ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 4(46) / 2022

Подписной индекс 73852 в каталоге «Почта России»

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

Свидетельство ПИ № ФС77-65765 от 20.05.2016

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

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

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

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 4(46) / 2022

FOUNDER

SOUTH URAL STATE UNIVERSITY (NIU)

SOUTH URAL LEGAL NEWSLETTER

Subscription index 73852

in the «Russian Post» catalog

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

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

Publisher: OOO « South Ural Legal Newsletter»

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

Electronic version of the magazine in the Internet:

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

16+

В НОМЕРЕ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

УДК

Вестник УрФО № 4(46) / 2022, с. 5–20

Поршнев С.В., Рябко Н.Ю.

DOI: 10.14529/secur220401

МЕТОДИКА ТРАНСФОРМАЦИИ ЭЛЕКТОРАЛЬНЫХ ДАННЫХ, РАЗМЕЩАЕМЫХ НА САЙТЕ ЦЕНТРАЛЬНОЙ ИЗБИРАТЕЛЬНОЙ КОМИССИИ, В ФОРМУ ПРИГОДНУЮ ДЛЯ ИХ АВТОМАТИЗИРОВАННОГО АНАЛИЗА

В статье на примере открытых официальных данных, представленных на сайте Центральной избирательной комиссии (ЦИК) Российской Федерации (РФ), по результатам выборов Президента РФ в 2018 г. описана автоматизированная методика трансформации электоральных в форму пригодную для их дальнейшего автоматизированного анализа, а также программные инструменты, обеспечивающие работоспособность предложенной методики. Обоснован выбор структур электоральных данных на уровнях избирательных комиссий (ИК) субъектов РФ, территориальных избирательных комиссий (ТИК) и участковых избирательных комиссий (УИК), извлеченных их единого файла, содержащего все электоральные данные, выгруженные с сайта ЦИК РФ.

Приведен пример использования преобразованных электоральных данных, подтверждающий отсутствие намерений их фальсификации на этапе формирования ИК, ТИК и УИК.

Ключевые слова: *выборы, электоральные данные, избирательная комиссия, анализ данных, информационный поиск.*

METHODOLOGY OF TRANSFORMATION OF ELECTORAL DATA POSTED ON THE WEBSITE OF THE CENTRAL ELECTION COMMISSION INTO A FORM SUITABLE FOR THEIR AUTOMATED ANALYSIS

The article presents the automated method for the transformation of electoral data provided by the Central Election Commission (CEC) of the Russian Federation (RF) based on the results of the presidential elections in RF in 2018. There are described software tools that ensure the operability of the proposed methodology and the structure of electoral data at the levels of election commissions (EC) of RF regions, territorial election commissions (TEC) and district election commissions (DEC), this data was extracted from a single file with all electoral data downloaded from the CEC website of RF.

There is an example with the use of transformed electoral data confirming the absence of intentions to falsify data at the stage of formation of the EC, TEC and DEC.

Keywords: *election, election data, election commission, data retrieval, data mining.*

Введение

Проблемы, связанные с оценкой достоверности результатов тех или иных выборов в органы власти и местного самоуправления в РФ и выявления возможных фальсификаций электоральных данных, в современной политической ситуации являются предметом острых научных и политических дискуссий, в которых принимают участие политики, политологи, юристы, специалисты по прикладной статистике (электоральные статистики), а также политически активные избиратели) (см., например, [1,2]). При этом, в большинстве случаев, мнения участников дискуссий по обсуждаемой проблеме, в зависимости занимаемой ими политической позиции, оказываются диаметрально противоположными: от полного отрицания каких-либо фальсификаций электоральных данных (например, члены ЦИК и избирательных комиссий нижних уровней), до полного отрицания возможности проведения в Российской Федерации (РФ) честных выборов (например, кандидаты, не получившие поддержки избирателей, а также члены либерально настроенного сообщества электоральных статистиков (см., например, [3]).

В [4] на основе анализа действующей нормативно-правовой базы в области защиты информации, доказано, что задачи обеспечения достоверности электоральных данных, как на этапе их получения, так и на этапе интерпретации, по своей сути, изоморфны задачам защиты информации, а потому для их решения необходимо применять соответствующие методы защиты информации. В этой связи, разработка методов защиты электоральных данных, к которым, безусловно, следует

отнести методы оценки достоверности выводов электоральных статистиков, является актуальной.

При этом основная проблема состоит в отсутствии электоральных данных, полученных по результатам «абсолютно честных» выборов, в которых отсутствие фальсификаций доказано с помощью методов, отличных от методов электоральной статистики (например, на основе данных, представленных независимыми наблюдателями, данных экзит-поллов и т.д.). Их анализ, как очевидно, мог бы позволить определить набор «эталонных» статистических характеристик, по значениям которых можно будет говорить об отсутствии или наличии фальсификаций электоральных данных.

Отметим, что проведение «абсолютно честных» выборов, процедура организации и проведения которых гарантировала недопущение каких-либо процедурных нарушений (как преднамеренных, так и не преднамеренных) и признание отсутствия таковых всеми сторонами избирательного процесса в реальных условиях, как очевидно, невозможно. В этой связи для оценки адекватности известных методов выявления электоральных аномалий представляется целесообразным использовать данные, представленные избирательными комиссиями (ИК) соответствующих уровней по результатам таких выборов, в которых преимущество одного из кандидатов являлось столь значительным, что его победа на выборах ни у кого не вызывала ни малейших сомнений, а потому использование каких-либо фальсификаций не требовалось. Таковыми были выборы Президента РФ в 2018 г., победа в которых за явным преимуществом была одержана действующим Президентом РФ В.В. Путиным.

Для автоматизированной выгрузки с сайта ЦИК РФ [5] соответствующих электоральных данных, представленных ИК субъектов РФ, территориальными избирательными комиссиями (ТИК) и участковыми избирательными комиссиями (УИК) о результатах выборов Президента РФ в 2018 г. (число которых превышало 97 тыс.) в файл CVS-формата была использована специальная технология, подробно описанная в [6]. (Отметим, что за время прошедшее с момента разработки данной технологии появилась новая версия сайта ЦИК РФ и обсуждаемые электоральные данные размешены на странице [7].) Наличие электоральных данных по каждой ИК субъекта РФ, ТИК и УИК позволяет провести количественный анализ особенностей избирательного процесса в каждом субъектах РФ. Например, в [8] на основе анализа электоральных данных, представленных ИК Свердловской области (которые были извлечены из соответствующего файла CVS-формата) вычислены оценки плотностей вероятностей второй после запятой цифры в электоральном показателе «отношение числа проголосовавших избирателей на данном избирательном участке к общему числу зарегистрированных избирателей», а также появления одинаковых цифр в первом и во втором разрядах после запятой (метод Бебера и Скакко), которые позволили сделать обоснованный вывод об отсутствии фальсификаций электоральных данных в СО на обсуждаемых выборах.

В данной статье обсуждаются автоматизированная методика извлечения из электоральных данных, полученных в ходе выборов Президента РФ в 2018 г., размещенных на сайте ЦИК РФ, а также их декомпозиция в соответствие со структурой ИК, ТИК и УИК, а также приводится пример анализа этих электоральных данных.

2. Структура электоральных данных о результатах выборов Президента РФ в 2018 г., выгруженных в файл CVS-формата, и ее модификация

Напомним, что система избирательных комиссий по выборам Президента РФ в 2018 г. имела следующую иерархическую структуру: ЦИК, избирательные комиссии (ИК) субъектов РФ, территориальные ИК, участковые ИК. Всего в 2018 г. было сформировано: 85 ИК субъектов РФ. Кроме того, было сформированы еще 2 ИК без образования в них ТИК: ИК «Территория за пределами РФ», которой были отнесены 394 УИК, и ИК «Город Байконур (Республика Казахстан)», на территории которого были сформированы 7 участковых УИК. Таким образом, было сформировано: 87 ИК, 2776 ТИК, 97314 УИК.

При разработке программного инструмента, обеспечивающего автоматическую выгрузку обсуждаемых электоральных данных в файл CVS-формата, предполагалось, что эти данные имеют следующую иерархическую структуру: вершина дерева – данные ЦИК (сводные электоральные данные по всей РФ), ветви первого уровня – данные ИК субъектов РФ (сводные электоральные данные по соответствующему субъекту РФ), ветви второго уровня – данные территориальных ИК (сводные данные по территориальным ИК соответ-

ствующих субъектов РФ), ветви третьего уровня – данные участковых ИК, а информационные модели электоральных данных, размещаемых на вершине, а также первом и втором уровнях описанной выше иерархической структуры, одинаковы.

Для автоматической выгрузки электоральных данных, представленных ИК после выборов Президента РФ в 2018 г., с сайта ЦИК [4] был использован обычный офисный компьютер (AMD Ryzen 5 4 ГГц, 32 Гб ОЗУ, Интернет со скоростью 50Мб/с. На выгрузку данных потребовалось 8 часов, в течение которых было выполнено 201156 http-запросов и скачано около 10 ГБ сырых данных. Далее из первичных («сырых») данных извлечено 11Мб полезных данных, которые были сохранены в CSV-файл (в формате RFC 4180) со следующей структурой (таблица 1).

Фрагмент скриншот программы Excel с

Таблица 1

Описание данных

Наименование столбца	Тип данных	Описание
I1	Строка	наименование ИК субъекта РФ
I2	Строка	Наименование территориальной ИК субъекта РФ
I3	Строка	Наименование участковой ИК 3 уровня, сформированной территориальной ИК субъекта РФ
c1	Целое число	Число избирателей, включенных в список избирателей
c2	Целое число	Число избирательных бюллетеней, полученных участковой избирательной комиссией
c3	Целое число	Число избирательных бюллетеней, выданных избирателям, проголосовавшим досрочно
c4	Целое число	Число избирательных бюллетеней, выданных в помещении для голосования в день голосования
c5	Целое число	Число избирательных бюллетеней, выданных вне помещения для голосования в день голосования
c6	Целое число	Число погашенных избирательных бюллетеней
c7	Целое число	Число избирательных бюллетеней в переносных ящиках для голосования
c8	Целое число	Число бюллетеней в стационарных ящиках для голосования
c9	Целое число	Число недействительных избирательных бюллетеней
c10	Целое число	Число действительных избирательных бюллетеней
c11	Целое число	Число утраченных избирательных бюллетеней
c12	Целое число	Число избирательных бюллетеней, не учтенных при получении
c13	Целое число	Число избирателей, проголосовавших за Бабурина Сергея Николаевича
c14	Целое число	Число избирателей, проголосовавших за Грудинина Павла Николаевича
c15	Целое число	Число избирателей, проголосовавших за Жириновского Владимира Вольфовича
c16	Целое число	Число избирателей, проголосовавших за Путина Владимира Владимировича
c17	Целое число	Число избирателей, проголосовавших за Собчак Ксению Анатольевну
c18	Целое число	Число избирателей, проголосовавших за Сурайкина Максима Александровича
c19	Целое число	Число избирателей, проголосовавших за Титова Бориса Юрьевич
c20	Целое число	Число избирателей, проголосовавших за Явлинского Григория Алексеевича

открытым файлом, содержащим результаты выгрузки электоральных данных, представленных ИК после выборов Президента РФ в 2018 г., подтверждающий работоспособность разработанного программного инструмента приведен на рисунке 1.

Данный файл содержал 100579 строк. В первой строке данного файла размещены на-

	A	B	C	D	E	F	G	H	I	J
1	I1	I2	I3	c1	c2	c3	c4	c5	c6	c7
7	Алтайский край	Алейская	УИК №559	215	220	0	143	13	64	13
8	Алтайский край	Алейская	УИК №560	469	470	0	350	33	87	33
9	Алтайский край	Алейская	УИК №561	428	420	0	326	42	52	42
10	Алтайский край	Алейская	УИК №562	76	79	0	66	3	10	3
11	Алтайский край	Алейская	УИК №563	886	820	0	585	139	96	139
12	Алтайский край	Алейская	УИК №565	220	210	0	136	29	45	29
13	Алтайский край	Алейская	УИК №566	880	860	0	561	117	182	117
14	Алтайский край	Алейская	УИК №567	357	340	0	287	18	35	18
15	Алтайский край	Алейская	УИК №568	160	160	0	131	13	16	13
16	Алтайский край	Алейская	УИК №569	178	170	0	143	19	8	19
17	Алтайский край	Алейская	УИК №570	450	460	0	361	33	66	33
18	Алтайский край	Алейская	УИК №571	779	720	0	546	43	131	43
19	Алтайский край	Алейская	УИК №572	52	67	0	45	3	19	3
20	Алтайский край	Алейская	УИК №573	455	460	0	332	48	80	48
21	Алтайский край	Алейская	УИК №574	583	560	0	411	42	107	42
22	Алтайский край	Алейская	УИК №575	464	480	0	333	77	70	77
23	Алтайский край	Алейская	УИК №578	141	130	0	107	8	15	8
24	Алтайский край	Алейская	УИК №579	73	80	0	55	6	19	6
25	Алтайский край	Алейская	УИК №580	439	430	0	327	25	78	25

Рис. 1. Фрагмент скриншота Excel с открытым файлом CSV-формата

звания столбцов, представленные в таблице 1. В остальных ячейках столбцов I1, I2, I3 размещены: названия субъекта РФ; названия созданной данным субъектом ТИК; упорядоченные по алфавиту, названия УИК, упорядоченные по алфавиту, созданных данным ТИК, в столбцах c1-c20 – соответствующие количественные показатели, описание которых представлено в таблице 2. Результаты анализ данного файла и далее их сравнение с аналогичными электоральными данными, размещенными на сайте ЦИК РФ [6], позволил сделать вывод из всех зарегистрированных УИК 21 не представили электоральные данные. В этой связи строки, соответствующие данным избирательным комиссиям были удалены из обсуждаемого файла.

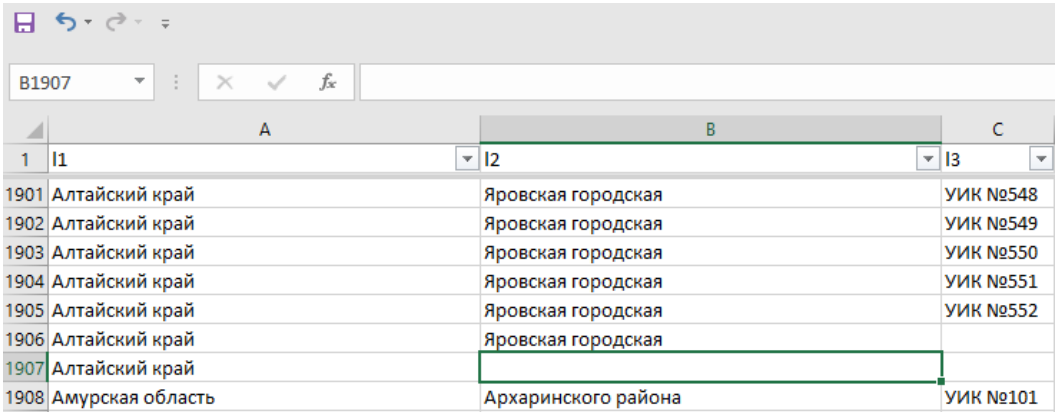
Таким образом, общее число УИК, представивших электоральные данные по результатам выборов Президента РФ в 2018 г. составило 97293.

Сводные результаты по данной ТИК записывались в строку, следующую за строкой последней УИК, созданной данной ТИК. При этом в соответствующую ячейку столбца I3 заносилось значение null-string (null-string="") (рис. 1.). Сводные данные результаты по данной ИК, записывались в строку, следующую за строкой, содержащей сводные данные по последней ТИК, созданной данной ИК (рис. 2). В результате число строк файла, содержащего обсуждаемые электоральные данные ЦИК, увеличилось до 1005879.

Дальнейший анализ данных показал, что ИК «Город Байконур (Республика Казахстан)» и ИК «Территория за пределами РФ» не создавали ТИК, но напрямую УИК – 9 и 369 в г. Байконур и за пределами РФ, соответственно. В связи с отсутствием обсуждаемых ТИК соответствующая информация по ТИК в файле отсутствовала (рис. 3).

Для автоматизации дальнейшей обработки электоральных данных о выборах Президента РФ в 2018 г. проведена следующая модификация файла CVS-формата: пустые ячейки с столбце I2, находящиеся в строках, содержащих электоральные данные УИК г. Байконур и УИК, созданных за пределами РФ, были заполнены текстом следующего содержания: «Без образования ТИК». Кроме того, в файл после строки с информацией, представленной последними из УИК г. Байконур и УИК территорий за пределами РФ были добавлены соответствующие строки, в ячейки которых находящиеся в столбцах c1c20 были оставлены пустыми (рис. 4).

Анализ результатов импорта обсуждаемого файла в рабочее пространство пакета MATLAB для его последующей обработки позволил обнаружить, что инструмент импорта



B1907

	A	B	C
1	l1	l2	l3
1901	Алтайский край	Яровская городская	УИК №548
1902	Алтайский край	Яровская городская	УИК №549
1903	Алтайский край	Яровская городская	УИК №550
1904	Алтайский край	Яровская городская	УИК №551
1905	Алтайский край	Яровская городская	УИК №552
1906	Алтайский край	Яровская городская	
1907	Алтайский край		
1908	Амурская область	Архаринского района	УИК №101

Рис. 2. Пример размещения сводных данных по Яровской городской ТИК Алтайского края и ИК Алтайского края

1	l1	l2	l3	c1	c2
12104	Город Байконур (Республика Казахстан)		УИК №8143	1769	1500
12105	Город Байконур (Республика Казахстан)		УИК №8144	1880	1500
12106	Город Байконур (Республика Казахстан)		УИК №8145	2047	1900
12107	Город Байконур (Республика Казахстан)		УИК №8146	2291	1900
12108	Город Байконур (Республика Казахстан)				
12109	город Москва	Академический район	УИК №2118	863	800

Рис. 3. Фрагмент файла CVS-формата, иллюстрирующий размещение электоральных данных каждой из УИК г. Байконур и сводных данных по этому городу

1	l1	l2	l3	c1	c2
12101	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8140	2132	2000
12102	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8141	2207	2000
12103	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8142	2249	2000
12104	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8143	1769	1500
12105	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8144	1880	1500
12106	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8145	2047	1900
12107	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8146	2291	1900
12108	Город Байконур (Республика Казахстан)	Без образования ТИК			
12109	Город Байконур (Республика Казахстан)	Пустое поле		14575	12800

Рис. 4. Фрагмент файла CVS-формата после добавления дополнительной строки в файл и заполнения пустых полей в столбце l2

данных выбранного пакета на смог определить тип данных, находящихся в столбце l2, в то время для пустых ячеек, находящихся в других столбцах таблицы такой проблемы не возникло. В этой связи в каждую пустую ячейку, находящуюся в столбце l2, был записан следующий текст: «Пустое поле».

В результате проведенных преобразований контента файла, содержащего электоральные данные, скаченные с сайта ЦИК, число его строк оказалось равным 100560.

Для удобства независимых исследователей электоральных данных о результатах выборов Президента РФ в 2018 сформулируем описанные выше действия с первичными данными в виде следующего алгоритма:

1. Открыть файл CVS-формата в инструменте для работы с электронными таблицами Excel.

2. Найти и удалить строки содержащие названия УИК, не представивших сведения о результатах выборов Президента РФ в2018 г. (для их нахождения достаточно включить фильтр «Пустые» в любом из столбцов c1-c20).

3. Добавить новую строку после строки, содержащей поля «г. Байконур (Республика Казахстан)» (столбец l1), и заполнить поле данной строки, находящееся в столбце l2 текстом «Пустое поле».

4. Добавить новую строку после строки, содержащей поля «Территория за пределами РФ» (столбец l1) и заполнить поле данной

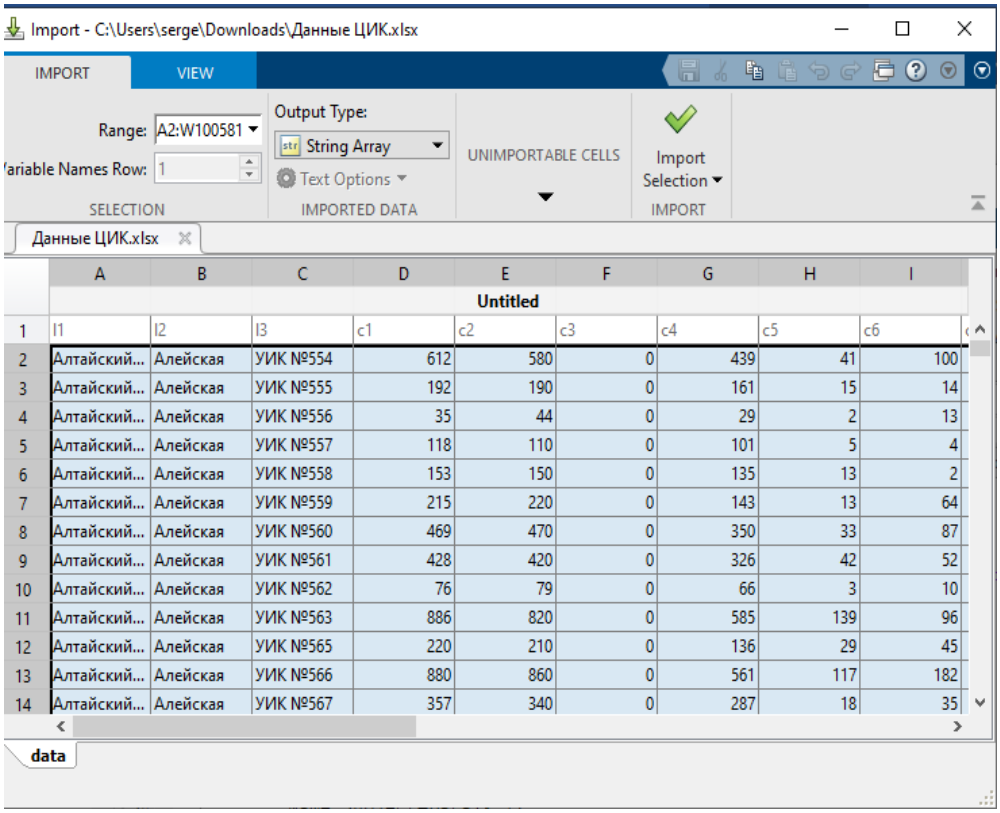
строки, находящееся в столбце I2, текстом «Пустое поле».

3. Автоматизированная методика трансформации электоральных данных, представленных Центральной избирательной комиссией по результатам выборов Президента Российской Федерации в 2018 г., в форму пригодную для их анализа

Из описания структуры файла, содержащего электоральные данные ЦИК РФ о результатах выборов Президента РФ в 2018 г., понятно, что целесообразно привести структуры информации, содержащуюся в данном файле, в соответствие структуре системы ИК, ТИК и УИК РФ. При этом, очевидно, что в связи с большим объемом первичных электоральных данных реализация обсуждаемой декомпозиции электоральных данных вручную будет весьма трудоемкой. В этой связи требуется автоматизировать процесс решения данной задачи.

Для решения данной задачи авторы выбрали пакет MATLAB, являющийся сегодня одним из лидеров на рынке прикладного программного обеспечения, предназначенного, в том числе, для анализа данных.

На первом шаге осуществлялся импорт электоральных данных ЦИК из файла «Данные ЦИК.xlsx» (рис. 4) в рабочее пространство MATLAB. (Отметим, что здесь следует выбрать в меню «Output Type» тип экспортируемых данных «String Array».)



	A	B	C	D	E	F	G	H	I
1	I1	I2	I3	c1	c2	c3	c4	c5	c6
2	Алтайский...	Алейская	УИК №554	612	580	0	439	41	100
3	Алтайский...	Алейская	УИК №555	192	190	0	161	15	14
4	Алтайский...	Алейская	УИК №556	35	44	0	29	2	13
5	Алтайский...	Алейская	УИК №557	118	110	0	101	5	4
6	Алтайский...	Алейская	УИК №558	153	150	0	135	13	2
7	Алтайский...	Алейская	УИК №559	215	220	0	143	13	64
8	Алтайский...	Алейская	УИК №560	469	470	0	350	33	87
9	Алтайский...	Алейская	УИК №561	428	420	0	326	42	52
10	Алтайский...	Алейская	УИК №562	76	79	0	66	3	10
11	Алтайский...	Алейская	УИК №563	886	820	0	585	139	96
12	Алтайский...	Алейская	УИК №565	220	210	0	136	29	45
13	Алтайский...	Алейская	УИК №566	880	860	0	561	117	182
14	Алтайский...	Алейская	УИК №567	357	340	0	287	18	35

Рис. 5. Фрагмент интерфейс инструмента импорта данных в процессе импорта электоральных данных ЦИК из файла «Данные ЦИК.xlsx»

В результате импорта в рабочем пространстве MATLAB создавалась переменная «Untitled», содержащая электоральные данные ЦИК, которая далее переименовывалась в переменную «Data». Далее были написаны на m-пакета MATLAB 3 скрипта, которые были сохранены в файлах «DataElection.m», «DataElection2.m», «DataElection3.m», соответственно. Листинги данных файлов приведены в Приложении, соответственно. Первый скрипт обеспечивает автоматическую выгрузку из переменной Data электоральных данных, представленных УИК, сформированными соответствующей ТИК, и их сохранение в папке «d:\Data» в mat-файлах, а также УИК г. Байконур и имена которых формируются в соответствие со следующим шаблоном:

«Название субъекта РФ, сформировавшего ИК Название ТИК».

В данный файл записывается матрица

размерности 20 × число УИК. Пример данной матрицы, содержащей электоральные данных, представленные УИК г. Байконур, приведен на рис. 6.

Результатом выполнения первого скрипта являются 2778 mat-файлов, размещенных в папке d\Data (рис. 6).

Для подтверждения правильности рабо-

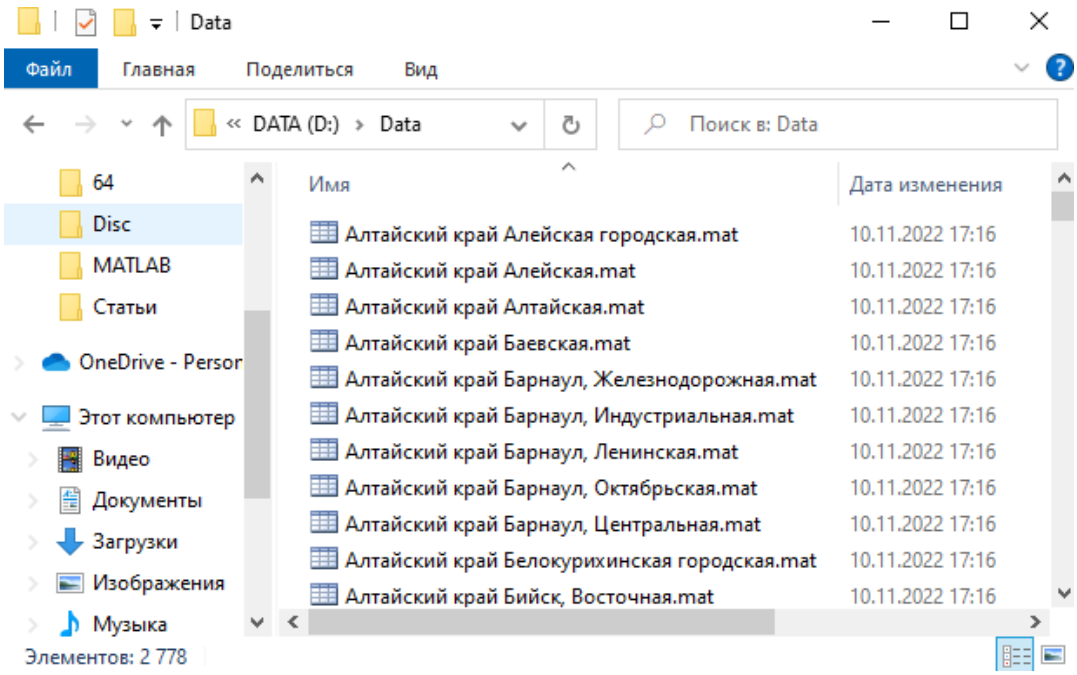


Рис. 6. Фрагмент каталога папки «d:\Data»

P

20x7 double

	1	2	3	4	5	6	7
1	2132	2207	2249	1769	1880	2047	2291
2	2000	2000	2000	1500	1500	1900	1900
3	0	0	0	0	0	0	0
4	1447	1470	1490	1065	1171	1302	1546
5	11	14	7	48	13	13	62
6	542	516	503	387	316	585	292
7	11	14	7	48	13	13	62
8	1447	1470	1490	1065	1171	1302	1546
9	9	14	27	20	10	14	10
10	1449	1470	1470	1093	1174	1301	1598
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	4	2	5	5	7	1	8
14	176	128	171	98	124	138	191
15	79	87	94	72	105	96	95
16	1136	1214	1162	882	902	1022	1250
17	30	19	17	17	7	18	22
18	9	4	3	8	9	9	9
19	5	7	12	5	10	5	6
20	10	9	6	6	10	12	17

Рис. 7. Данные, загруженные из файла «Город Байконур (Республика Казахстан).mat»

ты скрипта на рисунке 8 представлены аналогичные электоральные данные, находящиеся в первичном файле «Данные ЦИК.xlsx».

Второй скрипт обеспечивает автоматическую выгрузку из переменной Data сводных электоральных данных, представленных в ИК

	A	B	C	D	E	F	G	H
1	I1	I2	I3	c1	c2	c3	c4	c5
12101	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8140	2132	2000	0	1447	11
12102	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8141	2207	2000	0	1470	14
12103	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8142	2249	2000	0	1490	7
12104	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8143	1769	1500	0	1065	48
12105	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8144	1880	1500	0	1171	13
12106	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8145	2047	1900	0	1302	13
12107	Город Байконур (Республика Казахстан)	Без образования ТИК	УИК №8146	2291	1900	0	1546	62
12108	Город Байконур (Республика Казахстан)	Без образования ТИК						
12109	Город Байконур (Республика Казахстан)	Пустое поле		14575	12800	0	9491	168

Рис. 8. Электоральные данные, представленных УИК г. Байконур (Республика Казахстан) (файл «Данные ЦИК.xlsx»)

субъекта РФ соответствующими ТИК[1], и их сохранение в папке «d:\Data2» в mat-файлах, имена которых формируются в соответствие со следующим шаблоном:

«Название субъекта РФ»,

а также автоматическую выгрузку из переменной Data сводных электоральных, представленных ИК субъектов РФ, УИК г. Байконур (Республика Казахстан) и УИК территорий, находящихся за пределами РФ и сохранение их в папке d:\Data3 в mat-файле «d:\Data3\All_Subject.mat», в который записывается таблица ячеек размером 20 × 87 ячеек (рис. 10).

Результатом выполнения данного скрипта являются 87 файлов, размещенных в папке «d:\Data2» (рис. 9) и файл «All_Subject.mat», размещенный в папке «d:\Data3».

