данных требует больших временных затрат и определенных профессиональных навыков.

Таким образом, анализ научных публикаций позволил выделить существующие недостатки в вопросах оценки рисков ИБ и технологий КМ:

- необходимость обработки большого количества данных;
- необходимость правильного формирования источников этих данных: недостаток данных или неправильная представительность обучающей выборки может повлиять на качество модели и ее способность к обобщению на новые данные;
- доступная информация об имеющихся угрозах и уязвимостях недостаточна;
- сложности формального определения функции итогового показателя оценки;
- необходима высокая квалификация экспертов, специалистов по ИБ;
- возможная разрозненность и несогласованность мнений нескольких экспертов;
- Сложность интерпретации топологии НКК и ограничения в возможности комплексной оценки воздействия множества концептов на один узел представляют вызовы в данной области.

В настоящей работе взят вектор на иссле-

дование внедрения НКК для снижения разрозненности и разрозненности мнений экспертов и устранения необходимости работать с большими объемами данных. Для этого предложено модернизировать функциональную модель оценки рисков ИБ, внедрив элементы КМ на этапе «Идентификация угроз», что может помочь качественнее определить концепты, влияющие на эффективность и точность процесса идентификации угроз.

Когнитивное моделирование в адаптивной оценке рисков ИБ

Среди технологий КМ наиболее распространенными являются: сети Байеса; НКК; системы экспертных знаний [9]. НКК обладают определенными преимуществами: удобство использования, визуального восприятия, возможность учитывать неопределенность и нечеткость в процессе оценки рисков, способность изменяться и адаптироваться в соответствии с новыми данными и требованиями. НКК используется для решения задач, связанных с определением и оценкой влияния факторов ситуации, а также для получения прогнозов развития ситуации на основе вычисленных влияний. Основные элементы, необходимые при создании НКК, приведены в таблице 3.

НКК для анализа рисков ИБ является набором множеств:

$$НКК = \{C, F, W\}, \quad (1)$$

где C – множество концептов, F – множество связей между концептами, W – множество весов этих связей.

Чтобы сформировать перечень концептов НКК, были приглашены эксперты университета, преподаватели и специалисты по ИБ в ВУЗе. Основываясь на данных из открытых источников: отчеты по утечкам информации ограниченного доступа, утечкам данных, статистика по киберугрозам, БДУ ФСТЭК России, эксперты сформировали факторы риска (таблица 4), которые могут стать концептами разрабатываемой НКК [13-15].

Из этих данных сформированы концепты и построена НКК (рисунок 2). Ниже приведена матрица ВС НКК, определенная экспертами.

- $C1$ – Управление доступом;
- $C2$ – Конфиденциальность персональных данных студентов;
- $C3$ – Физическая безопасность;
- $C4$ – Сетевая безопасность;
- $C5$ – Мошенничество в области исследований и публикаций;

Архитектура нечеткой когнитивной карты

№	Элемент НКК	Описание
1.	Узлы	Переменные или концепты, которые моделируются в НКК. Каждый узел имеет свою активацию, отражающую текущее состояние переменной. Узлы могут быть бинарными (0 или 1) или иметь непрерывные значения.
2.	Связи	Взаимодействие между узлами в НКК, определяют направление и силу влияния одного узла на другой. Каждая связь имеет вес, указывающий на важность влияния. Связи могут быть однонаправленными или двунаправленными.
3.	Матрица весов связей (ВС)	Содержит значения ВС между узлами. Представляет собой двумерный массив, где каждый элемент указывает на силу и направление связи между двумя узлами.
4.	Функция активации	Определяет, как изменяется активация узла в зависимости от активаций связанных с ним узлов. Могут использоваться в зависимости от требований моделирования.
5.	Обучение и обновление	В процессе обучения НКК, активации узлов обновляются на основе входных данных и текущих активаций связанных с ними узлов. Это позволяет модели НКК адаптироваться к новым данным и улучшать свою производительность.
6.	Распространение активации	Происходит через связи между узлами, где активация одного узла передается другим узлам, влияя на их активации. Распространение активации может быть односторонним или многосторонним, в зависимости от архитектуры.

Таблица 4

Факторы риска для оценки рисков ИБ в образовательной сфере

№	Фактор риска	Подробнее по фактору
1.	Управление доступом	НСД к системам и данным; Неправильное управление аккаунтами пользователей; Недостаточная защита паролей и учетных записей.
2.	Конфиденциальность данных (персональных данных) студентов	Утечка конфиденциальных данных студентов: личная информация, оценки, финансовая информация; Нарушение правил регулирования в области защиты ПД.
3.	Физическая безопасность	НСД к физическим активам: компьютеры, серверы, хранилища данных, помещения с конфиденциальными документами.
4.	Сетевая безопасность	Атаки на сетевую инфраструктуру, уязвимости в системах, недостаточное обновление и патчинг ПО, атаки на сетевые устройства: маршрутизаторы и коммутаторы.
5.	Мошенничество в области исследований и публикаций	Подделка научных результатов, нарушение правил публикаций, плагиат.
6.	Управление уязвимостями	Недостаточное обнаружение и исправление уязвимостей в системах и приложениях, неправильная конфигурация сетевого оборудования.
7.	Социальная инженерия	Манипуляции для получения конфиденциальных данных или выполнения нежелательных действий путем обмана персонала или студентов.
8.	Отказ в обслуживании (DoS)	Атаки на системы, направленные на перегрузку ресурсов и приведение к отказу в обслуживании.
9.	Безопасность мобильных устройств	Утеря или кража мобильных устройств с конфиденциальной информацией, уязвимости мобильных приложений.
10.	Обучение и осведомленность	Недостаточное обучение персонала и студентов в области ИБ, недостаточное осведомление о правилах безопасного поведения в сети.

C6 – Управление уязвимостями;
 C7 – Социальная инженерия;
 C8 – Отказ в обслуживании (DoS);
 C9 – Безопасность мобильных устройств;

C10 – Обучение и осведомленность.
 Матрица W с экспертными оценками ВС, в которой принималось $c = 1$, имеет следующий вид:

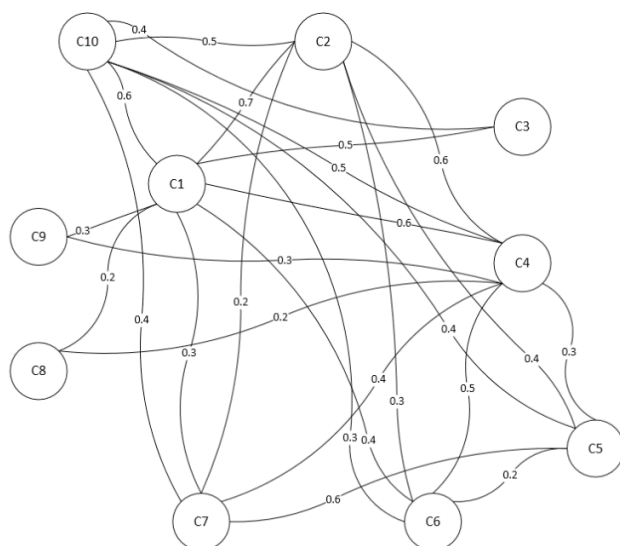


Рис. 2. НКК модели пространства рисков

$$W = \begin{bmatrix} 1 & 0.7 & 0.5 & 0.6 & 0 & 0.4 & 0.3 & 0.2 & 0.3 & 0.6 \\ 0.7 & 1 & 0 & 0.6 & 0.4 & 0.3 & 0.2 & 0 & 0 & 0.5 \\ 0.5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 \\ 0.6 & 0.6 & 0 & 1 & 0.3 & 0.5 & 0.4 & 0.2 & 0.3 & 0.5 \\ 0 & 0.4 & 0 & 0.3 & 1 & 0.2 & 0.6 & 0 & 0 & 0.4 \\ 0.4 & 0.3 & 0 & 0.5 & 0.2 & 1 & 0 & 0 & 0 & 0.3 \\ 0.3 & 0.2 & 0 & 0.4 & 0.6 & 0 & 1 & 0 & 0 & 0.4 \\ 0 & 0 & 0 & 0.4 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0.3 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0.6 & 0.5 & 0.4 & 0.5 & 0.4 & 0.3 & 0.4 & 0 & 0 & 1 \end{bmatrix}$$

Сформирована НКК и матрица ВС для одного из этапов оценки рисков ИБ, которая показывает, какие факторы могут иметь высокое или низкое значение при оценке рисков ИБ конкретно в имеющейся ситуации. При формировании этой НКК автоматически, мы получаем возможность адаптивно оценивать риски ИБ, приспосабливаясь к изменяющимся условиям. Ключевым моментом является корректное определение ВС, чаще всего это происходит в виде экспертной оценки. Но при росте количества концептов данный подход усложняется, и повышается вероятность субъективных ошибок. Для решения этой проблемы можно использовать автоматическую подстройку весов связей с помощью нейронных сетей (НС). В [16] рассмотрено обучение НКК с помощью нейросетевого подхода. Смысл данного подхода в том, чтобы позволить ВС изменяться так, будто они являют-

ся синапсами НС. Дальнейшее исследование направлено на применение нейронных сетей в оценке ВС НКК.

Заключение

Результаты проведенного анализа ГО-СТов, международных стандартов, методик, освещающих вопросы оценки рисков ИБ, позволили сформировать функциональную модель оценки рисков ИБ, реализующую статический подход. В процессе исследования были обнаружены проблемные моменты такого подхода: сложность проведения оценки рисков за счет необходимости высоких компетенций экспертов, возможная рассогласованность и разрозненность их мнений, большие объемы входных данных, что усложняет и значительно замедляет сам процесс оценки рисков. Для устранения этого предложено применение технологий КМ, а именно НКК, для придания процессу оценки рисков ИБ

свойств адаптивности, что способствует более быстрой адаптации модели оценки к изменяющимся условиям.

Предложено внедрить на одном из этапов функциональной модели оценки рисков ИБ – «Идентификация угроз» НКК, содержащую в себе концепты по возможным угрозам ИБ в образовательной сфере. Были приглашены 10 экспертов ВУЗа из области ИБ: преподаватели, специалисты по ЗИ. Опираясь на открытые источники данных: отчеты компаний, занимающихся вопросами ИБ, статистика утечек данных за крайние годы, БДУ ФСТЭК России, а также на свой опыт, эксперты сфор-

мировали 10 концептов для НКК в сфере образования, а также расставили ВС между ними. Предложен задел для обучения НС составлять ВС автоматически. Дальнейшее развитие данного исследования заключается в проведении экспериментов по созданию и обучению НС выставлять ВС, подбора оптимальной архитектуры НС, размерности слоев с целью подбора наиболее оптимальной версии, а также поиск других блоков из предложенной функциональной модели, в которых можно использовать такую комбинацию технологий как НС и КМ.

Литература

1. ISO/IEC 31010:2019 Менеджмент риска. Принципы и руководство. 2019.
2. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска. 2011. – 4 с.
3. ГОСТ Р № ИСО/МЭК 27001-2021 от 01.01.2022. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. 2022.
4. ISO 27001 Системы менеджмента информационной безопасности. 2021.
5. ISO/IEC 27005:2018 «Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности». 2018.
6. Фомин Г. П., Сухорукова И. В., Грибов А. Ф Адаптивная многокритериальная система управления рисками/ Вестник ростовского государственного экономического университета (РИНХ), 2022. № 1 (77). С. 98-103. URL: <https://www.elibrary.ru/item.asp?id=49424923> (дата обращения 30.06.2023 г.)
7. Глушенко С. А. Адаптивная нейро-нечеткая система оценки рисков информационной безопасности организации/ Бизнес-информатика, 2017. № 1 (39). С. 68-77. URL: <https://bijournal.hse.ru/data/2017/08/30/1173956328/%D0%93%D0%BB%D1%83%D1%88%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%A0%D0%A3%D0%A1%D0%9F%D0%95%D0%A0%D0%95%D0%92%D0%9E%D0%94%20-%20v2F.pdf> (дата обращения 30.06.2023 г.)
8. Джамай Е. В., Зинченко А. С. Разработка адаптивной многокомпонентной системы управления риском высокотехнологичных предприятий/ Вестник Московского государственного областного университета. Серия: Экономика, 2022. № 2. URL: <https://cyberleninka.ru/article/n/razrabotka-adaptivnoy-mnogokomponentnoy-sistemy-upravleniya-riskom-vysokotekhnologichnyh-predpriyatij> (дата обращения 30.06.2023 г.)
9. Гузаиров М. Б., Вульфин А. М., Картак В. М., Кириллова А. Д., Мионов К. В. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности/ Труды ИСА РАН, 2019. № 4. Том 69. URL: <http://www.isa.ru/proceedings/images/documents/2019-69-4/62-69.pdf> (дата обращения 25.07.2023 г.)
10. Петухова А. В., Коваленко А. В., Теунаев Д. М. Обзор динамических свойств и алгоритмов обучения нечетких когнитивных карт/ Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2021. № 163. Том 3. URL: <https://cyberleninka.ru/article/n/obzor-dinamicheskikh-svoystv-i-algoritmov-obucheniya-nechetkikh-kognitivnyh-kart> (дата обращения 28.07.2023 г.)
11. Васильев В. И., Вульфин А. М., Герасимова И. Б., Картак В. М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт/DOI:10.21681/2311-3456-2020-2-11-21. URL: https://cyberrus.com/wp-content/uploads/2020/06/11-21-236-20_2.-Vasilyev.pdf (дата обращения 28.07.2023 г.)
12. Васильев В. И., Вульфин А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining/ Системы управления, связи и безопасности, 2021. № 3. URL: <https://cyberleninka.ru/article/n/metodika-otsenki-aktualnyh-ugroz-i-uyazvimostey-na-osnove-tehnologiy-kognitivnogo-modelirovaniya-i-text-mining> (дата обращения 29.07.2023 г.)
13. Отчет об исследовании утечек информации ограниченного доступа в I половине 2022 года.

Экспертно-аналитический центр InfoWatch. 2022 г. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (accessed: 12.09.2023)

14. Утечки данных. TAdviser. 2022. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85 (accessed: 16.09.2023)

15. Актуальные киберугрозы: I квартал 2022 года. Positive Technologies. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/> (accessed: 17.09.2023)

16. Ефремова Н. А., Аверкян А. Н., Ярушев С. А. Гибридные нечеткие когнитивные карты в задачах поддержки принятия решений и прогнозирования/ Software journal theory and applications, 2017. № 4. DOI: 10.15827/2311-6749.25.291 URL: <http://swsys-web.ru/hybrid-fuzzy-cognitive-maps-in-decision-support-tasks.html> (дата обращения 19.09.2023 г.)

References

1. ISO/IEC 31010:2019 Menedzhment riska. Printsipy i rukovodstvo. 2019.
2. GOST R ISO/MEK 31010-2011. Menedzhment riska. Metody otsenki riska. 2011. – 4 s.
3. GOST R № ISO/MEK 27001-2021 ot 01.01.2022. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoy bezopasnosti. Trebovaniya. 2022.
4. ISO 27001 Sistemy menedzhmenta informatsionnoy bezopasnosti. 2021.
5. ISO/IEC 27005:2018 «Informatsionnyye tekhnologii. Metody obespecheniya bezopasnosti. Menedzhment riskov informatsionnoy bezopasnosti». 2018.
6. Fomin G. P., Sukhorukova I. V., Gribov A. F. Adaptivnaya mnogokriterial'naya sistema upravleniya riskami/ Vestnik rostovskogo gosudarstvennogo ekonomicheskogo universiteta (RINKH), 2022. № 1 (77). S. 98-103. URL: <https://www.elibrary.ru/item.asp?id=49424923> (data obrashcheniya 30.06.2023 g.)
7. Glushenko S. A. Adaptivnaya neyro-nechetkaya sistema otsenki riskov informatsionnoy bezopasnosti organizatsii/ Biznes-informatika, 2017. № 1 (39). S. 68-77. URL: <https://bijournal.hse.ru/data/2017/08/30/1173956328/%D0%93%D0%BB%D1%83%D1%88%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%A0%D0%A3%D0%A1%D0%9F%D0%95%D0%A0%D0%95%D0%92%D0%9E%D0%94%20-%20v2F.pdf> (data obrashcheniya 30.06.2023 g.)
8. Dzhamay Ye. V., Zinchenko A. S. Razrabotka adaptivnoy mnogokomponentnoy sistemy upravleniya riskom vysokotekhnologichnykh predpriyatij/ Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Ekonomika, 2022. № 2. URL: <https://cyberleninka.ru/article/n/razrabotka-adaptivnoy-mnogokomponentnoy-sistemy-upravleniya-riskom-vysokotekhnologichnykh-predpriyatij> (data obrashcheniya 30.06.2023 g.)
9. Guzairov M. B., Vul'fin A. M., Kartak V. M., Kirillova A. D., Mironov K. V. Sravnitel'nyy analiz algoritmov kognitivnogo modelirovaniya pri otsenke riskov informatsionnoy bezopasnosti/ Trudy ISA RAN, 2019. № 4. Tom 69. URL: <http://www.isa.ru/proceedings/images/documents/2019-69-4/62-69.pdf> (data obrashcheniya 25.07.2023 g.)
10. Petukhova A. V., Kovalenko A. V., Teunayev D. M. Obzor dinamicheskikh svoystv i algoritmov obucheniya nechetkikh kognitivnykh kart/ Politematicheskij setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta, 2021. № 163. Tom 3. URL: <https://cyberleninka.ru/article/n/obzor-dinamicheskikh-svoystv-i-algoritmov-obucheniya-nechetkikh-kognitivnykh-kart> (data obrashcheniya 28.07.2023 g.)
11. Vasil'yev V. I., Vul'fin A. M., Gerasimova I. B., Kartak V. M. Analiz riskov kiberbezopasnosti s pomoshch'yu nechetkikh kognitivnykh kart/DOI:10.21681/2311-3456-2020-2-11-21. URL: https://cyberrus.com/wp-content/uploads/2020/06/11-21-236-20_2.-Vasilyev.pdf (data obrashcheniya 28.07.2023 g.)
12. Vasil'yev V. I., Vul'fin A. M., Kirillova A. D., Kuchkarova N. V. Metodika otsenki aktual'nykh ugroz i uyazvimostey na osnove tekhnologiy kognitivnogo modelirovaniya i Text Mining/ Sistemy upravleniya, svyazi i bezopasnosti, 2021. № 3. URL: <https://cyberleninka.ru/article/n/metodika-otsenki-aktualnykh-ugroz-i-uyazvimostey-na-osnove-tehnologiy-kognitivnogo-modelirovaniya-i-text-mining> (data obrashcheniya 29.07.2023 g.)
13. Otchet ob issledovanii utechek informatsii ogranichenного доступа v I polovine 2022 goda. Ekspertno-analiticheskij tsentr InfoWatch. 2022 g. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (accessed: 12.09.2023)
14. Uteчки данных. TAdviser. 2022. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85 (accessed: 16.09.2023)
15. Aktual'nyye kiberugrozy: I квартал 2022 года. Positive Technologies. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/> (accessed: 17.09.2023)

16. Yefremova N. A., Averkhan A. N., Yarushev S. A. Gibridnyye nechetkiye kognitivnyye karty v zadachakh podderzhki prinyatiya resheniy i prognozirovaniya/ Software journal theory and applications, 2017. № 4. DOI: 10.15827/2311-6749.25.291 URL: <http://swsys-web.ru/hybrid-fuzzy-cognitive-maps-in-decision-support-tasks.html> (data obrashcheniya 19.09.2023 g.)