Правильность работы данного скрипта

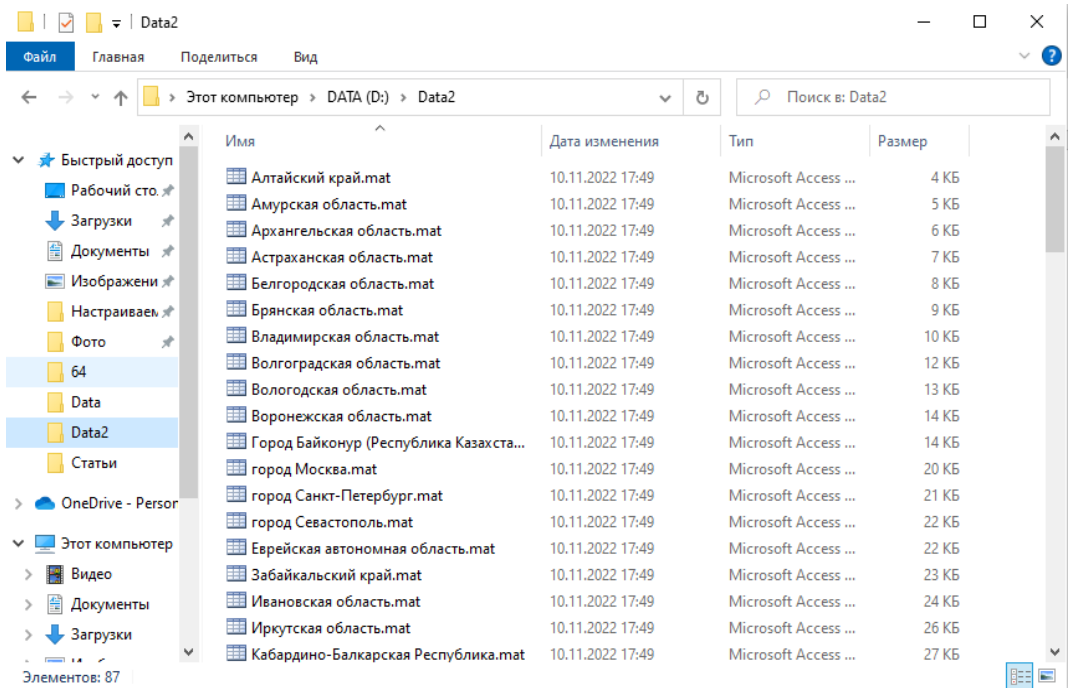


Рис. 9. Фрагмент каталога папки «D:\Data2»

подтверждается результатами сравнения данных, представленных на рис. 10, с соответствующими данными, размещенными в файле «Данные ЦИК.xlsx». Например, на рисунке 10 приведены сводные электоральные данные, представленные ИК Алтайского края.

Из рисунков 10, 11, видно, что электоральные данные, размещенные в столбце № 1 в ячейках № 1-20, совпадают с данным размещенными в файле «d:\Data3\All_Subject.mat» в строке № 1907 в столбцах c1-c20.

Таким образом, приведенные результаты подтверждают правильность функционирования описанных выше скриптов, предназна-

Editor - DataElection3.m

P

20x87 double

	1	2	3	4	5	6	7
1	1822203	635083	914218	736206	1218896	978509	1141236
2	1650783	578918	884150	700193	1162467	950080	1066871
3	61	3498	3942	432	0	0	0
4	1106745	365862	514021	417312	806610	692036	678717
5	84824	25321	23229	27074	86165	87912	63247
6	459153	184237	342958	255375	269692	170132	324907
7	84869	28810	27168	27487	86165	87903	63241
8	1106390	365743	513794	417239	806269	691575	678160
9	14203	5383	4880	4340	8749	7177	9351
10	1177056	389170	536082	440386	883685	772301	732050
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	7581	2358	4448	2185	5218	4472	5440
14	281978	73485	51868	64047	93102	68375	93649
15	84785	37909	46925	19339	49685	43940	58822
16	770278	264493	407190	342195	711392	636087	546042
17	11788	4428	10588	5060	8474	7463	10777
18	7855	2466	3842	2823	6534	4265	5075
19	5532	2080	4982	2233	4835	4175	6098
20	7259	1951	6239	2504	4445	3524	6147

Рис. 10. Фрагмент таблицы, сохраненной в файле «d:\Data3\All_Subject.mat»

A1907 | Алтайский край

	A	B	C	D	E	F	G
1	I1	I2	I3	c1	c2	c3	c4
1907	Алтайский край	Пустое поле		1822203	1650783	61	1106745

Рис. 11. Фрагмент строки со сводными электоральными данными, представленными ИК Алтайского края

ченных для извлечения электоральных данных из файла «d:\Data3\All_Subject.mat» в соответствие со структурой ИК, ТИК и УИК РФ, проводивших выборы президента РФ в 2018 г.

4. Некоторые результаты анализа электоральных данных ЦИК РФ, собранных в ходе выборов Президента РФ в 2018 г.

Одно из традиционных обвинений ЦИК со стороны ОЭС состоит в искусственном увеличении числа ТИК и УИК, что облегчает по их утверждениям фальсификацию на данных уровнях электоральной статистики (см, например, [9]). В этой связи авторы исследовали функциональные зависимости между числом ТИК, организованных в РФ для проведения выборов Президента РФ в 2018 г., и числом избирателей, отнесенных к данной ТИК (функциональная зависимость № 1), а также числом УИК и числом УИК, отнесенных к данной УИК (функциональная зависимость № 2).

Для анализа функциональной зависимости № 1 на основе анализа электоральных данных, размещенных в папке «D:\Data2», для каждой ИК субъекта РФ подсчитывалось число ТИК, созданных данной ИК, а также число избирателей, зарегистрированных данной ИК. При этом число ТИК, созданных на территориях, находящиеся за пределами РФ, и в г. Байконур принималось равными единице. Таким образом, общее число значений функциональной зависимости № 1, представленных на рисунке 12, составило 87 пар значений.

При этом значение коэффициента R2, характеризующего качество линейной аппрок-

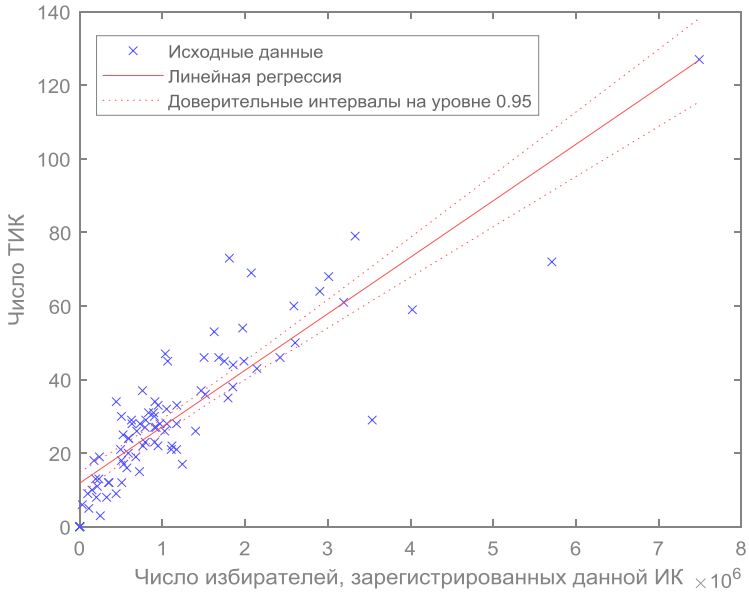


Рис. 12. Функциональная зависимость № 1

симации функциональной зависимости № 1, оказалось равным 0.757. Данный результат позволяет сделать обоснованный вывод о том, что ИК субъектов РФ при создании ТИК, стремились следующему следовать принципу: «число ТИК должно быть прямо пропорционально числу избирателей, зарегистрированных ИК данного субъекта РФ». Этот результат, с нашей точки зрения, свидетельствует об отсутствии преднамеренной организации такого числа ТИК, которые непропорционально числу избирателей, с целью последующих фальсификаций электоральных данных.

Для анализа функциональной зависимости № 2 на основе анализа электоральных данных, размещенных в папке «D:\Data», для каждой ТИК, созданной соответствующей ИК субъекта РФ, подсчитывалось число УИК и число избирателей в каждой из УИК. Таким образом, общее число значений функциональной зависимости № 1, представленных на рисунке 13, составило 2778 пар значений.

При этом значение коэффициента R2, характеризующего качество линейной аппроксимации функциональной зависимости № 2, оказалось равным 0.654, что также позволяет

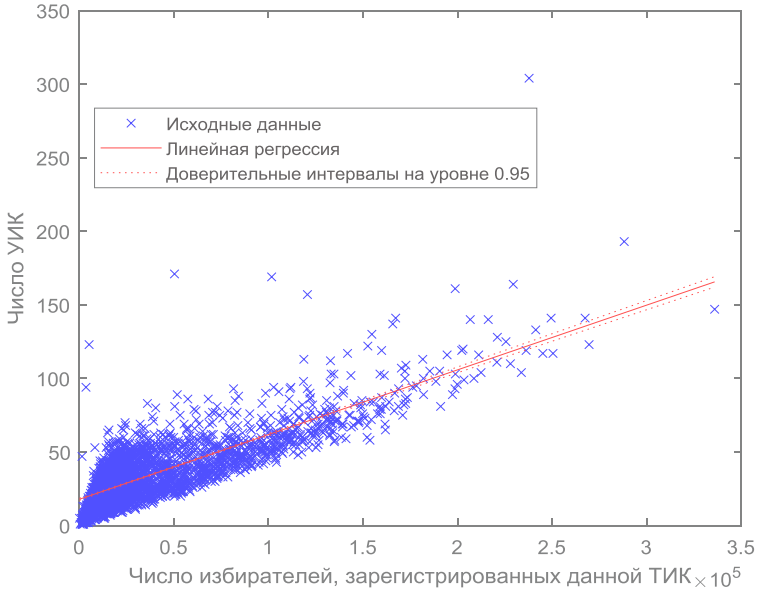


Рис. 13. Функциональная зависимость № 2

говорить о значимой линейной связи между числом УИК и числом избирателей, зарегистрированных данной ТИК. Меньшее, чем в предыдущем случае, значение коэффициента R2, с нашей точки зрения, объясняется тем, что при выборе числа УИК, созданных данной ТИК, приходится учитывать не только численность избирателей, но их распределение по территории, относящейся к данной ТИК.

Таким образом, анализ функциональных зависимостей № 1, № 2 позволяет сделать вывод об отсутствии попыток организаторов выборов Президента РФ в 2018 г. произвольного выбора числа ТИК и УИК в субъектах РФ с целью последующей фальсификации электоральных данных.

Заключение

Разработана автоматизированная методика извлечения электоральных данных из файла «D:\Data3\All_Subject.mat» в соответствие со структурой ИК, ТИК и УИК РФ, проводивших выборы президента РФ в 2018 г., и ПО, обеспечивающее его работоспособность.

С помощью разработанного ПО реализована выгрузка:

1) электоральных данных, представленных УИК в соответствующие ТИК, созданные ИК каждого из субъектов РФ, а также УИК г. Байконура и УИК территорий расположенных за пределами РФ (2778 файлов);

2) сводных электоральных данных по каждой ТИК, созданные ИК каждого из субъектов РФ, а также УИК г. Байконура и УИК территорий расположенных за пределами РФ (87 файлов);

3) сводных электоральных данных по каждой ИК, созданные ИК каждого из субъектов РФ, а также УИК г. Байконура и УИК территорий расположенных за пределами РФ (1 файл).

Можно ожидать, что наличие электоральных данных, декомпозированных по уровням ИК, ТИК и УИК РФ, обеспечит проведение статистического анализа результатов выборов Президента РФ в 2018 г. и получение объективных оценок адекватности методов выявления аномалий, активно используемых оппозиционными электоральными статистиками.

Литература

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

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

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

4. Поршнев С.В. Рябко Н.Ю., Уксусников Н.А. Обеспечение достоверности экзит-поллов, как задача информационной безопасности//Вестник УрФО. Безопасность в информационной сфере, 2021, № 3(41) / 2021, с. 49–56.

5. URL: http://www.vybory.izbirkom.ru (дата обращения 19.02.2022).

6. Мирвода С.Г., Поршнев С.В., Рябко Н.Ю. Автоматизация процедуры доступа к электоральным данным, размещенным на сайте Центральной избирательной комиссии Российской Федерации// Вестник УрФО. Безопасность в информационной сфере, 2022, № 1(43). С. 28–34. DOI: 10.14529/secur220104.

7. URL:http://www.vybory.izbirkom.ru/region/izbirkom?action=show&global=1&vrn=100100084849062&region=0&prver=0&pronetvd=null (дата обращения 09.11.2022).

8. Поршнев С.В., Рябко Н.Ю. Опыт применения метода Берра и Скакко для проверки достоверности электоральных данных// Вестник УрФО. Безопасность в информационной сфере, 2022, № 2(44), С. 12–24.

9. https://www.yaplakal.com/forum7/topic2079742.html.

References

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

2. SHen' A. Kak doklad ROIIP delegitimiruet vybory. URL: https://trv-science.ru/2020/09/kak-doklad-roiip-delegitimiruet-vybory/ (data obrashcheniya 19.02.2022).

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

4. Porshnev S.V. Ryabko N.YU., Uksusnikov N.A. Obespechenie dostovernosti ekzit-pollov, kak zadacha informacionnoj bezopasnosti//Vestnik UrFO. Bezopasnost' v informacionnoj sfere, 2021, № 3(41) / 2021, s. 49–56.

5. URL: http://www.vybory.izbirkom.ru (data obrashcheniya 19.02.2022).

6. Mirvoda S.G., Porshnev S.V., Ryabko N.YU. Avtomatizaciya procedury dostupa k elektoral'nym dannym, razmeshchennym na sajte Central'noj izbiratel'noj komissii Rossijskoj Federacii// Vestnik UrFO. Bezopasnost' v informacionnoj sfere, 2022, № 1(43). S. 28–34. DOI: 10.14529/secur220104

7. URL:http://www.vybory.izbirkom.ru/region/izbirkom?action=show&global=1&vrn=100100084849062®ion=0&prver=0&pronetvd=null (data obrashcheniya 09.11.2022).

8. Porshnev S.V., Ryabko N.YU. Opyt primeneniya metoda Berra i Skakko dlya proverki dostovernosti elektoral'nyh dannyh// Vestnik UrFO. Bezopasnost' v informacionnoj sfere, 2022, № 2(44), S. 12–24.

9. https://www.yaplakal.com/forum7/topic2079742.html.

Приложение

```
% Листинг скрипта № 1
% назначение скрипта:
% выгрузка электоральных данных УИК,
% созданных данной ТИК
% выгрузка электоральных данных
% по всем ТИК, созданных
% ИК субъектов РФ
clear all
load Data.mat Data
N=size(Data,1);
Name_Subject=Data(1,1);
Name_Region=Data(1,2);
Null_Str="";
k=2;
n_min=1;
K=1;
clear('P');
while k<=N-1
  while Name_Region==Data(k,2)
      k=k+1;
      K=K+1;
  end
  K=K-1;
  k=k-1;
  if Data(k,1)=="Город Байконур (Республика Казахстан)"||Data(k,1)=="Территория
за пределами РФ"
     K=K-1;
  end
  P=zeros(20,K);
  for m=1:20
      for n=n_min:n_min+K-1
        P(m,n-n_min+1)=Data(n,m+3);
      end
  end
  File_Name="d:\Data\"+string(Name_Subject)+" "+string(Name_Region)+".mat";
  save(File_Name,'P')
  tmp1=Data(k,3);
  tmp2=Data(k+1,2);
  if (tmp1==Null_Str)&&~(tmp2==Null_Str)
       k=k+1;
       K=0;
  end
  if (tmp1==Null_Str)&&(tmp2==Null_Str)
       Name_Subject=Data;
       Name_Region=Data;
```

```
        k=k+2;
        K=0;
    end
    n_min=k;
    if k<=N
       Name_Subject=Data(k,1);
       Name_Region=Data(k,2);
    end
end

% Листинг скрипта № 2
% назначение скрипта:
% выгрузка в файлы ИК субъектов РФ
% электоральных данных,
% представленной каждой ТИК,
% а также сводных данных
% по всем ИК субъектов РФ
clear all
load Data.mat Data
N=size(Data,1);
Null_Str="";
k=2;
n_min=1;
K1=1;
K2=1;
for i=2:N-1
    if (Data(i,3)==Null_Str)&&~(Data(i,2)==Null_Str)&&~(Data(i,1)=='Город
Байконур (Республика Казахстан)')&&~(Data(i,1)=='Территория за пределами
РФ')
        P1(K1,:)=Data(i,:);
        K1=K1+1;
    end
    if (Data(i,1)=='Город Байконур (Республика
Казахстан)')&&(Data(i,3)==Null_Str)
        if ~(Data(i,4)==Null_Str)
           P1(K1,:)=Data(i,:);
           K1=K1+1;
        end
    end
    if (Data(i,1)=='Территория за пределами РФ')&&(Data(i,3)==Null_Str)
        if ~(Data(i,4)==Null_Str)
           P1(K1,:)=Data(i,:);
           K1=K1+1;
        end
    end
    if (Data(i,3)==Null_Str)&&(Data(i,2)==Null_Str)&&~(Data(i,1)=='Город
Байконур (Республика Казахстан)')&&~(Data(i,1)=='Территория за пределами
РФ')
        P2(K2,:)=Data(i,:);
        K2=K2+1;
    end
    if (Data(i,1)=='Город Байконур (Республика
Казахстан)')&&(Data(i,3)==Null_Str)
        if ~(Data(i,4)==Null_Str)
           P2(K2,:)=Data(i,:);
           K2=K2+1;
        end
    end
    if (Data(i,1)=='Территория за пределами РФ')&&(Data(i,3)==Null_Str)
        if ~(Data(i,4)==Null_Str)
           P2(K2,:)=Data(i,:);
           K2=K2+1;
        end
```

```
    end
end
if Data(i+1,1)=="Ярославская область"
        P2=[P2;Data(N,:)];
        for k=1:size(P2,1)
            for n=4:size(P2,2)
                P2_Num(k,n-3)=str2num(P2(k,n));
            end
        end
        File_Name="D:\Data3\"+"All_Subject"+'.mat';
        save(File_Name,'P2_Num')
end
M=size(P1,1);
K1=1;
m=1;
while m<=M-1
    if P1(m,1)=="Город Байконур (Республика
Казахстан)"||P1(m,1)=="Территория за пределами РФ"
        Line=P1(m,4:23);
        for i=1:20
            P1_Num(i,K1)=Line(1,i);
        end
        K1=1;
        File_Name="D:\Data2\"+' '+P1(m,1)+'.mat';
        save(File_Name,'P1_Num')
    end
    if (P1(m,1)=="Ненецкий автономный округ")
        Line=P1(m,4:23);
        for i=1:20
            P1_Num(i,K1)=str2num(Line(1,i));
        end
        K1=K1+1;
        m=m+1;
        Line=P1(m,4:23);
        for i=1:20
            P1_Num(i,K1)=str2num(Line(1,i));
        end
    end
    if P1(m,1)==P1(m+1,1)
        Line=P1(m,4:23);
        for i=1:20
            P1_Num(i,K1)=str2num(Line(1,i));
        end
        K1=K1+1;
    end
    if ~(P1(m,1)==P1(m+1,1))
        File_Name="D:\Data2\"+' '+P1(m,1)+'.mat';
        save(File_Name,'P1_Num')
        clear('P1_Num')
        K1=1;
    end
    if P1(m+1,1)=="Ярославская область"&&P1(m+1,2)=="Ярославская"
        Line=P1(m+1,4:23);
        for i=1:20
            P1_Num(i,K1)=str2num(Line(1,i));
        end
        File_Name="D:\Data2\"+' '+P1(m,1)+'.mat';
        save(File_Name,'P1_Num')
    end
    m=m+1;
end
```

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» федерального государственного авто-

номного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: s.v.porshnev@urfu.ru

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

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

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

УДК 004.056 Вестник УрФО № 4(46) / 2022, с. 21–25

Зырянова Т. Ю.

DOI: 10.14529/secur220402

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ МЕТОДЫ В СИСТЕМАХ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В сфере технологий обеспечения безопасности информации огромное значение имеют технологии анализа больших информационных массивов данных. Информационно-аналитические системы безопасности – одно из современных и активно развивающихся направлений в сфере теории, методологии и практики защиты информации. Статья посвящена обзору основных понятий, положений и категорий, связанных с информационно-аналитическими системами и описанию основных подходов к выполнению интеллектуального анализа данных с применением современных информационных технологий. Обоснована необходимость применения информационно-аналитических систем при разработке систем менеджмента информационной безопасности, приведены их основные особенности.

Ключевые слова: *информационно-аналитическая система, система менеджмента информационной безопасности, база данных, хранилище данных, анализ данных.*

Zyryanova T. Yu.

INFORMATION-ANALYTICAL METHODS IN INFORMATION SECURITY MANAGEMENT SYSTEMS

In the field of information security technologies, technologies for analyzing large information data arrays are of great importance. Information-analytical security systems is one of the modern and actively developing areas in the field of theory, methodology and practice of information security. The article is devoted to an overview of the basic concepts, provisions and categories associated with information and analytical systems and a description of the main approaches to the implementation of data mining using modern information technologies. The necessity of using information-analytical systems in the development of information security management systems is substantiated, their main features are given.

Keywords: *information-analytical system, information security management systems, database, data warehouse, data analysis.*

Понятие системы менеджмента информационной безопасности (СМИБ) введено Международным стандартом ИСО/МЭК 27000 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология». Согласно стандарту СМИБ – это часть общей системы менеджмента, основанная на подходе бизнес-рисков по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению информационной безопасности. Основные функции СМИБ должны состоять в оценке степени критичности ситуации, связанной с нарушением информационной безопасности, оценке уровня риска нарушения информационной безопасности и в поддержке принятия решений относительно действий в данной ситуации. Принятие решений в такой системе затруднено по ряду причин: не всегда возможно сформировать полное множество угроз информационной безопасности, количественно оценить степень критичности возникшей ситуации, построить прогноз ее развития. Для решения таких слабоструктурированных задач, характеризующихся высокой степенью неопределенности исходных данных может быть эффективно применение подходов, характерных для современных информационно-аналитических систем.

Существуют различные определения понятия информационно-аналитической системы (ИАС), которые во многом характеризуют различные сферы применения ИАС, такие как экономика, управление, бизнес и многие другие. Приведем некоторые, наиболее общие, из них.

ИАС – компьютерная система, позволяющая получать информацию, создавать ее, проводить ее обработку и анализ.

ИАС – автоматизированная система, позволяющая экспертам быстро анализировать большие объемы знаний.

Прообразом современных ИАС систем стали развивающиеся с конца 70-х годов XX века системы поддержки принятия решений (СППР) – интерактивные автоматизированные системы, помогающие лицу, принимающему решения, использовать данные и математические модели для решения структурированных проблем. Принципиальное отличие современных ИАС от СППР состоит в том, что, как правило, в качестве исходных данных в ИАС используются большие объемы изначально неструктурированной информации, которые необходимо преобразовывать и анализировать для получения значимых результатов.

В соответствии со своим назначением ИАС должны решать задачи:

1. Поиска, сбора, передачи и хранения информации;

2. Обобщения и сортировки информации;

3. Анализа информации, формирования выводов и заключений.

Подробному описанию информационно-аналитических систем безопасности (ИАСБ) посвящена, например, работа [1].

Для решения первой и второй задач в ИАС применятся технология хранилищ данных. Для решения третьей задачи применяется целый комплекс различных технологий анализа. Это технология произвольных информационных запросов SQL, технология гиперкубического представления и многомерного анализа данных OLAP, технологии интеллектуального анализа данных Data Mining.

Основоположниками теории хранилищ данных стали Уильям Х. Инмон (Билл Инмон) в 1991 году и Ральф Кимбалл в 1998 году.

Билл Инмон сформулировал определение хранилища данных как «предметно-ориентированные, интегрированные, стабильные, поддерживающие хронологию наборы данных, организованные для целей поддержки управления, призванные выступать в роли единственного источника истины» [2].

Определение Ральфа Кимбалла более простое, короткое и обобщенное: «хранилища данных – место, где люди могут получать доступ к своим данным» [3].

Существуют принципиальные различия между хранилищами данных и ставшими уже привычными традиционными базами данных. Они состоят в следующем.

1. Базы данных применяются, как правило, для обеспечения повседневной работы и не предназначены для решения аналитических задач. Хранилища данных – это структуры данных, предназначенные непосредственно для поддержки принятия решений на основе анализа помещенной в них информации.

2. Информация в базах данных терпит постоянные изменения в режиме реального времени в процессе работы пользователей. Для информации в хранилищах данных характерна относительная стабильность. Добавление данных в хранилища производится в определенные моменты времени.

3. В базах данных хранятся, как правило, внутренние данные той или иной информационной системы. Хранилища данных используются большие массивы данных из внешних источников.

4. В базах данных набор запросов пользователей, с которыми они могут обратиться, четко регламентирован и известен уже на этапе проектирования базы данных. Для хранилищ данных характерны нерегламентированные запросы аналитиков.

На этапе становления технологии баз данных применялись различные подходы к структуризации информации. В результате ее эволюции появилась модель данных, получившая название реляционной (от слова relationship – отношение), впервые описанная в статье Эдгара Кодда «Реляционная модель данных для больших коллективных банков данных» [4]. Отличительной особенностью этой модели от предшествующих стало представление данных об объектах реального мира с учетом связей между ними в форме самого естественного их представления – прямоугольных таблиц. С целью реализации реляционной модели данных был разработан стандарт высокоуровневого языка программирования реляционных баз данных, получившего название SQL – Structured Query Language – Структурированный язык запросов – единый интегрированный язык, содержащий все средства для работы с реляционными базами данных, такие как:

1. Операторы формулирования запросов;

2. Средства определения схемы базы данных и манипулирования схемой;

3. Операторы для определения ограничений и триггеров;

4. Средства определения представлений;

5. Средства авторизации доступа к отношениям и их атрибутам;

6. Средства управления транзакциями.

Именно язык запросов SQL используется для сбора исходных данных в современных информационно-аналитических системах.

Основной технологией, применяемой в информационно-аналитических системах является OLAP – On-Line Analytical Processing – Оперативная аналитическая обработка данных. Ее основоположником также стал Эдгар Кодд, который в 1993 году дал этой технологии следующее определение: «OLAP – динамический анализ, включающий в себя возможность выявления новых или непредвиденных отношений между переменными, способность работать с большими объемами данных, создавать неограниченное число измерений (частей консолидации) и определять условия и выражения пересечения переменных» [5]. Вообще говоря, OLAP – это не отдельно взятый продукт и даже не конкретная технология, а скорее концепция, основанная на математической модели представления данных в виде многомерных кубов.

Массив данных в терминологии OLAP называется кубом. Кубы OLAP не обязательно имеют одинаковое число элементов по всем осям, могут быть многомерными. Ввиду своей многомерности сам куб для анализа непригоден. Из него извлекаются двумерные таблицы по интересующим аналитика параметрам (операция разрезания куба), из которых затем создаются многоуровневые объединения, называемые иерархиями. Исходные данные берутся из нижнего уровня иерархий и суммируются для получения данных на более высоком уровне.

Для поиска закономерностей и извлечения знаний в ИАС широкое применение нашла технология Data Mining, получившая свое название от английского слова mining – дословно – добыча полезных ископаемых – процесс, требующий просеивания большого количества сырого материала для поиска ценностей.

Согласно определению, данному Григорием Пятецким-Шапиро: «Data Mining – процесс обнаружения в сырых данных ранее неизвестных, нетривиальных, полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности» [6].

Также известно определение Data Mining, данное Вячеславом Анатольевичем Дюком: «Поиск в больших объемах данных неочевидных, объективных и полезных на практике закономерностей» [7]. Слово «неочевидных» в данном определении означает, что закономерности не обнаруживаются стандартными методами обработки информации, например, статистическими, или экспериментальным путем.

Согласно В. А. Дюку выделяют пять видов

закономерностей в данных, которые могут быть обнаружены применением технологии Data Mining:

1. Ассоциация – взаимосвязь событий друг с другом;

2. Последовательность – наличие цепочки событий, связанных друг с другом последовательно во времени;

3. Классификация – наличие признаков, характеризующих группу объектов;

4. Кластеризация – аналог классификации, при котором изначально не задано ни количество групп объектов, ни признаки, по которым объекты будут распределяться на группы;

5. Прогнозирование – наличие исторической информации, содержащей шаблоны в поведении процесса, которые можно использовать для предсказания параметров процесса в будущем.

Методы, применяемые в ИАС для поиска таких закономерностей разнообразны. Это и классические статистические методы, и методы интеллектуального анализа данных, основанные на применении принципов работы человеческого мышления.

Для решения задач поиска ассоциаций могут применяться методы корреляционно-регрессионного анализа. Корреляционный анализ позволяет оценить существенность влияния одного объекта, процесса или явления на другой, регрессионный анализ применяется для установления вида зависимости между объектами, процессами, явлениями.

Наиболее эффективным статистическим методом прогнозирования является метод анализа временных рядов. Временным рядом называется последовательность измерений значений переменной (процесса) за определенный период времени через одинаковые промежутки.

Термин «кластерный анализ» впервые ввел математик Р. Трион в 1939 году [8]. Этот метод включает в себя набор различных алгоритмов классификации и предназначен для того, чтобы организовать наблюдаемые данные в группы (кластеры), содержащие в себе объекты с похожими свойствами. Кластеризация относится к так называемой разведочной добыче данных, так как помогает выделить информацию о связях объектов, событий или явлений, которые не видны визуально, в огромных объемах данных. Принципиальное отличие методов добычи данных от классического статистического анализа состоит в том, что аналитик не знает заранее, какую информацию он ищет.

Интеллектуальные методы анализа данных применяются в тех случаях, когда предполагается, что из имеющихся данных можно будет извлечь знания для принятия решения в условиях неопределенности. В отличие от классического разведочного анализа данных аналитика не интересует конкретный вид зависимостей между параметрами задачи. Главной целью не является выяснение природы участвующих в задаче функций или конкретной формы зависимостей. Основное внимание уделяется поиску решений. Оно достигается путем совмещения методов классического разведочного анализа и интеллектуальных методов. Data Mining часто называют смесью статистики и искусственного интеллекта. К методам Data Mining относятся, например, теория нечетких множеств и нечеткой логики, теория искусственных нейронных сетей, эволюционное программирование, генетические алгоритмы.

Необходимость создания информационно-аналитических систем в СМИБ обусловлена в первую очередь, следующими предпосылками:

1. В настоящее время происходит активная интеллектуализация информационных технологий в целом;

2. Как следствие постоянно реализуются новые интеллектуальные системы защиты информации;

3. Проблемой остается недостаточная эффективность систем обеспечения безопасности, связанных с получением в реальном времени аналитических оценок и прогнозированием состояния, направления развития и уровней угроз безопасности информации.

При разработке ИАС, предназначенных для решения проблем управления информационной безопасностью не следует упускать из внимания следующие их особенности.

1. Возможность не только анализа оперативных данных, относящихся к обеспечению безопасности объекта, но и решения задач прогнозирования уровня безопасности с использованием математических моделей.

2. Вовлечение в процесс анализа разноплановых данных из внешних источников, непосредственно не используемых в системе управления предприятием.

3. Ориентирование на хранение всей совокупности документов.

4. Поддержка интеллектуальных функций

(автоматическая классификация документов, ассоциативный поиск, поиск по образцу и т.д.) с распространением на различные формы представления информации.

Как минимум, инструментальные средства таких ИАС должны включать:

1. Средства статистического анализа данных (традиционные отчеты, диаграммы);

2. Средства динамического анализа данных (динамические системы поддержки принятия решений);

3. Средства моделирования и прогнозирования;

4. Средства визуализации связей и отношений между объектами.

В статье проанализированы наиболее актуальные направления развития технологий информационно-аналитических систем в их применении к проблемам обеспечения информационной безопасности. В настоящее время наблюдается повышенный спрос на разработку интеллектуальных систем защиты информации, способных оказывать поддержку принятия решений во множестве ситуаций – от фиксации нетипичного поведения пользователей до выявления различных аномалий в процессах передачи, хранения и обработки информации. Описанные в статье методы могут стать эффективной математической и методологической основой для разработки таких систем.