ПАЛЮТИНА Галия Наилевна, аспирант, младший научный сотрудник Федерального государственного бюджетного образовательного учреждения высшего образования «Ростовский государственный экономический университет (РИНХ)». 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69. E-mail: hello616@yandex.ru

PALYUTINA Galiya Nailevna, postgraduate student, junior researcher at the Federal State Budgetary Educational Institution of Higher Education "Rostov State Economic University (RINH)". 344002, Rostov-on-Don, st. Bolshaya Sadovaya, 69. E-mail: hello616@yandex.ru

ИССЛЕДОВАНИЕ АТАК НА БЕСКОНТАКТНЫЕ СМАРТ- КАРТЫ И RFID-МЕТКИ

В данной статье рассматриваются особенности безопасности бесконтактных смарт-карт и RFID-меток, широко используемых в настоящее время. Приведены результаты практического исследования уязвимостей и потенциальных атак на эти устройства, также представлены результаты экспериментов по созданию и использованию скиммера для считывания данных с карт. Описаны атаки, основанные на восстановлении секретных ключей, которые могут быть использованы злоумышленниками. Рассматриваются такие атаки, как Lock Attack, Darkside Attack, Nested Attack и Communication Interception Attack, и описываются методы и инструменты для их реализации. Предлагаются рекомендации по улучшению защиты и безопасности бесконтактных смарт-карт и RFID-меток.

Ключевые слова: информационная безопасность, угроза безопасности информации, системы контроля и управления доступом, RFID-метка, бесконтактная карта, скимминг, смарт-карта.

Neklyudov D.N., Lebed A.S., Kuzmina U.V.

RESEARCH ON ATTACKS AGAINST CONTACTLESS SMART CARDS AND RFID TAGS

This article examines the security features of contactless smart cards and RFID tags, which are widely used today. The results of a practical study of vulnerabilities and potential attacks on these devices are presented, and the results of experiments on the creation and use of a skimmer for reading data from cards are also presented. Attacks based on the recovery of secret keys that could be exploited by malicious actors are described. Attacks such as the Lock Attack, Darkside Attack, Nested Attack, and Communication Interception Attack are discussed, along with methods and tools for their implementation. Recommendations for improving the protection and security of contactless smart cards and RFID tags are also provided.

Keywords: information security, information security threat, access control and management system, RFID-tag, contactless card, skimming, smart card.

В связи с растущей потребностью в обеспечении безопасности транспорта и контрольно-пропускных пунктов бесконтактные карты и брелоки становятся все более популярными способами идентификации ввиду

простоты устройства, низкой стоимости и практичности. Обеспечение охраны путем разграничения доступа данной технологией используется на большинстве современных объектов. Несмотря на обширность примене-

ния, системы имеют критические незакрытые уязвимости, из-за которых обеспечение безопасности таких систем является большой проблемой, о которой некоторые пользователи даже не подозревают.

Информация на самых популярных метках MIFARE Classic 1K состоит из 16 секторов памяти, каждый из которых включает 4 блока. Другие же метки могут отличаться количеством блоков и памятью, однако, это несущественно. Нулевой блок нулевого сектора содержит уникальный идентификатор и информацию о производителе, за которым идет контрольный байт (BCC), вычисленный при

помощи операции XOR. Блок программируется при производстве чипа и имеет защиту от перезаписи. Каждый четвертый блок сектора называется трейлер, он содержит 2 ключа доступа к каждому блоку и условия доступа [2]. Трейлер хранит ключ А, обязательный для чтения и опциональный ключ В, а также условия доступа к 6 – 9 блоку. Условия доступа определяют, какие операции доступны для этого сектора. Считыватель должен пройти аутентификацию для сектора, прежде чем будут разрешены какие-либо операции с памятью. Схема памяти карты mifare Classic 4k представлена на рисунке 1.

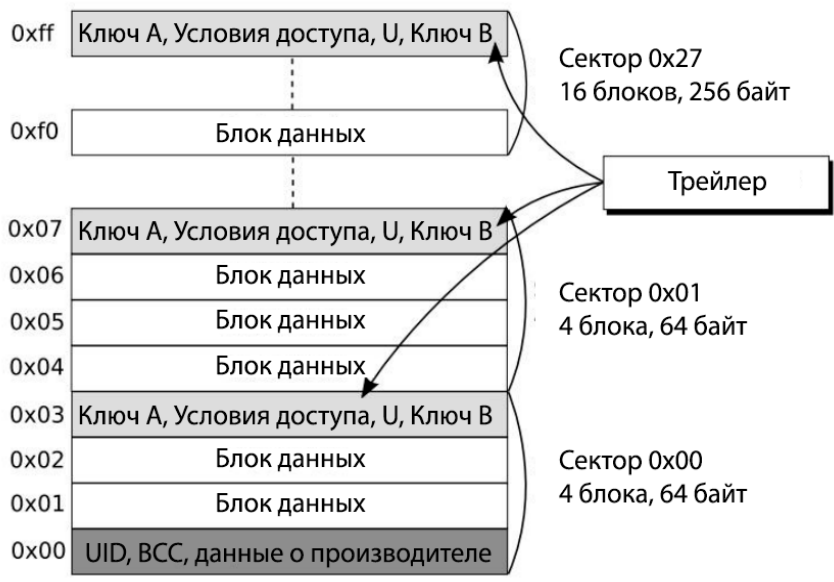


Рис. 1. Устройство памяти карты MIFARE Classic 4k

Трейлер имеет особые условия доступа. Ключ А никогда не читается, а ключ В может быть настроен как читаемый или нет. В этом случае память используется только для хранения данных, а ключ В не может использоваться в качестве ключа аутентификации. Помимо АС – условий доступа, и ключей, остается один байт данных – U, неопределенный байт, который может использоваться для хранения данных.

Блок данных используется для хранения произвольных данных или может быть настроен как блок значений. При использовании в качестве блока значений 4-байтовое значение со знаком сохраняется последовательно: дважды неинвертированным и один раз инвертированным. Эти четыре байта хранятся от младшего значащего байта слева до старшего значащего байта справа. Оставшиеся 4 байта используются для хранения блок

адреса, который может быть задействован в качестве указателя. Схема трейлера представлена на рисунке 2.

Большинство команд связаны с блоком данных (набор команд MIFARE Classic) требуют, чтобы считыватель был аутентифицирован для сектора. Условия доступа проверяются каждый раз при выполнении команды, чтобы определить, разрешено это или нет. Блок данных может быть настроен только для чтения.

Существует несколько способов осуществления атак на восстановление секретных ключей карт, с помощью которых злоумышленник может скомпрометировать информацию с карты жертвы:

- card-only attacks (злоумышленник имеет считыватель, ему достаточно только карта для осуществления атаки);
- перехват логов во время обмена данными карты и считывателя.



Рис. 2. Содержание трейлера

В обоих случаях злоумышленнику необходимо определенное устройство, выполняющее функции считывателя. Таким устройством может выступать как смартфон с NFC-чипом и установленной утилитой (например, NXP TagInfo), так и специализированное оборудование, такое как Proxmark3 [8]. В первом случае смартфон не может прочесть все стандарты карт, а Proxmark3, несмотря на то, что это уже готовое решение, не подвержено модификации, в случае необходимости, не говоря о том, что стоимость данного продукта в несколько раз выше, чем стоимость реализации такого устройства своими руками. Несмотря на то, что за создание и дистрибьюцию такого устройства предусмотрена уголовная ответственность по статье 138.1 УК РФ «Незаконный оборот специальных средств, предназначенных для негласного получения информации» в виде лишения свободы на срок до четырех лет, устройство, как и его комплектующие, свободно распространяются в сети Интернет.

В рамках исследования был собран скиммер. Для этого нам понадобилось: программируемый микроконтроллер; модуль, считывающий смарт карты; источник питания; перезаписываемые карты; программное обеспечение.

В качестве микроконтроллера подойдут любые контроллеры, например, семейства Arduino (для компактности можно использовать Arduino Mini). Устройство для считывания смарт карт и RFID-меток высокой частоты – Mifare RC522 или, в случае, если понадобится считать карты, работающие на низкой частоте – RDM6300 UART. Перезаписываемые карты – Mifare Zero. Источником питания может быть все, начиная от батарейки до портативного аккумулятора или смартфона.

Собранное устройство (рис. 3), может считывать, как низкочастотные карты, так и высокочастотные, из-за двух считывающих модулей.

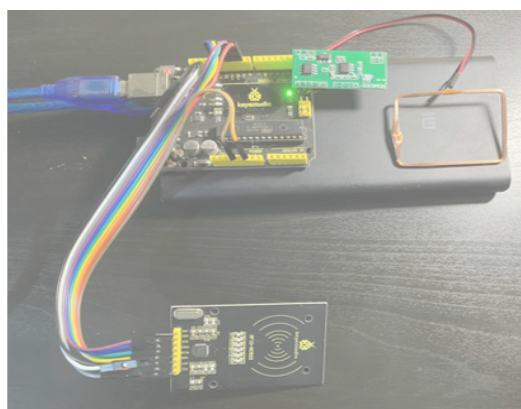


Рис. 3. Разработанный скиммер

За счет его программируемости, оно может осуществлять следующие атаки:

- Lock Attack;
- Nested Attack;
- Darkside Attack;
- Communication interception Attack;

Lock Attack - атака, использующая возможность изменения лок-битов карты, преимущественно применима для транспортных карт.

Например, в lock секторе карты MIFARE ULTRALIGHT мы можем заблокировать статус сектора OTP, что делает невозможным изменение его битов на 1.

Путем установки 4-ого бита первого байта в значение 1, мы заблокировали сектор OTP (рис. 4).

HEX	F2 03
BIN	11110010 00000011
HEX	FA 03
BIN	11111010 00000011

Рис. 4. Изменение lock бита

Изменяя лок-биты, можно добиться невозможности перезаписи контрольной суммы (т.е. количество поездок) валидатором, с

сохранением доступа в транспортную систему. Как итог – «вечный» проездной [1].

Darkside Attack – атака, которая заключается в том, что во время аутентификации, тег проверяет биты четности. Если один из восьми битов четности неверен, тег не отвечает. Однако, если все восемь битов четности верны, но ответ неверен, тэг ответит 4-битным кодом ошибки 0x5 (NACK), указывающий на ошибку передачи [9]. Более того, этот 4-битный код

ошибки отправляется в зашифрованном виде. Если злоумышленник объединит (XOR) значение кода ошибки 0x5 (известный открытый текст) с его зашифрованной версией, он может восстановить четыре бита ключевого потока.

Атака может осуществляться с помощью утилиты MFCUK (MiFare Classic Universal toolKit) [10]. Утилита помогает, при помощи перебора словарей, получить первичный ключ сектора (рис. 5, 6).

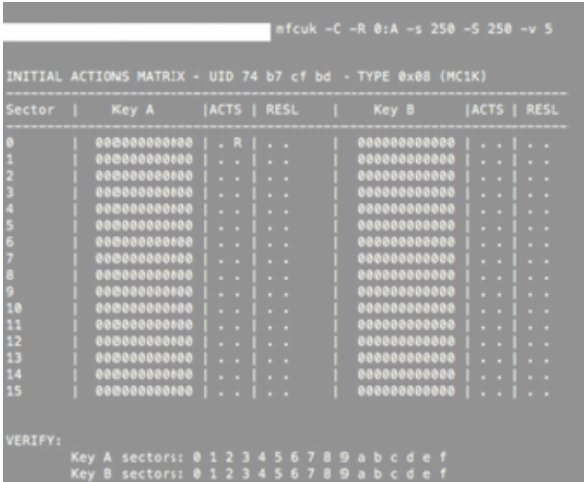


Рис. 5. MFCUK

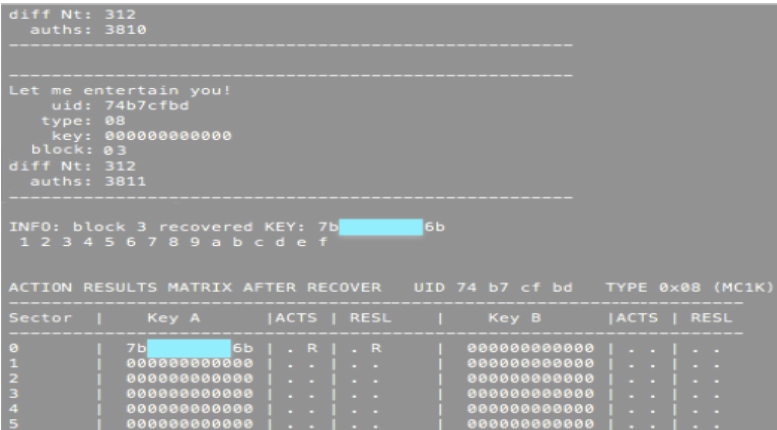


Рис. 6. Получение ключа используя Darkside attack

Полученный ключ можно использовать при реализации следующих атак.

Nested Attack – смысл атаки заключается в подборе паролей исходя из известного ключа к одному блоку данных. Атака является результатом уязвимости генератора псевдослучайных чисел (ГПСЧ), которая заключается в утечке битов кода ошибки и битов четности. Чтобы атака считалась успешной необходимо знать хотя бы один секретный ключ любого блока, из-за чего можно восстановить ключи к оставшимся блокам [3]. Атака работает для любых карт с CRYPTO1.

Реализованный нами скиммер может осуществлять данную атаку за счет записи дампа смарт-карты. Благодаря открытой утилите MFOC (Mifare Classic Offline Cracker) (рисунок 7), зная один из секретных ключей, можно восстановить второй секретный ключ сектора или всех секторов сразу (рис. 9). Данный алгоритм, как и MFCUK, при большом объеме памяти микроконтроллера, можно вшить в само устройство, тем самым реализовать атаку без использования второстепенных устройств.

Communication Interception Attack – ата-

```

root@_ ~ >> mfoc -k 45a4777d6b3 -O card.mfd
The custom key 0x45a4777d6b3 has been added to the default keys
Found Mifare Classic 1k tag
ISO/IEC 14443A (106 kbps) target:
  ATQA (SENS_RES): 00 04
* UID size: single
* bit frame anticollision supported
  UID (NFCID1): 3a da 67 16

```

Рис. 7. Запуск MFOC

```

Sector 00 - Found Key A: 45a4777d6b3 Found Key B: 22609a620491
Sector 01 - Unknown Key A Unknown Key B
Sector 02 - Unknown Key A Unknown Key B

```

Рис. 8. Восстановление ключа B

ка, позволяющая провести откат состояния регистра LFSR (от англ. Linear Feedback Shift Register – линейный регистр с обратной связью) до первоначального. Заключается в восстановлении ключа для шифрования перехваченной фазы аутентификации между интерrogатором и транспондером. Важным условием, стоит отметить то, что оба устройства должны знать секретный ключ. Атака использует два ключевых недостатка в потоковом шифре CRYPTO1, а именно возможность восстановления состояния LFSR вследствие того, что в генераторе фильтров используются только нечетные биты, что в свою очередь позволяет откатить состояние регистра до первоначального из-за того, что первые де-

вать битов LFSR не используются генератором фильтров [4]. Данная атака основана на механизме двух вышеупомянутых атак.

В качестве рекомендаций по защите бесконтактных смарт карт и RFID-меток может быть предложено их хранение в картхолдерах, футлярах или кошельках из радио непроницаемых материалов (например, они могут быть изготовлены из алюминия, карбона или других менее дорогих материалов, таких как фольга). Осуществить переход на более современные стандарты карт с более совершенными алгоритмами шифрования данных. В прошивке интерrogатора установить дополнительную проверку на блокировку сектора OTP.