Литература

1. Васильев В. И. Интеллектуальные системы защиты информации. – М.: Машиностроение, 2017.
2. William H. Inmon. Building the Data Warehouse. – Wiley Publishing, Inc., 2006.
3. Kimball R. The Data Warehouses Lifecycle Toolkit. – Wiley Publishing, Inc., 2008.
4. Codd E. F. A Relational Model of Data for Large Shared Data Banks // Communications of the ACM, 1970. – С. 377-387.
5. Codd E. F., Codd S. B., Salley C. T. Providing OLAP (on-line analytical processing) to user-analysts. – E. F. Codd & Associates, 1993.
6. Piatetsky–Shapiro G. Advances In Knowledge Discovery and Data Min ing, 1996.
7. Дюк В. А., Самойленко А. П. Data Mining. – СПб: Питер, 2001.
8. Tryon R. C. Cluster analysis. — London: Ann Arbor Edwards Bros, 1939.

References

1. Vasil'ev V. I. Intellektual'nye sistemy zashhity informacii. – M.: Mashinostroenie, 2017.
2. William H. Inmon. Building the Data Warehouse. – Wiley Publishing, Inc., 2006.
3. Kimball R. The Data Warehouses Lifecycle Toolkit. – Wiley Publishing, Inc., 2008.
4. Codd E. F. A Relational Model of Data for Large Shared Data Banks // Communications of the ACM, 1970. – С. 377-387.
5. Codd E. F., Codd S. B., Salley C. T. Providing OLAP (on-line analytical processing) to user-analysts. – E. F. Codd & Associates, 1993.
6. Piatetsky–Shapiro G. Advances In Knowledge Discovery and Data Min ing, 1996.
7. Djuk V. A., Samojlenko A. P. Data Mining. – SPb: Piter, 2001.
8. Tryon R. C. Cluster analysis. — London: Ann Arbor Edwards Bros, 1939.

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

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

УДК 004.056 Вестник УрФО № 4(46) / 2022, с. 26–31

Маслова М.А.

DOI: 10.14529/secur220403

ПРОГРАММНЫЕ МЕТОДЫ ВЫРАБОТКИ РЕКОМЕНДАЦИЙ ПРИ ЭКСПЕРТНОМ АУДИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Проведение экспертной оценки при анализе и оценке рисков информационной безопасности является одним из актуальных и постоянно применяемых методов в организациях. Получение грамотных составленных рекомендаций, относящихся непосредственно к рассматриваемому направлению работы организации есть одним из залогов уменьшения и предупреждения возможных рисков. В данной работе будет рассмотрены и приведены составленные уникальные рекомендации для входных параметров, выделенных и объединенных в одну большую базу данных из уже применяемых методик, на основе рассмотренных методов анализа и оценки рисков информационной безопасности в работах [1 3], а также нормативных актов, законодательной базы и необходимых мер по обнаружению, предупреждению и устранению рисков информационной безопасности в организациях.

Ключевые слова: *рекомендации, риски информационной безопасности, входные данные, анализ и оценка рисков информационной безопасности.*

Maslova M.A.

PROGRAM METHODS FOR DEVELOPING RECOMMENDATIONS IN EXPERT AUDIT OF INFORMATION SYSTEMS

Conducting peer review in the analysis and assessment of information security risks is one of the relevant and constantly used methods in organizations. Obtaining competently compiled recommendations related directly to the considered direction of the organization's work is one of the keys to reducing and preventing possible risks. In this paper, unique recommendations will be considered and presented for input parameters selected and combined into one large database from already used methods, based on the considered methods for analyzing and assessing information security risks in [1 3], as well as regulations, the legal framework and the necessary measures to detect, prevent and eliminate information security risks in organizations.

Keywords: *recommendations, information security risks, input data, analysis and assessment of information security risks.*

Процесс управления рисками информационной безопасности (ИБ) в России набирает все большее значение и становится системным и формализованным, появляются новые программные средства, с помощью которых можно автоматизировать процессы оценки и анализа рисков ИБ и принимаются новые стандарты и методы с грамотным описанием алгоритмов управления рисками. Недостатки в них есть, так как нет полностью комплексного подхода, который бы рассматривал и нормативно-технические, и организационные, и технические меры защиты одновременно [4 - 7].

Но прогресс не стоит на месте и постоянно появляются и усовершенствуются существующие методы оценки и анализа рисков ИБ.

В данной работе будет рассматриваться разрабатываемый программный модуль для анализа и оценки рисков ИБ в организации, который позволит проработать большую базу входных данных и с помощью метода экспертных оценок получить рекомендации по их устранению и предотвращению.

Метод экспертных оценок является одним из самых распространенных и часто применяемых методов оценки рисков.

После проведения метода экспертных оценок в результате выдаются рекомендации по принятию, предупреждению, устранению выявленных рисков для организаций, где решающую роль в данном процессе уже определяет руководство организации для которой проводилась экспертиза. Так как эксперты не могут на 100% дать правильные ответы и выводы из-за различных скрытых аспектов, неучтенных факторов, существующих в организации [8 - 10].

В разрабатываемом программном модуле были определены входные и выходные параметры анализируемых методик анализа и оценки рисков информационной безопасности: CORAS, Risk IT, ГРИФ, MSAT, СТО БР ИББС, CRAMM, MOF, Risk Watch, OCTAVE, FRAP, ISO/IEC 27001 [2]. Далее на основе метода Дельфи проводится экспертная оценка и рассчитаны параметры сходимости, которые выдаются в числовом значении от главного до не значащего параметра риска [8]. В итоге по каждому значению выдается составленная рекомендация для уменьшения, устранения риска.

Рассмотрим примеры некоторых рекомендаций для входных параметров:

1) Программное обеспечение:

– Применение специальных алгоритмов и компонент для программного обеспечения для контроля, защиты от НСД и разграничения доступа;

– Защита программного обеспечения от атак, модификаций, хищения, редактирования и разрушения с помощью шифрования, алгоритмов запутывания и обфускации, эмуляция процессов и методы периодической проверки программного кода и целостности данных;

– Установка парольной защиты на запуск с ограничениями и разграничением прав доступа пользователей, использование ключевых флешек для работы и запуска программ;

– Регулярное обновление базы данных, программ и программных модулей с помощью защиты криптографическими методами;

– При установки нового программного обеспечения необходимо получать доступ у руководства, с подтверждением их цели и использования для поддержания среды безопасности локальной информационной системы с соблюдением политики безопасности предприятия;

– Проводить проверку на совместимость с различными компонентами системы аппаратные и программные средства;

– Проводить анализ всех функциональных системных и интерфейсных требований необходимых для программной реализации на отсутствие неопределенностей, противоречий и несоответствий;

– Регистрировать и вести журнал учета по выявленным недочетам, исправлениям, несоответствиям и неопределенностям входной информации;

– Контроль спецификации в документе требований для верхнего уровня установленных системных требований для реализации программного процесса;

– Для предотвращения риска необходимо определить требования для верхнего уровня с учетом установленных системных требований;

– Проводить оценку безопасности системы производных требований верхнего уровня [11].

2) Конкурентное преимущество:

– Наличие в организации квалифицированного работника;

– Проведение постоянного аудита рынка относящиеся к конкурентам;

– Мониторинг и составление отчетов отношения базовых показателей к достигнутым успехам, промежуточных, полных и итоговых отчетов организации;

– Составление отчетов по главным параметрам: финансирование, инвестиции, затраты на рекламу и дополнительную раскрутку, оценка рисков по разным параметрам и т.д.;

– Постоянный (установленный период в организации) по мониторингу безопасности к различным значимым критериям: программное обеспечение, персонал, процессы, технологии и т.д.;

– Создание полного отчета организации на основе промежуточных, раз в квартал по увеличению результативности и уровня безопасности.

3) Атаки злоумышленников (взломы, DDOS):

– Периодическое обновление операционной системы;

– Использование лицензированного программного обеспечения;

– Установка и постоянное обновление антивирусов, имеющих встроенную изолированную среду;

– Установка межсетевых экранов и сервисов анти-DDoS;

– Установка паролей относящимся к сложным и смена их не менее чем раз в три месяца;

– Применение SIEM-решений;

– Установка двухфакторной аутентификации;

– Ежемесячное проведение тестирования на проникновения и анализ защищенности Web-приложений;

– Составление отчетов об угрозах, мерах их устранения и уровню безопасности;

– Разработка планов и стратегий по улучшению безопасности учитывая показатели рисков, их оценку, изменение и устранение [12, 13].

4) Неумышленное раскрытие сотрудниками конфиденциальной информации:

– Постоянный мониторинг возможных нежелательных инцидентов, угроз и уязвимостей;

– При приеме на работу сотрудников подписывать документ о неразглашении конфиденциальной информации;

– Проведение периодических инструктажей о рисках, угрозах, потерях, возможных последствиях при разглашении конфиденциальной информации;

– Доведение до сотрудников мер и возможных наказаний по гражданско-правовой, административной, дисциплинарной и уголовной ответственности;

– Оценка и составление отчетностей по возможным нежелательным инцидентам и вероятностям их возникновения;

– Оценка ущерба, возникшего из-за потери или утечки персональных данных определенных лиц;

– Анализ имеющихся информационных рисков, их градация, частота повторения и влияние на работу системы организации;

– Разработка и рекомендации по действиям во время восстановления работоспособности и их постоянного обновления;

– Выявления и просчет потерь связанных с выполнением обязанностей сотрудников;

– Оценку рисков проводить, используя разные подходы: на начальном этапе – качественным методом, на заключительном – количественным [14].

5) Преднамеренное несанкционированное действие сотрудников:

– Постоянный контроль 24/7, выявление и прогнозирование угроз, возможных условий и причин, по которым производится ущерб заинтересованными пользователями по функционированию информационной системы организации;

– Вход / выход сотрудников осуществляется по пропускам в организацию, вход в систему организации осуществляется по логинам и паролям, имеющим соответствующую защиту и сложность доступа, подбора и взлома;

– Проверка и контроль входа/ выхода сотрудников, внос и вынос имущества;

– Для важных объектов ввести контроль входа с дополнительными параметрами аутентификации пользователя;

– Проводить периодические встречи по повышению квалификации, доведения инструкций по грамотному использованию системы, хранению, составлению и смене паролей;

– Проводить повышение квалификации для администраторов и сотрудников, отвечающих за безопасность организации;

– При приеме на работу тщательная проверка и отбор сотрудников;

– Постоянный подбор кадров для резерва;

– Смена всех паролей и лишения прав доступа пользователя при увольнении с работы;

– Мониторинг и выявление потенциальных угроз нарушения целостности, конфиденциальности и доступности;

– Мониторинг и разработка мер по снижению и ликвидации потенциальных угроз как для кратковременных, так и долговременных перспектив организации;

– Составление и просчет финансовых затрат и потерь от разглашения данных, информации, репутации и др. важных параметров организации;

– Составление матрицы угроз и мер по предотвращению и ликвидации [15].

6) Доступ к сетям и сетевым службам:

Выделяют требования по безопасности:

– Идентификацию и аутентификацию пользователей;

– Грамотное управление доступом к системам по времени, местоположению, доверенным маршрутом, количеством неудачных входов, разграничения действий между субъектами;

– Отказ в доступе неавторизированного персонала;

– Контроль процесса ввода и обработки данных с последующим корректным их завершение на выходе;

– При создании политики безопасности организации необходимо учитывать следующие параметры и правила:

– Установление требований к безопасности используемых прикладных программ и рисков, касающихся их;

– Установить принципы, уровни безопасности и классификации по распространению информации;

– Установить согласованность между управлением доступа и политикой классификации информации для различных сетей и систем;

– Применять полное соответствие и требования нормативной документации для защиты доступа к данным или услугам;

– Установить стандартные профили доступа относительно пользователей для должностных руководств;

– Установить менеджмент прав доступа в распределенной среде или сетях, учитывая всевозможные типы доступных соединений;

– Установка распределения ролей управления доступом с запросом на доступ и возможностью периодического пересмотра к доступу и его аннулированию.

Политика должна действовать для: сетей и сетевых сервисов к которым разрешен доступ; к процедурам авторизации; мерам их управления и защиты доступа к сетевым соединениям и сетевым сервисам; средства, используемые для доступа к данным сетям и сетевым сервисам; требований аутентификации пользователя по доступу к разным сетевым сервисам и их мониторингу; принятия быстрых и четких решений по внедрению новых мер, механизмов безопасности новых или модификации старых учитывая их приемлемость, затраты и последующую выгоду; составления списка рекомендаций по улучшению и модификации мер и процедур управления и контролем непосредственно влияющих на информационную безопасность [16, 17].

Выводы

В данной работе были рассмотрены и приведены выборочные составленные уникальные рекомендации для входных параметров, применяемых для анализа и оценки угроз информационной безопасности описанных в предыдущих работах, основанные на уже применяемых в мире методах для анализа и оценки рисков информационной безопасности, а также нормативных актах, законодательной базы и необходимых мер по обнаружению, предупреждению и устранению рисков информационной безопасности в организациях. С помощью составленной расширенной базы рекомендаций для ста восьмидесяти четырех входных параметров экспертам предоставляется возможность тщательнее и глубже проработать всевозможные рисковые ситуации и пути их решения для оцениваемой организации.

Благодарность. Работа выполнена в рамках Соглашения от 30.06.2022 г. № 40469-21/2022-к.

Литература

1. Маслова, М. А. Сравнительный анализ методов оценки рисков информационной безопасности, основанных на стандартных и интеллектуальных подходах / М. А. Маслова, Е. Н. Тищенко // Про-

блемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики: материалы XIX Международной научно-практической конференции, Ростов-на-Дону, 28–29 октября 2019 года / Ростовский государственный экономический университет (РИНХ). – Ростов-на-Дону: Ростовский государственный экономический университет «РИНХ», 2019. – С. 211-215.

2. Маслова, М. А. Анализ сходимости входных данных для методик оценки рисков информационной безопасности / М. А. Маслова, Н. С. Смирнов // Современные проблемы радиоэлектроники и телекоммуникаций. – 2021. – № 4. – С. 215.

3. Маслова, М. А. Инструментальный подход к оценке рисков информационной безопасности / М. А. Маслова // Информация и безопасность. – 2022. – Т. 25. – № 2. – С. 209-216.

4. Анализ рисков информационной безопасности URL: taxpravo.ru/analitika/statya-131560-naliz_riskov_informatsionnoy_bezopasnosti.html (дата обращения 26.04.2022).

5. Макарова, О. С. Методика прогнозирования динамики вероятности проведения компьютерной атаки с точки зрения нарушителя / О. С. Макарова, С. В. Поршнев // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 1(43). – С. 64-73.

6. Минбалеев, А. В. Проблемы и перспективы обеспечения защиты персональных данных граждан в цифровом профиле / А. В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 4(42). – С. 59-63.

7. Риски информационной безопасности | Управление рисками информационной безопасности URL: https://www.dialognauka.ru/press-center/article/5990/?ysclid=laxz579slh74947120 (дата обращения 16.10.2022).

8. Маслова, М. А. Анализ, применение и модификация метода Дельфи / М. А. Маслова // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 2(44). – С. 25-29.

9. Санжапов, Б. Х. Метод принятия решений на основе многокритериальных распределенных экспертных оценок / Б. Х. Санжапов, И. С. Калина // Прикаспийский журнал: управление и высокие технологии. – 2008. – № 2(2). – С. 62-67.

10. Федоров, В. А. Метод экспертных оценок как способ оценки риска / В. А. Федоров, Е. Н. Маковеева // Развитие науки и техники: механизм выбора и реализации приоритетов: сборник статей Международной научно-практической конференции: в 3 частях, Екатеринбург, 15 июня 2017 года. Том Часть 1. – Екатеринбург: Общество с ограниченной ответственностью «Аэтерна», 2017. – С. 146-148.

11. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

12. ФСТЭК РОССИИ. «МЕТОДИЧЕСКИЙ ДОКУМЕНТ. Методика определения безопасности информации в информационных системах».

13. ГОСТ Р ИСО/МЭК 27033-3-2014. «НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. Information technology. Security techniques. Network security. Part 3. Reference networking scenarios. Threats, design techniques and control issues».

14. ГОСТ Р 51275-99 Группа Э00 «Государственный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения Protection of information. Object of informatization. Factors influencing the information. General outlines».

15. ГОСТ Р 51904-2002 «Государственный стандарт Российской Федерации. Программное обеспечение встроенных систем. Общие требования к разработке и документированию. Embedded system software. General requirements for development and documentation».

16. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности».

17. ГОСТ Р 57628— 2017 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».

References

1. Maslova, M. A. Sravnitel'nyy analiz metodov otsenki riskov informatsionnoy bezopasnosti, osnovannykh na standartnykh i intellektual'nykh podkhodakh / M. A. Maslova, Ye. N. Tishchenko // Problemy proyektirovaniya, primeneniya i bezopasnosti informatsionnykh sistem v usloviyakh tsifrovoy ekonomiki: materialy XIX Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Rostov-na-Donu, 28–29 oktyabrya 2019 goda / Rostovskiy gosudarstvennyy ekonomicheskiy universitet (RINKH). – Rostov-na-Donu: Rostovskiy gosudarstvennyy ekonomicheskiy universitet "RINKH", 2019. – S. 211-215.

2. Maslova, M. A. Analiz skhodimosti vkhodnykh dannykh dlya metodik otsenki riskov informatsionnoy

bezopasnosti / M. A. Maslova, N. S. Smirnov // Sovremennyye problemy radioelektroniki i telekommunikatsiy. – 2021. – № 4. – S. 215.

3. Maslova, M. A. Instrumental'nyy podkhod k otsenke riskov informatsionnoy bezopasnosti / M. A. Maslova // Informatsiya i bezopasnost'. – 2022. – T. 25. – № 2. – S. 209-216.

4. Analiz riskov informatsionnoy bezopasnosti URL: taxpravo.ru/analitika/statya-131560-naliz_riskov_informatsionnoy_bezopasnosti.html (data obrashcheniya 26.04.2022).

5. Makarova, O. S. Metodika prognozirovaniya dinamiki veroyatnosti provedeniya komp'yuternoy ataki s tochki zreniya narushitelya / O. S. Makarova, S. V. Porshnev // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2022. – № 1(43). – S. 64-73. 6. Minbaleyev, A. V. Problemy i perspektivy obespecheniya zashchity personal'nykh dannykh grazhdan v tsifrovom profile / A. V. Minbaleyev // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2021. – № 4(42). – S. 59-63.

7. Riski informatsionnoy bezopasnosti | Upravleniye riskami informatsionnoy bezopasnosti URL: https://www.dialognauka.ru/press-center/article/5990/?ysclid=laxz579slh74947120 (data obrashcheniya 16.10.2022).

8. Maslova, M. A. Analiz, primeneniye i modifikatsiya metoda Del'fi / M. A. Maslova // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2022. – № 2(44). – S. 25-29. 9. Sanzhapov, B. KH. Metod prinyatiya resheniy na osnove mnogokriterial'nykh raspredelennykh ekspertnykh otsenok / B. KH. Sanzhapov, I. S. Kalina // Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii. – 2008. – № 2(2). – S. 62-67.

10. Fedorov, V. A. Metod ekspertnykh otsenok kak sposob otsenki riska / V. A. Fedorov, Ye. N. Makoveyeva // Razvitiye nauki i tekhniki: mekhanizm vybora i realizatsii prioritetov: sbornik statey Mezhdunarodnoy nauchno-prakticheskoy konferentsii: v 3 chastyakh, Yekaterinburg, 15 iyunya 2017 goda. Tom Chast' 1. – Yekaterinburg: Obshchestvo s ogranichennoy otvetstvennost'yu "Aeterna", 2017. – S. 146-148.

11. GOST R ISO/MEK 27002-2012 «Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informatsionnoy bezopasnosti».

12. FSTEK ROSSII. «METODICHESKIY DOKUMENT. Metodika opredeleniya bezopasnosti informatsii v informatsionnykh sistemakh».

13. GOST R ISO/MEK 27033-3-2014. «NATSIONAL'NYY STANDART ROSSIYSKOY FEDERATSII. Informatsionnaya tekhnologiya. METODY I SREDSTVA OBESPECHENIYA BEZOPASNOSTI. Bezopasnost' setey. Chast' 3. Etalonnyye setevyye stsenarii. Ugrozy, metody proyektirovaniya i voprosy upravleniya. Information technology. Security techniques. Network security. Part 3. Reference networking scenarios. Threats, design techniques and control issues».

14. GOST R 51275-99 Gruppa E00 «Gosudarstvennyy standart Rossiyskoy Federatsii. Zashchita informatsii. Ob"yekt informatizatsii. Faktory, vozdeystvuyushchiye na informatsiyu. Obshchiye polozheniya Protection of information. Object of informatization. Factors influencing the information. General outlines».

15. GOST R 51904-2002 «Gosudarstvennyy standart Rossiyskoy Federatsii. Programmnoye obespecheniye vstroyennykh sistem. Obshchiye trebovaniya k razrabotke i dokumentirovaniyu. Embedded system software. General requirements for development and documentation».

16. GOST R ISO/MEK 27002-2021 «Informatsionnyye tekhnologii. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil primeneniya mer obespecheniya informatsionnoy bezopasnosti».

17. GOST R 57628— 2017 «Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Rukovodstvo po razrabotke profiley zashchity i zadaniy po bezopasnosti».

МАСЛОВА Мария Александровна, старший преподаватель кафедры «Информационная безопасность» Федеральное государственное автономное образовательное учреждение высшего образования Севастопольский государственный университет. Россия, 299053, г. Севастополь, Университетская улица, дом 33; аспирант, м.н.с. Федеральное государственное автономное образовательное учреждение высшего образования Ростовский государственный экономический университет (РИНХ). Россия, 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69. E–mail: mashechka–81@mail.ru

MASLOVA Maria Aleksandrovna, Senior Lecturer of the Information Security Department Federal State Autonomous Educational Institution of Higher Education Sevastopol State University. Universitetskaya street, 33, Sevastopol, 299053, Russia; postgraduate student, junior researcher Federal State Autonomous Higher Educational Institution Rostov State University of Economics (RINH). st. Bolshaya Sadovaya, 69, Rostov-on-Don, 344002, Russia. E-mail: mashechka–81@mail.ru;

УДК 681.322 Вестник УрФО № 4(46) / 2022, с. 32–38

Япаров Д.Д.

DOI: 10.14529/secur220404

ОЦЕНКА МЕТОДА ВОССТАНОВЛЕНИЯ ВХОДНОГО СИГНАЛА ПО ЗАШУМЛЕННЫМ ДАННЫМ

Представлена оценка точности метода восстановления сигнала по зашумленным данным, основанном на саморегляризирующем подходе. Представлена передаточная функция с заданными начальными условиями. Находится численное решение дифференциального уравнения 2-ого порядка, полученное из передаточной функции после обратных преобразований Лапласа, путем перехода к конечно-разностной схеме. Проведены вычислительные эксперименты по восстановлению сигнала из зашумленных исходных данных, с разными тестовыми сигналами и различным уровнем шума, подтверждающие теоретическую оценку точности метода.

Ключевые слова: *восстановление сигнала, обработка данных, конечно-разностная схема, саморегуляризации.*

Yaparov D.D.

EVALUATION OF THE METHOD OF RECOVERY OF THE INPUT SIGNAL FROM NOISY DATA

An estimation of the accuracy of the signal recovery method from noisy data based on the self-regularizing approach is presented. A transfer function with given initial conditions is presented. The numerical solution of the differential equation of the 2nd order is found, obtained from the transfer function after the inverse Laplace transformations, by passing to the finite-difference scheme. Computational experiments were carried out to restore the signal from noisy initial data, with different test signals and different noise levels, confirming the theoretical estimate of the method's accuracy.

Keywords: *signal recovery, data processing, finite difference scheme, self-regularizations.*

ВВЕДЕНИЕ

При работе со сложными объектами или технологическими процессами крайне важно корректно обработать информацию, оценить уровень достоверности результатов обработки, т.е. насколько точно полученная информация отображает реальное состояние системы. Разработка высокоточных средств измерения является важной составляющей в области ресурсосбережения.

Проблеме обработки зашумленных динамических сигналов посвящены работы многих исследователей, А.Л. Шестакова [1 – 3], В.А. Бесекерского [4], А.Ф Верлань [5], В.А Грановский.[6, 7], Г.Н Солопченко[10,11], Г.Н Солопченко [12], S. Engelberg[13], K. Ruhm

[14,15]. Как правило для уменьшения влияния шума в исходных данных на результаты измерений, добавляют дополнительные фильтры, что в свою очередь ведет к огрублению результатов и удорожанию технологического процесса.

Учитывая выше сказанное, возникает необходимость создания алгоритмов обработки зашумленных динамических измерений, не требующих значительной перенастройки параметров измерительной системы. При создании таких алгоритмов возникает проблема достоверности результатов этих методов.

1 ПОСТАНОВКА ЗАДАЧИ

Обработка результатов динамических измерений осуществляется исходя из модели измерительной системы без обратных связей:

Полагаем что передаточная функция датчика будет имеет следующий вид:

$$W(p) = \frac{b_0}{a_2 p^2 + a_1 p + a_0} = \frac{Y(p)}{U(p)} \qquad (1)$$

При построении модели используем следующие обозначения U(p) – входной сигнал датчика, Y(p) – выходной сигнал модели без обратных связей рис. 1. Построенная динамическая модель датчика, исключающую обратные связи, в которой проблема шумов решается настройкой параметра τ.

Основная идея метода исключения обратных связей заключается в следующем. На первом этапе осуществляют переход от передаточной функции (1) к дифференциальному уравнению, связывающему выходной сигнал $Y_\delta(t)$ с входным сигналом U(t). Далее, используя полученное уравнение, осуществляют численное моделирование функции $Y_M(t)$ по из-

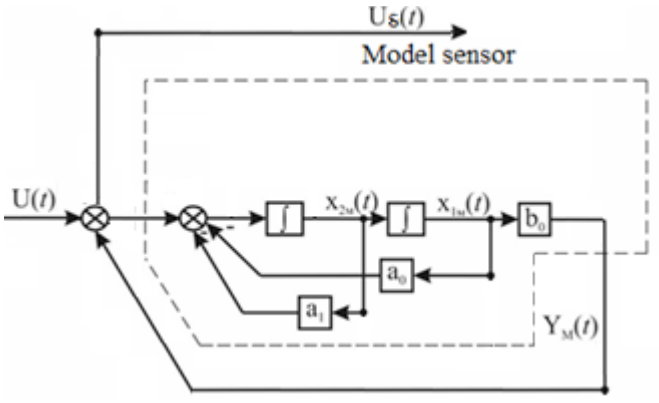


Рис. 1. Модель без обратных связей

U(t) – входной сигнал, $Y_M(t)$ – выходной сигнал модели, $U_\delta(t)$ – восстановленный сигнал, a_0, a_1, a_2, b_0 технические характеристики

вестному входному сигналу U(t). Затем оценивают отклонение $Y_M(t)$ от $Y_S(t)$. В случае, когда оценка отклонения не превышает некоторый заданный уровень точности, процесс исключения обратных связей считается успешным.

Перейдем от передаточной функции (1) к дифференциальному уравнению:

$$a_2 y'' + a_1 y' + a_0 y = b_0 u, \qquad (2)$$

Для вычисления значения выходного сигнала в момент времени , используем конечно-разностные соотношения. Тогда значения определяются по следующей явной схеме:

$$y_1 = r, \quad y_2 = \tau q + r \qquad (3)$$

$$y_{i+2} = (bu_i - \left(\frac{a_1}{\tau} - \frac{2a_2}{\tau^2}\right) y_{i+1} - \left(a_0 - \frac{a_1}{\tau} + \frac{a_2}{\tau^2}\right) y_i) \frac{\tau^2}{a_2}, \qquad (4)$$

2 ОЦЕНКА ПОГРЕШНОСТИ МЕТОДА ИСКЛЮЧЕНИЯ ОБРАТНЫХ СВЯЗЕЙ

С целью получения оценки погрешности метода относительно уровня шума в исходных данных, оценим величину отклонения численных значений v_{i+2} от действительных значений выходного сигнала y_{i+2}.

Пусть y_{i+2} – действительные значение выходного сигнала в момент времени t_{i+2}, а v_{i+2} – значения функции $Y_M(t_{i+2})$ в момент времени t_{i+2}. Оценим наибольшее уклонение величин v_{i+2}, соответствующих моделированному сигналу, полученному с помощью метода исключения обратных связей, от значений y_{i+2}, соответствующих действительному выходному сигналу. Для этого введем величины:

$$z_{i+2} = |v_{i+2} - y_{i+2}|$$

Из (6) получаем:

$$z_{i+2} = \left(2 - \frac{a_1 \tau}{a_2}\right) z_{i+1} + \left(\frac{a_1 \tau}{a_2} - \frac{a_0 \tau^2}{a_2} - 1\right) z_i$$

В силу того, что исходные данные известны с погрешностью, получаем

$$z_1 \le \delta,$$

$z_2 = |v_2 - y_2| \le \delta(1+\tau) + O(\tau) \le \delta(1+\tau) + C\tau$

Учитывая, что $z_{i+1} \ge z_i$, получаем следующую оценку

$$z_{i+2} \le \left|2 - \frac{a_1\tau}{a_2}\right| z_{i+1} + \left|\frac{a_1\tau}{a_2} - \frac{a_0\tau^2}{a_2} - 1\right| z_{i+1}$$

Обозначим $\mu = \left|2 - \frac{a_1\tau}{a_2}\right|$ и $\eta = \left|\frac{a_1\tau}{a_2} - \frac{a_0\tau^2}{a_2} - 1\right|$. Тогда

$$z_{i+2} \le (\mu + \eta) z_{i+1} + C\tau$$

Для обеспечения гарантированного уровня точности, необходимо подобрать так чтобы выполнялось следующее условие:

$$\mu + \eta \le 1 \qquad (5)$$

При выполнении условия (5), на N+1 шаге получим следующую оценку:

$$z_{N+1} \le (\mu+\eta)^N z_2 + \frac{1}{1-(\mu+\eta)} C\tau \le (\mu+\eta)^N \delta(1+\tau) + + \frac{1}{1-(\mu+\eta)} C\tau$$

С учетом условия $\mu + \eta < 1$, получаем следующую оценку

$$z_{N+1} \le \delta(1+\tau) + \frac{1}{1-(\mu+\eta)} C\tau \qquad (6)$$

Из (5), (6) получаем, что выбор параметра τ осуществляется, исходя из условий:

$$\frac{\tau}{1-(\mu+\eta)} < \delta \qquad (7)$$

Таким образом, при выполнении (5) – (7) гарантированно обеспечивается контролируемость величины динамической погрешности и достаточный уровень точности метода исключения обратных связей. При предлагаемом подходе осуществляется коррекция динамической погрешности, благодаря эффекту саморегуляризации, уровень шума остается на допустимом уровне.

3 ВЫЧИСЛИТЕЛНЫЙ ЭКСПЕРИМЕНТ

Основной целью вычислительного эксперимента являлось подтверждение теоретической оценки. В качестве входного сигнала модели u(t) использовались различные функции. В данной работе приведены результаты эксперимента для импульсного входного сигнала следующего вида:

$$u(t) = \begin{cases} 0, & t = 0 \\ 1, & t > 0 \end{cases}.$$

В эксперименте моделировали функцию $y_M(t)$ выходного сигнала выбирая величину параметра τ из условия (7). Далее моделировали функцию $y_\delta(t)$, добавляя к функции $y_M(t)$ аддитивный шум с уровнем 5%. Затем по зашумленному сигналу $y_\delta(t)$ восстанавливали входной сигнал $u_\delta(t)$ с помощью уравнений (4).

Численные значения параметров модели измерительной системы представлены в таблице 1.

В эксперименте интервал измерения

Таблица 1

Параметры модели

Порядок уравнения	Передаточная функция	Параметры
II	$\frac{1}{(T_1{}^2 p^2 + 2\xi_1 T_1 p + 1)}$	T1=0,1; ξ_1=0,3.

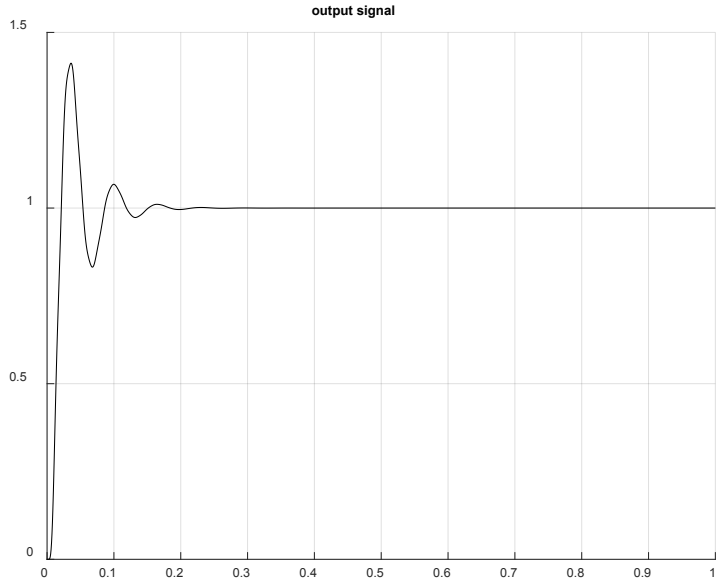


Рис. 2. Результаты моделирования выходного сигнал $Y_M(t)$

[0, Ω] составлял [0,1]. Выбор величины шага дискретизации является основополагающим для обеспечения требуемого уровня точности решения задачи динамического измерения.

На рис. 2 показан смоделированный выходной сигнал $Y_м(t)$ с параметром τ удовлетворяющим условие (9).

На рис. 3 представлена функция выходного сигнала модели без обратных связей $Y_м(t)$ с аддитивным шумом 5%.

Для восстановления входного сигнала $U_δ(t)$, к зашумленному выходном сигналу $Y_м(t)$ применялась конечно-разностное уравнение (10). На рис. 4 изображен восстановленный входной сигнал $U_δ(t)$.

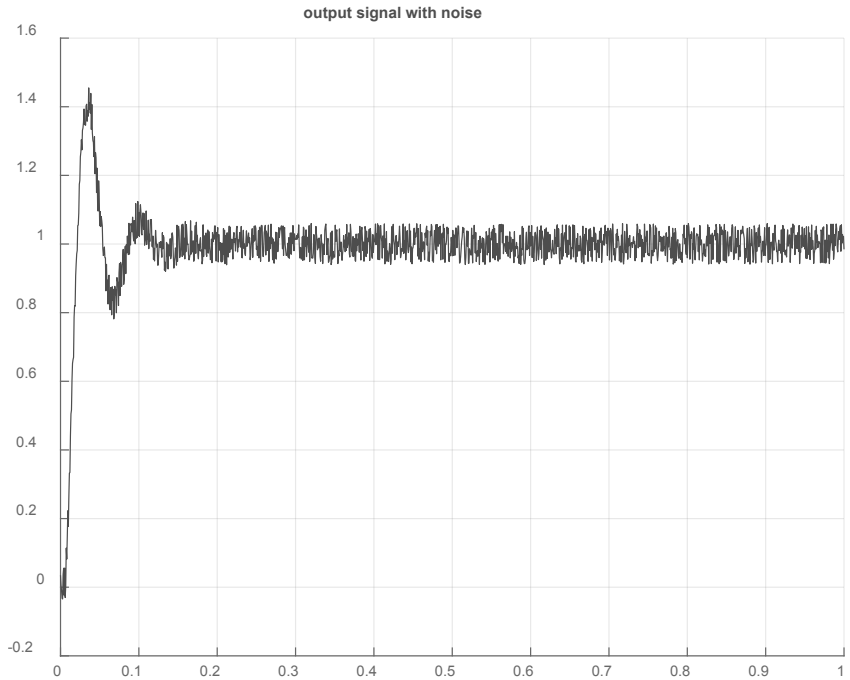


Рис. 3. Функция выходного сигнал $Y_м(t)$ с 5% аддитивным шумом

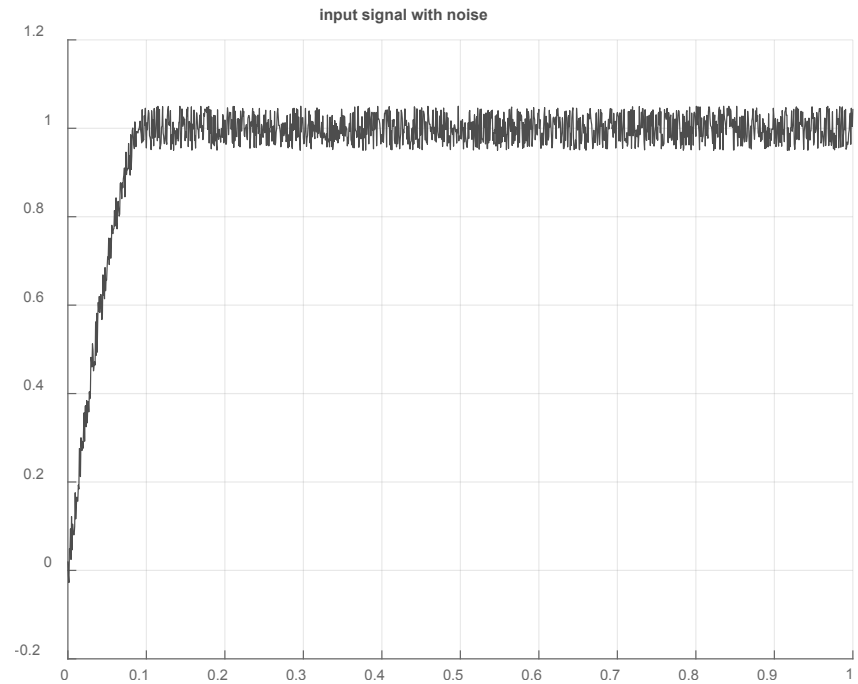


Рис. 4. Функция восстановленного входного сигнала $U_δ(t)$

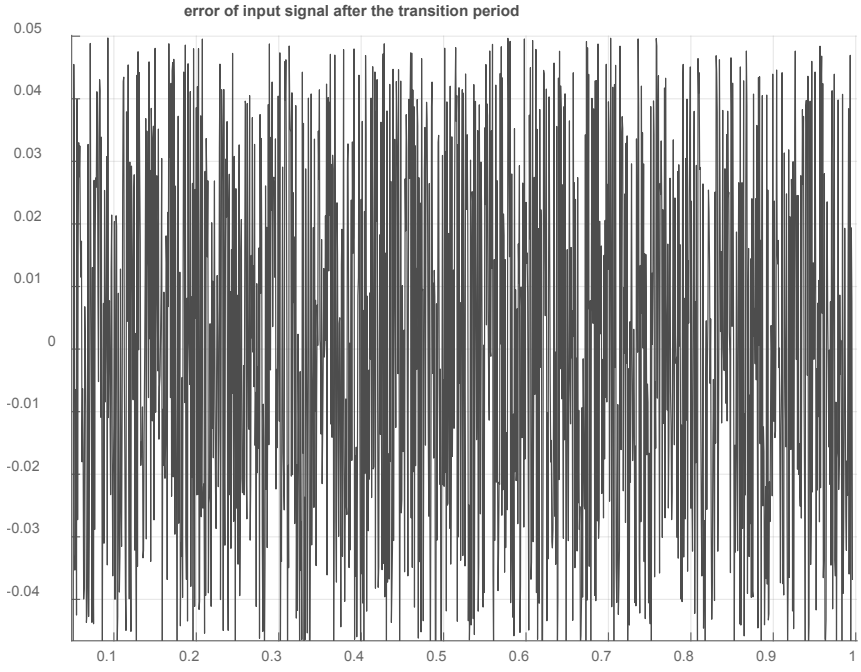


Рис. 5. Функция отклонение восстановленного сигнала $U_\delta(t)$ от исходного U(t)

Далее оценивалось отклонение восстановленного сигнала от входного сигнала модели $U_\delta(t_i)$ - $U(t_i)$. Отклонение восстановленного сигнала от исходного не превышала 0,05 (рис. 5).

Результаты экспериментов подтвердили теоретическую оценку. Метод восстановления входного сигнала позволяет восстанавливать входной сигнал с достаточным уровнем точности по зашумленному выходному сигналу.

ЗАКЛЮЧЕНИЕ

В статье предложена оценка метода восстановления входного сигнала по зашумленным данным. Основная идея методов заключается в том, что для уменьшения влияния шума исходных данных на результаты восстановления входного сигнала используется регуляризирующий алгоритм. В работе получена теоретическая оценка погрешности вычислительной схемы, установлена зависимость величины шага дискретизации от уровня шума и найдены соотношения, обеспечивающие устойчивость вычислительной схемы метода исключения обратных связей. На основе предложенных методов были проведены вычислительные эксперименты и выполнен сравнительный анализ результатов восстановления входного сигнала с тестовым сигналом. Результаты эксперимента подтвердили теоретическую оценку.

Исследование выполнено при финансовой поддержке Министерство образования и науки Челябинской области в рамках регионального гранта «Методы регуляризации при обработке зашумленных данных в многоканальных измерительных системах».

Литература

1. Шестаков А.Л. Методы теории автоматического управления в динамических измерениях. Челябинск: Издат. центр ЮУрГУ, 2013. 257 с.

2. Шестаков, А.Л. Нейросетевая динамическая модель измерительной системы с фильтрацией восстанавливаемого сигнала / А.Л. Шестаков, А.С. Волосников // Вестн. ЮжУрал. гос ун-та. Серия "Компьютерные технологии, управление, радиоэлектроника". –2006. – № 14 (69), вып. 4. – С. 16–20.

3. Шестаков А. Л., Свиридюк Г. А., "Новый подход к измерению динамически искаженных сигналов", Вестн. ЮУрГУ. Сер. Матем. моделирование и программирование, 2010, 5, 116–120.

4. Бесекерский В.А., Попов Е.П. Теория систем автоматического управления. — М.: Наука, 1975. — 768 с.

5. Верлань А.Ф., Сизиков В.С. Методы решения интегральных уравнений с программами для ЭВМ. — Киев: Наукова думка, 1978. — 291 с.

6. Грановский В.А., Этингер Ю.С. Методика определения динамических свойств средств измерений // Метрология. — 1974. — №10. — С.9-12.

7. Грановский В.А. Динамические измерения. — Л.: Энергоатомиздат, 1984. — 224 с.

8. Лаврентьев М.М., Романов В.Г., Шишатский С.П. Некорректные задачи математической физики и анализа. —: М.: Наука, 1980. — 285 с.

9. Леонов В.В. Метод понижения порядков номиналов передаточных функций// Измерительная техника.—1980.—№10.—С. 16-18.

10. Солопченко Г.Н. Определение параметров дробно-рациональной передаточной функции средств измерений по. экспериментальным данным // Метрология. — 1978. — №5. — С.20-24.

11. Солопченко Г.Н., Челпанов И. Б. Компенсация динамических погрешностей при неполных сведениях о свойствах приборов и измеряемых сигналов// Метрология.—1979—№6.—С. 3-13.

12. Солопченко Г.Н. Обратные задачи в измерительных процедурах// Измерения, контроль, автоматизация.—1983.—№2.—С.32-46.

13. S. Engelberg, "Tutorial 15: control theory, part I," in IEEE Instrumentation & Measurement Magazine, vol. 11, no. 3, pp. 34-40, June 2008, doi: 10.1109/MIM.2008.4534376.

14. K. Ruhm, Measurement plus observation – A new structure in metrologyr, Measurement, 2017, ISBN 0263-2241, DOI http://dx.doi.org/10.1016/j.measurement.2017.03.040, Band 126, Seiten 421-432

15. K. Ruhm, Dynamics and Stability – A Proposal for Related Terms in Metrology from a Mathematical Point of View, Measurement (Elsevier), 2015, London, Vereinigtes Königreich

References

1. Shestakov A.L. Metody teorii avtomaticheskogo upravleniya v dinamicheskikh izmereniyakh. Chelyabinsk: Izdat. tsentr YUUrGU, 2013. 257 s.

2. Shestakov, A.L. Neyrosetevaya dinamicheskaya model' izmeritel'noy sistemy s fil'tratsiyey vosstanavlivayemogo signala / A.L. Shestakov, A.S. Volosnikov // Vestn. YuzhUral. gos un-ta. Seriya "Komp'yuternyye tekhnologii, upravleniye, radioelektronika". –2006. – № 14 (69), vyp. 4. – S. 16–20.

3. Shestakov A. L., Sviridyuk G. A., "Novyy podkhod k izmereniyu dinamicheski iskazhennykh signalov", Vestn. YUUrGU. Ser. Matem. modelirovaniye i programmirovaniye, 2010, 5, 116–120.

4. Besekerskiy V.A., Popov Ye.P. Teoriya sistem avtomaticheskogo upravleniya. — M.: Nauka, 1975. — 768 s.

5. Verlan' A.F., Sizikov B.C. Metody resheniya integral'nykh uravneniy s programmami dlya EVM. — Kiyev: Naukova dumka, 1978. — 291 s.

6. Granovskiy V.A., Etinger YU.S. Metodika opredeleniya dinamicheskikh svoystv sredstv izmereniy // Metrologiya. — 1974. — №10. — S.9-12.

7. Granovskiy V.A. Dinamicheskiye izmereniya. — L.: Energoatomizdat, 1984. — 224 s.

8. Lavrent'yev M.M., Romanov V.G., Shishatskiy S.P. Nekorrektnyye zadachi matematicheskoy fiziki i analiza. —: M.: Nauka, 1980. — 285 s.

9. Leonov V.V. Metod ponizheniya poryadkov nominalov peredatochnykh funktsiy// Izmeritel'naya tekhnika. — 1980. — №10. — S. 16-18.

10. Solopchenko G.N. Opredeleniye parametrov drobno-ratsional'noy peredatochnoy funktsii sredstv izmereniy po. eksperimental'nym dannym // Metrologiya. — 1978. — №5. — S.20-24.

11. Solopchenko G.N., Chelpanov I. B. Kompensatsiya dinamicheskikh pogreshnostey pri nepolnykh svedeniyakh o svoystvakh priborov i izmeryayemykh signalov// Metrologiya. — 1979 — №6. — S. 3-13.

12. Solopchenko G.N. Obratnyye zadachi v izmeritel'nykh protsedurakh// Izmereniya, kontrol', avtomatizatsiya. — 1983. — №2. — S.32-46.

13. S. Engelberg, "Tutorial 15: control theory, part I," in IEEE Instrumentation & Measurement Magazine, vol. 11, no. 3, pp. 34-40, June 2008, doi: 10.1109/MIM.2008.4534376.

14. K. Ruhm, Measurement plus observation – A new structure in metrologyr, Measurement, 2017, ISBN 0263-2241, DOI http://dx.doi.org/10.1016/j.measurement.2017.03.040, Band 126, Seiten 421-432

15. K. Ruhm, Dynamics and Stability – A Proposal for Related Terms in Metrology from a Mathematical Point of View, Measurement (Elsevier), 2015, London, Vereinigtes Königreich.

ЯПАРОВ Дмитрий Данилович, аспирант кафедры математического обеспечения информационных технологий ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). 45080 г.Челябинск, пр. Ленина, д. 76. E-mail: iaparovdd@susu.ru

YAPAROV Dmitry Danilovich, post-graduate student of the Department of Mathematical Support of Information Technologies, SUSU. 45080 Chelyabinsk, Lenin Ave., 76. E-mail: iaparovdd@susu.ru

УДК 004.896 + 004.056.5 Вестник УрФО № 4(46) / 2022, с. 39–51

Рагозин А.Н., Плетенкова А.Д.

DOI: 10.14529/secur220405

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ПРОГНОЗИРОВАНИЯ ВРЕМЕННЫХ РЯДОВ ДАННЫХ В СИСТЕМАХ ОБНАРУЖЕНИЯ АНОМАЛИЙ В НАБЛЮДАЕМЫХ ПРОЦЕССАХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ[1]

Прогнозирование динамических временных рядов данных играет важную роль при построении систем обнаружения аномалий при защите информации в различных системах управления технологическими процессами (АСУ ТП). Для повышения точности прогнозирования динамических временных рядов данных применяется предварительная цифровая обработка (цифровая фильтрация) сигналов для разложения наблюдаемого временного ряда, поступающего с сенсоров АСУ ТП на отдельные компоненты. При таком подходе производится компонентное разложение и фильтрация исходного сигнала с использованием гребенки цифровых фильтров, что существенно повышает качество формируемого прогноза. Проведен анализ сигнала ошибки результата прогнозирования с использованием цифрового спектрального и биспектрального анализа. Показано, что для случая «идеального прогноза» сигнал ошибки предсказания является непредсказуемым остатком, то есть стремится к состоянию белого шума. В работе показано, что анализ ошибки прогноза с использованием методов цифрового спектрального и биспектрального анализа позволяет формировать оценку качества результата прогнозирования. Проведенное сравнение показывает существенное повышение эффективности использования предварительной цифровой фильтрации с це-

[1] Исследование поддержано грантом Российского научного фонда (проект № 22-71-10095).

лью повышения точности прогнозирования наблюдаемых динамических временных рядов данных АСУ ТП. Работа с нейронными сетями проводилась в пакете расширения MATLAB «Deep Learning Toolbox». Для спектрального и биспектрального анализа сигналов использовался пакет «Higher Order Spectral Analysis Toolbox».

Ключевые слова: *цифровая фильтрация, нейронная сеть, прогнозирование, спектральный анализ, биспектральный анализ, вертикальный сигнал, горизонтальный сигнал.*

Ragozin A.N., Pletenkova A.D.

THE APPLICATION OF DIGITAL SIGNAL PROCESSING TECHNOLOGY TO IMPROVE THE ACCURACY OF FORECASTING TIME SERIES DATA IN ANOMALY DETECTION SYSTEMS IN THE OBSERVED PROCESSES OF AUTOMATED PROCESS CONTROL SYSTEMS

Forecasting dynamic time series of data plays an important role in the construction of anomaly detection systems for information protection in various automated process control systems (APCS). To improve the accuracy of forecasting dynamic time series of data, preliminary digital processing (digital filtering) of signals is used to decompose the observed time series coming from the APCS sensors into separate components. With this approach, component decomposition and filtering of the original signal are performed using a digital filter comb, which significantly improves the quality of the generated forecast. The error signal of the prediction result was analyzed using digital spectral and bispectral analysis. It is shown that for the case of «perfect prediction» the prediction error signal is an unpredictable residual, that is, it tends to the state of white noise. The paper shows that the analysis of the forecast error using the methods of digital spectral and bispectral analysis makes it possible to form an assessment of the quality of the forecast result. The comparison shows a significant increase in the efficiency of using preliminary digital filtering to improve the accuracy of forecasting the observed dynamic time series of APCS data. Work with neural networks was carried out in the MATLAB «Deep Learning Toolbox» extension package. For spectral and bispectral analysis of signals, the «Higher Order Spectral Analysis Toolbox» package was used.

Keywords: *digital filtering, neural network, forecasting, spectral analysis, bispectral analysis, vertical signal, horizontal signal.*

Введение

Кибератаки, направленные на работу автоматизированных систем управления технологическими процессами (АСУ ТП), могут приводить к катастрофическим последствиям [1-3], поэтому актуальной является задача повышения точности обнаружения кибератак на АСУ ТП.Для обнаружения вторжений в АСУ ТП применяются нейронные сети и с их использованием процедура прогнозирования наблюдаемых сигналов [4-8]. Кибератаки вызывают аномалии (то есть, неожидаемое изменение) в поведении наблюдаемых процессов (в динамике временных рядов данных) при работе АСУ ТП. При построении прогноза нейросеть обучается при нормальной (без влияния дестабилизирующих воздействий) работе АСУ ТП. Детектирование (обнаружение) аномалий происходит в результате сравнения каждого отдельного временного ряда из наблюдаемого множества всех временных рядов, с каждым соответствующим прогнозом этого отдельного временного ряда из наблюдаемого множества всех временных рядов. При формировании аномалий в работе АСУ ТП будут происходить структурные изменения в сигнале ошибки формируемого прогноза, по обнаружению этих структурных изменений, собственно, происходит обнаружение аномалий в наблюдаемых процессах АСУ ТП. Очевидно, что качество (то есть, точная настройка) формирования прогноза наблюдаемого сигнала играет важную роль.

Метод предварительной цифровой фильтрации при формировании прогноза сигнала с использованием нейросетей ранее рассматривался в работах [9-11]. Применение метода предварительной цифровой фильтрации сигнала в задачах обнаружения аномалий рассматривалось в работах [12-13]. Другие методы обнаружения аномалий с использованием нейронных сетей рассмотрены в работах [14-18].

В работе исследуется влияние параметров блока предварительной цифровой фильтрации на качество получаемого прогноза.

Необходимо отметить, что построение обнаружителей аномалий наблюдаемых процессов можно рассматривать с позиции формирования компактного кластера наблюдаемых процессов «нормально» работающей АСУ ТП. Аномальным считается наблюдаемый процесс, выходящий за границы компактного кластера, сформированного при обучении нейронной сети построению прогноза в режиме нормально работающей АСУ ТП (без дестабилизирующих воздействий).

1. Этап предварительной цифровой обработки (фильтрации) наблюдаемых сигналов

Предлагаемый в исследовании подход заключается в предварительной подготовке данных наблюдаемого временного ряда с использованием технологии цифровой фильтрации. Предварительно подготовленные данные более помехозащищены, что существенно улучшает качество прогноза наблюдаемого временного ряда.

В работе исследуется влияние изменения значений параметров и структуры блока предварительной цифровой фильтрации на качество прогноза. Предлагаемый метод предварительной цифровой обработки прогнозируемого временного ряда заключается в прохождении сигнала через гребенку цифровых фильтров нижних частот (цифровые ФНЧ с конечными импульсными характеристиками (КИХ))) и в получении на выходе набора отфильтрованных компонентов исходного сигнала. Набор полученных компонентов сигнала с выхода гребенки ФНЧ назовем «вертикальным сигналом». То есть, «вертикальный сигнал», это многоканальный сигнал с выхода гребенки ФНЧ с последовательно уменьшающимися частотами среза их частотных характеристик. При таком подходе производится компонентное разложение исходного сигнала и последовательная фильтрация шумов с использованием параллельного набора цифровых ФНЧ. При этом исходный сигнал (до применения предварительной цифровой фильтрации), назовем горизонтальным входным сигналом.

Проведенное исследование является развитием направления, отраженного в более ранних работах [9-12] и заключающееся, именно в анализе влияния структуры и параметров блока предварительной цифровой фильтрации на качество прогноза исходного временного сигнала, а также в применении технологии цифрового спектрального и биспектрального анализа в оценке качества и точности получаемого прогноза.

Метод биспектрального анализа рассмотрен в обзорных работах [19,20].

2. Формирование прогноза наблюдаемого временного ряда

Рассмотрим входной анализируемый сиг-

нал. На рисунке 1 в качестве примера представлен сложный сигнал (временной ряд данных), отражающий протекающий процесс в технической системе. Временная ось представлена в отсчетах.

На рисунке 2 отражен участок временного ряда (рис. 1), который не будет задействован в обучении нейронной сети для формирования прогноза.

После выбора участка (рис.2) временного ряда данных для анализа формирования прогноза, оставшийся временной ряд (из рис.1) будет использован для обучения нейронной сети.

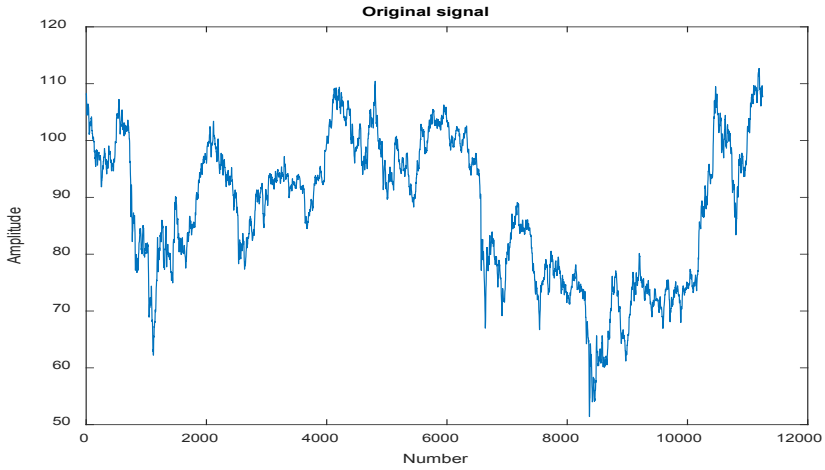


Рис. 1 Входной временной ряд

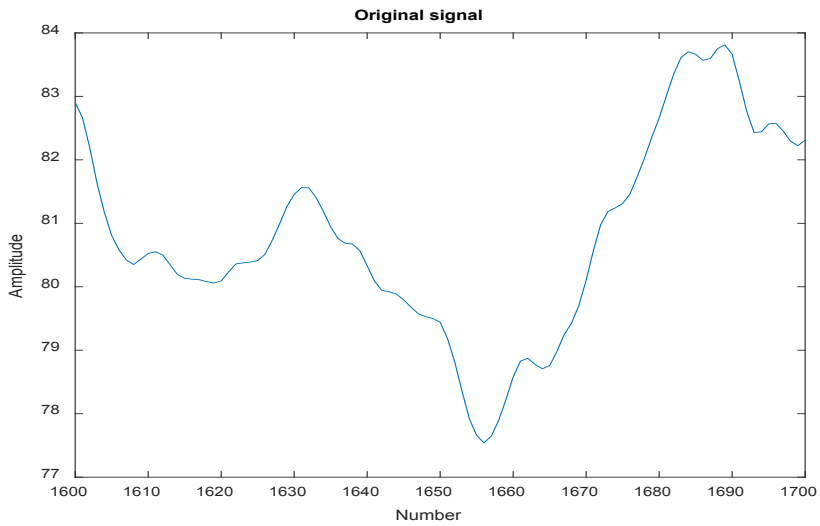


Рис. 2 Временной ряд данных для формирования прогноза

Результат предварительной цифровой фильтрации наблюдаемого временного ряда (рисунок 1) показан на рисунке 3 для участка исходного сигнала, отраженного на рисунке 2.

На рисунке 3 показан набор полученных компонентов временного ряда с выхода гребенки фильтров нижних частот (ФНЧ). После прохождения временного ряда через гребенку ФНЧ с конечными импульсными характеристиками (КИХ) получаем базовые компоненты данного временного ряда. В данном сравнении гребенка ФНЧ состоит из 31 КИХ-ФНЧ с последовательно уменьшающимися частотами среза их частотных характеристик.

В этом примере горизонтальным сигналом называется исходный сигнал (рис. 2), а вертикальным сигналом (длина вертикального сигнала равна 31 отсчету) является последовательный набор последнего временного отсчета каждой из 31 полученной компоненты с выхода гребенка ФНЧ из 31 КИХ-ФНЧ с последовательно уменьшающимися частотами среза их частотных характеристик.

При сравнении качества полученного

прогноза для варианта горизонтального или вертикального типов сигналов используется (показано на рисунке 4) двухслойная нейронная сеть с гиперболическими функциями активации в первом слое и линейной функцией активации во втором слое. Для машинного обучения использовалось 7000 точек анализируемого временного ряда в пропорции 60% - тренировка, 30% - проверка и 10% - тестирование. Размерность горизонтального и вертикального сигналов, подаваемых на вход нейронной сети одинаковая и равна 31 отсчету.