Литература

1. Медведев Н.М., Лукьянов Г.И., Баранкова И.И. Оценка надежности использования RFID-технологии / Сбродова Е.А., М.А. Загребин // Безопасность информационного пространства. 2018. Т.1. С. 169-173.
2. Цапов А.Е., Литвинова А.В., Лукьянов Г.И. Оценка безопасности СКУД на базе RFID-системы / Баранкова И.И., Михайлова У.В., Лукьянов Г.И. // Актуальные проблемы современной науки, техники и образования. 2021. Т.1. С. 404.
3. Garcia Flavio D., Peter van Rossum, Roel Verdult, Ronny Wichers Schreur Wirelessly Pickpocketing a Mifare Classic Card / Garcia Flavio D., Peter van Rossum, Roel Verdult, Ronny Wichers Schreur [Электронный ресурс] // Researchgate:[сайт].—URL: https://www.researchgate.net/publication/220713937_Wirelessly_Pickpocketing_a_Mifare_Classic_Card.
4. Шинкевич Н.Н. ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ БЕСКОНТАКТНЫХ СМАРТ-КАРТ НА ПРИМЕРЕ MIFARE CLASSIC / Шинкевич Н.Н. [Электронный ресурс] // Cyberleninka : [сайт]. — URL: <https://cyberleninka.ru/article/n/issledovanie-bezopasnosti-beskontaktnyh-smart-kart-na-primere-mifare-classic/viewer>.
5. Sarrias M. B., Jordi H. J. Security in RFID devices / Marti Berini Sarrias, Jordi Herrera Joancomartí [Электронный ресурс] // Universitat Autònoma de Barcelona. Escola d'Enginyeria.: [сайт]. — URL: https://ddd.uab.cat/pub/treecpro/2013/hdl_2072_232718/PFC_MartiBeriniSarrias.pdf.
6. Garcia Flavio D., Gerhard de Koning Gans, Ruben Muijrrers et al Dismantling MIFARE Classic / Garcia Flavio D., Gerhard de Koning Gans, Ruben Muijrrers et al [Электронный ресурс] // 13th European Symposium on Research in Computer Security: [сайт]. — URL: <https://www.cs.bham.ac.uk/~garciaf/publications/Dismantling.Mifare.pdf>.
7. Lupták P. Mifare Classic analysis / Pavol Lupták [Электронный ресурс] // nethemba: [сайт]. — URL: <https://nethemba.com/resources/mifare-classic-slides.pdf>.

8. Larson K. Mifare Smart Card Security / Larson Kevin [Электронный ресурс] // Incyber: [сайт]. — URL: <https://incyber.org/en/mifare-smart-card-security-by-kevin-larson>.
9. Courtois N.T. THE DARK SIDE OF SECURITY BY OBSCURITY and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime / Nicolas T. Courtois [Электронный ресурс] // eprint: [сайт]. — URL: <https://eprint.iacr.org/2009/137.pdf>.
10. Márcio Almeida Hacking Mifare Classic Cards / Márcio Almeida [Электронный ресурс] // www.blackhat.com: [сайт]. — URL: <https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf>

References

1. Medvedev N.M., Luk'janov G.I., Barankova I.I. Ocenka nadezhnosti ispol'zovaniya RFID-tehnologii / Sbrodova E.A., M.A. Zagrebin // Bezopasnost' informacionnogo prostranstva. 2018. T.1. S. 169-173.
2. Capov A.E., Litvinova A.V., Luk'janov G.I. Ocenka bezopasnosti SKUD na baze RFID-sistemy / Barankova I.I., Mihajlova U.V., Luk'janov G.I. // Aktual'nye problemy sovremennoj nauki, tehniki i obrazovaniya. 2021. T.1. S. 404.
3. Garcia Flavio D., Peter van Rossum, Roel Verdult, Ronny Wichers Schreur Wirelessly Pickpocketing a Mifare Classic Card / Garcia Flavio D., Peter van Rossum, Roel Verdult, Ronny Wichers Schreur [Electronic resource] // Researchgate:[website].—URL: https://www.researchgate.net/publication/220713937_Wirelessly_Pickpocketing_a_Mifare_Classic_Card.
4. Shinkevich N.N. SECURITY RESEARCH OF CONTACTLESS SMART CARDS ON THE EXAMPLE OF MIFARE CLASSIC / Shinkevich N.N. [Electronic resource] // Cyberleninka: [website]. — URL: <https://cyberleninka.ru/article/n/issledovanie-bezopasnosti-beskontaktnyh-smart-kart-na-primere-mifare-classic/viewer>.
5. Sarrias M. B., Jordi H. J. Security in RFID devices / Marti Berini Sarrias, Jordi Herrera Joancomartí [Electronic resource] // Universitat Autònoma de Barcelona. Esc ola d'enginyeria.: [website]. — URL: https://ddd.uab.cat/pub/trerecpro/2013/hdl_2072_232718/PFC_MartiBeriniSarrias.pdf.
6. Garcia Flavio D., Gerhard de Koning Gans, Ruben Muijers et al Dismantling MIFARE Classic / Garcia Flavio D., Gerhard de Koning Gans, Ruben Muijers et al [Electronic resource] // 13th European Symposium on Research in Computer Security: [website]. — URL: <https://www.cs.bham.ac.uk/~garciaf/publications/Dismantling.Mifare.pdf>.
7. Lupták P. Mifare Classic analysis / Pavol Lupták [Электронный ресурс] // nethemba: [сайт]. — URL: <https://nethemba.com/resources/mifare-classic-slides.pdf>.
8. Larson K. Mifare Smart Card Security / Larson Kevin [Электронный ресурс] // Incyber: [сайт]. — URL: <https://incyber.org/en/mifare-smart-card-security-by-kevin-larson>
9. Courtois N. T. THE DARK SIDE OF SECURITY WITH THE HELP OF OBSCURITY and cloning of classic MiFare railway and construction passes anywhere and anytime / Nicholas T. Courtois [Electronic resource] // eprint: [website]. — URL: <https://eprint.iacr.org/2009/137.pdf>.
10. Márcio Almeida Hacking Mifare Classic Cards / Márcio Almeida [Electronic resource] // www.blackhat.com: [website]. — URL: <https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf>.

НЕКЛЮДОВ Данил Николаевич, студент 4 курса по специальности «Информационная безопасность автоматизированных систем» кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: dejksdan@gmail.com

NEKLYUDOV Danil Nikolaevich, 4th year student majoring in “Information Security of Automated Systems” department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: dejksdan@gmail.com

ЛЕБЕДЬ Александр Сергеевич, студент 4 курса по специальности «Информационная безопасность автоматизированных систем» кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: mail23032019@mail.ru

LEBED Alexander Sergeevich, 4th year student majoring in “Information Security of Automated Systems” department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: mail23032019@mail.ru

КУЗЬМИНА 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: Ylianapost@gmail.com

KUZMINA Ulyana Vladimirovna, candidate of Technical Sciences, associate professor of the department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: Ylianapost@gmail.com

О ПРИМЕНЕНИИ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОЦЕНКИ ВЕСОВ СВЯЗЕЙ МЕЖДУ КОНЦЕПТАМИ НЕЧЕТКОЙ КОГНИТИВНОЙ КАРТЫ В АДАПТИВНОЙ ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ¹

В статье обсуждаются результаты анализа применения нейронных сетей (НС) в оценке весов связей (ВС) между концептами нечеткой когнитивной карты (НKK) в адаптивной оценке рисков информационной безопасности (РИБ).

Были проанализированы научные публикации в области НKK и НС, определены особенности проектирования архитектуры и обучения НС, был сформирован алгоритм обучения НС проводить оценку весов связи НKK.

Продemonстрирован процесс обучения НС осуществлять оценку ВС, произведенный на обучающем наборе данных. Предложен программный код для решения данной задачи, определена эффективность применения технологий НС и КМ для адаптивной оценки рисков ИБ.

Ключевые слова: информационная безопасность, адаптивная оценка рисков информационной безопасности, нечеткие когнитивные карты, веса связи, нейронные сети.

¹ В рамках исполнения гранта ИБ МТУСИ № 40469-23/2022-к 15.06.2022г. протокол №2

ON THE APPLICATION OF NEURAL NETWORKS FOR ESTIMATING THE WEIGHTS OF CONNECTIONS BETWEEN THE CONCEPTS OF A FUZZY COGNITIVE MAP

The article discusses the results of the analysis of the use of neural networks (NN) in estimating the weights of connections (BC) between the concepts of a fuzzy cognitive map (FCM) in adaptive information security risk assessment (ISS).

Scientific publications in the field of NCC and NN were analyzed, the features of designing the architecture and training of NN were determined, and an algorithm for training NN to evaluate the NCC communication weights was formed.

The process of training a NN to evaluate the aircraft produced on a training data set is demonstrated. A program code for solving this problem is proposed, and the effectiveness of using NN and CM technologies for adaptive information security risk assessment is determined.

Keywords: *information security, adaptive information security risk assessment, fuzzy cognitive maps, connection weights, neural networks.*

Введение

В современном информационном обществе вопросы информационной безопасности (ИБ) всегда являются важными и актуальными. Одним из важных компонентов эффективной стратегии ИБ в любой компании или организации является оценка рисков. Традиционные методы оценки рисков ИБ часто основываются на статических моделях и предположениях, которые могут быть недостаточными для учета динамических изменений в информационной системе и угрозах. Адаптивная оценка РИБ стремится преодолеть эту проблему, обеспечивая гибкость и способность модели адаптироваться к новым данным и условиям.

Подход адаптивной оценки РИБ основан на постоянном мониторинге и анализе угроз и уязвимостей, а также на принятии мер по обеспечению безопасности в реальном времени. В этом контексте уместно вспомнить про НКК, которые могут быть применены в адаптивной оценке РИБ.

НКК – это модель, представленная в графическом виде и отражающая связи между различными концептами, факторами и событиями, связанными с ИБ.

НКК позволяют моделировать сложные взаимосвязи и динамические изменения в ИБ-среде, а также имеют способность прогнозировать и адаптироваться к новым угрозам и уязвимостям.

Одним из важных моментов, связанных с работой НКК, является оценка ВС между концептами в НКК. Она позволяет определить степень влияния одного концепта на другой и учесть сложные зависимости и взаимодействия между ними. В этом контексте, НС предлагают эффективный инструмент для оценки и определения ВС на основе обучающих данных.

Целью настоящей работы является рассмотрение возможности применения НС в контексте оценки ВС между концептами в НКК для адаптивной оценки РИБ. Представлена методика оценки ВС с использованием НС, а также приведены результаты экспериментов для оценки эффективности предложенного подхода.

Нечёткие когнитивные карты и нейронные сети в адаптивной оценке рисков ИБ

При использовании НКК [1-3] в адаптив-

ной оценке РИБ, эксперты могут оценивать взаимосвязь между различными факторами: угрозы, уязвимости, защитные меры и последствия. НКК позволяют моделировать и представлять сложные зависимости и взаимодействия между этими факторами [4].

Одним из преимуществ использования НКК в адаптивной оценке РИБ является их способность учитывать неопределенность и нечеткость данных, различные уровни вероятности и степени влияния факторов на РИБ. НКК могут быть адаптированы и обновлены с учетом изменений в ИБ-среде. Это позволяет проводить динамическую оценку РИБ и принимать актуальные решения на основе изменений в концепциях и связях между ними.

Рассмотрим пример НКК для образовательной сферы со следующими концептами:

- C1 – Управление доступом;
- C2 – Конфиденциальность студентов и персональных данных;
- C3 – Физическая безопасность;
- C4 – Сетевая безопасность;
- C5 – Мошенничество в области исследований и публикаций;
- C6 – Управление уязвимостями;
- C7 – Социальная инженерия;
- C8 – Отказ в обслуживании (DoS);
- C9 – Безопасность мобильных устройств;
- C10 – Обучение и осведомленность.

Дальнейшим шагом по работе с данной НКК является оценка ВС между ее концептами. Традиционно эту задачу решают экспертным путем, что допускает вероятность рассогласованности экспертов и увеличения сложности оценки ВС с ростом факторов. Для решения этого предложено применить НС, а именно обучить НС самостоятельно оценивать ВС.

Результаты исследований вопросов НС отражены в работах многих исследователей, так в [5] представлена общая схема оценки защищенности объектов информатизации с использованием нейронных сетей. Авторы подчеркивают, что результаты оценки зависят от множества факторов и сложно формально определить итоговый показатель из-за неизвестной взаимосвязи между показателями защищенности. Для решения этой проблемы авторы используют искусственные нейронные сети и анализируют групповые и частные показатели в качестве входных данных, основываясь на отечественных и зарубежных методиках и стандартах. Они также

отмечают важность опыта экспертов для качественной оценки и считают задачу исключения вероятности ошибочного суждения экспертов ключевой.

Одним из важных вопросов в использовании НС является их обучение, в [6] приведен обзор методов обучения глубоких НС, содержащих более одного скрытого слоя. Автор работы указывает, что искусственные НС могут аппроксимировать любую непрерывную функцию с требуемой точностью. Однако, он отмечает, что в настоящее время не существует конструктивного подхода, который гарантированно позволял бы создавать НС с заранее заданными свойствами, что является ограничением для их применения. Автор делает вывод, что на данный момент два типа архитектур НС являются доминирующими: сверточные и рекуррентные сети. Он также отмечает перспективность совместного использования обоих типов архитектур с обучением с подкреплением. Одним из преимуществ рекуррентных НС является возможность обучения без учителя и без предварительного размеченного набора данных. В [7] автор расширяет существующие методы обучения и рассматривает различные способы инициализации весов. Он обсуждает применение принципов обучения с учителем, self-taught learning и transfer learning. В ходе экспериментов автор обнаружил проблему затухания градиента в процессе обучения, при которой первые слои многослойного перцептрона учатся менее эффективно. В связи с этим, автор предлагает использовать итеративный алгоритм инициализации весов, который основан на уточнении весов скрытых слоев НС через решение исходной задачи классификации или регрессии. Он также предлагает использовать этот алгоритм для построения ансамбля НС. Этот аспект работы подчеркивает необходимость исследования особенностей организации ансамблей НС и в целом НС.

Обучение НС проводить оценку весов связи НКК

Ключевыми моментами в создании НС являются выбор ее типа, архитектуры и метода обучения [8]. Наиболее распространенные типы НС, их достоинства, недостатки и применимость в выбранной области приведены в таблице 1 [6, 8, 9]. Основные элементы архитектуры НС приведены в таблице 2 [6]. Распространенные алгоритмы обучения НС – в таблице 3 [6, 7, 9].

Типы нейронных сетей

№	Тип НС	Характеристика
1.	Многослойный персептрон (MLP)	Состоит из нескольких слоев нейронов: входной, скрытые слои и выходной. Каждый нейрон в слоях, кроме входного, получает сигналы от предыдущего слоя и передает свой выход следующему слою. Входные данные распространяются через нейроны слоев вперед, от входного слоя к выходному, без циклических связей. Используется в различных областях, включая распознавание образов, классификацию, регрессию и другие задачи обработки данных.
2.	Рекуррентные НС (RNN)	Используют направленную последовательность связи между узлами. Результат вычислений на каждом этапе используется в качестве исходных данных для следующего. Подходят для анализа последовательных данных: временные ряды, что может быть полезным для анализа данных ИБ. Могут использоваться для анализа последовательностей событий, связанных с ИБ-инцидентом: временная метка, тип инцидента, источник атаки. Могут улавливать долгосрочные зависимости и паттерны, могут обрабатывать входные данные разной длины, учитывать контекст и зависимости между данными в последовательности.
3.	Сверточные НС (CNN)	Используют свертки для извлечения признаков из входных данных. Подходят для анализа изображений и других типов данных, которые можно представить в виде матрицы. Могут использоваться для анализа логов и других текстовых данных. Способны извлекать значимые признаки из входных данных, позволяют моделировать иерархическую и локальную структуру данных, могут быть модульными и легко масштабируемыми.

Таблица 2

Архитектура нейронной сети

№	Элемент архитектуры	Характеристика
1.	Входной слой	Для ввода данных: параметры системы безопасности или другие характеристики, которые могут влиять на риски ИБ.
2.	Скрытые слои	Используются для обработки входных данных. Количество слоев и количество нейронов зависит от сложности задачи и размера обучающего набора данных.
3.	Выходной слой	Используются для выдачи результата оценки рисков. Количество нейронов зависит от количества классов рисков, которые необходимо оценивать.
4.	Функция активации	Используются для нелинейной обработки данных в скрытых слоях и выходном слое. Подходящие функции: ReLU, sigmoid или tanh.
5.	Функция потерь	Используются для определения ошибки между предсказанными и фактическими значениями. Подходящие функции: mean squared error, categorical cross-entropy.
6.	Оптимизатор	Для обновления весов НС на каждой итерации обучения. Подходящие оптимизаторы: Adam, SGD или RMSProp.

Таблица 3

Алгоритмы обучения НС

№	Алгоритм	Характеристика
1.	Обратное распространение ошибки	Основывается на минимизации функции потерь, которая измеряет разницу между выходом сети и желаемым выходом. После расчета ошибки, алгоритм обновляет веса в соответствии с градиентом функции потерь.
2.	Метод стохастического градиентного спуска	Обновляет веса в соответствии с градиентом функции потерь, но использует только случайное подмножество обучающих данных на каждой итерации, что позволяет быстрее обучать модель на больших данных.
3.	Метод адаптивного градиентного спуска	Адаптивно изменяет скорость обучения для каждого параметра в соответствии с его градиентом, что позволяет более эффективно обновлять веса в сети.

№	Алгоритм	Характеристика
4.	Метод Адам	Использует комбинацию метода стохастического градиентного спуска с моментом и метода адаптивного градиентного спуска. Это позволяет более эффективно обновлять веса в сети, учитывая как градиент, так и его предыдущие значения.
5.	Метод максимального правдоподобия	Минимизирует разницу между распределением вероятностей, предсказанным моделью, и распределением вероятностей, заданным обучающими данными. Часто используется в задачах классификации.
6.	Метод генетического алгоритма	Эволюционный алгоритм, использует популяцию индивидуальных решений и эмуляцию естественного отбора, чтобы найти оптимальные веса для НС.

На основе вышеперечисленного анализа типов НС, их архитектуры и методов обучения сформируем НС, способную решить поставленную задачу – обучить НС оценивать ВС между концептами НКК.