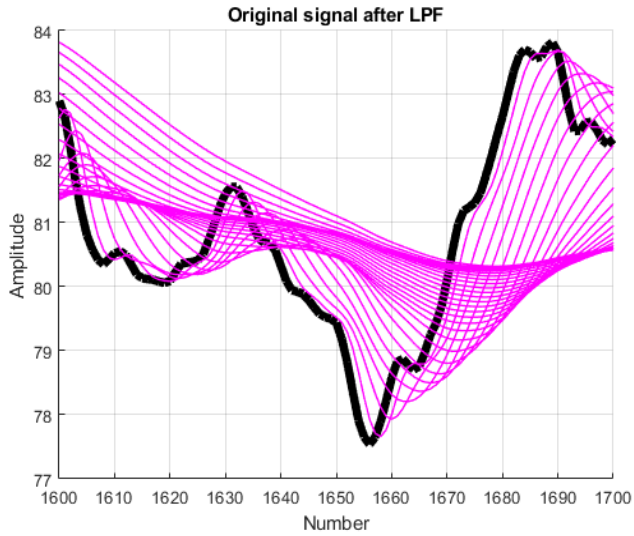


Рис. 3 Результат компонентного преобразования временного ряда данных для формирования прогноза

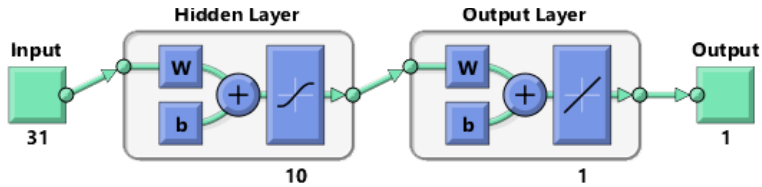


Рис. 4 Структура нейросетевого экстраполятора

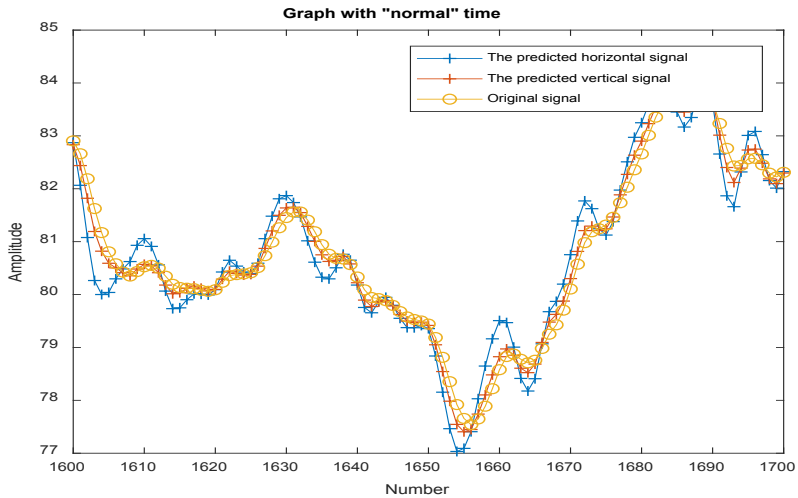


Рис. 5 Результат построения прогноза

3. Анализ результатов прогнозирования наблюдаемого временного ряда

Результат построения прогноза для вертикального сигнала и горизонтального сигнала отображен на рисунке 5, увеличенный участок результата отображен на рисунке 6. «Желтым» на рисунках 5 и 6 отображен исходный сигнал, то есть сигнал, который опережа-

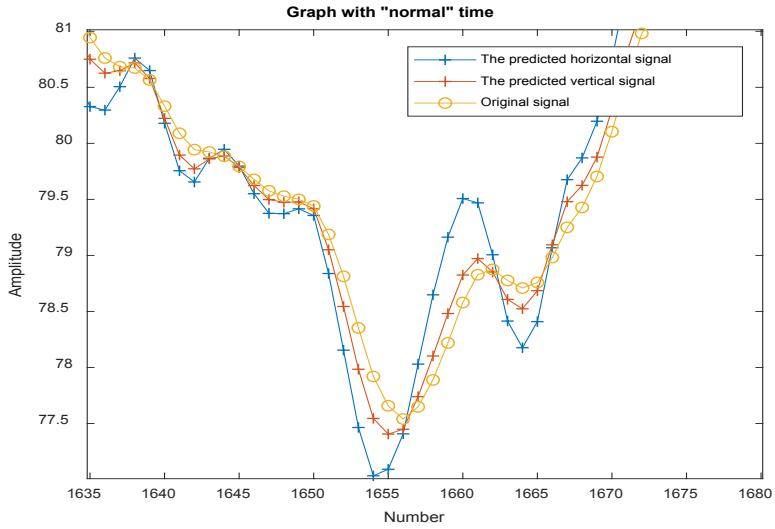


Рис. 6 Увеличенный участок результата построения прогноза (рис.5)

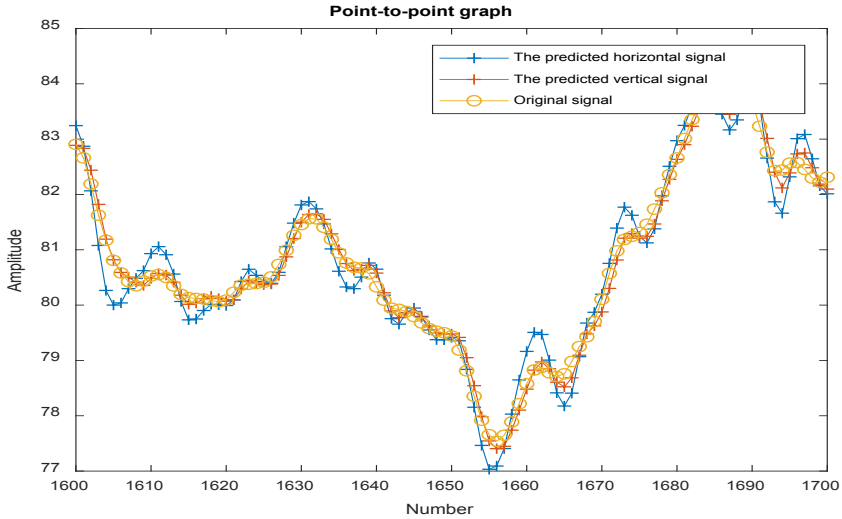


Рис. 7 Наложение прогноза на исходный временной ряд

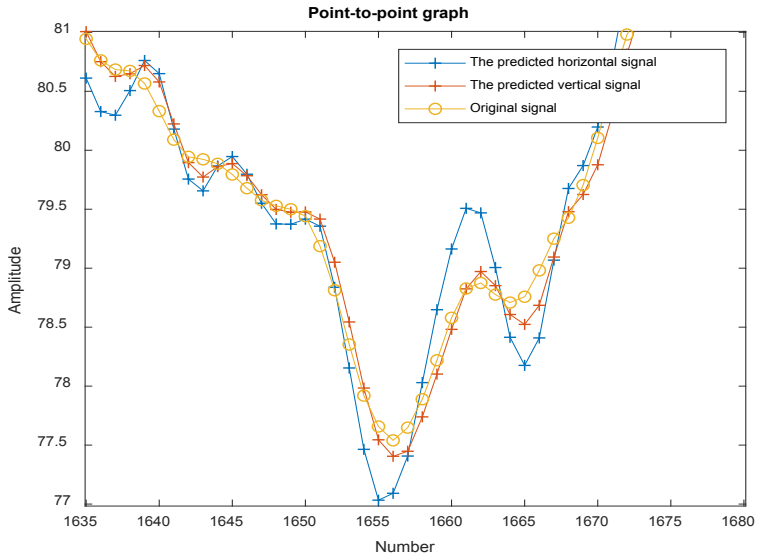


Рис. 8 Увеличение наложения прогноза на исходный временной ряд

ет сигналы прогнозов на один дискретный отсчет времени «вперед».

Результат построения прогноза для вертикального сигнала и горизонтального сигнала также, отображен на рисунке 7, увеличенный участок результата отображен на рисунке 8. В данном случае «жёлтым» на рисунках 7 и 8 отображен исходный «целевой» сигнал, то есть сигнал, к которому сигналы прогнозов должны стремиться, то есть в идеальном случае совпадать с ним.

Из графика на рисунке 6 и 8, а также, 5 и 7 видно, что метод прогнозирования при использовании вертикального сигнала (то есть, с использованием технологии предварительной цифровой фильтрации) имеет более высокое качество и точность прогнозирования.

4. Анализ результатов ошибки прогнозирования наблюдаемого временного ряда

В таблице 1 приведена сводка результатов прогнозирования для случая горизонтального сигнала (то есть, без применения предварительной фильтрации) и вертикального сигнала (то есть, с применением предварительной фильтрации). Ошибка прогнозирования оценивалась в виде зависимости значения СКО от длины (количества дискрет) горизонтального или вертикального сигналов, подаваемых на вход нейронной сети. По этому количеству дискрет реализуется прогноз на последующую одну точку (дискрет) этого сигнала. Результаты таблицы 1 отображены на рисунке 9.

Таблица 1

Численное сравнение СКО и процента ошибки спрогнозированного временного ряда

Значения СКО и процент ошибки на временном ряде данных для формирования прогноза			
Тип входного сигнала	Количество точек	СКО	Процент ошибки по сигналу
Вертикальный	121	0.1817	0.6793
Вертикальный	61	0.1834	0.7671
Вертикальный	31	0.182	0.7752
Вертикальный	16	0.1811	0.8936
Вертикальный	11	0.1807	0.7293
Вертикальный	8	0.1813	0.6798
Вертикальный	4	0.1815	0.8345
Вертикальный	2	0.1985	0.7584
Горизонтальный	121	0.2446	1.6737
Горизонтальный	61	0.2901	2.036
Горизонтальный	31	0.2776	1.9836
Горизонтальный	16	0.2732	2.1163
Горизонтальный	11	1.1362	9.4731
Горизонтальный	8	1.0859	9.3066
Горизонтальный	4	1.0578	9.3307
Горизонтальный	2	0.6074	5.1555

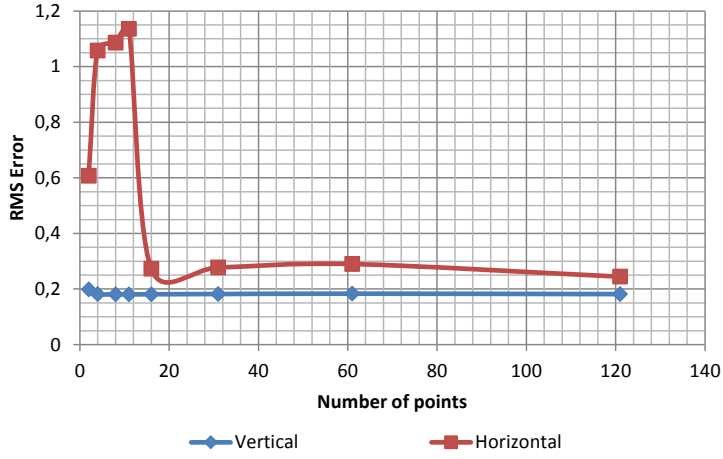


Рис. 9 График зависимости СКО от количества точек, использованных для предсказания

По результатам данных представленных на рисунках 8 и 9 видно, что качество прогноза существенно выше при использовании предложенного метода предварительной цифровой фильтрации, то есть при переходе от горизонтального сигнала к вертикальному сигналу фактически при любой размерности (длине) прогнозируемых сигналов.

Проведем спектральный анализ сигнала ошибки результатов прогнозирования, что дает возможность получить данные о том, какие ошибки предсказания преобладают при той или иной структуре подаваемого на нейросеть сигнала.

На рисунках 10 и 11 приведены результаты спектрального анализа для случая горизонтального и вертикального сигналов соответственно. Размерность (длина) сигналов, подаваемых на вход нейронной сети равна 31. Ось частот на графиках рисунков 10 и 11 отображена в нормированных частотах [Рад.].

Сравнивая спектры сигналов ошибки

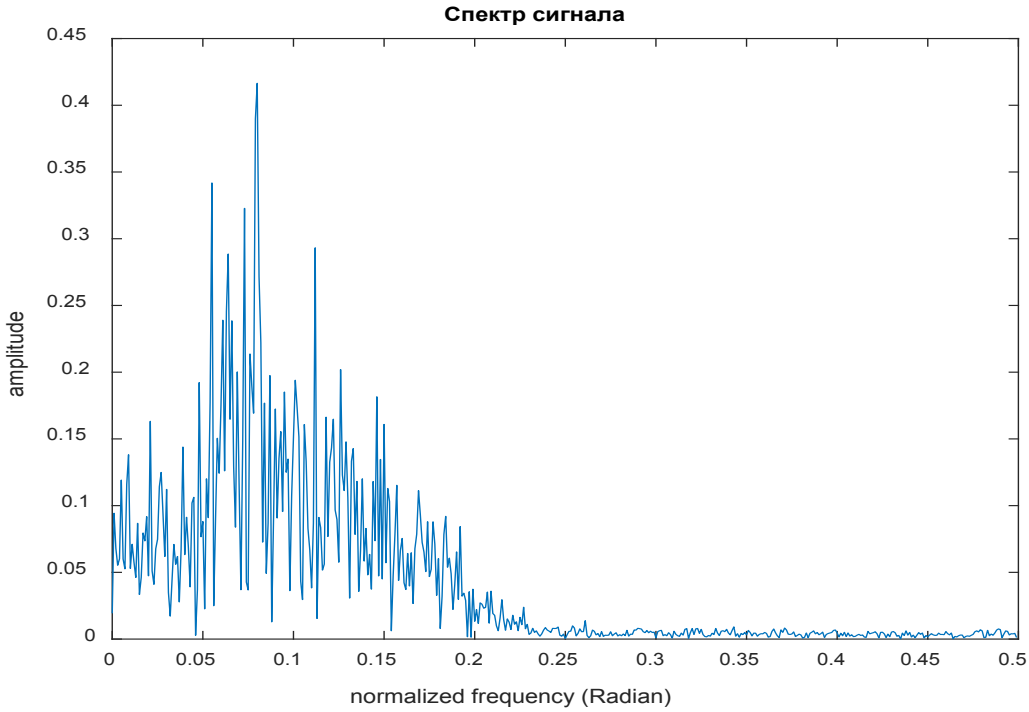


Рис. 10 Спектр ошибки прогнозирования временного ряда горизонтального сигнала

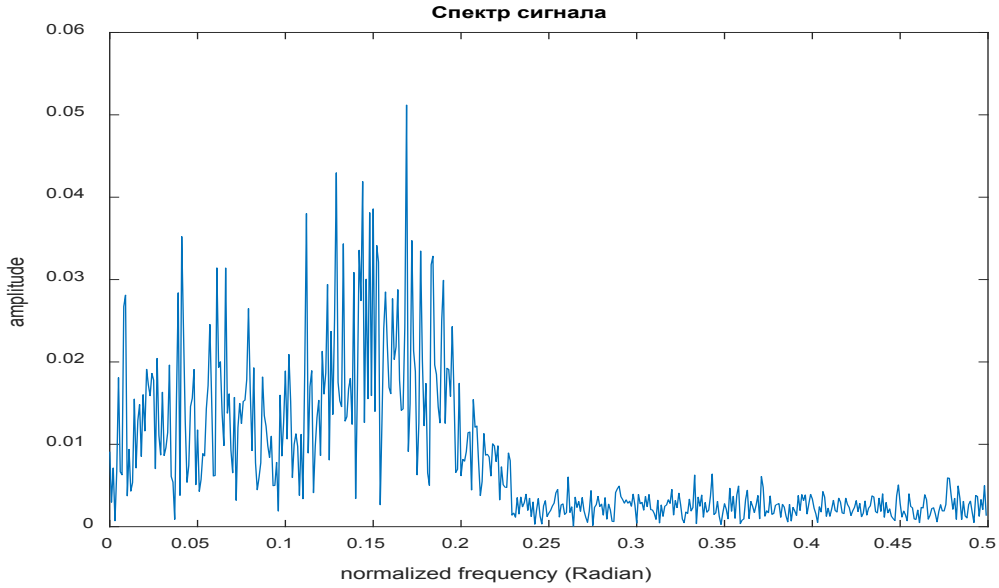


Рис. 11 Спектр ошибки прогнозирования временного ряда вертикального сигнала

прогноза на рисунках 10 и 11, можно отметить, что в случае с сигналом ошибки вертикального сигнала амплитуда спектра гораздо меньше. В спектре ошибки горизонтального сигнала (рис.10) помимо гармоник, появляющихся в спектре ошибки вертикального сигнала, выражены более низкочастотные составляющие, что свидетельствует об ухудшении динамических характеристик предиктора, формирующего прогноз без использования технологии предварительной цифровой фильтрации.

На рисунках 12–15 представлены результаты биспектрального анализа сигнала ошибки прогноза. Биспектральный анализ позволяет определить отклонение сигнала ошибок от распределения по «нормальному закону». Также, биспектральный анализ отображает нелинейные взаимодействия гармоник, присутствующих в спектре сигнала ошибки прогноза.

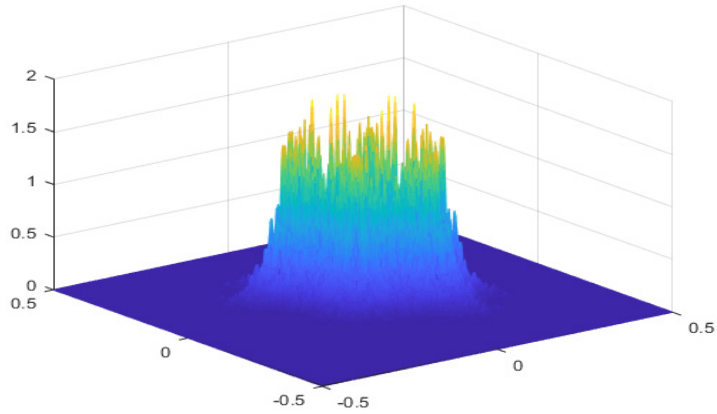


Рис. 12 Трехмерное представление биспектра сигнала ошибки прогнозирования горизонтального временного ряда

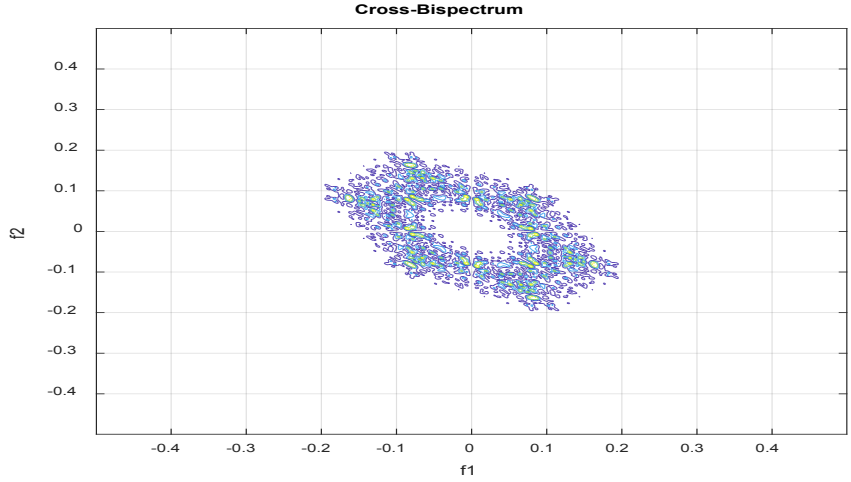


Рис. 13 Вид биспектра сигнала ошибки прогнозирования горизонтального временного ряда в горизонтальном разрезе

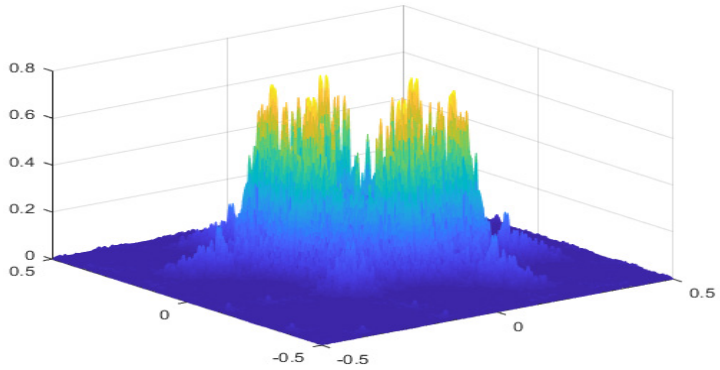


Рис. 14 Трехмерное представление биспектра сигнала ошибки прогнозирования вертикального сигнала

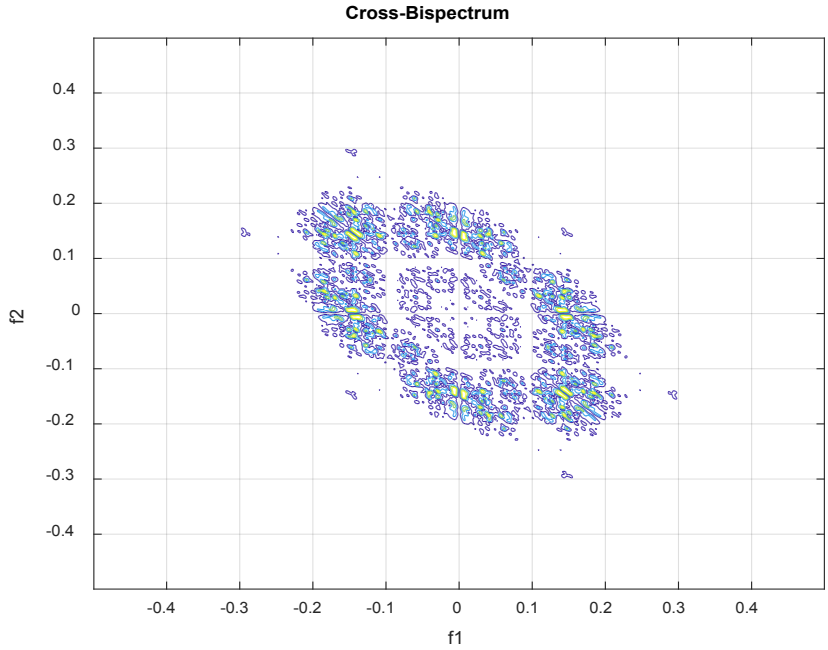


Рис. 15 Вид биспектра сигнала ошибки прогнозирования вертикального временного ряда в горизонтальном разрезе

При сравнении рисунков 12 и 14 видно, что во временном ряде сигнала ошибки для случая горизонтального сигнала нелинейная связь между гармоническими составляющими выражена в большей степени (более высокий уровень амплитуды биспектра). Это связано с тем, что при прогнозировании для случая горизонтального сигнала, в точках перегиба прогнозируемого временного ряда возникают выраженные локальные переходные процессы в работе предиктора, что существенно снижает его динамические характеристики. Предиктор, работающий в режиме «вертикального сигнала», не имеет такого выраженного недостатка.

При сравнении рисунков 12 и 14, а также рисунков 13 и 15 (вид «сверху», горизонтальный срез) видно, что биспектр сигнала ошибки предиктора, работающего в режиме «вертикального сигнала» имеет более низкий уровень, а также занимает более широкую полосу частот, что свидетельствует, также что сигнал ошибки прогнозирования в режиме «вертикального сигнала» более близок по своей структуре к «гауссовскому шуму», что также свидетельствует о более высоком качестве прогноза.

Заключение

При формировании аномалий в работе АСУ ТП будут происходить структурные изменения в сигнале ошибки формируемого прогноза, по обнаружению этих структурных изменений, собственно, происходит обнаружение аномалий в наблюдаемых процессах АСУ ТП. Очевидно, что качество (то есть, точная настройка) формирования прогноза наблюдаемого сигнала играет важную роль.

В спектре сигнала ошибки предиктора в режиме горизонтального сигнала помимо гармоник, появляющихся в спектре сигнала ошибки предиктора в режиме вертикального сигнала, выражены, также более низкочастотные составляющие, что свидетельствует об ухудшении динамических характеристик предиктора, формирующего прогноз без использования технологии предварительной цифровой фильтрации.

При прогнозировании для случая горизонтального сигнала (то есть, без предварительной цифровой фильтрации), в точках перегиба прогнозируемого временного ряда возникают выраженные локальные переходные процессы в работе предиктора, что существенно снижает его динамические характеристики и точность настройки прогноза. Предиктор, работающий в режиме вертикального сигнала, не имеет такого выраженного недостатка.

Качество формируемого прогноза существенно выше при использовании предложенного метода предварительной цифровой фильтрации, то есть при переходе от горизонтального сигнала к вертикальному сигналу фактически при любой размерности (длине) прогнозируемых сигналов.

Литература

1. Falliere, N., Murchu, L. O., &Chien, E. (2011). W32. Stuxnet Dossier Version 1.4. Symantec Security Response.

2. Lee, R., Assante, M., &Connway, T. (2014). ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper–German steel mill cyber attack. Sans ICS.

3. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems, 23.

4. Xiao, Y. J., Xu, W. Y., Jia, Z. H., Ma, Z. R., & Qi, D. L. (2017). NIPAD: a Non-Invasive Power-Based Anomaly Detection Scheme for Programmable Logic Controllers. Frontiers of Information Technology & Electronic Engineering, 18(4), 519-534.

5. Wang, W., Xie, Y., Ren, L., Zhu, X., Chang, R., & Yin, Q. (2018, May). Detection of Data Injection Attack in Industrial Control System Using Long Short Term Memory Recurrent Neural Network. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 2710-2715). IEEE.

6. Kravchik, M., & Shabtai, A. (2018, October). Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 72-83). ACM.

7. Filonov, P., Kitashov, F., &Lavrentyev, A. (2017). RNN-Based Early Cyber-Attack Detection for the Tennessee Eastman Process. arXiv preprint arXiv:1709.02232.

8. Filonov, P., Lavrentyev, A., &Vorontsov, A. (2016). Multivariate Industrial Time Series with Cyber-Attack Simulation: Fault Detection Using an Lstm-Based Predictive Data Model. arXiv preprint arXiv:1612.06676.

9. A. Ragozin, V.Telezhkin, P.Podkorytov. Prediction of Aggregate Multicomponent Time Series in Industrial Automated Systems Using Neural Network, Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2019, 13-15 March, 2019, Hong Kong, pp 17-19.

10. A.N. Ragozin, A.A. Razumov. Neural Networks Forecasting with Preliminary Digital Filtering of Complex Radio Signals: The Physics and Technology of Wave Processes 2018, September 10 – 14, 2018, Miass, pp. 37-38.

11. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov. State Prediction in Control Systems via Compound Time Series: Neural Network Approach. EEE SoutheastCon 2019 Von Braun Center Huntsville, Alabama April 11th-14th, 2019. Pages 1–6.

12. A.N. Ragozin, V.F. Telezhkin, P. S. Podkorytov. Forecasting Complex Multi-Component Time Series within Systems Designed to Detect Anomalies in Dataflows of Industrial Automated Systems. SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks September 2019 Article No.: 2 Pages 1–5.

13. Alexander N. Sokolov, Andrey N. Ragozin, Ilya A. Pyatnitsky, Sergei K. Alabugin, Applying of Digital Signal Processing Techniques to Improve the Performance of Machine Learning-Based Cyber Attack Detection in Industrial Control System. SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks September 2019 Article No.: 23 Pages 1–4.

14. Muna, A. H., Moustafa, N., &Sitnikova, E. (2018). Identification of Malicious Activities in Industrial Internet of Things Based on Deep Learning Models. Journal of Information Security and Applications, 41, 1-11.

15. Potluri, S., Diedrich, C., &Sangala, G. K. R. (2017, September). Identifying False Data Injection Attacks in Industrial Control Systems Using Artificial Neural Networks. In 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-8). IEEE.

16. Yang, H., Chen, T., Guo, X., Wang, X., & Li, F. (2017, December). Research on Intrusion Detection of Industrial Control System Based on OPSO-BPNN Algorithm. In 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 957-961). IEEE.

17. Demertzis, K., Iliadis, L., &Spartalis, S. (2017, August). A Spiking One-Class Anomaly Detection Framework for Cyber-Security on Industrial Control Systems. In International Conference on Engineering Applications of Neural Networks (pp. 122-134). Springer, Cham.

18. Wu, Z., Albalawi, F., Zhang, J., Zhang, Z., Durand, H., &Christofides, P. (2018). Detecting and Handling Cyber-attacks in Model Predictive Control of Chemical Processes. Mathematics, 6(10), 173.

19. Ch.L. Nikias, A.P. Petropulu Higher-Order Spectral Analysis, PTR Prentice Hall, Englewood Cliffs NJ, 1993.

20. Nikias C.L., Raghuveer M.R. Bispektral Estimation: a Digital Signal Processing Framework // Proceedings of the IEEE. 1987. V. 75. p. 869-891.

References

1. Falliere, N., Murchu, L. O., &Chien, E. (2011). W32. Stuxnet Dossier Version 1.4. Symantec Security Response.

2. Lee, R., Assante, M., &Connway, T. (2014). ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper–German steel mill cyber attack. Sans ICS.

3. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems, 23.

4. Xiao, Y. J., Xu, W. Y., Jia, Z. H., Ma, Z. R., & Qi, D. L. (2017). NIPAD: a Non-Invasive Power-Based Anomaly Detection Scheme for Programmable Logic Controllers. Frontiers of Information Technology & Electronic Engineering, 18(4), 519-534.

5. Wang, W., Xie, Y., Ren, L., Zhu, X., Chang, R., & Yin, Q. (2018, May). Detection of Data Injection Attack in Industrial Control System Using Long Short Term Memory Recurrent Neural Network. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 2710-2715). IEEE.

6. Kravchik, M., & Shabtai, A. (2018, October). Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 72-83). ACM.

7. Filonov, P., Kitashov, F., &Lavrentyev, A. (2017). RNN-Based Early Cyber-Attack Detection for the Tennessee Eastman Process. arXiv preprint arXiv:1709.02232.

8. Filonov, P., Lavrentyev, A., &Vorontsov, A. (2016). Multivariate Industrial Time Series with Cyber-Attack Simulation: Fault Detection Using an Lstm-Based Predictive Data Model. arXiv preprint arXiv:1612.06676.

9. A. Ragozin, V.Telezhkin, P.Podkorytov. Prediction of Aggregate Multicomponent Time Series in Industrial Automated Systems Using Neural Network, Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2019, 13-15 March, 2019, Hong Kong, pp 17-19.

10. A.N. Ragozin, A.A. Razumov. Neural Networks Forecasting with Preliminary Digital Filtering of Complex Radio Signals: The Physics and Technology of Wave Processes 2018, September 10 – 14, 2018, Miass, pp. 37-38.

11. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov. State Prediction in Control Systems via Compound Time Series: Neural Network Approach. EEE SoutheastCon 2019 Von Braun Center Huntsville, Alabama April 11th-14th, 2019. Pages 1–6.

12. A.N. Ragozin, V.F. Telezhkin, P. S. Podkorytov. Forecasting Complex Multi-Component Time Series within Systems Designed to Detect Anomalies in Dataflows of Industrial Automated Systems. SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks September 2019 Article No.: 2 Pages 1–5.

13. Alexander N. Sokolov, Andrey N. Ragozin, Ilya A. Pyatnitsky, Sergei K. Alabugin, Applying of Digital Signal Processing Techniques to Improve the Performance of Machine Learning-Based Cyber Attack Detection in Industrial Control System. SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks September 2019 Article No.: 23 Pages 1–4.

14. Muna, A. H., Moustafa, N., &Sitnikova, E. (2018). Identification of Malicious Activities in Industrial Internet of Things Based on Deep Learning Models. Journal of Information Security and Applications, 41, 1-11.

15. Potluri, S., Diedrich, C., &Sangala, G. K. R. (2017, September). Identifying False Data Injection Attacks in Industrial Control Systems Using Artificial Neural Networks. In 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-8). IEEE.

16. Yang, H., Chen, T., Guo, X., Wang, X., & Li, F. (2017, December). Research on Intrusion Detection of Industrial Control System Based on OPSO-BPNN Algorithm. In 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 957-961). IEEE.

17. Demertzis, K., Iliadis, L., &Spartalis, S. (2017, August). A Spiking One-Class Anomaly Detection Framework for Cyber-Security on Industrial Control Systems. In International Conference on Engineering Applications of Neural Networks (pp. 122-134). Springer, Cham.

18. Wu, Z., Albalawi, F., Zhang, J., Zhang, Z., Durand, H., &Christofides, P. (2018). Detecting and Handling Cyber-attacks in Model Predictive Control of Chemical Processes. Mathematics, 6(10), 173.

19. Ch.L. Nikias, A.P. Petropulu Higher-Order Spectral Analysis, PTR Prentice Hall, Englewood Cliffs NJ, 1993.

20. Nikias C.L., Raghuveer M.R. Bispektral Estimation: a Digital Signal Processing Framework // Proceedings of the IEEE. 1987. V. 75. p. 869-891.

РАГОЗИН Андрей Николаевич, кандидат технических наук, доцент кафедры защиты информации, доцент кафедры инфокоммуникационных технологий высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). Россия, 454080, г. Челябинск, пр. Ленина, 76. E-mail: ragozinan@susu.ru

ПЛЕТЕНКОВА Анастасия Дмитриевна, аспирант кафедры защита информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, E-mail: pletenkovaad@susu.ru

RAGOZIN Andrey Nikolaevich, Candidate of Sciences in Technology, Department of Information Security, Department of Information Technology, Federal State Autonomous Educational Institution of Higher Education «South Ural State University» (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: ragozinan@susu.ru

PLETENKOVA Anastasia Dmitrievna, post-graduate student of the Information Security Department, Federal State Autonomous Educational Institution of Higher Education «South Ural State University» (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: pletenkovaad@susu.ru

УДК 004.942 + 519.157 Вестник УрФО № 4(46) / 2022, с. 52–57

Бердюгин В.Ю., Аверьянов А.А., Шадрив В.В.

DOI: 10.14529/secur220406

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ УГРОЗ ФИЗИЧЕСКОГО ПРОНИКНОВЕНИЯ ЗЛОУМЫШЛЕННИКА НА ЗАЩИЩЕННЫЙ ОБЪЕКТ

Для современных объектов информатизации одной из наиболее актуальных проблем является повышение эффективности или создание эффективной защиты от угроз, связанных с неправомерным физическим доступом к защищаемым информационным объектам. При этом возникает потребность в объективной оценке как вероятности реализации подобных угроз, так и эффективности организационных и инженерно-технических средств их реализации. В работе представлен результат разработки математической модели, на основе которой возможно решение перечисленных задач.

Ключевые слова: *математическое моделирование, информационная безопасность, дискретная математика, система безопасности, инженерно-техническая защита информации, оценка защищенности, объект информатизации.*

Berdugin V.U., Averyanov A.A., Shadriv V.V.

MATHEMATICAL MODEL FOR ASSESSING THREATS OF PHYSICAL INTRUSION OF AN INTRUDER INTO A PROTECTED OBJECT

For modern informatization objects, one of the most pressing problems is to increase the efficiency or create effective protection against threats associated with unlawful physical access to protected information objects. At the same time, there is a need for an objective assessment of both the likelihood of such threats and the effectiveness of organizational and engi-

neering means of their implementation. The paper presents the result of the development of a mathematical model, on the basis of which it is possible to solve the listed problems.

Keywords: *mathematical modeling, information security, discrete mathematics, security system, engineering and technical protection, security assessment, information object.*

Ввиду разнообразия и уникальности каждого объекта, на котором обрабатывается защищаемая информация, разработка системы физической защиты является трудоемким процессом, в котором для каждого объекта требуется индивидуальный подход. Создание системы защиты требует значительного количества ресурсов, но не всегда эти ресурсы расходуются эффективно [1]. Под «защищаемым» объектом будем понимать объект, обладающий определенной степенью защищенности и нуждающийся в модернизации защиты, а также оптимизации ресурсов, затрачиваемых на защиту.

Согласно пункту 2.4 Методики оценки угроз безопасности информации, утвержденной ФСТЭК России 5 февраля 2021 года [2] (далее – Методика) оценка угроз безопасности информации должна носить систематический характер и осуществляться как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии и модернизации систем. По результатам такой оценки должны быть выявлены актуальные угрозы, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах информации и (или) к нарушению, прекращению функционирования этих систем. Систематический подход к оценке угроз безопасности информации позволит поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов систем [2].

Оценка угроз проводится на всех этапах разработки систем защиты объектов. На этапе создания систем результаты оценки угроз безопасности информации должны быть направлены на обоснование выбора организационных и технических мер по защите информации (обеспечению безопасности), а также на выбор средств защиты информации и их функциональных возможностей [2]. При этом на этапе эксплуатации систем защиты в результате оценки могут быть найдены дополнительные угрозы безопасности. В этом случае по ним должны быть предложены обоснованные меры по улучшению или созданию систем защиты. Обобщая вышесказанное, можно сделать вывод о том, что для обеспечения высокого уровня безопасности информации нужно постоянно и в полном объеме проводить мероприятия по оценке и улучшению систем безопасности.

В связи с необходимостью постоянного проведения оценки безопасности на разных объектах, особый интерес представляют программные решения, эффективно моделирующие и рассчитывающие возможные пути проникновения, а также способы их устранения и решения, уменьшающие или полностью исключающие влияние человеческого фактора на расчёт защищенности объекта. Нормативные акты так же не противоречат использованию данных решений: пункт 2.9 Методики разрешает при оценке угроз безопасности использовать программные средства, позволяющие автоматизировать данную деятельность.

Исследование и моделирование систем физической защиты широко представлено в работах как отечественных, так и зарубежных ученых. Так, М.Гарсия в своей работе по проектированию и оценке систем физической защиты рассмотрел подходы к проектированию, анализу и оценке систем физической защиты [3], уделил большое внимание разным типам внешних и внутренних датчиков, средств связи, приборам, применяемым для обнаружения оружия, наркотических и взрывчатых веществ, и др. А.С. Боровский в своей работе [4] представил собственный метод обоснования требований (показателей качества) к системам физической защиты, разработал модифицированный алгоритм Дейкстры для поиска наименее защищенного пути с использованием нечетких чисел и т.д. И.М. Янников представил структурную схему интеллектуальной интегрированной системы безопасности критически важных и потенциально опасных объектов [5]. А.Д. Тарасов в 2017 году спроектировал систему физической защиты с использованием адаптивного генетического алгоритма [6], который содержит в себе алгоритм для расчета безопасности территории объекта. В 2019 году А.Д. Япаров предложил алгоритм имитационного мо-

делирования угрозы физического доступа к значимому объекту критической информационной инфраструктуры [7].

Однако, по нашему мнению, перечисленные выше модели и прилагающиеся к ним программные решения либо применимы только на стадии тестирования систем физической защиты, либо не обладают достаточной гибкостью. Ситуация усугубляется отсутствием нормативной базы для определения и стандартизации систем физической защиты информации [8].

Задачей представленной работы является создание модели, учитывающей варианты проникновения злоумышленника на защищаемые объекты с целью повышения эффективности систем защиты.

Предлагаемая модель учитывает все возможные пути проникновения со стороны злоумышленника, так как в реальности невозможно оценить какой информацией, навыками и знаниями обладает злоумышленник, проникающий на объект (далее – нарушитель), а также учесть все средства получения доступа к информации о защищенном объекте. Для построения общей модели нарушителя определены следующие условия:

• нарушителю известна подробная информацию об объекте, план здания со всеми средствами защиты;

• нарушитель использует все возможные технические средства проникновения на объект;

• нарушитель стремится оптимизировать свой путь проникновения на объект.

При этом модель защищаемого объекта представлена в виде расширенного мультиграфа, что позволяет учитывать дополнительную информацию, в частности, замки для ребер, ключи и ценность информации для вершин. Вершиной такого графа являются определенные позиции внутри защищаемого объекта. Ребро же – путь перехода нарушителя от одной вершины в другую. Например, в случае, если принять вершину за комнату, то ребрами будут являться коридоры, по которым можно перейти в эту комнату. На рис. 1 представлен пример используемого графа.

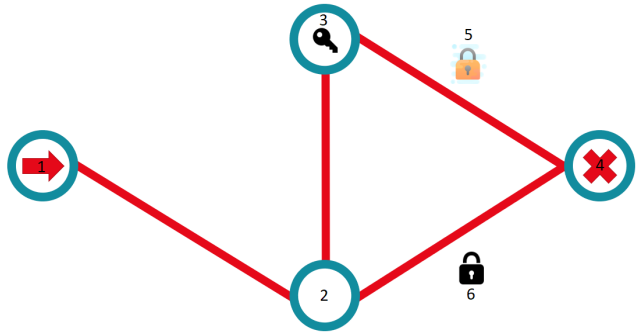


Рис. 1. Пример графа с моделью «ключи-замки»

Разработанная модель подразумевает использование устройств физической защиты, требующих наличия «ключа» для последующего доступа. При этом подразумевается, что замки устанавливаются как средство защиты от физического проникновения и к каждому ключу есть замок (но не к каждому замку есть ключ). На рис. 1 расположены два замка: 5 и 6 на переходах из вершин 3 и 2 в 4 соответственно. Ключ, расположенный в вершине 3 подходит только для замка 6. Если у нарушителя нет ключа от замка, он должен приложить некоторые усилия для преодоления данного замка. Под замком может подразумеваться не только устройство, закрывающее двери: как замок можно рассматривать, например, охранника – он будет замком без ключа (как, например, замок 5 на рис. 1). Нарушителю необходимо будет приложить определенные усилия для преодоления замка. На рис. 1 точка проникновения нарушителя на объект обозначена цифрой 1, целевая точка – цифрой 4. После попадания нарушителя в вершину 1 у него есть только один путь, после перехода по нему в вершину 2 у него появляется выбор: он может взломать замок 6 (т.е. затратить определенное количество усилий), или же перейти в вершину 3, взять ключ и, вернувшись в 2, открыть замок 6 и проникнуть в целевую вершину 4. Нарушитель так же может перейти в вершину 3 и попытаться взломать замок 5 и пройти в вершину 4. В конечном итоге мы имеем полный набор возможных путей проникновения нарушителя и понимание того, какой из путей требуется защитить. Таким образом, можно

представить и распределить практически любые меры защиты и создать систему физической защиты высокого уровня.

Сформулируем задачу математически. Пусть некоторый объект имеет некоторое множество путейпроникновения к конечной точке (защищаемой информации, например: серверу). Если к конечной точке нет путей проникновения, то задача является бессмысленной, поскольку нарушитель не может проникнуть к защищаемой информации каким-либо способом, то есть, считаем, что множество не пусто.

Далее определим некоторое подконтрольное множество ребер, которое не является пустым, поскольку если на текущую ситуацию повлиять невозможно, то задача является бессмысленной.

Для учета имеющихся у заказчика ресурсов для физической защиты информации – финансов и технического обеспечения, которые могут быть использованы или используются при защите, введена величина «капитал защиты» X. Пусть S – это множество распределений X. Таким образом, имеется множество вариантов распределения X на конечное множествор E. При этом, если есть хотя бы одно подконтрольное ребро, то имеется хотя бы один вариант распределения капитала защиты: S ≠ ∅.

Также, для каждого пути p из множества всех путей p ∈ P определим множество подконтрольных ребер, которые в него входят $E' \subseteq E$. Оно не может являться пустым, поскольку если нарушитель имеет способ получения информации, не подконтрольный нам, то задача является бессмысленной. В итоге получим выражение:

$$e(p) = E', \quad (1)$$

где $p \in P$; $E' \subseteq E$; $E' \neq \emptyset$.

Далее определим сложность преодоления нарушителем конкретного пути ω' при текущем распределении капитала защиты s ∈ S для каждого пути p ∈ P:

$$\omega(p,s) = \omega', \quad (2)$$

где $\omega' \in \mathbb{R}+$; $p \in P$; $s \in S$.

В итоге требуется выбрать оптимальное распределение весов, при котором вес пути с минимальным весом $min_{p\in P}\omega(p,s)$ будет максимален $max_{s\in S}$:

$$r(P,S) = max_{\ s\in S}(min_{\ p\in P}\,\omega\,(p,s)). \quad (3)$$

При этом функция расчета веса для пути ω является непрерывно возрастающей, а ее производная стремиться к нулю:

$$\omega(p,s) = \sum_{e\,\in\, e(p)} \frac{\sqrt[3]{\omega'(e,s)}}{\sum_{e\,\in\, E}\sqrt[3]{\omega'(e,s)}}, \quad (4)$$

где $p \in P$; $s \in S$.

В (4) представлены абсолютные значения весов $\omega' \in \mathbb{R}$ из текущего варианта распределения капитала защиты $s \in S$ на ребре $e \in P$:

$$\omega'(e,s) = \omega'_i,$$

где $\omega'_i \in \mathbb{R}+$; $e \in E$; $s \in S$.

Сумма нормированных кубических корней (4) выбрана из-за простоты вычисления и ее практической применимости: чем больше будет потрачено ресурсов на то или иное ребро, тем меньший выигрыш может быть получен в дальнейшем: такой подход моделирует ситуации из реальной жизни.

Так как функция (4) не зависит от порядка разложения аргументов (имеется ввиду, что веса будут неизменны), используем итеративный подход для определения оптимального значения весов для распределения капитала защиты. Для этого введем величину ε> 0 – точность расчета распределения капитала защиты, на каждом шаге добавим ε к текущему набору весов и выберем вариант, при котором наименьший путь будет иметь максимальное значение.

Для реализации модели «ключи-замки» определим замки (для ребер) и ключи (для вершин). Тогда поиск весов для всех путей изменится: если нарушитель нашел ключ, которого у него до этого не было, то текущая вершина становится начальной вершиной пути нарушителя, а новые пути ищутся рекурсивно и добавляются к конечному пути, пройденному ранее, обнуляя при этом множество всех посещенных вершин. Определим коэффициент сложности прохода по ребру $\omega' \in \mathbb{R}$:

$$\omega(p,s) = \sum_{e\,\in\, e(p)} \frac{\sqrt[3]{\omega'(e,s)\cdot w'(e)}}{\sum_{e\,\in\, E}\sqrt[3]{\omega'(e,s)\cdot w'\,(e)}}, \quad (5)$$

где $p \in P$; $s \in S$; $w'(e) = w'_i$, где $w'_i \in \mathbb{R}+$; $e \in E$.

При отсутствии замка этот коэффициент будет равен 1, а при наличии замка он может различаться в зависимости от текущей связки ключей у нарушителя.

Чтобы учесть несколько точек, в которых хранится защищенная информация, а также обозначить их «значимость» в рамках текущей системы, вводится нормированное значение значимости защищаемой области в вершине $w''(p) \in \mathbb{R}$, на которую умножается значение, определяемое формулой (5). Это позволяет располагать веса на ребра более рационально, в зависимости от важности информации:

$$\omega(p,s) = \sum_{e\,\in\, e(p)} \frac{\sqrt[3]{\omega'(e,s)\cdot w'(e)}}{\sum_{e\,\in\, E}\sqrt[3]{\omega'(e,s)\cdot w'(e)}} \cdot w''(p), \quad (6)$$

где $p \in P$; $s \in S$; $w''(p) = w''_i$, где $w''_i \in \mathbb{R}+$; $p \in P$.

Таким образом, получено итоговое выражение для расчета системы физической защиты объекта (6), содержащего защищаемую информацию, с учетом значений весов, нескольких точек хранения защищаемой информации, наличия ключей и замков.

Построенная математическая модель может использоваться для разработки программного обеспечения, моделирующего систему защиты для помещений различного объема, корпусов защищаемых объектов и для модернизации существующих систем защиты. В качестве входных данных программного обеспечения и модели используется план здания (объекта) с указанием мест расположения средств нейтрализации неправомерного физического доступа.

Разработанная модель может быть применена для решения проблемы безопасности при защите периметра, создании защищенной сети внутри или снаружи предприятия, для улучшения защиты существующих сетей от угроз физического доступа к информации.

Литература

1. Боровский А.С. Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов / А.С. Боровский, А.Д. Тарасов // Труды ИСА РАН, научный журнал. — Том 61, выпуск №1. — 2011. — С. 3–14.

2. Методика оценки угроз безопасности информации: порядок оценки угроз безопасности информации (от 5 февраля 2021 г.) // Федеральная служба по техническому и экспортному контролю. — 2021. — С. 6 – 12.

3. Гарсия М. Проектирование и оценка систем физической защиты/ М. Гарсия. — Москва: Мир, 2003. — 392 с.

4. Боровский А. С. Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки системы физической защиты объектов информатизации/А. С. Боровский. // АВТОРЕФЕРАТ диссертации на соискание ученой степенидоктора технических наук. —2015.

5. Янников И.М. Структурная схема интеллектуальной интегрированной системы безопасности критически важных и потенциально опасных объектов // Известия Самарского научного центра. — 2015. —Т.17. — №6(2). —С. 570–571.

6. Тарасов А.Д. Метод и алгоритмы проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации // АВТОРЕФЕРАТ диссертации на соискание ученой степени кандидата технических наук. — 2017.

7. Япаров А.Д. Имитационное моделирование и оценка угроз физического доступа к значимому объекту критической информационной инфраструктуры // XVIII Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых «Безопасность информационного пространства – 2019». Сборник трудов. — 2019. — С. 98–102.

8. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. — М.: Горячая линия — Телеком, 2016. — 417 с.

9. Ищейнов В.Я. Основные положения информационной безопасности: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — М.: Форум, Инфра-М, 2015. — 208 с.

References

1. Borovskiy A.S. Integrirovannyy podkhod k razrabotke obshchey modeli funktsionirovaniya sistem fizicheskoy zashchity ob»yektov / A.S. Borovskiy, A.D. Tarasov // Trudy ISA RAN, nauchnyy zhurnal. — Tom 61, vypusk №1. — 2011. — S. 3–14.

2. Metodika otsenki ugroz bezopasnosti informatsii: poryadok otsenki ugroz bezopasnosti informatsii (ot 5 fevralya 2021 g.) // Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu. — 2021. — S. 6 – 12.

3. Garsiya M. Proyektirovaniye i otsenka sistem fizicheskoy zashchity/ M.Garsiya. — Moskva: Mir, 2003. — 392 s.

4. Borovskiy A. S. Modeli, metody i algoritmy intellektual'noy podderzhki prinyatiya resheniy v zadachakh razrabotki i otsenki sistemy fizicheskoy zashchity ob"yektov informatizatsii/A. S. Borovskiy. // AVTOREFERAT dissertatsii na soiskaniye uchenoy stepenidoktora tekhnicheskikh nauk. —2015.

5. Yannikov I.M. Strukturnaya skhema intellektual'noy integrirovannoy sistemy bezopasnosti kriticheski vazhnykh i potentsial'no opasnykh ob"yektov // Izvestiya Samarskogo nauchnogo tsentra. — 2015. —T.17. — №6(2). —S. 570–571.

6. Tarasov A.D. Metod i algoritmy proyektirovaniya sistem fizicheskoy zashchity ob"yektov informatizatsii na osnove obrabotki nechetkoy informatsii // AVTOREFERAT dissertatsii na soiskaniye uchenoy stepeni kandidata tekhnicheskikh nauk. — 2017.

7. Yaparov A.D. Imitatsionnoye modelirovaniye i otsenka ugroz fizicheskogo dostupa k znachimomu ob"yektu kriticheskoy informatsionnoy infrastruktury // KHVIII Vserossiyskaya nauchno-prakticheskaya konferentsiya studentov, aspirantov i molodykh uchenykh «Bezopasnost' informatsionnogo prostranstva – 2019». Sbornik trudov. — 2019. — S. 98–102.

8. Buzov G.A. Zashchita informatsii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam / G.A. Buzov. — M.: Goryachaya liniya — Telekom, 2016. — 417 c.

9. Ishcheynov V.YA. Osnovnyye polozheniya informatsionnoy bezopasnosti: uchebnoye posobiye / V. YA. Ishcheynov, M.V. Metsatunyan. — M.: Forum, Infra-M, 2015. — 208 c.

АВЕРЬЯНОВ Антон Александрович, студент кафедры защиты информации, Южно-Уральский государственный университет. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: averianovaa@susu.ru

ШАДРИВ Владимир Владимирович, студент кафедры защиты информации, Южно-Уральский государственный университет. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: shadrivvv@susu.ru

БЕРДЮГИН Владимир Юрьевич, доцент кафедры защиты информации, Южно-Уральский государственный университет. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: berdiuginvi@susu.ru

AVERYANOV Anton Aleksandrovich, student of the Department of Information Security, South Ural State University. 454080, Chelyabinsk, Lenin Ave., 76. E-mail: averianovaa@susu.ru

SHADROV Vladimir Vladimirovich, Student of the Department of Information Security, South Ural State University, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: shadrivvv@susu.ru

BERDYUGIN Vladimir Yuryevich, Associate Professorof the Department of Information Security, South Ural State University, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: berdiuginvi@susu.ru

УДК 004.056 Вестник УрФО № 4(46) / 2022, с. 58–67

Гладышева В. А., Зырянова Т. Ю.

DOI: 10.14529/secur220407

ОРГАНИЗАЦИЯ РАБОТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА В УСЛОВИЯХ НОВЫХ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ ЭЛЕКТРОННОЙ ПОДПИСИ

В условиях современности переход на электронный документооборот коснулся деятельности абсолютного большинства малых и крупных компаний. Государственные структуры, как и представители бизнеса, интегрируют свою деятельность в быстрорастущую информационную сферу. Легитимность электронного документооборота напрямую зависит от юридического качества процессов применения электронной подписи.

В последние годы многие компании перешли на дистанционный формат работы, что требовало функционирования безопасной среды оборота информации. Такая потребность, несомненно, способствовала распространению использования электронной подписи.

Никакая сфера не может оставаться статичной в течение длительного периода времени, поэтому так важно актуализировать законодательство особенно в информационной сфере. Адаптируясь к актуальным направлениям деятельности, законодатель пришел к выводу о необходимости развития и совершенствования организационно–правовой базы удостоверяющих центров.

В статье приводится анализ и систематизация изменений законодательства Российской Федерации в сфере применения электронной подписи за период 2002-2022 гг.

Ключевые слова: *удостоверяющий центр, электронная подпись, правовое регулирование, доверенная третья сторона, квалифицированный сертификат.*

ORGANIZATION OF THE WORK OF THE CERTIFICATION CENTER UNDER THE NEW REQUIREMENTS OF THE RUSSIAN FEDERATION LEGISLATION ON ELECTRONIC SIGNATURE

In modern conditions, the transition to electronic document management has affected the activities of the vast majority of small and large companies. State structures, as well as business representatives, are integrating their activities into the rapidly growing information sphere. The legitimacy of electronic document management directly depends on the legal quality of the processes for applying an electronic signature.

In recent years, many companies have switched to a remote work format, which required the functioning of a secure information circulation environment. Such a need has undoubtedly contributed to the spread of the use of electronic signatures.

No sphere can remain static for a long period of time, therefore it is so important to update the legislation, especially in the information sphere. Adapting to current areas of activity, the legislator came to the conclusion that it is necessary to develop and improve the organizational and legal framework of certification centers.

The article provides an analysis and systematization of changes in the legislation of the Russian Federation in the field of application of electronic signature for the period 2002-2022.

Keywords: *certification centre, electronic signature, legal regulation, trusted third party, qualified certificate.*

В начале 2000–х годов в России появляется практика использования электронных подписей (далее – ЭП), основная их концентрация происходит в коммерческом обороте. Первые электронные подписи получили распространение в банковской сфере. Отечественные банки использовали ЭП, в первую очередь, как инструмент обеспечения информационной безопасности в своих корпоративных информационных системах (далее – ИС), а чуть позже и для безопасной работы в системах «банк–клиент».

В законодательстве понятие ЭП появляется еще в 1995 г., оно вводится в первой главе Гражданского кодекса Российской Федерации, где ЭП указана в качестве одного из аналогов собственноручной подписи, однако ее использование либо ограничивалось корпоративными информационными системами, либо требовалось заключение двусторонних соглашений между участниками. А в 2002 году вступает в силу первый в этой сфере Федеральный закон от 10.01.2002 г. №1–ФЗ «Об электронной цифровой подписи».

По мере информатизации коммерческой сферы и органов государственной власти, начинается закономерное распространение ЭП в обществе. Актуальным был вопрос принятия соответствующего закона, который бы значительно расширил области применения ЭП и позволил вести юридически значимый электронный документооборот. Для большего распространения были необходимы государственные гарантии правомерности использования ЭП.

Новый Федеральный закон от 06.04.2011

г. № 63–ФЗ «Об электронной подписи» вступил в силу с 8 апреля 2011 года.

Закон предусматривает три вида электронных подписей: «простая электронная подпись; усиленная неквалифицированная электронная подпись; усиленная квалифицированная электронная подпись» [1].

Одним из условий действительности квалифицированной электронной подписи в российском законодательстве является факт выдачи такой подписи аккредитованным удостоверяющим центром (далее – УЦ), аккредитация которого действительна на день выдачи указанного сертификата. Аккредитация удостоверяющего центра обозначает признание уполномоченным федеральным органом соответствия данного центра требованиям Федерального закона «Об электронной подписи». Она предполагает выполнение удостоверяющим центром определенных организационно–технических и экономических требований.

Изменения в правовой базе, оказавшие наиболее значимое влияние на УЦ, представлены в Таблице 1.

Таблица 1

Основополагающие изменения в деятельности УЦ

Федеральный закон	Результат
1. Федеральный закон от 10.01.2002 г. №1–ФЗ «Об электронной цифровой подписи»	Заложены основы решения проблемы обеспечения правовых условий для использования ЭП в процессах обмена электронными документами
2. Федеральный закон от 06.04.2011 г. №63–ФЗ «Об электронной подписи».	Закон, направленный на устранение недостатков Закона 2002 г. об ЭЦП, а также расширение сферы использования и допустимых видов ЭП.
3. Федеральный закон от 27.07.2010 г. №210–ФЗ «Об организации предоставления государственных и муниципальных услуг» (Редакция от 06.04.2011 г.)	За УЦ закрепились функции по созданию и поддержанию единого пространства доверия при электронном взаимодействии федеральных органов государственной власти.
4. Федеральный закон от 06.04.2011 г. №63–ФЗ «Об электронной подписи» (Редакция от 02.07.2013 г. с изменениями и дополнениями, вступил в силу с 01.09.2013 г.)	Были усилены требования к квалификации штатных работников УЦ.
5. Федеральный закон от 06.04.2011 №63–ФЗ «Об электронной подписи» (Редакция от 30.12.2015 г. с изменениями и дополнениями, вступил в силу с 30.01.2016 г.)	В определение УЦ добавлены слова «государственный орган или орган местного самоуправления», таким образом, на законодательном уровне закреплена возможность создания ведомственных УЦ.
6. Федеральный закон от 06.04.2011 №63–ФЗ «Об электронной подписи» (Редакция от 30.12.2015 г. с изменениями и дополнениями, вступил в силу с 08.07.2016 г.)	Сумма чистых активов, необходимая для открытия УЦ, возросла с 1 млн. руб. до 7 млн. руб., кроме того, сумма, на которую должна быть застрахована ответственность УЦ, выросла с 1,5 млн. руб. до минимальных 30 млн. руб. и максимальных 100 млн. руб.
7. Федеральный закон от 06.04.2011 №63–ФЗ (ред. от 02.07.2021 г.) «Об электронной подписи» (вступил в силу с 01.01.2021 г.)	Кроме изменения условий аккредитации УЦ, в функционале появляются новые обязанности. Вводится положение о доверенных третьих сторонах.
8. Федеральный закон от 06.04.2011 №63–ФЗ (ред. от 02.07.2021 г.) «Об электронной подписи» (вступил в силу с 01.03.2022 г.)	Введена отсрочка на обязательное применение машиночитаемой доверенности

8 ноября 2019 года стало известно, что Государственная Дума приняла в первом чтении законопроект о внесении поправок в Закон «Об электронной подписи». Теперь электронные подписи юридическим лицам будут выдавать удостоверяющие центры Федеральной налоговой службы Российской Федерации, а кредитным организациям — удостоверяющий центр Центробанка. Должностные лица госорганов и органов местного самоуправления и подведомственных им учреждений, а также нотариусы смогут получить ключи ЭП только в удостоверяющих центрах Федерального казначейства. Физические лица будут получать ключи ЭП в аккредитованных коммерческих удостоверяющих центрах.

В конце декабря 2019 года Президентом Российской Федерации был подписан Федеральный закон от 27 декабря 2019 г. № 476–ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1

Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». В целях обеспечения подготовки всех информационных систем для выполнения нового порядка, положения закона вступали в силу поэтапно. Последние поправки вступили в силу 14 июля 2022 года [2]. Этот закон вносит многочисленные изменения в действующее законодательство об ЭП и деятельности УЦ. Приведем наиболее значимые из них.

Метка доверенного времени

Федеральный закон №476–ФЗ дополняет понятийный аппарат Федерального закона №63-ФЗ. Так, появляется понятие «Метка доверенного времени». В других положениях закона это понятие не используется. Однако на основании данного пункта был утвержден Порядок создания и проверки метки доверенного времени Приказом Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, действующим до 1 января 2027 года [3]. Для использования такой метки необходимо использовать Службы меток доверенного времени, в их роли могут выступать доверенные третьи стороны (далее – ДТС), УЦ или операторы информационных систем.

Дополнительные особенности признания электронной подписи

Седьмая статья дополняется условием признания ЭП, созданной в соответствии с международными стандартами, соответствующей признакам усиленной электронной подписи (далее – УЭП): «такие ЭП признаются действительными в случае подтверждения соответствия их требованиям указанных международных договоров аккредитованной доверенной третьей стороной, аккредитованным УЦ, иным лицом, уполномоченными на это международным договором России, с учетом комментируемого Закона» [1]. Международные правовые акты также содержат в себе положения о взаимном признании ЭП странами–подписантами. Так, согласно статье 12 «Признание иностранных сертификатов и электронных подписей» Типового закона ЮНСИТРАЛ об электронных подписях предусмотрено при определении юридической силы сертификата или электронной подписи не учитывать место выдачи, создания и использования электронной подписи. Электронная подпись, созданная или используемая за пределами принимающего государства, обладает такой же юридической силой в принимающем государстве, как и электронная подпись, созданная или используемая в принимающем государстве, если она обеспечивает эквивалентный уровень надежности [4].

Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи

Пересматриваются и дополняются полномочия ведомств в сфере ЭП. Так, к функциям уполномоченного федерального органа, после введения законом института «доверенной третьей стороны», добавляется требование об аккредитации и осуществления проверок таких лиц. Таким федеральным органом является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России).

Запрет на ограничения признания усиленной квалифицированной электронной подписи

Разработчиками изменений к закону отмечалось, что при взаимодействии с различными ведомствами пользователи сталкиваются с проблемой отсутствия возможности применять для идентификации и аутентификации один сертификат ключа проверки УКЭП (далее – квалифицированный сертификат). Причиной такой проблемы является требование ведомств по содержанию в квалифицированных сертификатах объектных идентификаторов (OID) тех или иных полномочий, закрепляемых за пользователем в рамках конкретной ИС. Из–за отсутствия требуемых идентификаторов, сертификаты, выданные аккредитованными УЦ, не могли быть использованы для проверки ЭП в отдельных ИС. Именно поэтому вторая часть статьи 10 запрещает участникам электронного взаимодействия устанавливать иные, за исключением предусмотренных Законом, ограничения признания УКЭП. По этой же причине из статьи 11 «Признание квалифицированной электронной подписи» исключается положение, указывающие на возможность установления ограничений использования квалифицированного сертификата.

Визуализация электронной подписи

Появляется пункт о требовании визуализации ЭП. В статье 12 указано, что визуализация должна содержать «информацию о том, что такой документ подписан электронной подписью, а также о номере, владельце и периоде действия сертификата ключа проверки электронной подписи» [1]. После процедуры

подписания создается штамп с визуализацией подписи.

Изменение порядка идентификации заявителя

Статья 13 посвящена удостоверяющему центру. Новой редакцией статьи меняется порядок идентификации заявителя, представленный на рис. 1.

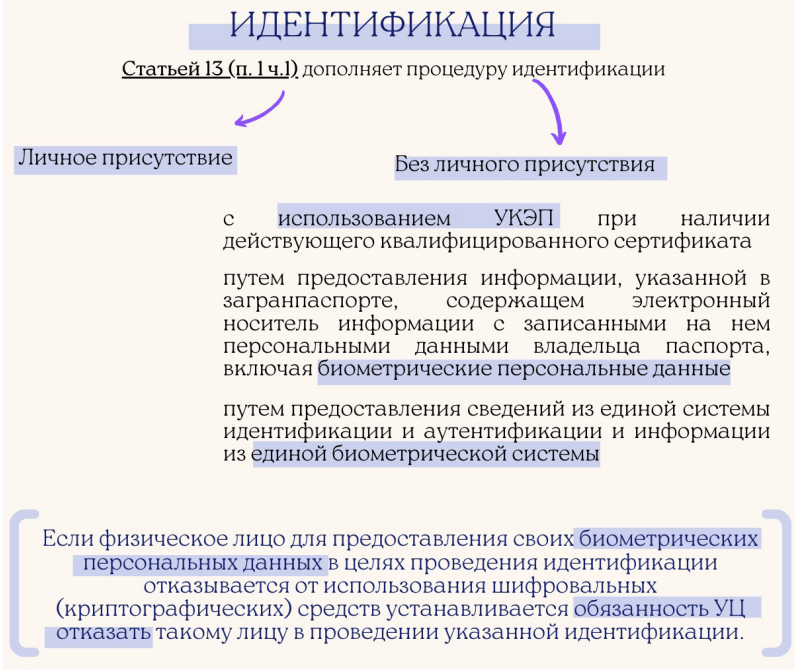


Рис. 1. Способы идентификации заявителя

Новые компетенции удостоверяющих центров

К обязанностям УЦ добавляется «информирование владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа ЭП» [1], также проинформировав о событиях, причинах и последствиях таких событий. Наряду с тем, владелец должен быть проинформирован УЦ «при возникновении обоснованных сомнений относительно лица, давшего поручение на использование хранимых ключей электронной подписи» [1].

Виды аккредитованных УЦ

Серьезные изменения коснулись УЦ. В соответствии с 15 статьей выделены виды аккредитованных УЦ, представленные на Рис. 2.