Для обучения НС проводить оценку ВС в НКК можно использовать тип НС – MLP. Входной слой принимает входные данные, скрытые слои выполняют вычисления, а выходной слой предоставляет оценку ВС НКК. Скрытых слоев может быть несколько, это позволяет моделировать сложные взаимосвязи между концептами в НКК и оценивать ВС более точно. Также MLP можно легко расширить, добавив больше скрытых слоев или изменяя количество нейронов в каждом слое. Размер скрытого слоя является гиперпараметром, который можно настраивать и экспериментировать с разными значениями, чтобы найти наилучшую производительность для решения задач.

В качестве входных данных были использованы данные, полученные при создании НКК: определенные экспертами 10 концептов, результаты оценки ВС, выставленные 10 экспертами. ВС, определенные экспертами, также их можно обозначить как желаемые ВС, представляют собой данные для обучающей выборки. Тестовая выборка задана произвольно.

Подходящими для решения поставленной задачи методами обучения являются: алгоритм обратного распространения ошибки и градиентного спуска. Для его реализации необходимо определить функцию потерь, которая будет минимизироваться в процессе обучения. В данном случае, функция потерь зависит от разницы между оценками ВС НКК и желаемыми значениями. Метод обратного распространения ошибки – для вычисления градиента функции потерь по ВС, и градиентный спуск – для обновления ВС с целью минимизации функции потерь.

Обучение НС проводить оценку ВС НКК будет выполняться итеративно. На каждой итерации, входные данные НКК будут подаваться на вход НС, оценки ВС будут вычисляться, а затем будут сравниваться с желаемыми значениями. После этого, будет происходить обновление ВС с использованием метода обратного распространения ошибки и градиентного спуска. Процесс будет повторяться до достижения требуемой точности или сходимости. Алгоритм обучения НС проводить оценку ВС НКК представлен на рис. 1.

Рассмотрим более подробно данный алгоритм:

1. Ввод 10 концептов НКК, каждый представлен в виде вектора, где каждый элемент соответствует определенному признаку или характеристике концепта.

2. Ввод желаемых ВС. На данном этапе вводится матрица ВС, которая была определена экспертами:

3. Инициализация ВС НС и параметров обучения.

4. Прямое распространение. Вычисление выходного значения НС на основе текущих ВС. Входные данные подаются на вход НС, и происходит прямое распространение сигнала. Каждый нейрон вычисляет свой выход на основе входных данных и текущих ВС.

5. Вычисление ошибки. Результаты прямого распространения сравниваются с желаемыми значениями ВС. Разница между предсказанными значениями и желаемыми значениями представляет ошибку.

6. Обратное распространение ошибки. Ошибка распространяется обратно через НС. Каждый нейрон вычисляет свою часть ошибки на основе ошибки предыдущего слоя и своей функции активации.

7. Обновление ВС. ВС обновляются с использованием алгоритма обратного распространения ошибки и градиентного спуска. Градиент ошибки по ВС вычисляется, и ВС об-

$$W = \begin{bmatrix} 1 & 0.7 & 0.5 & 0.6 & 0 & 0.4 & 0.3 & 0.2 & 0.3 & 0.6 \\ 0.7 & 1 & 0 & 0.6 & 0.4 & 0.3 & 0.2 & 0 & 0 & 0.5 \\ 0.5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 \\ 0.6 & 0.6 & 0 & 1 & 0.3 & 0.5 & 0.4 & 0.2 & 0.3 & 0.5 \\ 0 & 0.4 & 0 & 0.3 & 1 & 0.2 & 0.6 & 0 & 0 & 0.4 \\ 0.4 & 0.3 & 0 & 0.5 & 0.2 & 1 & 0 & 0 & 0 & 0.3 \\ 0.3 & 0.2 & 0 & 0.4 & 0.6 & 0 & 1 & 0 & 0 & 0.4 \\ 0 & 0 & 0 & 0.4 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0.3 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0.6 & 0.5 & 0.4 & 0.5 & 0.4 & 0.3 & 0.4 & 0 & 0 & 1 \end{bmatrix}$$

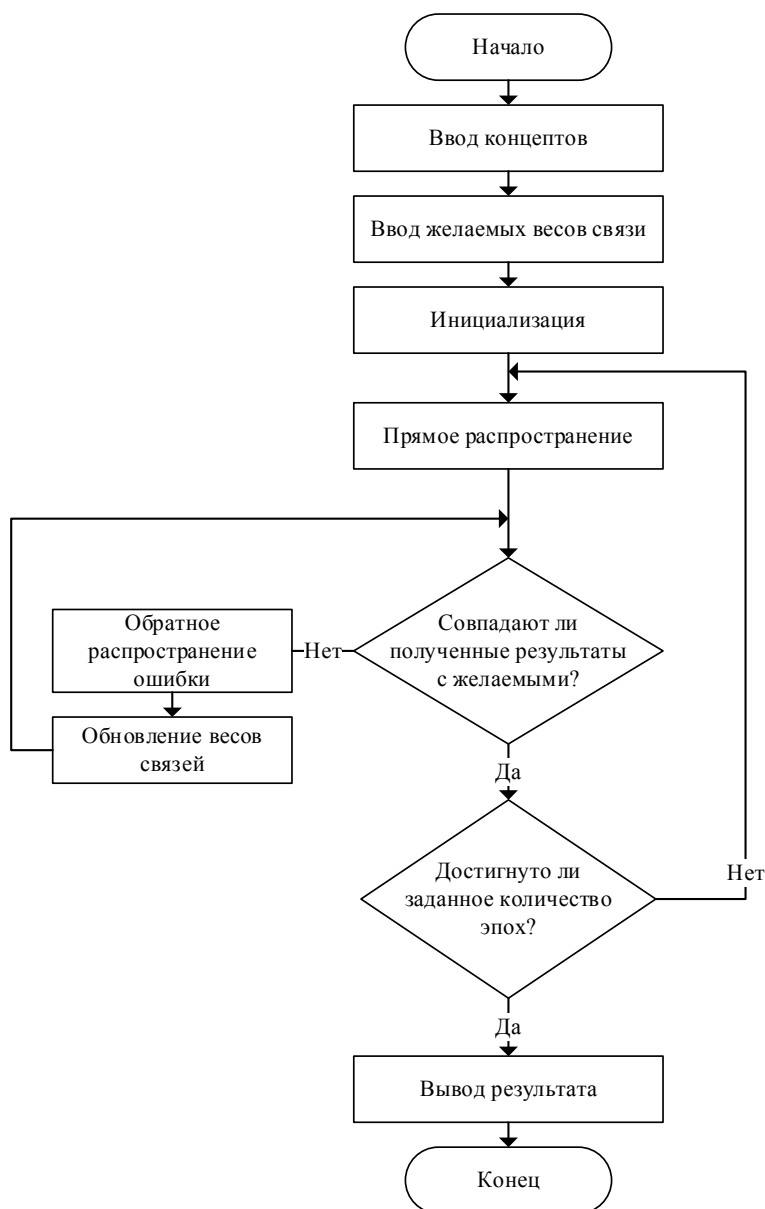


Рис. 1. Алгоритм обучения НС проводить оценку весов связи НКК

новляются в направлении, противоположном градиенту, чтобы минимизировать ошибку.

8. Итерационный процесс. Процессы прямого и обратного распространения ошибки повторяются для каждого обучающего при-

мера в обучающем наборе данных. Обновление ВС происходит на каждой итерации, пока не достигнута заданная точность или не пройдено определенное количество эпох.

9. Завершение обучения. Обучение НС завершается, когда достигнуты требуемые кри-

терии остановки, например, заданное количество эпох или достижение определенной точности на обучающем наборе данных.

Ниже приведен программный код на Python для обучения MLP с использованием алгоритма обратного распространения ошибки и градиентного спуска.

```
# Импорт необходимых библиотек
import numpy as np

class MLP:
    def __init__(self, input_size, hidden_size, output_size):
        # Инициализация весовых коэффициентов
        self.W1 = np.random.randn(input_size, hidden_size)
        self.b1 = np.zeros((1, hidden_size))
        self.W2 = np.random.randn(hidden_size, output_size)
        self.b2 = np.zeros((1, output_size))
    def forward(self, X):
        # Прямое распространение сигнала
        self.hidden_output = np.dot(X, self.W1) + self.b1
        self.hidden_activation = self.sigmoid(self.hidden_output)
        self.output = np.dot(self.hidden_activation, self.W2) + self.b2
        return self.output
    def backward(self, X, y, learning_rate):
        # Обратное распространение ошибки
        delta_output = self.output - y
        delta_hidden = np.dot(delta_output, self.W2.T) * self.sigmoid_derivative(self.hidden_output)
        # Обновление весовых коэффициентов
        self.W2 -= learning_rate * np.dot(self.hidden_activation.T, delta_output)
        self.b2 -= learning_rate * np.sum(delta_output, axis=0, keepdims=True)
        self.W1 -= learning_rate * np.dot(X.T, delta_hidden)
        self.b1 -= learning_rate * np.sum(delta_hidden, axis=0)
    def train(self, X, y, epochs, learning_rate):
        # Обучение MLP
        for epoch in range(epochs):
            output = self.forward(X)
            self.backward(X, y, learning_rate)
    def sigmoid(self, x):
        # Сигмоидная функция активации
        return 1 / (1 + np.exp(-x))
    def sigmoid_derivative(self, x):
        # Производная сигмоидной функции активации
```

```
        return self.sigmoid(x) * (1 - self.sigmoid(x))
        # Подготовка обучающих данных
        X = np.array([[0, 0, 0, 0, 0, 0, 0, 0, 0],
            # Входные данные для концепта 1 (K1)
            [0, 1, 1, 0, 1, 0, 0, 0, 1, 0],
            # Входные данные для K2
            [1, 0, 0, 1, 0, 1, 0, 0, 0, 1],
            # Входные данные для K3
            [0, 1, 1, 0, 1, 0, 0, 0, 1, 0],
            # Входные данные для K4
            [0, 1, 0, 1, 0, 1, 0, 1, 0, 1],
            # Входные данные для K5
            [0, 1, 1, 0, 1, 0, 0, 0, 1, 0],
            # Входные данные для K6
            [1, 0, 0, 1, 0, 1, 0, 0, 0, 1],
            # Входные данные для K7
            [0, 1, 1, 0, 1, 0, 0, 0, 1, 0],
            # Входные данные для K8
            [1, 0, 0, 1, 0, 1, 0, 0, 0, 1],
            # Входные данные для K9
            [1, 1, 1, 1, 1, 1, 1, 1, 1, 1]])
        # Входные данные для K10
        y = np.array([[1, 0.7, 0.6, 0, 0.4, 0.3, 0.2, 0.3, 0.6],
            # Желаемые значения ВС для K1
            [0.7, 1, 0, 0.6, 0.4, 0.3, 0.2, 0, 0, 0.5],
            # Желаемые значения ВС для K2
            [0.5, 0, 1, 0, 0, 0, 0, 0, 0, 0.4],
            # Желаемые значения ВС для K3
            [0.6, 0.6, 0, 1, 0.3, 0.5, 0.4, 0.2, 0.3, 0.5]])
        # Желаемые значения ВС для K4
        [0, 0.4, 0, 0.3, 1, 0.2, 0.6, 0, 0, 0.4]])
        # Желаемые значения ВС для K5
        [0.4, 0.3, 0, 0.5, 0.2, 1, 0, 0, 0, 0.3]])
        # Желаемые значения ВС для K6
        [0.3, 0.2, 0, 0.4, 0.6, 0, 1, 0, 0, 0.4]])
        # Желаемые значения ВС для K7
        [0, 0, 0, 0.4, 0, 0, 0, 1, 0, 0]])
        # Желаемые значения ВС для K8
        [0, 0, 0, 0.3, 0, 0, 0, 0, 1, 0]])
        # Желаемые значения ВС для K9
        [0.6, 0.5, 0.4, 0.5, 0.4, 0.3, 0.4, 0, 0, 1]])
        # Желаемые значения ВС для K10
        # Создание и обучение MLP
        mlp = MLP(input_size=10, hidden_size=4, output_size=4)
        mlp.train(X, y, epochs=1000, learning_rate=0.1)
        # Тестирование обученной MLP
        test_input = np.array([[0, 1, 0, 1, 0, 1, 0, 1, 0, 1]])
        # Входные данные для тестирования (концепт 5)
        predicted_output = mlp.forward(test_input)
        print(predicted_output)
        Приведенный код создает класс MLP, ко-
```

торый представляет MLP с одним скрытым слоем. В методе forward выполняется прямое распространение сигнала, а в методе backward производится обратное распространение ошибки и обновление весовых коэффициентов. Метод train используется для обучения MLP на обучающих данных.

Чтобы оценить работоспособность предложенного подхода, важно учитывать то, на сколько быстро и хорошо НС обучается оценивать ВС НКК. Для этого был использован показатель средней абсолютной ошибки (MAE, Mean Absolute Error) [10]. MAE представляет собой разность между спрогнозированным и фактическим значениями. Чем ближе MAE к нулю, тем точнее модель. MAE рассчитывается по формуле:

$$MAE = (1/n) * \sum |y - \hat{y}| \quad (2)$$

где y – действительные значения, $\hat{y}$ – предсказанные значения, n – количество примеров данных.

Во время тестирования НС на предложенных входных данных было произведено несколько итераций, и на 200 итерации MAE максимально приблизилось к нулю. Таким образом, предложенный подход с сочетанием НКК и НС является применимым к решению вопроса совершенствования процесса оценки рисков ИБ.

Заключение

В работе предложен подход, сочетающий в себе технологии НКК и НС для этапов оценки рисков ИБ. Подход представляет собой применение НКК, содержащей в себе концепты по возможным угрозам ИБ в образовательной сфере. Для оценки ВС было предло-

жено применение НС, с целью устранения разрозненности мнений экспертов во время оценки и устранения необходимости работать с большими данными. Что ускоряет процесс проведения оценки, и делает ее адаптивной.

Для обучения НС требуются входные данные, которые формируются на основе работы экспертов. Были приглашены 10 экспертов ВУЗа из области ИБ: преподаватели, специалисты по ЗИ. Опираясь на открытые источники данных: отчеты компаний, занимающихся вопросами ИБ, статистика утечек данных за крайние годы, БДУ ФСТЭК, а также на свой опыт, эксперты сформировали 10 концептов для НКК в сфере образования, а также расставили ВС между ними. Эти данные далее были использованы для обучения НС расставлять ВС. Был сформирован алгоритм обучения НС, выбрана ее архитектура, представлен программный код на Python для решения данной задачи. Критерием применимости этих технологий является качество и скорость обучения НС оценивать ВС. Для оценки этого критерия был использован показатель средней абсолютной ошибки – MAE.

Дальнейшее развитие данного исследования заключается в проведении экспериментов по совершенствованию НС, корректировке ее архитектуры, размерности слоев с целью подбора наиболее оптимальной версии, а также поиск других блоков из предложенной функциональной модели, в которых можно использовать такую комбинацию технологий как НС и НКК.

Литература

1. Фомин Г. П., Сухорукова И. В., Грибов А. Ф. Адаптивная многокритериальная система управления рисками/ Вестник ростовского государственного экономического университета (РИНХ), 2022. № 1 (77). С. 98-103. URL: <https://www.elibrary.ru/item.asp?id=49424923> (дата обращения 30.07.2023 г.)
2. Глушенко С. А. Адаптивная нейро-нечеткая система оценки рисков информационной безопасности организации/ Бизнес-информатика, 2017. № 1 (39). С. 68-77. URL: <https://bijournal.hse.ru/data/2017/08/30/1173956328/%D0%93%D0%BB%D1%83%D1%88%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%A0%D0%A3%D0%A1%D0%9F%D0%95%D0%A0%D0%95%D0%92%D0%9E%D0%94%20-%20v2F.pdf> (дата обращения 30.07.2023 г.)
3. Джамай Е. В., Зинченко А. С. Разработка адаптивной многокомпонентной системы управления риском высокотехнологичных предприятий/ Вестник Московского государственного областного университета. Серия: Экономика, 2022. № 2. URL: <https://cyberleninka.ru/article/n/razrabotka-adaptivnoy-mnogokomponentnoy-sistemy-upravleniya-riskom-vysokotekhnologichnyh-predpriyatiy> (дата обращения 30.07.2023 г.) DOI: 10.18384/2310-6646-2022-2-49-55
4. Заграновская А. В. Системный анализ на основе нечетких когнитивных карт/Вестник Российского экономического университета им. Г. В. Плеханова, 2018. №4. URL: <https://cyberleninka.ru/article/n/sistemnyy-analiz-na-osnove-nechetkih-kognitivnyh-kart/viewer> (дата обращения 25.08.2023 г.)
5. Пивкин Е.Н., Белов В.М., Белкин С.А. К вопросу об анализе защищенности объектов информа-

тизации с использованием нейронных сетей/ Доклады Томского государственного университета систем управления и радиоэлектроники, 2014. № 2 URL: <https://journal.tusur.ru/storage/44773/30.pdf?1465976630> (дата обращения 25.08.2023 г.)

6. Созыкин А. В. Обзор методов обучения глубоких нейронных сетей/ Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика, 2017. № 3. Том 6. URL: <https://cyberleninka.ru/article/n/obzor-metodov-obucheniya-glubokih-neyronnyh-setey> (дата обращения 29.08.2023 г.)

7. Дрокин И. С. Об одном алгоритме последовательной инициализации весов глубоких нейронных сетей и обучении ансамбля нейронных сетей/ Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления, 2016. № 4. URL: <https://cyberleninka.ru/article/n/ob-odnom-algoritme-posledovatel'noy-initsializatsii-vesov-glubokih-neyronnyh-setey-i-obucheni-ansamblya-neyronnyh-setey> (дата обращения 10.09.2023 г.)