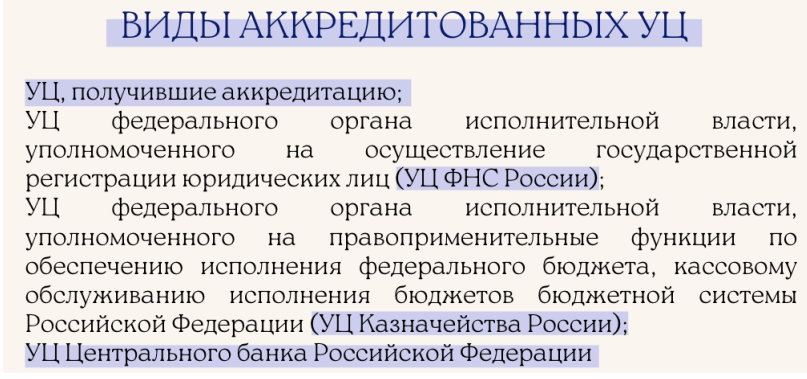


Рис. 2. Виды аккредитованных УЦ

«Дистанционная» электронная подпись

Законодатель наделил УЦ полномочиями по хранению и использованию по поручению клиента ключа ЭП. По требованию владельца должна предоставляться информация об использовании ключа ЭП и предоставляться история его использования. Вместе с тем для УЦ, которые осуществляют эти действия,

установлены дополнительные требования аккредитации.

Удостоверяющий центр федеральной налоговой службы России

15 статьей рассматриваемого закона предусмотрено, что УЦ ФНС России вправе «наделить доверенных лиц полномочиями на прием заявлений о получении квалифицированного сертификата юридического лица и выполнение требований при выдаче такого сертификата от имени данного УЦ», «на создание ключа ЭП (при условии исключения возможности доступа работников таких доверенных лиц к ключам ЭП заявителей), а также на хранение ключей УКЭП для дистанционного использования и на создание при помощи указанных ключей ЭП для электронных документов».

Ответственность удостоверяющих центров и их работников

Серьезным изменением стало введение уголовной ответственности для сотрудников УЦ. Виды ответственности работников УЦ представлены в Таблице 2.

Таблица 2

Виды ответственности сотрудников УЦ

Вид ответственности	Ответственность
гражданско–правовая	Подразумеваются общие нормы гл. 25 «Ответственность за нарушение обязательств» и гл. 59 «Обязательства вследствие причинения вреда» Гражданского Кодекса Российской Федерации
административная	Федеральный закон от 28 декабря 2016 г. №471–ФЗ, которым Кодекс об административных правонарушениях Российской Федерации дополнен статьей 13.33 «Нарушение обязанностей, предусмотренных законодательством Российской Федерации в области электронной подписи»
уголовная	Сведений о принятии соответствующего закона нет.

Министерство связи и массовых коммуникация Российской Федерации (Минкомсвязи России) России предлагало введение статьи 200.6 «Умышленное нарушение обязанностей, предусмотренных законодательством в области электронной подписи» в Уголовный кодекс Российской Федерации, но впоследствии от этого решения отказались. На данный момент формулировка об «уголовной ответственности» сотрудника УЦ нормативно не подкреплена никакой соответствующей статьей.

Аккредитация удостоверяющего центра

Законом ужесточены требования к порядку аккредитации УЦ и деятельности УЦ, в том числе предусматривается следующее.

1. Аккредитация УЦ осуществляется в два этапа: установлено, что на первом этапе аккредитация УЦ осуществляется уполномоченным федеральным органом, а на втором – правительственной комиссией.

2. Сокращение срока аккредитации УЦ с пяти до трех лет.

3. Высокий порог собственного капитала УЦ. «Минимальный размер собственных средств (капитала) должен составлять не менее чем один миллиард рублей или пятьсот миллионов рублей при наличии не менее чем в трех четвертях субъектов Российской Федерации одного или более филиала или представительства УЦ» [1].

4. Вводится требование о необходимости получения «лицензии на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием таких средств и …» [1].

5. Увеличивается размер финансового обеспечения ответственности за убытки, причиненные третьим лицам.

6. Вводится требование о необходимости наличия права собственности на аппаратные средства ЭП и средства УЦ, и наличия права использования программных средств ЭП и средств УЦ.

7. Вводится требование к деловой репутации руководителя и учредителей УЦ, владеющих более 10% капитала.

8. Вводится требование об отсутствии в отношении УЦ досрочно прекращенной аккредитация в течение трех лет до подачи заявления.

9. Вводится ограничение к лицу, действующему от имени удостоверяющего центра без доверенности.

Государственный надзор в сфере электронной подписи

Исключаются части статьи 16, которыми определялись особенности осуществления государственного и муниципального контроля в отношении аккредитованных УЦ. На их место введена статья 16.1, посвященная федеральному государственному контролю в сфере ЭП. Некоторые положения исключенных частей перенесены в новую статью. Устанавливается, что надзор в сфере ЭП осуществляется Министерством цифрового развития Российской Федерации. Организация такого контроля осуществляется в соответствии с Федеральным законом от 31 июля 2020 г. №248–ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» и Постановлением Правительства Российской Федерации от 29 июня 2021 г. №1044. Также указывается, что при осуществлении государственного надзора плановые проверки аккредитованных УЦ и доверенных третьих сторон не проводятся.

Использование ЭП в системе государственного управления и деловой деятельности

Статья 17.1, регламентирующая использование УКЭП при участии в правоотношениях физического лица, вводит новый вид документа – «документ о полномочиях», который заменяет ранее использовавшиеся для этих же целей доверенности.

Квалифицированный сертификат

Серьезным фактом является внесение изменений в определение термина «квалифицированный сертификат» (п. 3). Он дополнен словами: «являющийся в связи с этим официальным документом» [1]. Таким образом, противоправные действия с квалифицированными сертификатами теперь потенциально могут рассматриваться в соответствии со следующими статьям Уголовного кодекса Российской Федерации: статья 238 «Производство, хранение, перевозка либо сбыт товаров и продукции, выполнение работ или оказание услуг, не отвечающих требованиям безопасности», статья 292 «Служебный подлог», статья 324 «Приобретение или сбыт официальных документов и государственных наград», статья 325 «Похищение или повреждение документов, штампов, печатей либо похищение акцизных марок, специальных марок или знаков соответствия», статья 327 «Подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков». При выдаче квалифицированного сертификата аккредитованный УЦ обязан идентифицировать заявителя, по новым требованиям, изложенным ранее. Статья 18 уточняет перечень сведений при прохождении процедуры идентификации.

«а) в отношении физического лица – фамилия, имя, а также отчество (при наличии), дата рождения, реквизиты документа, удостоверяющего личность, ИНН, СНИЛС гражданина в системе обязательного пенсионного страхования;

б) в отношении юридического лица, зарегистрированного в соответствии с законодательством Российской Федерации, – наименование, организационно–правовая форма, ИНН, а также ОГРН и адрес юридического лица;

в) для юридического лица, зарегистрированного в соответствии с законодательством иностранного государства, – наименование, регистрационный номер, место регистрации и адрес юридического лица на территории государства, в котором оно зарегистрировано» [1].

Далее определяются способы подтверждения достоверности сведений, о которых говорилось ранее:

1. С использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;

2. С использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, ПФР, ФФОМС, единой информационной системы нотариата;

3. С использованием единой системы идентификации и аутентификации.

При получении квалифицированного сертификата заявителем он должен быть ознакомлен аккредитованным УЦ с информацией, содержащейся в квалифицированном сертификате. «Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку» а также «УЦ обязан хранить информацию, подтверждающую ознакомление заявителя» с такой информацией [1].

Поднимается вопрос взимания платы за выдачу аккредитованным УЦ квалифицированного сертификата, у УЦ появляется возможность установить такую плату, но при условии, что ее размер не превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации.

Закреплена обязанность аккредитованного УЦ одновременно с выдачей квалифицированного сертификата предоставить владельцу руководство по обеспечению безопасности использования УКЭП и средств УКЭП. Данное положение взаимосвязано с обязанностью УЦ информировать заявителей об условиях и о порядке использования ЭП и средств ЭП.

Последняя часть статьи предусматривает безвозмездное осуществление регистрации по желанию заявителя в ЕСИА со стороны аккредитованного УЦ при выдаче квалифицированного сертификата.

Доверенная третья сторона

Разработчиками проекта закона предлагалось создание нового института доверенных третьих сторон. Данные организации будут осуществлять деятельность после получения аккредитации в Минцифры России. Статья 18.1. содержит регулирование, посвященное доверенной третьей стороне. Первая часть данной статьи определяет перечень ее функций. Оказание таких услуг осуществляется в рамках гражданско–правового договора, регулируемого положениями гл. 39 «Возмездное оказание услуг» Гражданского кодекса Российской Федерации.

В третьей части статьи говорится об ответственности доверенной третьей стороны. В отношении самой такой ответственности указано, что доверенная третья сторона несет гражданско–правовую и (или) административную ответственность. Соответствующая административная ответственность доверенной третьей стороны законодательством Российской Федерации в настоящее время не установлена. Разработчиками законопроекта, принятого в качестве Закона 2019 г. №476–ФЗ, указывалось, что принятие законопроекта потребует принятия Федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (ответственный исполнитель – Минкомсвязь России). Однако до настоящего времени соответствующий закон не принят.

Статья 18.2. регламентирует аккредитацию доверенной третьей стороны. Процедура аккредитации доверенной третьей стороны во многом аналогична процедуре аккредитации УЦ. Аккредитация осуществляется на добровольной основе. Срок, на который осуществляется аккредитация три года; при этом доверенной третьей стороне предоставляется право указать в своем заявлении на более короткий срок. Также определен перечень требований, при условии одновременного выполнения которых осуществляется аккредитация доверенной третьей стороны.

Одной из целей принятия закона было сокращения числа коммерческих УЦ. Законодатели в своих рассуждениях напрямую сопоставляли количественную и качественную сторону этого вопроса.

В результате количество аккредитованных коммерческих УЦ изменилось следующим образом.

На момент 15 сентября 2021 года в стране действовало 322 коммерческих удостоверяющих центра, среди них только 24 были аккредитованы по новым требованиям (Рис. 3).

С 1 июля 2021 года не прошедшие аккредитацию УЦ не могли выдавать ЭП, а срок

Рис. 3. Соотношение аккредитованных по новым требованиям УЦ к неаккредитованным на 15.09.2021 г.

действия ЭП, которые были выданы ранее устанавливался до 1 января 2022 года.

1 марта 2022 года все положения Федерального закона №476–ФЗ вступили в силу. По данным Министерства цифрового развития на 6 июня 2022 года перечень аккредитованных УЦ содержит 42 записи. Ситуация на рынке коммерческих УЦ представлена на Рис. 4.

Высокий порог собственного капитала,

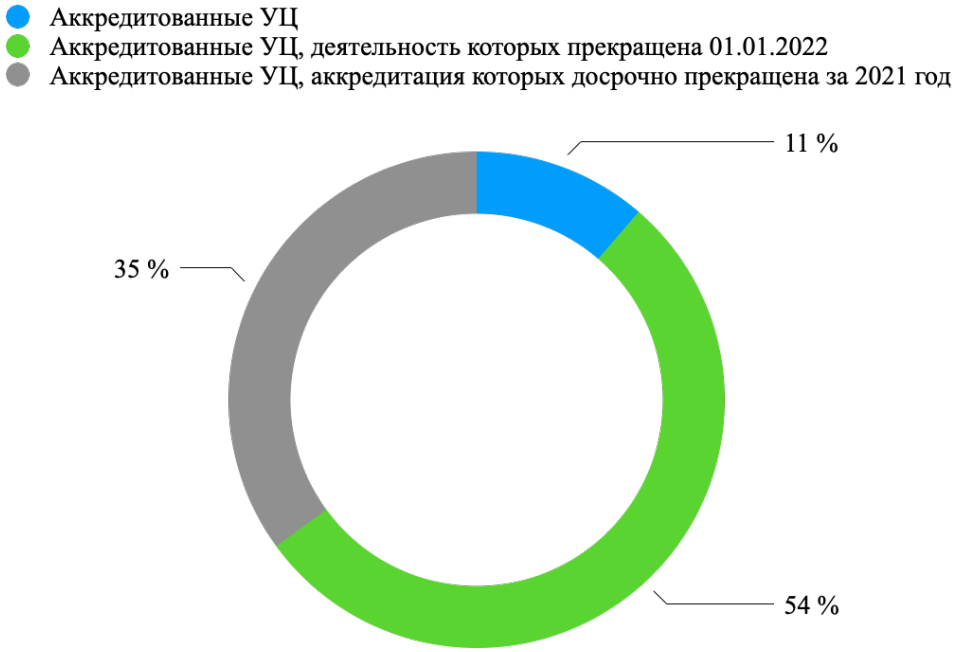


Рис. 4. Ситуация на рынке коммерческих УЦ на 06.06.2022 г.

как требование к аккредитации УЦ, «отсеял» значительное количество малых предпринимателей рынка услуг УЦ. Таким образом, сегодня на рынке преобладают крупные компании.

Электронная подпись получает все большее распространение, и сферы ее влияния будут закономерно увеличиваться, а значит деятельность удостоверяющих центров, которые выдают такие подписи, продолжит свое существование. И несомненно, в будущем деятельность УЦ будет также преобразовываться и видоизменяться, адаптируясь к новым реалиям.

Изменения в законодательстве об электронной подписи, проанализированные в данной статье, были продиктованы целью создания единого пространства доверия к электронной подписи, в связи с чем они, безусловно, актуальны. Так Минцифры России еще с 2017 года планировало уменьшить число удостоверяющих центров. Последними изменениями Федерального закона №63-ФЗ «Об электронной подписи» эти планы были реализованы, однако необходимо продолжение этой работы в решении и других задач, которые ставились указанным законом. Нормативная база для решения этих задач продолжает совершенствоваться.

Литература

1. Федеральный закон от 06.04.2011 №63–ФЗ (ред. от 02.07.2021) «Об электронной подписи» (с изм. и доп., вступ. в силу с 01.03.2022).

2. Федеральный закон от 14.07.2022 №339-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

3. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 6 ноября 2020 г. №580 «Об утверждении порядка создания и проверки метки доверенного времени».

4. Типовой закон ЮНСИТРАЛ об электронных подписях (принят ЮНСИТРАЛ 5 июля 2001 г.).

References

1. Federal'nyj zakon ot 06.04.2011 №63–FZ (red. ot 02.07.2021) «Ob jelektronnoj podpisi» (s izm. i dop., vstup. v silu s 01.03.2022).

2. Federal'nyj zakon ot 14.07.2022 №339-FZ «O vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federacii».

3. Prikaz Mincifry Rossii ot 6 nojabrja 2020 g. N 580 «Ob utverzhdenii porjadka sozdanija i proverki metki doverennogo vremeni».

4. Tipovoj zakon JuNSITRAL ob jelektronnyh podpisjah (prinjat JuNSITRAL 5 ijulja 2001 g.).

ГЛАДЫШЕВА Вероника Антоновна, технолог II категории Екатеринбургского информационно-вычислительного центра – структурного подразделения Главного вычислительного центра – филиала ОАО «Российские железные дороги». 620027, г. Екатеринбург, ул. Челюскинцев, д. 11Б. E-mail: verunya.gladysheva@mail.ru

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

GLADYShEVA Veronika Antonovna, technologist II category of Yekaterinburg Information and Computing Center - structural subdivision of the Main Computing Center – branch of Joint Stock Company «Russian Railways». 620027, Yekaterinburg, st. Chelyuskintsev, 11B. E-mail: verunya.gladysheva@mail.ru

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

УДК 004.7.056.5 Вестник УрФО № 4(46) / 2022, с. 68–75

Захаров А.А., Шабалин А.М., Ханбеков Ш.И., Джалилзода Д.Б., Пономарев К.Ю

DOI: 10.14529/secur220408

ПРИМЕНЕНИЕ ГОЛОСОВОГО ПОМОЩНИКА В КАЧЕСТВЕ ВИРТУАЛЬНОГО КОНСУЛЬТАНТА ДЛЯ АДМИНИСТРИРОВАНИЯ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ[1]

В статье представлена технология создания интеллектуального голосового помощника для обеспечения информационной безопасности сетевой инфраструктуры локальных компьютерных сетей. Потребность в таком помощнике может возникнуть в организациях, предоставляющих хостинг небольшим сетевым инфраструктурам, например, для домашних телемедицинских стационаров или IT-стартапам, для которых вопросы, связанные с защитой информации, являются важными, а также при обучении студентов технологиям защиты сетевой инфраструктуры. Полученные результаты также имеют практическую значимость для решения задач обеспечения информационной безопасности лицами, совмещающими выполнение обязанностей администратора сети (NetOps) и администратора защиты (SecOps).

Ключевые слова: *виртуальный голосовой помощник, онтологии, распознавание речи, сетевая безопасность, системное администрирование, Cisco.*

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-47-720005

Zakharov A.A., Shabalin A.M., Khanbekov Sh.I., Dzhalilzoda D.B., Ponomarev K. Y.

USING A VOICE ASSISTANT AS A VIRTUAL CONSULTANT FOR ADMINISTRATION OF THE SECURITY OF THE LOCAL COMPUTER NETWORK INFRASTRUCTURE

The article presents the technology to create intellectual voice assistant for the tasks related to providing local area network information security. This technology may be found useful by organizations, offering hosting to small area network infrastructures, e.g. home health care telemedicine or IT-startups aimed at information security, or when teaching students how to protect the network infrastructure. The results obtained in this research also provide practical value in solving information security related tasks for employees occupied with network operations (NetOps) and security operations (SecOps) simultaneously.

Keywords: *virtual voice assistant, ontologies, speech recognition, network security, system administration, Cisco.*

Решение практических проблем обеспечения информационной безопасности (ИБ) системными администраторами во многом опирается на многолетний опыт работы с цифровой информацией, создающей следующие потенциальные риски:

• информация может быть раскрыта (конфиденциальность скомпрометирована);

• информация может быть модифицирована (целостность нарушена);

• информация может быть уничтожена или потеряна (доступность нарушена).

Указанные риски наносят ущерб как напрямую, непосредственно снижая стоимость цифрового актива, так и косвенно - ухудшая репутацию и приводя к юридическим последствиям. Организация может управлять рисками в повседневной деятельности. Стоимость ущерба от события риска ИБ обычно оценивается как произведение вероятности неблагоприятного события и отрицательной суммы стоимости ликвидации его последствий, происходящих в течение конкретного временного периода. Обычно мерой стоимости риска являются годовые убытки (Annual Loss Expectance, ALE). Ожидаемую стоимость ущерба можно уменьшить, например, за счет его страхования или снижения вероятности возникновения неблагоприятного события, а также, если событие произошло, путем минимизации последствий. Это позволяет определить ИБ как управленческий процесс, цель которого заключается в управлении (минимизации стоимости) информационными рисками для бизнеса.

В контексте решения задач обеспечения ИБ компьютерных сетей дополнительную сложность составляет то, что информация о частоте возникновения нежелательных явлений и об их последствиях обычно скрывается. То есть сведений об эффективности мер, которые можно предпринимать для предотвращения нежелательных явлений и/или смягчения последствий, обычно недостаточно или вообще не имеется, поскольку у организаций с проблемами в области ИБ отсутствуют мотивы для сообщения о них. При этом имеется множество стимулов для замалчивания этой информации. В конечном счете все это затрудняет оценку эффективности тех мер, которые в идеале должны обеспечить:

1) защиту телекоммуникационного оборудования и оконечных устройств (маршрутизаторов, коммутаторов, межсетевых экранов, серверов);

2) соблюдение требований регулятора и корпоративного регламента;

3) защиту от несанкционированного внутреннего или внешнего доступа к информации разной степени конфиденциальности (коммерческая тайна, персональные данные или бухгалтерская информация).

Условно, с точки зрения объектов защиты, информационную сеть можно разделить на две составляющие: 1) операционные системы, прикладное программное обеспечение и данные на хостах и серверах; 2) коммуникационная сеть для информационного взаимодействия внутренних и внешних пользователей (маршрутизаторы, коммутаторы и линии связи). Отметим, что по сравнению с сетевым оборудованием, операционные системы и прикладное программное обеспечение обновляются чаще, например, вследствие появления новых версий, тогда как коммуникационная сеть достаточно стабильна. Это послужило предпосылкой развития двух подходов к организации и поддержке безопасности информационной сети.

В том, что касается операционных систем и прикладного программного обеспечения на конечных устройствах как объектов защиты, необходимо отметить, что в настоящее время используются постоянно актуализируемые базы и одновременно платформ для сбора и распространения информации об уязвимостях. Базы содержат описания выявленных уязвимостей, оценку потенциального воздействия и (при наличии) способы их устранения. Можно выделить по крайней мере шесть популярных и поддерживаемых в актуальном состоянии подобных баз.

1. Common Vulnerabilities and Exposures (CVE) [1]. База хранит данные об общеизвестных уязвимостях информационной безопасности. Предназначена для применения в системах обнаружения и/или предотвращения атак, сканерах безопасности, при разработке сигнатурных правилах.

2. Exploit Database (ED) [2]. В данной базе реализован альтернативный подход к информации об уязвимостях программного обеспечения, а именно, осуществляется регистрация сценариев эксплуатации эксплойтов. Также в базе представлены примеры эксплуатации уязвимости.

3. National Vulnerability Database (NVD) [3]. База опирается на стандарты протокола (Security Content Automation Protocol – SCAP), которые определяют потенциальные уязвимости программного кода и его некорректные конфигурации.

4. Flexera – Secunia Advisory and Vulnerability Database SAaVD [4]. База обобщает доступную информацию об обнаруженных угрозах и уязвимостях ПО на основе агрегации данных из публичных источников.

5. Vulnerability Notes Database (VND) [5]. База агрегирует информацию о множестве сходных уязвимостей для определенных типов программного обеспечения.

6. Банк данных угроз безопасности информации «ФСТЭК России» [6]. Данная база считается ключевой в РФ. Принципиально важно, что «ФСТЭК России» поддерживает собственный реестр известных угроз информационной безопасности и уязвимостей программного обеспечения с 2014 года.

Определенная стабильность коммуникационной сети создает специфические условия для обеспечения ИБ. А именно, для настройки безопасности непосредственно на сетевых устройствах представляется целесообразным определить набор онтологий, связанных с безопасностью, например, NRL [7, 8] в качестве точного описания концепций безопасности информационной сети на различных уровнях детализации. Использование онтологий как спецификаций настройки безопасности позволяет создать базу семантических выражений для конфигурирования сетевого оборудования [9-11], а дополнительным преимуществом данного подхода является возможность анализа, накопления и повторного применения знаний о настройке сетевой безопасности, в том числе и в автоматическом режиме с помощью специализированных программных продуктов.

Отметим, что результатом использования онтологий в нашем случае является не только анализ ситуации с уровнем защищенности конкретной сети, но и создание базы знаний, выступающей в качестве одного из основных компонентов интеллектуального программного обеспечения для интерактивного администрирования с помощью голосового помощника [12]. Таким образом, цель настоящего исследования заключается в проектировании и разработке на основе онтологического подхода интеллектуального голосового помощника для обеспечения информационной

безопасности сетевой инфраструктуры локальных компьютерных сетей.

Прототип кроссплатформенного программного решения «NEVA (Network Engineer Voice Assistant)» (Голосовой Помощник Сетевого Инженера) содержит голосовой (VUI) и графический (GUI) интерфейсы, взаимодействующие друг с другом через специальный программный интерфейс (API), запускаемый на рабочей станции системного администратора, который служит связующим звеном всех программных компонентов (модулей) голосового помощника и предоставляет приложению доступ к компьютерной сети организации.

Функциональные возможности голосового помощника распределены между его модулями. Архитектура приложения представлена на рисунке 1.

За синтез входящей текстовой информа-

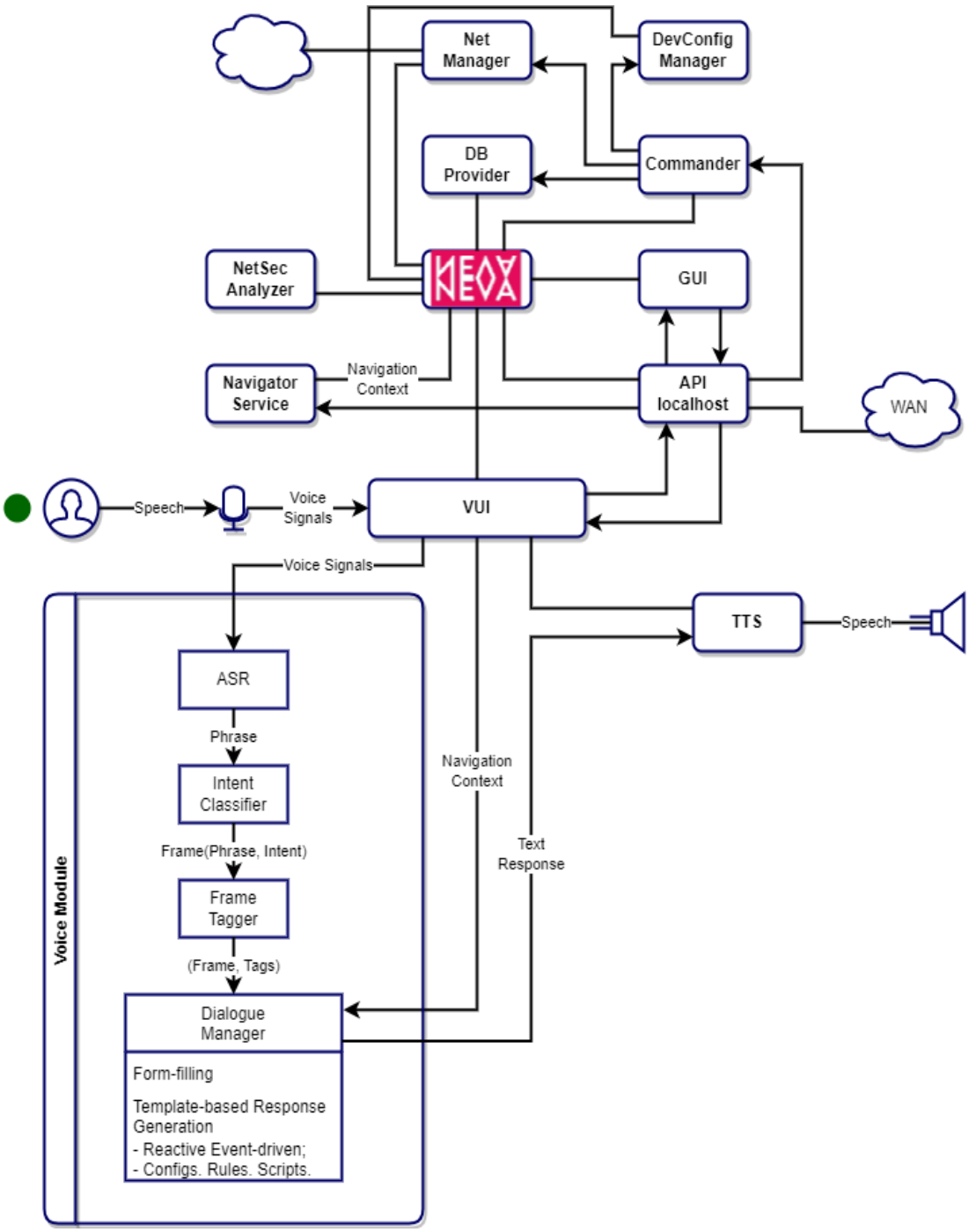


Рис. 1. Архитектура виртуального голосового помощника

ции в речь и последующее озвучивание отвечает сервис «TTS» (Text-to-Speech). Следует отметить, что существует потребность в предоставлении пользователю возможности регулирования скорости озвучивания информации.

Графический интерфейс служит для визуализации сведений, с которыми работают и программа, и системный администратор. Интерфейс состоит из двух частей: основного окна и окна диалога. Окно диалога показывает взаимодействие системного администратора с голосовым помощником (в привычном и удобном для восприятия пользователя виде), а основное окно отвечает за предоставление иной информации.

В приложении присутствует также сервис навигации (Navigator Service), хранящий сведения о контексте происходящих событий и выполняющихся процессов, которые предоставлены системным администратором или операционной системой и которыми руководствуются модули приложения в ходе работы программы (в том числе модули, отвечающие за процессы принятия решений).

За сетевое взаимодействие с коммуникационными устройствами компьютерной сети отвечает модуль «Net Manager» или «Менеджер Сети», позволяющий управлять сетевым оборудованием подключенной компьютерной сети через специальные консольные команды, перечень которых зависит от установленной операционной системы на сетевом устройстве. Модуль также взаимодействует (при необходимости) с конфигурационными и иными файлами, хранящимися в памяти сетевых устройств, через модуль «DevConfig Manager» или «Менеджер Настроек Устройств» для получения сведений по решению актуальных задач.

За принятие решений отвечает модуль «Commander» или «Командующий Модуль», которому на вход подаются все необходимые данные для инициализации той или иной операции.

Онтологии по настройке определенных технологий размещаются в базах данных, которые хранятся локально или централизованно на выделенных серверах в виде таблиц данных. Приложение работает с этими данными в формате JSON через сериализацию объектов, предоставляемых системе управления базами данных (СУБД). Нами рекомендуется использование свободной объектно-реляционной СУБД «PostgreSQL», которая имеет широкий спектр возможностей. Мостом между СУБД и компонентами приложения служит модуль «DB Provider» или «Провайдер Баз Данных». Онтологии состоят из перечня правил, программных сценариев, справочной информации и ссылок на входные шлюзы для взаимодействия с собственными анализирующими средствами.

За предоставление пользователю сведений рекомендательного характера на основе анализа активных конфигураций коммуникационных устройств, подключенных к компьютерной сети, отвечает модуль «NetSec Analyzer», или «Модуль Анализа Безопасности Сети», в котором дополнительно предусмотрена возможность анализа степени защищенности сети путем применения ряда соответствующих инструментов с открытым исходным кодом (Open Source) от сторонних производителей (Third-Party), а также – собственные средства анализа. Кроме того, данный модуль руководствуется онтологиями по безопасной настройке сетевых технологий, обеспечиваемыми модулем «DB Provider».

В качестве примера нами рассматривается алгоритм настройки безопасности протокола SSH для работы системного администратора в локальной сети [13]. Предполагается, что в модельной компьютерной сети выполнены следующие минимальные настройки:

- все узлы в сети имеют IP-связность;
- на коммутационных устройствах предварительно настроен протокол telnet.

Моделируемая топология в среде эмуляции GNS3 компьютерной сети, построенной на коммуникационном оборудовании компании Cisco, представлена на рисунке 2.

Программа реагирует на команды, начинающиеся с обращения: «Нева, …». Так, при словах системного администратора – «Нева, включи поддержку SSH версии 2» – сначала речь передается на службе автоматического распознавания речи (Automatic Speech Recognition, ASR), которая потом превращает его в текст: «Нева, включи поддержку эсэсаш версии два».