8. Макаренко А. В. Глубокие нейронные сети: зарождение, становление, современное состояние/ Проблемы управления, 2020. № 2. URL: <https://cyberleninka.ru/article/n/glubokie-neyronnye-seti-zarozhdenie-stanovlenie-sovremennoe-sostoyanie> (дата обращения 12.09.2023 г.)

9. Гудфеллоу Ян, Бенджио Иосуа, Курвилль Аарон. Глубокое обучение. 2018

10. How to interpret MAE. URL: <https://stephenallwright.com/interpret-mae/?ref=helenkapatsa.ru> (дата обращения 15.09.2023)

References

1. Fomin G. P., Sukhorukova I. V., Gribov A. F. Adaptivnaya mnogokriterial'naya sistema upravleniya riskami/ Vestnik rostovskogo gosudarstvennogo ekonomicheskogo universiteta (RINKH), 2022. № 1 (77). S. 98-103. URL: <https://www.elibrary.ru/item.asp?id=49424923> (data obrashcheniya 30.07.2023 g.)

2. Glushenko S. A. Adaptivnaya neyro-nechetkaya sistema otsenki riskov informatsionnoy bezopasnosti organizatsii/ Biznes-informatika, 2017. № 1 (39). S. 68-77. URL: <https://bijournal.hse.ru/data/2017/08/30/1173956328/%D0%93%D0%BB%D1%83%D1%88%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%A0%D0%A3%D0%A1%D0%9F%D0%95%D0%A0%D0%95%D0%92%D0%9E%D0%94%20-%20v2F.pdf> (data obrashcheniya 30.07.2023 g.)

3. Dzhamay Ye. V., Zinchenko A. S. Razrabotka adaptivnoy mnogokomponentnoy sistemy upravleniya riskom vysokotekhnologichnykh predpriyatiy/ Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Ekonomika, 2022. № 2. URL: <https://cyberleninka.ru/article/n/razrabotka-adaptivnoy-mnogokomponentnoy-sistemy-upravleniya-riskom-vysokotekhnologichnykh-predpriyatiy> (data obrashcheniya 30.07.2023 g.) DOI: 10.18384/2310-6646-2022-2-49-55

4. Zagranovskaya A. V. Sistemnyy analiz na osnove nechetkikh kognitivnykh kart/ Vestnik Rossiyskogo ekonomicheskogo universiteta im. G. V. Plekhanova, 2018. №4. URL: <https://cyberleninka.ru/article/n/sistemnyy-analiz-na-osnove-nechetkikh-kognitivnykh-kart/viewer> (data obrashcheniya 25.08.2023 g.)

5. Pivkin Ye.N., Belov V.M., Belkin S.A. K voprosu ob analize zashchishchennosti ob'yektov informatizatsii s ispol'zovaniyem neyronnykh setey/ Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki, 2014. № 2 URL: <https://journal.tusur.ru/storage/44773/30.pdf?1465976630> (data obrashcheniya 25.08.2023 g.) 6. Sozykin A. V. Obzor metodov obucheniya glubokikh neyronnykh setey/ Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Vychislitel'naya matematika i informatika, 2017. № 3. Tom

6. URL: <https://cyberleninka.ru/article/n/obzor-metodov-obucheniya-glubokih-neyronnyh-setey> (data obrashcheniya 29.08.2023 g.)

7. Drokin I. S. Ob odnom algoritme posledovatel'noy initsializatsii vesov glubokikh neyronnykh setey i obucheni ansamblya neyronnykh setey/ Vestnik Sankt-Peterburgskogo universiteta. Prikladnaya matematika. Informatika. Protsessy upravleniya, 2016. № 4. URL: <https://cyberleninka.ru/article/n/ob-odnom-algoritme-posledovatel'noy-initsializatsii-vesov-glubokih-neyronnyh-setey-i-obucheni-ansamblya-neyronnyh-setey> (data obrashcheniya 10.09.2023 g.)

8. Makarenko A. V. Glubokiye neyronnyye seti: zarozhdeniye, stanovleniye, sovremennoye sostoyaniye/ Problemy upravleniya, 2020. № 2. URL: <https://cyberleninka.ru/article/n/glubokie-neyronnye-seti-zarozhdenie-stanovlenie-sovremennoe-sostoyanie> (data obrashcheniya 12.09.2023 g.)

9. Gudfellow Yan, Bendzhio Ioshua, Kurvill' Aaron. Glubokoye obucheniye. 2018

10. How to interpret MAE. URL: <https://stephenallwright.com/interpret-mae/?ref=helenkapatsa.ru> (data obrashcheniya 15.09.2023)

ПАЛЮТИНА Галия Наилевна, аспирант, младший научный сотрудник Федерального государственного бюджетного образовательного учреждения высшего образования «Ростовский

государственный экономический университет (РИНХ)». 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69. E-mail: hello616@yandex.ru

PALYUTINA Galiya Nailevna, postgraduate student, junior researcher at the Federal State Budgetary Educational Institution of Higher Education "Rostov State Economic University (RINH)". 344002, Rostov-on-Don, st. Bolshaya Sadovaya, 69. E-mail: hello616@yandex.ru

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ПЛАТФОРМЕ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ КАК ЭФФЕКТИВНОЕ СРЕДСТВО УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ¹

Платформы реагирования на инциденты помогают администраторам информационной безопасности управлять инцидентами. Несмотря на преимущества, которые несет автоматизация, многие компании всё ещё продолжают предоставлять IRP как платформу, основной функционал которой направлен на ведение документации и не работает без Threat Intelligence.

В данной статье рассмотрена типовая структура платформ реагирования на инциденты. Описаны плюсы и варианты использования машинного обучения, тонкости его применения в IRP. Предлагается вариант автоматизации реагирования посредством использования нейронных сетей. Приведены архитектура нейронной сети для определения алгоритма действий специалиста информационной безопасности L2, описаны эксперименты с архитектурами нейросетей и набором входных параметров на ограниченном датасете. Описана обучающая выборка, особенности её сбора, приведены основные категории входных параметров. Рассматриваются требования к датасетам. Приводятся рекомендации по автоматизации реагирования на инциденты.

Ключевые слова: информационная безопасность, платформа реагирования на инциденты, нейронная сеть, машинное обучение, датасет, предобработка данных.

¹ Работа выполнена в рамках гранта ИБ МТУСИ № 04/22-д «Методология построения систем анализа инцидентов информационной безопасности для распределенных информационных систем».

USING NEURAL NETWORKS IN AN INCIDENT RESPONSE PLATFORM AS AN EFFECTIVE MEANS OF CYBERSECURITY MANAGEMENT

Incident response platforms help information security administrators manage incidents. Despite the benefits that automation brings, many companies still continue to provide IRP as a platform whose main functionality is aimed at maintaining documentation, or does not work without Threat Intelligence.

This article discusses the typical structure of incident response platforms. The advantages and use cases of machine learning and the subtleties of its application in IRP are described. An option is proposed to automate the response through the use of a neural network. The architecture of the neural network for determining the algorithm of actions of the L2 information security specialist is presented, experiments with the architecture of the neural network and a set of input parameters are described. Requirements for datasets are considered. The training sample, the features of its collection are described, and the main categories of input parameters are given. Recommendations for automating incident response are provided.

Keywords: *information security, incident response platform, neural network, machine learning, dataset, data preprocessing.*

Введение

Платформы реагирования на инциденты (Incident Response Platform, IRP) — это класс платформ, позволяющих обеспечить управление реагированием на компьютерные инциденты. IRP занимает значимое место в системе обеспечения информационной безопасности. Она позволяет упростить работу аналитиков L1 и L2. [1,2]

За обнаружение инцидента отвечает система управления информационной безопасностью и событиями безопасности (SIEM), а IRP отвечает на реагирование на инцидент: специалисту информационной безопасности (ИБ) из SIEM приходят уведомления об инциденте. IRP помогает в выборе алгоритма действия для устранения, определение приоритетов событий и составления документации по событиям. Ввиду увеличения числа атак на информационные инфраструктуры [1, 2], растет и число инцидентов. Часто, время на реагирование должно занимать от 15 минут до часу для критичных инцидентов [2, 5] и от 2

часов до 8 для большинства остальных [2, 5]. Таким образом даже незначительные улучшения в сторону автоматизации очень важны. Если своевременно не закрыть инцидент, может быть нанесен ущерб всей инфраструктуре предприятия [5,7]. Искусственный интеллект (ИИ) также снижает утомляемость и человеческие ошибки. Мониторинг сетей и анализ огромных объемов данных для обнаружения угроз — утомительная работа, которая может привести к ошибкам и пропущенным инцидентам.

Несмотря на преимущества, которые несет автоматизация, многие компании всё ещё продолжают предоставлять IRP как платформу (продукт) для выполнения собственных скриптов по реагированию на инциденты, а основной функционал направлен на ведение, и категорирование политик, плейбуков и прочей документации (Innostage IRP) [5], либо они не работают без ТИ (TheHive) [6,7].

Основные преимущества использования платформ реагирования на инциденты:

- увеличение точности обнаружения и мониторинга инцидентов;
- возможность автоматической координации действий;
- оптимизация времени реагирования и сокращение потенциальных ущербов;
- централизованное управление процессом реагирования;
- автоматизация задач и максимизация эффективности команды по реагированию.

В реагировании на инциденты и работе IRP выделяют следующие этапы:

1. Подготовка, создание плейбуков/сценариев реагирования.
2. Проверка, является ли событие, пришедшее из SIEM инцидентом.
3. Определение приоритета инцидента.
4. Сдерживание, локализация инцидента.
5. Устранение инцидента.
6. Восстановление системы/инфраструктуры.
7. Составление отчетов и рекомендаций, по результатам расследования.

1. На данном этапе определяются риски ИТ-инфраструктуры, создаются политики безопасности для пользователей, прописываются сценарии действия специалистов ИБ в случае реализации той или иной угрозы.

2. Из событий, собираемых SIEM, выбираются нежелательные и передаются IRP, однако, иногда случаются ложноположительные срабатывания, потому необходимо убедиться, что событие является инцидентом.

3. Определяется уровень значимости/приоритет инцидентов. Важный этап, из-за ошибки на котором дальнейшая работа может быть выполнена над идентифицированной угрозой неверно, что повлечет несвоевременное закрытие события.

4. Сдерживание, локализация инцидента – этап, на котором аналитик ИБ определяет, что именно произошло и какие действия необходимо выполнить. На этом этапе выполня-

ются шаги по предотвращению дальнейшего разрастания проблемы.

5. Непосредственно устранение инцидента в соответствии со сценариями реагирования.

6. Восстановление инфраструктуры, пострадавшей от реализации угрозы.

7. Анализ действий аналитиков ИБ/группы реагирования на инциденты, составление новых плейбуков, политик безопасности и т.п.

Некоторые выделяют детектирование инцидентов как задачу IRP, хотя на практике за это отвечает SIEM, а платформа реагирования лишь проверяет корректно ли были выбраны нежелательные события или нет. [4, 7].

Хотя машинное обучение можно применять на разных этапах обнаружения и закрытия инцидентов [3, 6, 10], в данной статье рассматривается применение нейронных сетей на наиболее значимых для IRP 4 и 5 этапах – непосредственно на реагировании.

Предпосылками для использования ИИ является увеличившееся количество инцидентов, уменьшение времени реагирования на них, неочевидная, неалгоритмическая задача определения алгоритма действий в той или иной ситуации, а также огромные объемы данных о событиях, с которыми хорошо справляются нейронные сети. Однако информацию об инцидентах трудно найти в открытом доступе, т.к. её бы могли использовать злоумышленники.

По этой причине для обучения нейронной сети и тестирования был собран тестовый датасет из 23 образцов, основанный на правилах корреляции SIEM из открытых источников [9]. На рис. 1 приведен фрагмент собранного набора данных.

Так выглядят и данные, подгружаемые из SIEM в IRP. На основании их, а также плейбуков/сценариев реагирования, специалист выбирает алгоритмы действий, необходимых для закрытия инцидента.

Incident Key	Date	Severity	Incident Name	Src IP	Src Port	Src Name	Dst IP	Dst Port	Dst Name	User ID	User Name	File Path	File Name	Command Line	Object Name	Реакция
1	17.10.2023, 10:13	Low	Попытка перебора паролей с одного источника	24.246.33.144	5256	None	10.10.125.135	22	HOST01	None	Alice Bob Ewa root user admin administrator	None	None	None	None	Закрытие порта
2	17.10.2023, 10:15	High	Успешная попытка перебора паролей на хосте	24.246.33.144	5256	None	10.10.125.135	22	HOST01	None	administrator	None	None	None	None	Блокировка УЗ
3	17.10.2023, 10:15	High	Создание привилегированного аккаунта пользоват...	None	None	None	10.10.125.7	None	HOST-DB	1000	root	None	None	None	adm_db	Отправка письма пользователю
4	17.10.2023, 10:23	Medium	Создание локального аккаунта учетной записи н...	None	None	None	10.10.125.64	None	ZABBIX	0	ivanov_zp	None	None	None	administrator	Блокировка УЗ
5	17.10.2023, 10:37	High	Обнаружение модификации файлов при загрузке си...	None	None	None	10.10.18.3	None	HOST34	0	root	/boot/	link	None	link	Запуск АВ

Рис. 1. Фрагмент датасета

На основании этих данных можно обучить и нейронную сеть. После обнаружения инцидента ИИ может помочь определить серьезность, масштаб, первопричину и необходимые действия гораздо быстрее, чем люди. ИИ может идентифицировать инцидент за считанные минуты, а не за часы или дни, которые могут потребоваться специалистам, чтобы обнаружить его. Благодаря ИИ, дополняющему работу аналитиков, время реагирования может быть значительно сокращено. Для каждого инцидента существует время реакции на него (время закрытия инцидента). Аналитики относительно хуже работают ночью и могут не пропускать множественные инциденты [1]. IRP может решить проблему недостаточной квалификации и способствует повышению качества реагирования и экономии денег. [1]

Набор данных был расширен до 96 элементов, путем зашумления и создания данных по образцу. В качестве входных данных выбраны дата, время, уровень приоритета, имя (краткое описание) инцидента, IP и порт источника и пункта назначения, имя пользователя и т.д. В качестве выходных данных указаны реакции: действия специалиста ИБ, которые были разделены на 3 группы: блокировка учетной записи, запуск антивирусного программного обеспечения (ПО) и в остальных случаях – отправка письма пользователю – администратору ИБ. Столь ограниченное количество реакций обусловлено небольшим набором данных, при масштабировании количество реакций может быть увеличено.

При внедрении такая система является рекомендательной: автоматически можно запустить антивирусное ПО, окончательное решение о блокировке пользователей принимает аналитик ИБ. Письмо администратору отправляется в неочевидных случаях.

Далее данные были преобразованы:

1. IP источника и назначения были разделены на частный и общий, таким образом мы сократили мерность данных критериев, увеличив их значимость.

2. User ID разделен по критерию: «является ли администратором или нет», при этом для датасета из тысяч данных было бы потеряно множество важных признаков, но на небольшом наборе это позволило сократить мерность до двух, сильно увеличив значимость.

3. Аналогично был разбит столбец «Command Line» на несколько наиболее значимых групп.

4. Уровень приоритета, порт источника были преобразованы методом `get_dummies` (`one-hot-encoding`).

5. Краткое описание инцидента было представлено в виде мешка слов (BOW), так как данных немного, разреженность такой кодировки будет незначительной, однако при масштабировании рекомендуется переходить на более гибкие методы обработки естественного языка, например, такие, как архитектура «Трансформер».

Таким образом из 15 входных параметров были получены 65.

Так как решалась задача классификации, тестовый датасет невелик, а в реагировании на инциденты важна скорость, тестировались полносвязные сети прямого распространения с добавлением слоев Dropout для уменьшения вероятности «заучивания» результатов.

Лучшие результаты показала нейронная сеть со следующей архитектурой, код построения такой НС приведен на рис. 2:

- 65 нейронов на входном слое;
- 24 нейрона на первом промежуточном слое;
- 6 нейронов на втором промежуточном слое;
- 3 выходных нейрона.

```
model01 = Sequential()
model01.add(Dense(j, input_dim=65, activation="sigmoid"))
model01.add(Dropout(0.25))
model01.add(BatchNormalization())

model01.add(Dense(6, activation="sigmoid"))
model01.add(Dropout(0.25))
model01.add(BatchNormalization())
model01.add(Dense(3, activation='sigmoid'))
```

Рис. 2. Код построения нейронной сети

При обучении использовался метод К-кратной перекрёстной проверки для «увеличения» обучающих данных. График точности обучения такой сети представлен на рис. 3.

Время обучения на 10 эпохах составляет около 2 секунд. Такое количество эпох не является необходимым, и в отдельных случаях результаты на большем или меньшем количестве были выше.

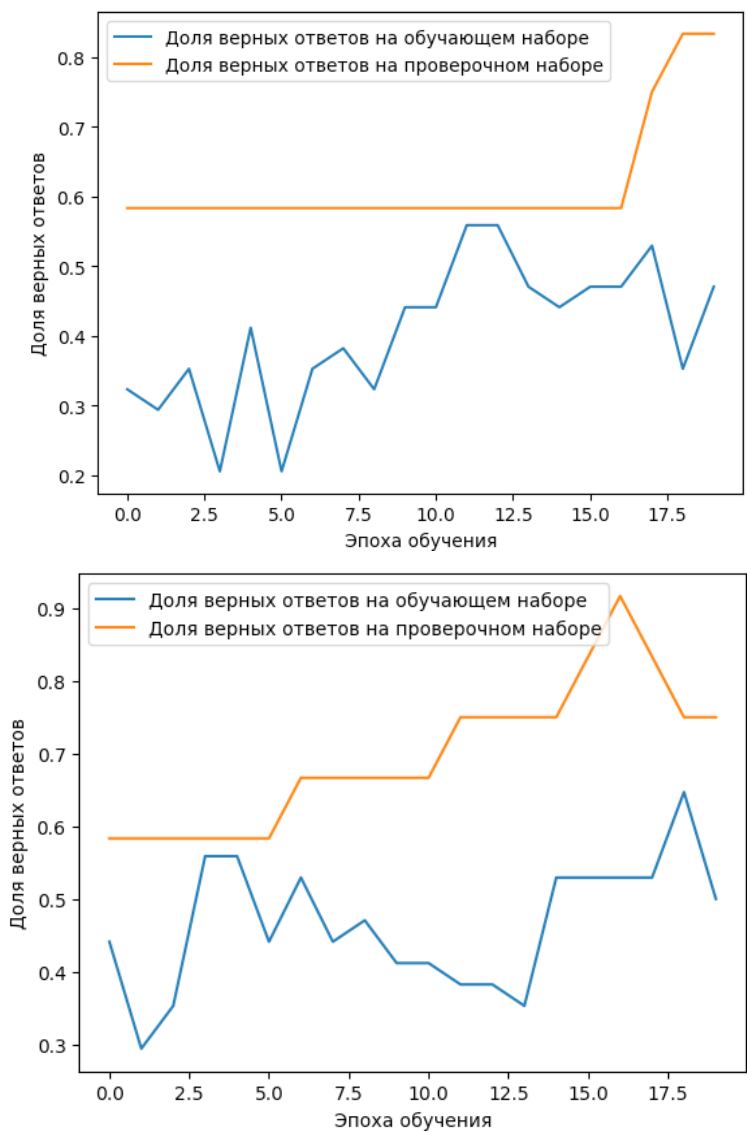


Рис. 3. График точности обучения НС в зависимости от эпохи

Так как параметры НС инициализируются случайным образом, каждая из них была запущена 50 раз для определения статистической точности. Наиболее значимые параметры обучения НС для IRP указаны в табл. 1.

Таким образом, на небольшом объеме данных приоритетное значение имеют правильно выбранные параметры обучения, а не архитектура сети, а избыточно выбранные параметры, наоборот, ухудшают точность (в некоторых случаях это можно отнести за счёт погрешности). При увеличении числа запи-

сей точность нейросетей, работающих на основе текста, немного повышается, тогда как эффективность прочих параметров растет значительно.

На итоговом датасете из 96 элементов тестировались сети с 65 параметрами на входе НС. Так как решалась задача множественной классификации, то 90 и даже 80% верных срабатываний являются значимыми и позволяют упростить работу аналитика ИБ L1/L2. Очевидно, что ввиду ограниченного набора данных результаты работы НС невысоки, таким

Статистика по результатам работы нейронных сетей

Архитектура нейронной сети, №	Количество записей	Количество параметров обучения	Средняя точность, %
1	23	34	36
2	23	34	39,3
1	23	44	44
2	23	44	44,7
2	23	65	44,1
1	46	34	42
2	46	34	42,4
1	46	44	50,1
2	46	44	50,8
2	46	65	69,6
1	96	65	76,3
2	96	65	82,1
3	96	65	89,8

образом, основное решение проблемы заключается в расширении датасета, что в компаниях со средствами мониторинга решается автоматически: можно собирать датасет действий, выполняемых специалистом ИБ.

Заключение

В результате проведенного исследования были выделены особенности и функции платформ реагирования на инциденты, указаны рекомендации по сбору датасетов и автома-

тизации IRP. Были построены нейросети, позволяющие определить действия в зависимости от характеристик инцидента. Даже несмотря на небольшие наборы данных, тестируемые нейросетевые архитектуры показали высокую среднюю точность около 90%. Кроме того, были указаны возможности и перспективы масштабирования подобных систем.

Литература

1. Containing the Uncontainable: Using AI for Incident Response, URL доступа: <https://www.linkedin.com/pulse/containing-uncontainable-using-ai-incident-response-bise-> (дата обращения: 15.10.2023)
2. Sarker I. H. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science*, №10(3), 2022. pages 1–26.
3. Очерedyкo A. P. Исследование irp-систем на основе анализа механизмов реагирования на инциденты информационной безопасности / А. Р. Очерedyкo, Д. А. Бачманов, М. М. Путятo, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 1(53). – С. 74-82. – DOI 10.21672/2074-1707.2021.53.1.074-082. – EDN LVMANX.
4. Махнев А. О. Исследование платформ реагирования на инциденты информационной безопасности / А. О. Махнев, Н. П. Деканова // Молодая наука Сибири. – 2023. – № 1(19). – С. 147-157. – EDN UDRWEZ.
5. Computer Security Incident Handling Guide NIST, URL доступа: <https://csrc.nist.gov/pubs/sp/800/61/r2/final> (дата обращения: 15.10.2023)
6. Частикова В. А. Нейросетевая технология обнаружения аномального сетевого трафика / В. А. Частикова, С. А. Жерлицын, Я. И. Воля, В. В. Сотников // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 1(49). – С. 20-32. – DOI 10.21672/2074-1707.2020.49.4.020-032. – EDN WUCDII.
7. Обзор Innostage IRP, автоматизированной системы управления ИБ, URL доступа: <https://www.anti-malware.ru/reviews/Innostage-IRP#part22> (дата обращения: 15.10.2023).
8. The Hive и Security Vision, URL доступа: <https://habr.com/ru/articles/571604/> (дата обращения: 15.10.2023).
9. Detection–Rule–Dump набор правил обнаружения, URL доступа <https://github.com/archanchoudhury/Detection-Rule-Dump> (дата обращения: 15.10.2023).
10. Chastikova V.A. Method of analyzing computer traffic based on recurrent neural networks / V.A.

References

1. Containing the Uncontainable: Using AI for Incident Response, URL dostupa: <https://www.linkedin.com/pulse/containing-uncontainable-using-ai-incident-response-bise-> (data obrashcheniya: 15.10.2023).
2. Sarker I. H. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science*, №10(3), 2022. pages 1–26.
3. Ochered'ko A.R. Issledovaniye irp-sistem na osnove analiza mekhanizmov reagirovaniya na intsidenty informatsionnoy bezopasnosti / A. R. Ochered'ko, D. A. Bachmanov, M. M. Putyato, A. S. Makaryan // *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii*. – 2021. – № 1(53). – S. 74-82. – DOI 10.21672/2074-1707.2021.53.1.074-082. – EDN LVMANX.
4. Makhnev A. O. Issledovaniye platform reagirovaniya na intsidenty informatsionnoy bezopasnosti / A. O. Makhnev, N. P. Dekanova // *Molodaya nauka Sibiri*. – 2023. – № 1(19). – S. 147-157. – EDN UDRWEZ.
5. Computer Security Incident Handling Guide NIST, URL dostupa: <https://csrc.nist.gov/pubs/sp/800/61/r2/final> (data obrashcheniya: 15.10.2023).
6. Chastikova V. A. Neyrosetevaya tekhnologiya obnaruzheniya anomal'nogo setevogo trafika / V. A. Chastikova, S. A. Zherlitsyn, YA. I. Volya, V. V. Sotnikov // *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii*. – 2020. – № 1(49). – S. 20-32. – DOI 10.21672/2074-1707.2020.49.4.020-032. – EDN WUCDII.
7. Obzor Innostage IRP, avtomatizirovannoy sistemy upravleniya IB, URL dostupa: <https://www.anti-malware.ru/reviews/Innostage-IRP#part22> (data obrashcheniya: 15.10.2023).
8. The Hive i Security Vision, URL dostupa: <https://habr.com/ru/articles/571604/> (data obrashcheniya: 15.10.2023).
9. Detection–Rule–Dump nabor pravil obnaruzheniya, URL dostupa <https://github.com/archanchoudhury/Detection-Rule-Dump> (data obrashcheniya: 15.10.2023).
10. Chastikova V.A. Method of analyzing computer traffic based on recurrent neural networks / V.A. Chastikova, V.V. Sotnikov // *Journal of Physics: Conference Series. International Conference "High-Tech and Innovations in Research and Manufacturing," 2019. S. 012133.*

ЧАСТИКОВА Вера Аркадьевна, кандидат технических наук, доцент, доцент кафедры «Кибербезопасность и защита информации» федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: chastikova_va@mail.ru

КОЗАЧЁК Константин Валериевич, аспирант кафедры «Кибербезопасность и защита информации» федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: Koza4ek.Konstantin@yandex.ru

CHASTIKOVA Vera Arkadyevna, candidate of Technical Sciences, associate professor, associate professor of the department «Cybersecurity and information protection» of the federal state budget educational institution of higher education «Kuban State Technological University». 350072, Krasnodar, Moskovskaya st., 2. E-mail: chastikova_va@mail.ru

KOZACHOK Konstantin Valerievich, post-graduate student of the department «Cybersecurity and information protection» of the federal state budget educational institution of higher education «Kuban State Technological University». 350072, Krasnodar, Moskovskaya st., 2. E-mail: Koza4ek.Konstantin@yandex.ru

АНАЛИЗ ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, С ИСПОЛЬЗОВАНИЕМ РАДИОМОДУЛЕЙ

Одним из направлений внедрения технологии RFID являются центральные процессоры средств вычислительной техники. Анализ спецификаций радиомодулей, устанавливаемых на подложке центральных процессоров компании Intel®, показал, что они имеют контакты для подключения двух антенн, линии шины SMBus, а также контакты питания и заземления. Память радиомодулей разделяется на два сегмента. Первый блок PIROM, содержит информацию о центральном процессоре (ядра, частота, объём кеш и т.д.). Данный блок памяти невозможно перезаписать. Второй блок EEPROM, является перезаписываемым сегментом памяти неизвестного объёма и неизвестного назначения. Высказано предположение, что данный блок может использоваться для промежуточного хранения перехваченной с СВТ конфиденциальной информации, или размещения специального программного обеспечения, реализующего функции несанкционированного доступа или несанкционированного воздействия на ЦП или СВТ. Рассмотрены два сценария атаки на СВТ при помощи радиомодуля. Первый основан на использовании для атаки шины SMBus и предполагает физический доступ злоумышленника к СВТ. Второй способ основан на удаленном управлении центральным процессором и устройствами СВТ с помощью радиомодуля по радиоканалу с использованием технологии Anti-Theft.

Ключевые слова: средство вычислительной техники, центральный процессор, радиомодуль, RFID технологии, угрозы безопасности информации, несанкционированный доступ.

ANALYSIS OF THE POSSIBILITY OF IMPLEMENTING THREATS TO THE SECURITY OF INFORMATION PROCESSED BY COMPUTER TECHNOLOGY USING RADIO MODULES

One of the directions of implementation of RFID technology is the central processors of computer equipment. An analysis of the specifications of the radio modules installed on the substrate[®] central processors showed that they have contacts for connecting two antennas, SMBus bus lines, as well as power and ground contacts. The memory of radio modules is divided into two segments. The first PIROM block contains information about the central processor (cores, frequency, cache size, etc.). This memory block cannot be overwritten. The second EEPROM block is a rewritable memory segment of unknown size and unknown purpose. It is suggested that this block can be used for intermediate storage of confidential information intercepted from the electronic computer, or for the placement of special software that implements the functions of unauthorized access or unauthorized impact on the CPU or electronic computer. Two scenarios of an attack on electronic computer using a radio module are considered. The first one is based on the use of the SMBus bus for an attack and assumes the attacker's physical access to the electronic computer. The second method is based on remote control of the central processor and electronic computer devices using a radio module over a radio channel using Anti-Theft technology.

Keywords: computer hardware, central processing unit, radio module, RFID technology, information security threats, unauthorized access.

1. Принципы работы технологии RFID

Для идентификации объектов используется несколько технологий, к одной из которых относится радиочастотная идентификация (Radio Frequency Identification, далее – RFID) [1].

Известно, что любая RFID система состоит из радиомодуля и считывателя. Радиомодуль иногда называют радиометкой или радиотранспондером.

Считыватель, представляющий собой приемо-передающее устройство, генерирует радиосигнал, который наводится в антенне радиомодуля. Наведенный сигнал «выпрямляется» и используется для питания радиомодуля, что позволяет организовать обмен дан-

ными между считывателем и радиомодулем (рис. 1 [2]).

В зависимости от назначения RFID системы, используемые в ней радиомодули можно классифицировать по следующим параметрам: диапазону рабочих частот, типу источника питания и используемой памяти.

По используемому диапазону частот радиомодули подразделяются на низкочастотные, высокочастотные, ультравысокочастотные и микроволновые радиомодули [3], [4].

Низкочастотные радиомодули (LF) работают в диапазонах частот 125 – 134,2 кГц и 140 – 148,5 кГц. Они характеризуются низкой скоростью передачи данных и малой дальностью действия (до 0,15 м) [4].

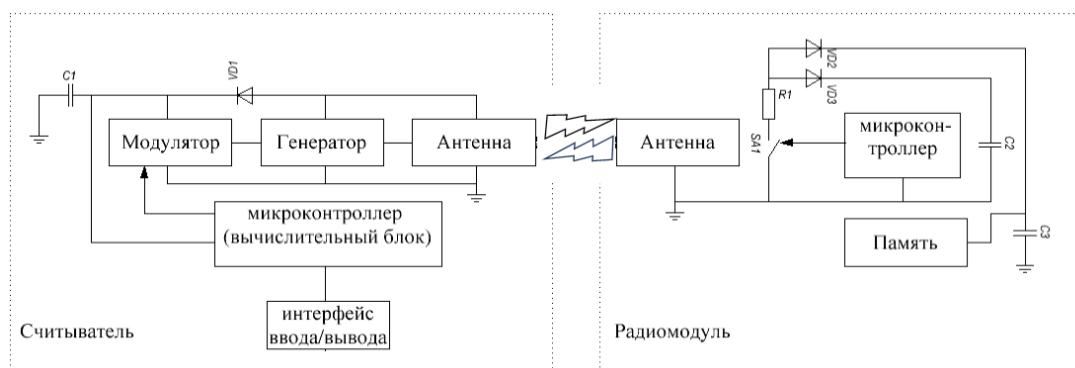


Рис. 1. Принцип работы технологии RFID

Высокочастотные радиомодули (HF) работают на частоте 13,56 МГц. Они характеризуются более высокими скоростями передачи данных и работают на дальностях от 0,8 до 1,5 м [4].

В низкочастотных и высокочастотных модулях в качестве антенн наиболее часто используются катушки индуктивности.

Ультравысокочастотные радиомодули (UHF) работают в диапазоне частот 433, 860 – 960 МГц [5]. Эти системы имеют одну из самых высоких скоростей передачи данных и дальность действия. В качестве антенн в радиомодулях используются диполи [3], [4].

Микроволновые радиомодули (SHF) работают в диапазоне частот 2,45 – 5,8 ГГц. Эти системы строятся в основном на компонентах, имеющих нелинейные характеристики (диоды, варикапы).

В России ограничения на использование низкочастотных и высокочастотных радиомодулей не вводятся. Разрешено использование ультравысокочастотных радиомодулей, работающих в полосах радиочастот 433 МГц, 864 – 865 МГц, 866 – 868 МГц, 868,7 – 869,2 МГц с максимальной эффективной мощностью излучения 25 мВт [5], [7].

Частотный диапазон 2,45 – 5,8 ГГц для RFID на территории РФ не выделен [6].

Ультравысокочастотные радиомодули имеют обширный перечень поддерживаемых и разрабатываемых протоколов и стандартов, как, например, разработанный организацией EPCglobal (Electronic Product Code™) и адаптированный для РФ ГОСТ Р 58701-2019 (ИСО/МЭК 18000-63:2015) «Информационные технологии. Идентификация радиочастотная для управления предметами. Параметры радиоинтерфейса для связи в диапазоне частот от 860 МГц до 960 МГц Тип С» [3], [8], [9].

По типу питания радиомодули подразде-

ляют на: пассивные, полупассивные и активные [10].

В пассивных радиомодулях нет встроенного источника питания. Они работают за счёт электрического тока, индуцированного в антенне электромагнитным излучением считывателя. Они имеют малые размеры и практически неограниченный срок службы. К недостаткам пассивных радиомодулей можно отнести малую дальность действия и низкое качество передаваемого сигнала [10].

Полупассивные радиомодули имеют мало-мощный источник питания, например, конденсатор, заряжаемый электрическим током, индуцированным в антенне электромагнитным излучением считывателя. Дальность их действия несколько больше, чем пассивных радиомодулей [10].

Активные радиомодули имеют встроенный источник питания и микроконтроллер, позволяющий обеспечить самую стабильную передачу информации на значительных расстояниях. Сроком работы таких модулей ограничен сроком работы встроенной аккумуляторной батареи [10].

Применяемые подходы к использованию памяти радиомодулей [10]:

RO (Read Only) – однократная запись (чаще всего аппаратная), произведённая на заводе-изготовителе. Такие радиомодули используются исключительно для идентификации (отправки идентификатора). Новую информацию в них записать невозможно.

WORM (Write Once Read Many) – модуль кроме идентификатора содержит блок памяти, подверженного однократной записи, и многократному считыванию.

RW (Read and Write) – блок памяти для многократного чтения/записи информации.

В настоящее время технологии RFID стали использоваться не только для идентифика-

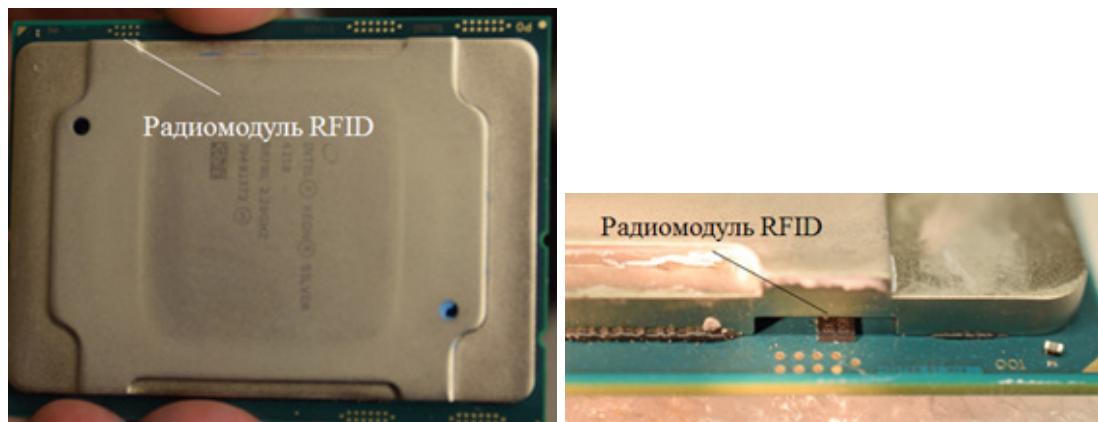
ции объектов, но и управления и контроля доступом, осуществления бесконтактных платежей путём эмулирования физических карт пользователей, оплаты проезда в общественном транспорте и т.д. [1], [11].

2. Анализ радиомодулей, работающих на базе технологии RFID, интегрированных на подложку центральных процессоров средств вычислительной техники

Одним из направлений внедрения технологии RFID являются центральные процессоры (далее – ЦП) средств вычислительной техники (далее – СБТ) [12].

Например, на подложке ЦП компании Intel® устанавливаются радиомодули, находящиеся на шине System Management Bus (далее – SMBus) [13]. Ниже представлены снимки серверного процессора Intel® xeon® silver 4210, на которых виден радиомодуль (рис. 2). Радиомодуль размещается под теплораспределительную крышку ЦП в труднодоступном для визуального обнаружения месте. На снимке ЦП Intel® Core® i9-7940X радиомодуль расположен в правом верхнем углу процессора (рис. 3).

SMBus – это последовательный протокол



а) б)
Рис. 2. Процессор Intel® xeon® silver 4210: а) вид сверху; б) вид сбоку



Рис. 3. Процессор Intel® Core® i9-7940X и интегрированный радиомодуль

обмена данными, предложенный компанией Intel®. Он является подмножеством протокола I2C, но в нем использует более низкий уровень напряжения (3.3В). Протокол используется для обмена данными с устройствами питания и внутренними устройствами СБТ. Шина, использующая данный протокол, имеет одноимённое название и является составной частью системной (главной) шины СБТ. Радиомодули, размещаемые в ЦП компании Intel®, имеют контакты для подключения к шине SMBus [13], [14]. Схематично схема связи

RFID с устройства СБТ через системную шину приведена рис. 4.

По данным компании Intel®, представленным авторам:

- радиомодули устанавливаются на всех процессорах серверов и рабочих станций (включая серию X) и используются для логистических нужд; [15]

- по умолчанию радиомодуль отключен и не может быть включен без специального программного обеспечения;

- радиомодуль не влияет и не воздей-

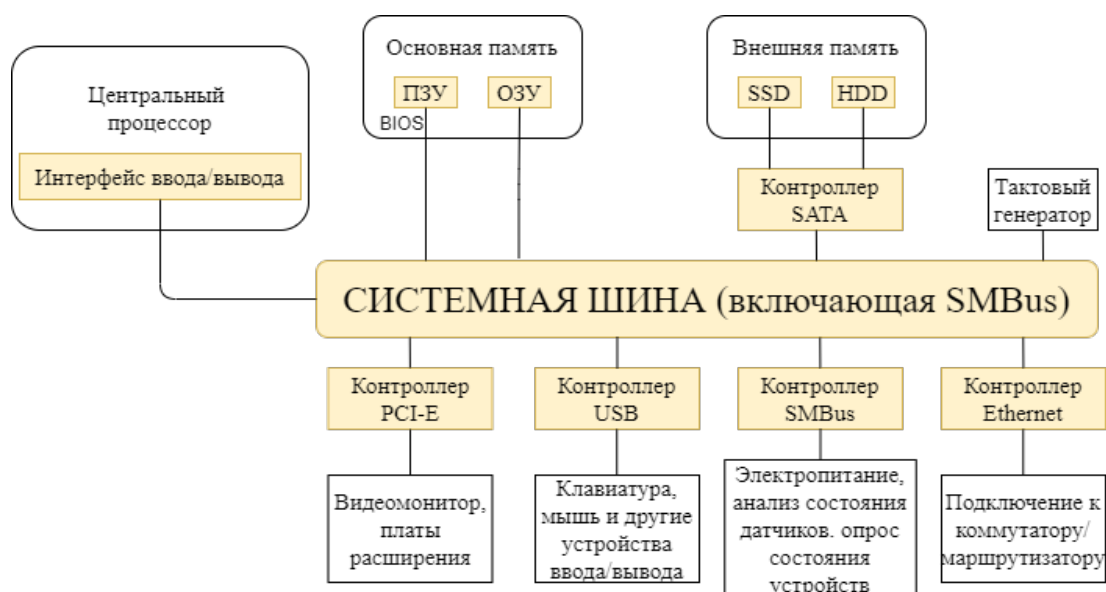


Рис. 4. Схема связи RFID с устройствами CBT через системную шину, включающую SMBus

ствует процессор и не оказывает никакого влияния на его производительность или работу;

- процессор разработан и предназначен для использования с радиомодулем. Наличие радиомодуля проверяет при загрузке, а затем он отключается. Не рекомендуется удалять радиомодуль, без него процессор работать не будет.

Если радиомодуль не влияет на работу процессора, то почему компания Intel® не может гарантировать возможность функционирования CBT без радиомодуля?

В доступной литературе отсутствует описание радиомодулей, установленных на центральных процессорах.

Путём анализа снимков процессоров компании было обнаружено, что радиомодуль интегрируется с 1998 года преимущественно в серверные решения Intel®, однако намечается тенденция на интеграцию радиомодулей в ЦП, используемые в персональных компьютерах.

Для выяснения целей внедрения и характеристик радиомодулей в ЦП CBT проведён анализ трёх спецификаций серверных процессоров Intel® Xeon® Processor, в которых имеется упоминание о радиомодулях RFID [15].

Первая спецификация от апреля 2011 года посвящена процессорам Intel® Xeon® Processor E7-8800/4800/2800 на микроархитектуре Westmere [16]. Вторая спецификация от февраля 2014 года посвящена процессорам Intel® Xeon® Processor E7-8800/4800/2800

v2 на микроархитектуре Ivy Bridge [17]. Третья спецификация от апреля 2019 года посвящена масштабируемым процессорам Intel® Xeon® второго поколения [18].

Из первой спецификации удалось найти данные об используемом радиомодуле. В соответствии с приведённым в 5-м разделе спецификации было установлено, что данная микросхема, используемая в серверных процессорах, имеет название PIROM (Processor Information ROM). Далее указано: PIROM – запоминающее устройство, расположенное на процессоре и доступное через шину управления системой SMBus, которое содержит информацию о функциях процессора. Это устройство используется совместно с Scratch EEPROM, программируется во время производства и защищено от записи.

PIROM предназначено для предоставления информации о процессоре. При воздействии на радиомодуль по шине SMBus или по каналу RFID партнёрам компании Intel® предоставляется исчерпывающая информация о ЦП CBT. Перечень выводимых данных представлен в таблице 5.1 спецификации на ЦП [16]. Из спецификации следует, что данные в PIROM защищены от перезаписи с целью исключения их преднамеренных или случайных изменений. Способы обеспечения защиты данных не указаны.

EEPROM – перезаписываемая программируемая память. Ее описание и цели использования в спецификации не отражены. PIROM использует лишь малую часть всей памяти радиомодуля, поэтому можно предположить,

что компания Intel® оставшуюся память помещает как EEPROM и использует для своих собственных нужд, поэтому и предусмотрена защита от записи.

Так как EEPROM и PIROM являются составляющими блоками общей памяти радиомодуля, то можно утверждать, что через шину SMBus/I2C имеется прямой доступ к системной шине [16].

Далее были определены контакты, подходящие к EEPROM, и их назначение. Сигналы SMBDAT (SDA), SMBCLK(SCL) и SM_WP(WP) относятся к шине SMBus. VCC33 напряжение 3.3. В используется для питания микросхемы и SMBus. SKTID [2:0] (A [2:0]) необходимы для получения данных из PIROM о ЦП. Предположительно, контакты для подключения антенн. GND – заземляющий вывод [16].

Шина SMBus в связке с блоком PIROM радиомодуля используется ЦП для получения сервисной информации (число ядер, тип сокета, диапазона рабочих частот, напряжения питания, для обозначения наборов, поддерживаемых процессором инструкций и т.д.) [16]. В спецификации описано на каких адресах находится эта информация [16].

Анализ двух других спецификаций показал, что информация, касающаяся радиомодуля, идентична. Незначительные отличия встречаются при описании адресов PIROM. Главное отличие спецификаций 2019 и 2014 годов от спецификации 2011 года в том, что информация, описывающая структуру и назначение радиомодуля, была значительно сокращена. Так, например, пропала функциональная схема подключения радиомодуля к ЦП, а также удалено описание зарезервированных адресов в PIROM [16] – [18]. Данное действие компании можно расценивать, как стремление скрыть назначение и принцип функционирования радиомодуля.

Вероятно, необнародованные данные о радиомодуле могут описывать алгоритм взаимодействия, позволяющий передавать любые данные, хранимые и обрабатываемые процессором, заинтересованным в этих данных лицам, а также управлять поведением радиомодуля вплоть до сокрытия факта наличия радиомодуля на системной шине SMBus от любого пользователя СБТ.

Таким образом, в ходе анализа спецификаций ЦП компании Intel® возник следующий вопрос: зачем для логистических нужд создавать данный модуль в виде отдельной микросхемы и помещать его на системную шину SMBus?

Использование данных радиомодулей для ведения складской логистики кажется неубедительным. Известны UHF метки, которые могут быть выполнены в виде миниатюрной наклейки и установлены на упаковку [19]. Это значительно выгоднее, чем интегрировать отдельно создаваемый модуль на подложку ЦП.

Не ясна также цель создания и применения в радиомодуле отдельного блока с перезаписываемой памятью. Информацию по данному вопросу не удалось найти ни в указанных выше спецификациях, ни в открытых источниках.

Компания Intel® не описывает, как осуществляется механизм считывания данных с радиомодуля, и какова цель его размещения на шину SMBus. Можно предположить, что использование радиомодуля в виде отдельной микросхемы необходимо для создания дополнительных возможностей управления ЦП, в том числе и реализации угроз безопасности информации, обрабатываемой СБТ.

3. Анализ способов несанкционированного доступа к информации, обрабатываемой на СБТ, с использования интегрированных в центральный процессор радиомодулей

Радиомодуль, интегрируемый в ЦП компании Intel®, производит взаимодействие с элементами СБТ путём обмена данных по шине SMBus. Так как SMBus является подмножеством шины I2C, то сказанное ниже к шине I2C будет иметь равное отношение к шине SMBus.

Ввиду наличия уникального алгоритма общения с радиомодулем, поддержка работы со стандартными устройствами шины I2C (мастер-устройствами) не возможна. Стоит учитывать, что мастер устройство шины I2C представляет из себя микросхему, являющуюся частью чипсета (набор микросхем, объединённых одним кристаллом). Ввиду того, что чипсет и ЦП производит и разрабатывает Intel®, то можно утверждать, что в программу управления контроллера шины I2C заведомо интегрирован алгоритм взаимодействия с радиомодулями.

Проведенный анализ показал, что возможны следующие угрозы безопасности информации, обрабатываемой СБТ, с использованием шины SMBus/I2C и радиомодуля:

1. Осуществление анализа (перехват) данных между устройствами шины I2C и арбитром (мастером) шины. В роли

устройств помимо радиомодуля могут выступать также извещатели, микросхемы памяти, аналого-цифровые преобразователи (далее – АЦП), цифро-аналоговые преобразователи (далее – ЦАП) и т.п., а также микроконтроллеры устройств или ЦП. В схеме подключения I2C/SMBus используется одно мастер-устройство (арбитр шины) и множество подключенных к нему по общей шине подчинённых устройств (slave).

При подключении логического анализатора к контактам шины I2C/SMBus можно произвести накопление данных, которые циркулируют по шине, для последующего анализа. Подключение к шине можно осуществить через любое устройство I2C, подключённое к ней, следить за поведением устройств и выявить наличие радиомодуля. Зная алгоритм взаимодействия радиомодуля с мастер-устройством, можно осуществить несанкционированное копирование конфиденциальной информации. В EEPROM может содержаться конфиденциальная информация, ключей, журналов и т. д., которые ЦП разместил туда для возможного хранения. Протокол SMBus способен обеспечивать обмен данными до 3 уровня модели OSI включительно. Следовательно, злоумышленник может подключиться как на прямую к контактам шины I2C/SMBus, так и через сеть, если сетевая карта имеет поддержку работы с протоколом I2C/SMBus и может быть обнаружена в сети [14].

Также перехватить данные можно путём воздействия на контроллер шины (позволяет опередить мастера, если их в системе несколько), который находится в чипсете (набор микросхем) CBT. Чипсет разрабатывается компанией Intel®, следовательно, путём воздействия на контроллер шины при помощи проприетарных программных инструментов партнёры компании могут получить доступ к любым данным, которые циркулируют на шине I2C/SMBus.

2. Анализ и последующее изменение данных в контроллерах, буферах и микросхемах памяти устройств, подключенных к шине I2C. Если данные на устройстве не защищены, злоумышленник может их модифицировать (изменить). Изменение данных в названных сегментах CBT может привести к повреждению системы или выводу её из строя. Например, путём воздействия через шину PMBus (шина управления питанием – подмножество шины I2C) можно изменить конфигу-

рационные данные питающих узлов серверов, что может привести к ситуациям, когда поведение системы может быть непредсказуемым. Нестабильное питание ЦП и контроллеров устройств может вызывать сбой в работе встроенных программных и аппаратных алгоритмов защиты, ввиду выхода оборудования и устройств за пределы допустимых диапазонов питающих напряжений. Имеются данные, что пониженное напряжение питания ЦП приводит к сбою аппаратной защиты, что позволяет злоумышленнику получить доступ ко всем блокам памяти ЦП [20].

3. Подключенное к шине I2C/SMBus устройство, к которому злоумышленник получил доступ, может быть использовано для воздействия на тактовый генератор шины с целью вызова в нём сбоя. Изменяя частоту тактирования при передаче сигналов между конкретным устройством (радиомодулем) и мастером можно вызвать сбой и задержки в передаче данных и в последующем осуществить несанкционированный доступа (НСД) к информации, содержащейся в радиомодуле [21].

Можно предположить следующий сценарий атаки на CBT при помощи радиомодуля и его шины SMBus:

При непосредственном доступе к CBT необходимо установить микросхемы, имеющих подключение к I2C или отвечающих за их функционирование, и определить контакты подключения на плате CBT.

Далее осуществляется подключение к шине и перехват сигналов, передаваемых по шине, с последующим сравнением их с известными (штатными устройствами, подключаемыми к шине). При наличии логического анализатора или специально разработанных программ можно осуществить накопление и анализ всех данных, передаваемых по шине. Логический анализатор способен отображать сигналы на линиях SDA и SCL шины I2C/SMBus.

Далее при помощи декодирования и сравнения сигналов согласно временной диаграмме протокола можно получить информацию о том, к какому адресу (устройству) происходит обращение и какие данные передаются на шине.

В случае, если методом сравнения полученных результатов не удалось описать адрес или данные на шине, необходимо при помощи устройства, которое способно выполнять функции мастер-устройства, подключиться к шине и осуществить попытку воздействия на

данный адрес и инициировать выгрузку всех данных устройства, которые содержит устройство по данному адресу.

Для доступа напрямую к конкретному устройству или блоку памяти необходимо описание алгоритма работы с ним, прописанного в его техническом описании. Имея информацию о том, как устройство взаимодействует с шиной, злоумышленник способен написать программу, реализующую алгоритм взаимодействия с устройством или микросхемой.

Устройство взаимодействия, содержащее в себе программу взаимодействия с анализируемым (атакуемым) устройством или микросхемой, можно подсоединить напрямую к шине или подсоединиться специальной контактной клипсой к самой микросхеме. В случаях отсутствия возможности подключения возможно отпаивание микросхемы и подключение напрямую к её выходам I2C для дальнейшего взаимодействия с блоками памяти.

Таким образом, для осуществления несанкционированного доступа к СБТ при помощи радиомодуля злоумышленнику необходимо непосредственное подключение к шине SMBus. Однако в случае, если злоумышленником выступает разработчик аппаратной платформы, которым может являться компания Intel®, необходимость в использовании описанного алгоритма отпадает. Ввиду наличия контроля за устройством управления злоумышленник в лице разработчика может получить любые данные из любого подключенного к шине устройства и передать его любым возможным способом за пределы СБТ.

С помощью радиомодуля теоретически можно организовать удалённое управление устройствами СБТ. По информации из открытых источников в 2012 году Intel® внедрила в свои ЦП технологию, позволяющую удалённо при помощи RFID отключать и дистанционно управлять ЦП, даже если компьютер не подключен к Интернету или не включен. Данной технологии было дано название Anti-Theft 3.0 [22]. Сделано это было по заявлению компании для осуществления невозможности работы ПК в случае его кражи.

Таким образом, можно предположить, что данная технология уже внедрена в радиомодуль и позволяет удалённо при помощи радиоканала RFID управлять и отключать аппаратно-связанные с ним ЦП или устройства

СБТ (искажать прошивки по шине I2C).

Реализация такой функции позволит не только отслеживать перемещение СБТ, даже когда он не подключен к сети или питанию, но и ставит под угрозу безопасность данных, обрабатываемых СБТ. Нет гарантий, что злоумышленник не воспользуется данным каналом и не перехватит информацию, передаваемую по радиоканалу, или не выведет ЦП или СБТ из строя.

Не так давно появилась информация об атаках с использованием уязвимостей типа Spectre [23] и Meltdown [24]. Способы их закрытия не гарантируют абсолютной безопасности. Существуют риски совместного использования данных уязвимостей вместе с интегрированным радиомодулем.

Вредоносный код, использующий данные уязвимости, может внедряться через радиоканал в пользовательскую память радиомодуля, и в последующем отправляться в оперативную память СБТ или же напрямую в кэш-память ЦП. Ввиду того, что радиомодуль по SMBus напрямую связан с процессором, а также имеет доступ к оперативной памяти, риск очевиден. В дальнейшем код может, например, эксплуатировать уязвимость Spectre, изъять из памяти СБТ конфиденциальные данные такие, как пароли аутентификации, банковские пароли и т.д. В последующем достаточно лишь выгрузить их обратно в пользовательскую память радиомодуля и считать их по RFID.

Даже если атаки типа Spectre и Meltdown, использующие уязвимость «спекулятивного» выполнения команд и развитого предсказания ветвлений, удастся закрыть, то это не решит обозначенных выше проблем. В апреле 2021 года была опубликована статья исследователей из инженерной школы Университета Вирджинии, в которой говорится о том, что была обнаружена линия атаки, которая ломает всю защиту от уязвимости Spectre [25].

Таким образом, осуществление несанкционированного доступа к конфиденциальным данным при помощи радиомодуля и эксплуатации уязвимостей Spectre и Meltdown представляют серьёзный риск неконтролируемой утечки этих данных по специально создаваемому радиоканалу или системной шине SMBus.

Ввиду связи через шину SMBus со всеми периферийными устройствами СБТ, может существовать возможность получения не только информации из оперативной памяти,

кэш-памяти процессора, но также из буферов периферийных устройств и т.д. Следовательно, злоумышленник теоретически может удалённо перехватить конфиденциальные данные пользователей, содержащиеся в потенциально уязвимых частях памяти, среди которых могут быть информация об идентификаторах пользователей, сведения, позволяющие осуществить аутентификацию от их лица, конфиденциальные документы, файлы и т.д.

В виду того, что устройства на шине могут обмениваться данными при отсутствующем питании, появляется возможность доступа к узлам CBT без запуска операционной системы CBT. Это создаёт возможность управления шиной и подключенными к ней устройствами в обход установленной на CBT операционной системы. Единственное, что необходимо – это наличие питания 3.3 В на материнской плате, являющегося дежурным, либо радиомодуль может получать питание от считывателя RFID. Ввиду того, что радиомодуль никак не отображается в операционной системе, контроль над устройством происходит на аппаратном уровне самим процессором или с помощью микрокоманд, отправляемых мастером шины SMBus.

Заключение

Одним из направлений внедрения технологии RFID являются центральные процессоры средств вычислительной техники.

Анализ спецификаций радиомодулей, устанавливаемых подложке центральных процессоров компании Intel®, показал, что они имеют контакты для подключения двух антенн, линии шины SMBus, а также контакты питания и заземления. Память радиомодулей разделяется на два сегмента. Первый блок PIROM, содержит информацию о центральном процессоре (ядра, частота, объём кеш и т.д.). Данный блок памяти невозможно перезаписать. Вто-

рой блок EEPROM, является перезаписываемым сегментом памяти неизвестного объёма и неизвестного назначения. Высказано предположение, что данный блок может использоваться для промежуточного хранения перехваченной с CBT конфиденциальной информации, или размещения специального программного обеспечения, реализующего функции несанкционированного доступа или несанкционированного воздействия на ЦП или CBT.

Рассмотрены два сценария атаки на CBT при помощи радиомодуля.

Первый сценарий основан на использовании для атаки шины SMBus и предполагает физический доступ злоумышленника к CBT. Однако в случае, если злоумышленником выступает разработчик аппаратной платформы, которым может являться компания Intel®, необходимость в физическом доступе к CBT злоумышленника отпадает.

Второй сценарий основан на удаленном управлении центральным процессором и устройствами CBT с помощью радиомодуля по радиоканалу с использованием технологии Anti-Theft.

Таким образом, с использованием радиомодулей, установленных на центральном процессоре, возможно не только отслеживать перемещение CBT, даже когда он не подключен к сети или питанию, но и осуществлять перехват данных, обрабатываемых CBT, и управлять центральным процессором или отключать аппаратно-связанные с центральным процессором устройства CBT.

Направлениями дальнейших исследований является создание лабораторного стенда, позволяющего моделировать и исследовать угрозы безопасности информации, реализуемые с использованием радиомодулей, установленных на центральном процессоре.

Литература

1. Применения RFID // Wikipedia. URL: <https://clck.ru/Tzote> (дата обращения: 07.12.2023).
2. RFID-Technology // SMART-TEC URL: <https://www.smart-tec.com/en/auto-id-world/rfid-technology> (дата обращения: 27.03.2023).
3. ГОСТ Р 58701-2019 (ИСО/МЭК 18000-63:2015) Информационные технологии (ИТ). Идентификация радиочастотная для управления предметами. Параметры радиоинтерфейса для связи в диапазоне частот от 860 МГц до 960 МГц (Тип C). – Москва: Стандартинформ, 2020.
4. RFID-Technology // SMART-TEC URL: <https://www.smart-tec.com/en/auto-id-world/rfid-technology> (дата обращения: 27.03.2023).
5. ГОСТ Р ИСО 17363-2010 Применение радиочастотной идентификации (RFID) в цепи поставок. Контейнеры грузовые, М.: Стандартинформ, 2019 год, – 20 с.
6. Какие частоты разрешены для RFID. — Текст: электронный // rfctest: [сайт]. — URL: <https://rfctest.ru/stati/kakie-chastoty-razresheny-dlya-rfid/> (дата обращения: 18.12.2023).

7. Заседание ГКПЧ от 07.05.2007 (протокол № 07-20) // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

8. UHF RFID PROTOCOLS AND STANDARTS. — Текст: электронный // TraceID: [сайт]. — URL: <https://www.trace-id.com/protocols-and-standards-of-uhf-rfid/> (дата обращения: 24.03.2023).

9. EPCglobal. — Текст: электронный // gs1: [сайт]. — URL: <https://www.gs1.org/epcglobal> (дата обращения: 24.03.2023).

10. RFID // Wikipedia. URL: <https://ru.wikipedia.org/wiki/RFID> (дата обращения: 27.03.2023).

11. FAQ RFID: от описаний к фактическим применениям // Gaw.ru URL: <http://www.gaw.ru/html.cgi/txt/publ/other/rfid.htm> (дата обращения: 27.03.2023).

12. Jean, Elyan Avec le RFID, Intel veut mieux recenser le matériel des datacenters / Elyan Jean. — Текст: электронный // Le Monde Informatique: [сайт]. — URL: <https://www.lemondeinformatique.fr/actualites/lire-avec-le-rfid-intel-veut-mieux-recenser-le-materiel-des-datacenters-61331.html> (дата обращения: 07.12.2023).

13. RFID-Tag im Intel Core X-Prozessor // HEISE ONLINE. URL: <https://www.heise.de/newsticker/meldung/RFID-Tag-im-Intel-Core-X-Prozessor-3730254.html> (дата обращения: 07.12.2023).

14. System Management Bus (SMBus) Specification, 2018. System Management Interface Forum, Inc., pp: 85.

15. Под крышкой процессоров Intel Core i9 скрывается микросхема NFC либо RFID // ixbt. URL: <https://www.ixbt.com/news/2017/06/05/intel-core-i9-nfc-rfid.html> (дата обращения: 07.12.2023).

16. INTEL® Intel® Xeon® Processor E7- 8800/4800/2800 Product Families. Datasheet Volume 1 of 2. - Reference Number: 325119-001 изд. INTEL®, April 2011. - 174 с.

17. INTEL® Intel® Xeon® Processor E7- 8800/4800/2800 v2 Product Family Datasheet - Volume One Electrical, Mechanical and Thermal Specifications - Volume 1 of 3. - Reference Number: 329594-001 изд. INTEL®, February 2014. - 190 с.

18. INTEL® Second Generation Intel® Xeon® Scalable Processor. Datasheet, Volume One: Electrical. - Reference Number: 338845-001US изд. INTEL®, April 2019. - 134 с.

19. UHF RFID метка на фары автомобиля ZKTeCo UHF Waterproof Tag (самоклеющаяся). — Текст: электронный // Системы безопасности US-PLAST: [сайт]. — URL: <https://us-plast.ru/product/new-uhf-waterproof-tag/> (дата обращения: 07.12.2023).

20. В массовых процессорах AMD нашлась «дыра», которую невозможно закрыть. В опасности все пользователи. — Текст: электронный // CNews: [сайт]. — URL: https://www.cnews.ru/news/top/2023-05-03_v_narodnyh_protsessorah (дата обращения: 07.12.2023).

21. Hardware Attacks on Mobile Robots: I2C Clock Attacking / Jiménez-Naharro Raúl, G. *. Fernando, Medina-García Jonathan, Sánchez-Raya, and, Juan, Antonio Manuel. — Текст: непосредственный // Robot 2015: Second Iberian Robotics Conference. — 2016. — С. 147-159.

22. Intel Developing RFID Tracking and Remote Controlled 'Kill Switch' for Laptops // The hacker news. URL: <https://thehackernews.com/2014/06/intel-developing-rfid-tracking-and.html> (дата обращения: 07.12.2023).

23. Spectre (уязвимость) // Википедия. Свободная энциклопедия URL: [https://ru.wikipedia.org/wiki/Spectre_\(уязвимость\)](https://ru.wikipedia.org/wiki/Spectre_(уязвимость)) (дата обращения: 07.12.2023).

24. Meltdown (уязвимость) // Википедия. Свободная энциклопедия URL: [https://ru.wikipedia.org/wiki/Meltdown_\(уязвимость\)](https://ru.wikipedia.org/wiki/Meltdown_(уязвимость)) (дата обращения: 07.12.2023).

25. X. Ren, L. Moody, M. Taram, M. Jordan, D. M. Tullsen, A. Venkat, «I See Dead μops: Leaking Secrets via Intel/AMD Micro-Op Caches». URL: <https://www.cs.virginia.edu/venkat/papers/isca2021a.pdf> (дата обращения: 24.12.2023).

References

1. Primeneniya RFID // Wikipedia. URL: <https://clck.ru/Tzote> (data obrashcheniya: 07.12.2023).

2. RFID-Technology // SMART-TEC URL: <https://www.smart-tec.com/en/auto-id-world/rfid-technology> (data obrashcheniya: 27.03.2023).

3. GOST R 58701-2019 (ISO/MEK 18000-63:2015) Informatsionnyye tekhnologii (IT). Identifikatsiya radiochastotnaya dlya upravleniya predmetami. Parametry radiointerfeysa dlya svyazi v diapazone chastot ot 860 MGts do 960 MGts (Tip S). – Moskva: Standartinform, 2020.

4. RFID-Technology // SMART-TEC URL: <https://www.smart-tec.com/en/auto-id-world/rfid-technology> (data obrashcheniya: 27.03.2023).

5. GOST R ISO 17363-2010 Primeneniye radiochastotnoy identifikatsii (RFID) v tsepi postavok. Konteynery gruzovyye, M.: Standartinform, 2019 god, ⇨ 20 с.

6. Kakiye chastoty razresheny dlya RFID. — Tekst: elektronnyy // rfctest: [sayt]. — URL: <https://rfctest.ru/stati/kakie-chastoty-razresheny-dlya-rfid/> (data obrashcheniya: 18.12.2023).
7. Zasedaniye GKRCH ot 07.05.2007 (protokol № 07-20) // Ministerstvo tsifrovogo razvitiya, svyazi i massovykh kommunikatsiy Rossiyskoy Federatsii.
8. UHF RFID PROTOCOLS AND STANDARDS. — Tekst: elektronnyy // TraceID: [sayt]. — URL: <https://www.trace-id.com/protocols-and-standards-of-uhf-rfid/> (data obrashcheniya: 24.03.2023).
9. EPCglobal. — Tekst: elektronnyy // gs1: [sayt]. — URL: <https://www.gs1.org/epcglobal> (data obrashcheniya: 24.03.2023).
10. RFID // Wikipedia. URL: <https://ru.wikipedia.org/wiki/RFID> (data obrashcheniya: 27.03.2023).
11. FAQ RFID: ot opisaniy k fakticheskim primeneniyam // Gaw.ru URL: <http://www.gaw.ru/html.cgi/txt/publ/other/rfid.htm> (data obrashcheniya: 27.03.2023).
12. Jean, Elyan Avec le RFID, Intel veut mieux recenser le matériel des datacenters / Elyan Jean. — Tekst: elektronnyy // Le Monde Informatique: [sayt]. — URL: <https://www.lemondeinformatique.fr/actualites/lire-avec-le-rfid-intel-veut-mieux-recenser-le-materiel-des-datacenters-61331.html> (data obrashcheniya: 07.12.2023).
13. RFID-Tag im Intel Core X-Prozessor // HEISE ONLINE. URL: <https://www.heise.de/newsticker/meldung/RFID-Tag-im-Intel-Core-X-Prozessor-3730254.html> (data obrashcheniya: 07.12.2023).
14. System Management Bus (SMBus) Specification, 2018. System Management Interface Forum, Inc., pp: 85.
15. Pod kryshkoy protsessorov Intel Core i9 skryvayetsya mikroskhema NFC libo RFID // ixbt. URL: <https://www.ixbt.com/news/2017/06/05/intel-core-i9-nfc-rfid.html> (data obrashcheniya: 07.12.2023).
16. INTEL® Intel® Xeon® Processor E7- 8800/4800/2800 Product Families. Datasheet Volume 1 of 2. - Reference Number: 325119-001 izd. INTEL®, April 2011. - 174 s.
17. INTEL® Intel® Xeon® Processor E7- 8800/4800/2800 v2 Product Family Datasheet - Volume One Electrical, Mechanical and Thermal Specifications - Volume 1 of 3. - Reference Number: 329594-001 izd. INTEL®, February 2014. - 190 s.
18. INTEL® Second Generation Intel® Xeon® Scalable Processor. Datasheet, Volume One: Electrical. - Reference Number: 338845-001US izd. INTEL®, April 2019. - 134 s.
19. UHF RFID metka na fary avtomobilya ZKTeco UHF Waterproof Tag (samokleyashchayasya). — Tekst: elektronnyy // Sistemy bezopasnosti US-PLAST: [sayt]. — URL: <https://us-plast.ru/product/new-uhf-waterproof-tag/> (data obrashcheniya: 07.12.2023).
20. V massovykh protsessorakh AMD nashlas' «dya», kotoruyu nevozmozhno zakryt'. V opasnosti vse pol'zovateli. — Tekst: elektronnyy // CNews: [sayt]. — URL: https://www.cnews.ru/news/top/2023-05-03_v_narodnyh_protsessorah (data obrashcheniya: 07.12.2023).
21. Hardware Attacks on Mobile Robots: I2C Clock Attacking / Jiménez-Naharro Raúl, G. *. Fernando, Medina-García Jonathan, Sánchez-Raya, and, Juan, Antonio Manuel. — Tekst: neposredstvennyy // Robot 2015: Second Iberian Robotics Conference. — 2016. — S. 147-159.
22. Intel Developing RFID Tracking and Remote Controlled 'Kill Switch' for Laptops // The hacker news. URL: <https://thehackernews.com/2014/06/intel-developing-rfid-tracking-and.html> (data obrashcheniya: 07.12.2023).
23. Spectre (uyazvimost') // Vikipediya. Svobodnaya entsiklopediya URL: [https://ru.wikipedia.org/wiki/Spectre_\(uyazvimost'\)](https://ru.wikipedia.org/wiki/Spectre_(uyazvimost')) (data obrashcheniya: 07.12.2023).
24. Meltdown (uyazvimost') // Vikipediya. Svobodnaya entsiklopediya URL: [https://ru.wikipedia.org/wiki/Meltdown_\(uyazvimost'\)](https://ru.wikipedia.org/wiki/Meltdown_(uyazvimost')) (data obrashcheniya: 07.12.2023).
25. X. Ren, L. Moody, M. Taram, M. Jordan, D. M. Tullsen, A. Venkat, «I See Dead μops: Leaking Secrets via Intel/AMD Micro-Op Caches». URL: <https://www.cs.virginia.edu/venkat/papers/isca2021a.pdf> (data obrashcheniya: 24.12.2023).

ХОРЕВ Анатолий Анатольевич, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность», Национальный исследовательский университет «МИЭТ». 124498, г. Зеленоград, площадь Шокина, дом 1. E-mail: horev.ya@yandex.ru

HOREV Anatoly Anatolevich, doctor of technical Sciences, Professor, head of the Department «Information security», National Research University of Electronic Technology. 124498, Zelenograd, Shokin square, house 1. E-mail: horev.ya@yandex.ru

ЧУМАКОВ Андрей Александрович, аспирант кафедры «Информационная безопасность», Национальный исследовательский университет «МИЭТ». 124498, г. Зеленоград, площадь Шокина, дом 1. E-mail: mr.jordan99@yandex.ru

CHUMAKOV Andrey Aleksandrovich, postgraduate student of the Department of Information Security, National Research University MIET. 124498, Zelenograd, Shokin Square, building 1. E-mail: mr.jordan99@yandex.ru

* Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article.. The authors declare no conflicts of interests.

***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 № 4(50) / 2023

Подписано в печать 16.12.2023. Дата выхода в свет 25.12.2023.

Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 7,79. Тираж 50 экз.

Заказ 000/000.

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. 4(50) / 2023

Signed to print December 16, 2023. Date of publication of the 25.12.2023.

Format 70×108 1/16. Screen printing. Conventional printed sheet 7,79. Circulation – 50 issues.

Order 000/000.

Open price.

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