Далее данный текст попадает в сервис «Классификатор интентов», задача которого – определить «намерения» пользователя относительно выполнения их программой. Классификатор интентов – машинообучаемая сущность, для которой заранее определяются все ключевые триггерные фразы, помогающие классифицировать намерение пользователя. Создаются определенные ключевые ка-

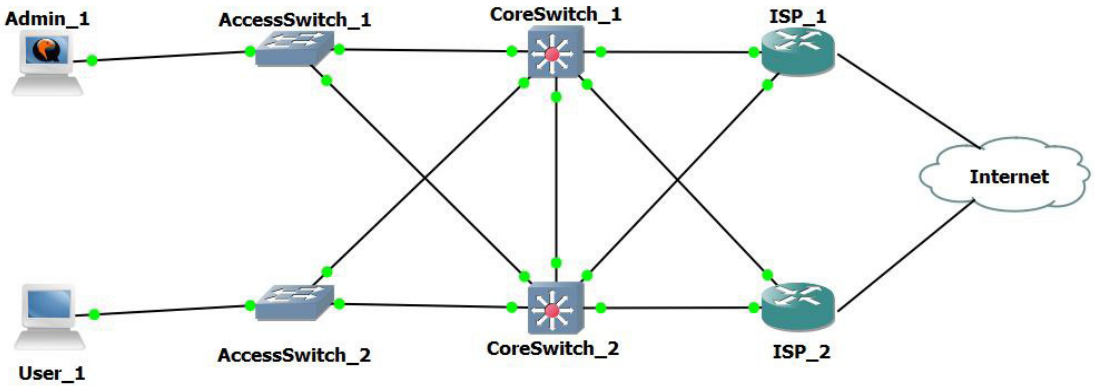


Рис. 2. Топология компьютерной сети

Рис. 3. Пример взаимодействия с голосовым помощником

тегории запросов, которые задействуются в ходе работы программы как важнейшие составляющие процесса принятия ею решений. Например, для вышеуказанного текста системой определяется категория запроса «setup_ssh_pragma_permit_version» по ключевым фразам «включи», «эсэсаш», «версии».

Данный запрос попадает в модуль «Менеджер диалогов», который отвечает пользователю сгенерированными на основе шаблонов голосовыми фразами, взаимодействуя с модулем синтеза речи, и, самое главное, принимает решения. Процесс принятия решений должен быть предсказуемым, так что не может быть, по нашему мнению, основан на машинном обучении (в целях безопасности). А потому основу модуля составляют правила, сценарии и конфигурационные файлы. Здесь нами реализована концепция «форм-филлинг», состоящая в том, что системный администратор своими репликами как бы заполняет некую виртуальную форму и, по мере заполнения им всех обязательных полей, задачу можно решить, применив необходимое действие. При этом менеджер следит за событиями, которые происходят в процессе взаимодействия пользователя с программой, а также – программы с коммуникационными устройствами, что конструирует логику диалога и влияет на процесс принятия решений. Поскольку данный запрос администратора после его семантического тегирования не включал информации о том, на каком сетевом оборудовании администратор хочет изменить конфигурацию, менеджер диалогов после заполнения соответствующей виртуальной формы может запросить недостающую информацию у пользователя (например, имя или тип устройства) или предоставить опцию изменения для текущего активного се-

тевого оборудования, на который системный администратор ранее произвел навигационный переход.

Указанный выше пример диалога между системным администратором и голосовым помощником продемонстрирован на рисунке 3.

Таким образом, мы считаем, что применение технологий, использующих виртуального голосового помощника на основе онтологий в системном администрировании безопасных компьютерных сетей, очень эффективно и способствует повышению уровня компетенций, необходимых системному администратору для организации приемлемого уровня защиты в небольшой локальной компьютерной сети.

Литература

1. Common Vulnerabilities and Exposures: сайт / The MITRE Corporation. – 1999 –. – URL: https://cve.mitre.org/ (дата обращения: 14.11.2022). – Текст: электронный.

2. Exploit Database: сайт / OffSec Services Limited. – 2009 –. – URL: https://www.exploit-db.com/ (дата обращения: 14.11.2022). – Текст: электронный.

3. National Vulnerability Database (NVD): сайт. – Gaithersburg. –. – URL: https://nvd.nist.gov/ (дата обращения: 14.11.2022). – Текст: электронный.

4. Secunia Advisories: сайт / Flexera. – Chicago. – . – URL: https://community.flexera.com/t5/Secunia-Advisories/ct-p/advisories (дата обращения: 14.11.2022). – Текст: электронный.

5. Vulnerability Notes Database: сайт / Carnegie Mellon University. – Pittsburgh. – . – URL: https://www.kb.cert.org/vuls/ (дата обращения: 14.11.2022). – Текст: электронный.

6. Банк данных угроз безопасности информации: сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва. – . – URL: https://bdu.fstec.ru/ (дата обращения: 14.11.2022). – Текст: электронный.

7. Kim A., Luo J., Kang M. Security ontology for annotating resources //OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". – Springer, Berlin, Heidelberg, 2005. – С. 1483-1499.

8. Котенко И. В., Полубелова О. В., Чечулин А. А. Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода //Информатика и автоматизация. – 2013. – №. 26. – С. 26-39.

9. Мирзагитов А. А., Пальчунов Д. Е. Методы разработки онтологии по информационной безопасности, основанные на прецедентном подходе //Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2013. – Т. 11. – №. 3. – С. 37-46.

10. Гаршина В. В., Степанцов В. А. Онтологический подход для анализа рисков безопасности информационных систем //Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 3 (29). – С. 18-22.

11. Загорулько Ю. А. Моделирование робота, управляемого речевыми сигналами //Известия Томского политехнического университета. Инжиниринг георесурсов. – 2011. – Т. 319. – №. 5. – С. 98-102.

12. Актаева А.У., Ниязова Р., Сералиева А., Сарсенбаева Ж., Даутов А., Кусаинова У, Жартанов С. КОГНИТИВНЫЕ ТЕХНОЛОГИИ ОНТОЛОГИИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. URL: http://ceur-ws.org/Vol-2064/paper01.pdf (дата обращения 14.11.2022).

13. Shabalin, A. M. Development of a Set of Procedures for Providing Remote Access to a Corporate Computer Network by means of the SSH Protocol (Using the Example of the CISCO IOS Operating System) / A. M. Shabalin, E. A. Kaliberda // Dynamics of Systems, Mechanisms and Machines, Dynamics: 15th International IEEE Scientific and Technical Conference, Omsk, 09–11 ноября 2021 года. – IEEE: Institute of Electrical and Electronics Engineers Inc., 2021. – DOI 10.1109/Dynamics52735.2021.9653723. – EDN OBZZYO.

References

1. Common Vulnerabilities and Exposures: sayt / The MITRE Corporation. – 1999 –. – URL: https://cve.mitre.org/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

2. Exploit Database: sayt / OffSec Services Limited. – 2009 –. – URL: https://www.exploit-db.com/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

3. National Vulnerability Database (NVD): sayt. – Gaithersburg. – . – URL: https://nvd.nist.gov/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

4. Secunia Advisories: sayt / Flexera. – Chicago. – . – URL: https://community.flexera.com/t5/Secunia-Advisories/ct-p/advisories (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

5. Vulnerability Notes Database : sayt / Carnegie Mellon University. – Pittsburgh. – . – URL: https://www.kb.cert.org/vuls/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

6. Bank dannykh ugroz bezopasnosti informatsii: sayt / FAU «GNIII PTZI FSTEK Rossii». – Moskva. – . – URL: https://bdu.fstec.ru/ (data obrashcheniya: 14.11.2022). – Tekst: elektronnyy.

7. Kim A., Luo J., Kang M. Security ontology for annotating resources //OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". – Springer, Berlin, Heidelberg, 2005. – C. 1483-1499.

8. Kotenko I. V., Polubelova O. V., Chechulin A. A. Postroenie modeli dannykh dlya sistemy modelirovaniya setevykh atak na osnove ontologicheskogo podkhoda //Informatika i avtomatizatsiya. – 2013. – №. 26. – S. 26-39.

9. Mirzagitov A. A., Pal'chunov D. E. Metody razrabotki ontologii po informatsionnoy bezopasnosti, osnovannye na pretsedentnom podkhode //Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionnye tekhnologii. – 2013. – T. 11. – №. 3. – S. 37-46.

10. Garshina V. V., Stepantsov V. A. Ontologicheskiy podkhod dlya analiza riskov bezopasnosti informatsionnykh sistem //Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2018. – №. 3 (29). – S. 18-22.

11. Zagorul'ko Yu. A. Modelirovanie robota, upravlyaemogo rechevymi signalami //Izvestiya Tomskogo politekhnicheskogo universiteta. Inzhiniring georesursov. – 2011. – T. 319. – №. 5. – S. 98-102.

12. Aktaeva A.U., Niyazova R., Seralieva A., Sarsenbaeva Zh., Dautov A., Kusainova U, Zhartanov S. KOGNITIVNYE TEKhNOLOGII ONTOLOGII V SISTEMAKh INFORMATsIONNOY BEZOPASNOSTI. URL: http://ceur-ws.org/Vol-2064/paper01.pdf (data obrashcheniya 14.11.2022).

13. Shabalin, A. M. Development of a Set of Procedures for Providing Remote Access to a Corporate Computer Network by means of the SSH Protocol (Using the Example of the CISCO IOS Operating System) / A. M. Shabalin, E. A. Kaliberda // Dynamics of Systems, Mechanisms and Machines, Dynamics: 15th International IEEE Scientific and Technical Conference, Omsk, 09–11 noyabrya 2021 goda. – IEEE: Institute of Electrical and Electronics Engineers Inc., 2021. – DOI 10.1109/Dynamics52735.2021.9653723. – EDN OBZZYO.

ЗАХАРОВ Александр Анатольевич, доктор технических наук, профессор, заведующий базовой кафедрой безопасности информационных технологий умного города, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: a.a.zakharov@utmn.ru

ШАБАЛИН Андрей Михайлович, кандидат педагогических наук, доцент, доцент кафедры информационной безопасности, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: a.m.shabalin@utmn.ru

ХАНБЕКОВ Шамиль Ирекович, аспирант 2 курса, ассистент кафедры информационной безопасности, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: s.i.khanbekov@utmn.ru

ДЖАЛИЛЗОДА Дунё Бехруз, ведущий инженер-программист, МКУ «Тюменьгортранс». 625019, г. Тюмень ул. Республики, 200. E-mail: d.jalilzoda@vk.com

ПОНОМАРЕВ Кирилл Юрьевич, Руководитель группы .NET ООО «АйТиТуДжи. 109544, г. Москва, ул. Большая Андреевская, 17. E-mail: drmckay-kirill@yandex.ru

ZAKHAROV Aleksandr Anatol'evich, doctor of technical sciences, professor, head of Base department of smart city technologies information security, Tyumen state university. 625003, Tyumen, Volodarskogo street, 6. E-mail: a.a.zakharov@utmn.ru

SHABALIN Andrey Mikhaylovich, candidate of pedagogical sciences, docent of Department of information security, Tyumen State University. 625003, Tyumen, Volodarskogo street, 6. E-mail: a.m.shabalin@utmn.ru

KHANBEKOV Shamil Irekovich, 2nd year graduate student, assistant of Department of information security, Tyumen State University. 625003, Tyumen, Volodarskogo street, 6. E-mail: s.i.khanbekov@utmn.ru

DZHALILZODA Dune Bekhruz, leading software engineer. 625019, Tyumen, st. Republic, 2 MKU "Tyumengortrans". E-mail: d.jalilzoda@vk.com

PONOMAREV Kirill Yuryevich, Head of the .NET group of LLC ITToGi. 109544, Moscow, Bolshaya Andreevskaya street, 17. E-mail: drmckay-kirill@yandex.ru

УДК 004.89+004.056 Вестник УрФО № 4(46) / 2022, с. 76–87

Ручай А.Н., Токарев И.В., Грибачёв А.С.

DOI: 10.14529/secur220409

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТАВ СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

В настоящее время обработка информации и работа с большим объемом данных является важными задачами, поэтому огромную роль играет защита этой информации, разработка и улучшение моделей безопасности, основанных на реальных наборах данных. Безопасность компьютерных систем и сетей передачи данных имеет определяющее значение не только для коммерческих структур и граждан, но и для государства в целом. Данная проблема подтверждается также тем, что количество компьютерных атак каждый год увеличивается, а их уровень подготовленности и направленности усиливается. Такое увеличение атак объясняется ростом зависимости промышленности от цифровой инфраструктуры и других сфер жизнедеятельности, а также трудностями поддержания компетенций специалистов в области кибербезопасности. В статье рассматривается научная литература по методам машинного обучения и искусственного интеллекта, которые применяются в сфере компьютерной безопасности.

Ключевые слова: *кибербезопасность, интеллектуальный анализ данных, искусственный интеллект, машинное обучение.*

METHODS OF MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE IN THE FIELD OF INFORMATION SECURITY: ANALYSIS OF THE CURRENT STATE AND PROSPECTS FOR DEVELOPMENT

Currently the processing of information and work with a large amount of data is important,therefore, the protection of this information, the development and improvement of security models based on real data sets, plays a huge role. The security of computer systems and data transmission networks is of decisive importance not only for commercial structures and citizens, but also states. This problem is also confirmed by the fact that the number of computer attacks is increasing every yearand they turn into be moresophisticated and distributed. This increase in attacks is due to the growing dependence of the industry on digital infrastructure and other areas of life, as well as the difficulties in maintaining the competencies of cybersecurity specialists. This article is review of scientific papers on the methods of machine learning and artificial intelligence used in the field of computer security.

Keywords: *cyber security, data mining, artificial intelligent, machine learning.*

1. Введение

Киберпространство в последние годы меняется так быстро, что не только обычные пользователи, но и специалисты в области компьютерных технологий и информационной безопасности не могут поспеть. С каждым днем растет объем обрабатываемых данных, добавляются новые устройства, приложения и сервисы, использующие сеть Интернет. Цифровизация дала мощный толчок к переводу большинства бизнес-процессов в онлайн, развитию концепций и технологий во всех сферах жизни человека.

Тренд цифровизации и скорость ее развития объясняется появлением принципиально новых технологий и инструментов. Массовое использование языков программирования, фреймворков и сред разработки, перевод инфраструктуры организации в «облака», контейнеризация и виртуализация, – все эти инструменты способствуют реализации серьезных проектов в максимально короткий срок. Однако, такие инструменты доступны и злоумышленникам, которые могут использовать их в своих целях, скорость появления новых киберугроз впечатляет, что способствует увеличению значимости области компьютерной безопасности, необходимости противодействиязлоумышленникам, которые используют такие же высокоэффективные инструменты разработки, но в иных целях.

Учитывая темп развития технологий, можно с уверенностью сказать, что в ближайшее время искусственный интеллект может стать сильным инструментом при обеспечении компьютерной безопасности. И несмотря на то, что участие человека остается достаточно важным аспектом не только вэтой сфере, но и в других отраслях, в решении некоторых определенных задач машина постепенно начинает нас опережать.

Диалоги о практическом использовании искусственного интеллекта, в частности, в области компьютерной безопасности, ведутся уже достаточно давно, однако применение продуктов с машинным обучением в корпоративной среде стало возможным лишь тогда, когда качество и эффективность работы начало оправдывать вложенные в них средства, а уровень подготовленности и оснащенности киберпреступников вырос настолько, что эффективно и своевременно оказывать противодействие им возможно лишь с использованием современных технологий.

Теме искусственного интеллекта в области кибербезопасности уделено внимание во многих специальных, педагогических, научно-популярных и художественных изданиях, такая литература доступна для широкого круга читателей [1, 2].

Развитие применения информационных технологий в различных областях способствует совершенствованию работы институтов государственной власти. Наряду с совершенствованием технологий, реализация задач цифровой трансформации системы государственного управления сталкивается с определенными сложностями, наблюдается рост направленных компьютерных атак на создаваемые информационные системы. При этом практика централизованного внедрения единых цифровых решений без одновременного создания системы обеспечения их информационной безопасности существенно повышает риски проявления угроз безопасности и, как следствие, нанесение ущерба интересам личности, общества и государства [3]. Новые технологии машинного обучения позволяют достигать значительного прогресса как в развитии информационно-вычислительной техники, так и в совершенствовании процессов обеспечения информационной безопасности компьютерного оборудования и информационных систем.

Согласно работам Ozlem Yavanoglu (2017) [4] и Sumeet Dua (2011) [5], компьютерная безопасность является важной областью исследований, поскольку абсолютно все сферы деятельности, а также обычные граждане, собирают, обрабатывают и хранят огромный объем данных на электронно-вычислительных машинах. Для обеспечения безопасности существования информационной системы компаниям требуется прикладывать огромные усилия. Компонентами информационной безопасности являются: обеспечение безопасности сетей, данных, конечных хостов, мобильная безопасность и многое другое. Сегодня значимость использования сети Интернет и компьютерных систем серьезно расширились, и они являются неотъемлемой частью жизни современного человека. В связи с экспоненциальным ростом компьютерных систем и использованием сетей, безопасность становится все более значимым условием обеспечения бесперебойной работы. Киберпреступники могут использовать различные пути, чтобы нанести ущерб конечным пользователям компьютерных сетей и систем, что является риском для утечки данных либо их потери. Огромную роль в обнаружении таких угроз безопасности информационных систем играет искусственный интеллект и машинное обучение [4 – 9].

Для того, чтобы оценить значимость применения искусственного интеллекта и машинного обучения необходимо явно представлять на какой стадии развития находится данная сфера. Для более подробного раскрытия выбранной темы структура данного обзора строится следующим образом: в первой части даются основные понятия, принципы и определения машинного обучения, краткая история развития искусственного интеллекта, в основной части освещены научные труды, анализирующие методы машинного обучения и искусственного интеллекта, приводятся примеры практического применения искусственного интеллекта и машинного обучения в области информационной безопасности, в заключении описаны наиболее значимые современные задачи и проблемы, а также ограничения данных методов в сфере информационной безопасности и направления дальнейшего исследования.

2. Искусственный интеллект и информационная безопасность

Прежде чем переходить к определениям и принципам машинного обучения, необходимо разобраться в определениях основных понятий информационной безопасности.

Кибербезопасность представляет собой набор мер по обеспечению безопасности, конфиденциальности, целостности и доступности данных [4]. Авторами Ankush Meshram (2017) [10] и Maryam Feily (2009) [11] объясняется известная триада конфиденциальности, целостности и доступности данных при обеспечении защиты информации.

Конфиденциальность направлена на ограничение раскрытия информации и пре-

доставления доступа информации только уполномоченным лицам. Благодаря конфиденциальности, компании могут защитить свои данные и активы от злоумышленников. В работе Malek BenSalem (2008) [12] описываются основные способы обеспечения конфиденциальности: шифрование, контроль доступа и стеганография.

Понятие целостности требует защиты данных последовательным, точным и надежным способом. Необходимо гарантировать, что данные не будут изменены в течение заданного периода времени. Для того, чтобы предотвратить внесение изменений неавторизованными пользователями, необходимо применять правильные процессы и действия. Такие инструменты и алгоритмы как хеширование, цифровые подписи, сертификаты, строгое выполнение инструкций обеспечивают целостность данных. [11, 12].

Доступность – это еще одна концепция безопасности, в соответствии с которой данные и ресурсы должны быть доступны тогда, когда людям нужен доступ к ним, особенно во время чрезвычайных ситуаций или стихийных бедствий. Специалисты по кибербезопасности должны справляться с тремя основными проблемами доступности: отказ в обслуживании, потеря информационной системы при возникновении чрезвычайной ситуации и отказы оборудования при нормальной работе [12].

Для более детального понимания проблематики искусственного интеллекта прежде всего нужно дать определения таким важным терминам как искусственный интеллект, нейронная сеть и машинное обучение и другим.

Под искусственным интеллектом понимается исполнение задач принятия решений непосредственно самими информационными системами, а также способность их обучению, подобно интеллекту живого существа.

Нейронная сеть – это набор искусственных нейронов, связанных между собой, которые выполняют простые логические операции, имеющие способность машинного обучения.

Машинное обучение представляет собой один из методов искусственного интеллекта, основой которого является не прямое решение задачи, а прежде всего обучение за счет использования решения большого количества сходных задач.

Существует несколько подходов машинного обучения:

• При использовании способа машинного обучения с учителем применяются определенные наборы данных, классифицированные по характерным признакам, для которых используется обучающая выборка, либо человек, который определяет корректные пары «вопрос – ответ». Подробнее с этим способом машинного обучения можно ознакомиться в [13].

• При обучении без учителя информационная система должна сама, посредством известных свойств объектов определить взаимосвязь между ними, при этом не применяются размеченные наборы данных и не задаются корректные пары «вопрос – ответ».

• Машинное обучение с частичным привлечением учителя заключается в том, что берется комбинация некоторого количества размеченных наборов данных и значительно большее количество неразмеченных.

• При применении машинного обучения с подкреплением, «учитель» представляет собой определенную среду функционирования, которая дает ответ информационной системе с учетом принятых данной системой решений.

При этом в машинном обучении возможно использование других алгоритмов, например градиентный бустинг, байесовские сети, цепи Маркова.

Глубокое обучение – один из частных случаев машинного обучения, который заключается в использовании сложной многослойной искусственной нейронной сети для эмуляции работы человеческого мозга, а также для возможности обработки речи, звуковых и визуальных образов. Подробнее ознакомиться с глубоким обучением можно в [14]. Сегодня использование машинного зрения представлено в системах обеспечения безопасности, контроля транспорта и пассажиров. Обработка речи и распознавание слов помогают голосовым ассистентам Siri, Алиса или Маруся взаимодействовать с пользователями таких систем.

Большие данные представляют собой огромный набор различных данных, имеющих определенные характеристики: объем, скорость изменения и разнообразие. Важной задачей является повышение ценности больших данных, для этого необходимо реализовать переход от разнородных данных к структурированным, а в дальнейшем – к знаниям. Полученный из релевантного массива больших данных набор данных, – один из самых

ценных компонентов для машинного обучения в современных системах.

Глубокий анализ данных – процесс получения необходимой информации из неструктурированного набора больших данных.

Нечёткая логика – использование нестрогих правил и ответов при решении задач в системах нейронных сетей и искусственного интеллекта. Одно из применений – моделирование поведения человека, например, для сужения или ограничения условий поиска ответа на вопрос в зависимости от контекста.

В исследованиях Micah Musser и AshtonGarriott (2021) [18] машинное обучение представляется как раздел науки о том, как компьютер станет действовать без явной типизации. Основная задача машинного обучения – это создание моделей, которые смогут обрабатывать набор входных данных и работать с ними, применяя статистический анализ для прогнозирования выходного значения в границах с подходящим диапазоном [4]. В сфере компьютерных наук машинное обучение – одно из самых быстроразвивающихся разделов с комплексным практическим применением. Алгоритмы машинного обучения классифицируются как контролируемое, неконтролируемое обучение и обучение с учителем. Контролируемые алгоритмы делятся на регрессию и классификацию [15 – 26].

Искусственный интеллект (ИИ) представляет собой область научных исследований, которая направлена на увеличение вычислительной мощности.

ИИ, как правило, применяется для решения сложных задач, которые не удалось решить без объединенного интеллекта, обнаружения скрытых закономерностей из данных и разработки интеллектуальных машин [2].

ИИ имеет множество практических применений для представления знаний, поиска информации, распознавание речи, распознавания естественного языка, компьютерного зрения, а также, он важен в биоинформатике, в экспертных системах, в робототехнике, в разработках игр и киберзащиты с помощью различных алгоритмов, таких как нечеткая логика, генетические алгоритмы, стохастические алгоритмы, искусственная нейронная сеть.

Искусственные нейронные сети (ИНС) представляют собой метод искусственного интеллекта, который включает в себя набор компьютерных алгоритмов для имитации процесса обработки нейронами головного мозга человека информации. ИНС собирают свои знания, обнаруживая модели и отношения между данными, и учатся через их архитектуры, передаточные функции и алгоритмы обучения.

Существует множество типов нейронных сетей для различных целей. Многослойные нейронные сети персептронного типа являются самыми простыми и наиболее часто используемой архитектурой нейронных сетей, которые обучаются с помощью множества алгоритмов обучения.

3. Применение искусственного интеллекта в кибербезопасности

После того, как рассмотрены основные принципы и определения машинного обучения, можно перейти к вопросу практического применения систем искусственного интеллекта в области компьютерной безопасности. В настоящее время наблюдается развитие угроз безопасности, а также рост возникающих инцидентов в информационных системах. Нехватка квалифицированных специалистов по защите информации, а также необходимость оперативного реагирования при наступлении киберинцидента прежде всего объясняет важность использования искусственного интеллекта в области информационной безопасности.

Необходимость выявления аномалий в большом количестве событий информационной безопасности объясняет незаменимость системы защиты на основе искусственного интеллекта. Один из примеров выявления аномалий – анализ журналов систем защиты информации, данных из SIEM-систем (систем реагирования на киберинциденты) или SOAR-решений (программ для координации и управления системами безопасности). Эта информация, в совокупности с данными уже отработанных и закрытых инцидентов, будет представлять собой качественный размеченный набор данных, на котором системе можно будет легко обучиться.

Выявление аномалий позволяет обеспечивать защиту пользовательских данных. Банковские сервисы могут собирать, обрабатывать и анализировать данные об определенных признаках в работе пользователей в целях оперативного определения скомпрометированных учетных записей.

Обладая знаниями о типичном поведении пользователей, система искусственного интеллекта может бороться с внутренними

нарушителями путем оповещения администраторов таких систем о возникновении нештатной ситуации, в случае изменения модели поведения пользователя.

Одной из самых серьезных проблем безопасности является то, что технологии доступны большой массе людей и могут использоваться не только во благо, но и во вред различными киберпреступниками, что в свою очередь определяет необходимость использования современных средств и методов защиты для своевременного реагирования на компьютерные инциденты.

Сформулируем наиболее значимые современные научно-исследовательские задачи в сфере искусственного интеллекта в области кибербезопасности: защита от сетевых атак с использованием технологии больших данных и эвристического анализа; создание моделей использования нейросетевых методов в задачах кибербезопасности; исследование и создание технологии автоматического управления информационной безопасностью; создание технологии защищенного доступа; разработка технологии высокопроизводительной обработки и визуализации больших массивов данных;анализ угроз кибербезопасности.

Приведем конкретные примеры.

Анализ сетевого трафика. Анализ сетевого трафика позволяет своевременно обнаруживать и предотвращать деятельность злоумышленников во внутренних сетях. Чаще всего это задача классификации трафика в реальном времени, в которой алгоритм машинного обучения выполняет роль системы обнаружения и предотвращения вторжений (Intrusion Detection System, Intrusion Prevention System) [30].

WAF (Web Application Firewall). Распространенность веб-приложений, а также их уязвимость, ставит вопрос о защите. В данной задаче алгоритм МО обучается обнаруживать и предотвращать атаки на веб-приложения. Данная задача классификации хорошо решается рекуррентными нейронными сетями [28] и автокодировщиками [32].

Анализ исходного кода. В данной задаче алгоритмы машинного обучения могут применяться в качестве аналогов статических анализаторов кода для выявлений уязвимостей ПО на стадиях разработки. Это задача классификации. Здесь применяются архитектуры рекуррентных нейронных сетей и модели типа Transformer [33].

Фаззинг (Fuzzing). Фаззинг– это один из способов тестирования ПО, при котором на вход приложения подаются данные, способные привести к неправильному функционированию приложения. Для эффективного фаззинга приложений исследователи применяют рекуррентные и генеративные нейронные сети [29].

SQL-инъекции. SQL-инъекции являются распространённой уязвимостью приложений, использующих базы данных. Важной задачей является своевременно детектирование SQL-атак, поэтому многие исследователи занимаются данной задачей [35]. Генеративные нейронные сети могут быть применены для генерации новых примеров SQL-инъекций [34].

Фильтрация фишинговых сообщений. Фишинг является распространённым видом интернет-мошенничества. Нейронные сети и другие методы машинного обучения хорошо подходят в качестве инструмента фильтрации фишинговых атак. В данной задаче широко исследуется применение следующих алгоритмов: деревья принятия решений (decisiontrees), случайные леса (randomforest), автокодировщики (autoencoders), SVM [31].

4. Проблемы кибербезопасности в искусственном интеллекте

Проблемы технологии методов синтеза изображения (дипфейков).

Технология дипфейков стала серьезным оружием. Например, создание поддельных политических, порнографических и видео с различным содержанием является серьезной угрозой информационной безопасности.

По всему миру принимаются различные меры для пресечения таких видов угроз: введение ответственности за публикацию подобного контента, разработка нормативных актов для решения проблем при использовании технологий.

Возникает вопрос об ответственности не только за распространение данного контента, но и о правах собственности на такого рода произведение. Автор программного обеспечения не всегда знает о конечном продукте, поэтому необходимо определиться с интеллектуальными правами преступников и жертв.

Проблема непонимания и недоверия к технологии искусственного интеллекта. По мнению кандидата юридических наук Романа Дремлюга, в наше время многие не понимают технологию искусственного интел-

лекта [27]. Одно из заблуждений – работа всей системы искусственного интеллекта зависит от программиста, а значит ответственность несет создатель системы. Программист же способен исключить лишь некоторые риски. Неверное суждение об ответственности программиста ведет к неверной оценке возможностей интеллекта. Сегодня искусственный интеллект охватывает все большие области нашей жизнедеятельности, его работу уже можно наблюдать в судебной деятельности, в экспериментах с постановкой медицинского диагноза.

Киберпреступления в сфере финансовых услуг. Развитие банковских продуктов и услуг не стоят на месте. Большинство из них можно получить в любом месте и в любое время, необходимо лишь иметь под рукой компьютер или смартфон и доступ в интернет. Однако, мошенники развиваются быстрее, чем системы безопасности, и безопасность предоставления таких услуг также не успевает за развитием услуг. Для обеспечения безопасности в оказании банковских услуг онлайн необходимо повышать ответственность и наделять финансовые организации дополнительными полномочиями.

Проблема потерь рабочих мест. Все чаще возникают вопросы о необходимости сотрудников в тех направлениях трудовой деятельности, где их возможно заменить роботизированными машинами. Действительно, технологический процесс быстро и успешно развивается: машины, позволяющие производить вычисления без ошибок и с высокой скоростью, электронные системы отслеживания и мониторинга и многое другое. Согласно прогнозамк2030 году промышленный сектор может сократить несколько миллионов сотрудников, их рабочие места займут роботизированные системы. Но не нужно думать, что с приходом роботов и искусственного интеллекта наступит безработица. Благодаря совершенствованию и роботизации рабочих процессов возрастет потребность в высококвалифицированных рабочих местах. Однако, последствия от роботизации производств в разных странах могут отличаться. Страны, в которых зависимость от низкоквалифицированных работников выше, сильнее пострадают от роботизации.

5. Применение машинного обучения в кибербезопасности

В работах [36 – 40] представлены многочисленные примеры использования машинного обучения и искусственного интеллекта в кибербезопасности.

Классификация данных по конфиденциальности. Соблюдение законов и защита конфиденциальности данных – одна из основных задач, стоящих перед организациями. Классификация помогает отделить данные, позволяющие произвести идентификацию пользователей, от неидентифицирующих данных.

Профили безопасности на основе поведения пользователей. Разработка моделей на основе поведения пользователей в системе может позволить совершенствовать систему безопасности в организации. Такие модели позволяют зафиксировать действия злоумышленника путем анализа изменений его поведения в системе. Создание профилей пользователей на основе их поведения может стать базой для предиктивной модели угрозы.

Профили безопасности на основе данных о работе системы. Проанализировав работу компьютерного рабочего места пользователя, также возможно составить профиль безопасности по следующим признакам: загрузка центрального процессора, оперативной памяти, интернет-канала. Их чрезмерная активность может означать наличие в системе вредоносного кода.

Блокировка ботов на основе поведения. Действия ботов могут парализовать работу веб-сайтов, что негативно скажется на работе организации в целом. Системы с применением машинного обучения позволяют не только определять активных ботов, но и произвести их блокировку. Основываясь на поведении злоумышленника, алгоритм сформирует прогнозную модель и превентивно заблокирует даже новых злоумышленников с похожей активностью.

6. Вклад искусственного интеллекта в решение проблем кибербезопасности

Разговаривая о современных способах использования машинного обучения и искусственного интеллекта в области информационной безопасности, нельзя не сказать о ряде проблем в этой сфере. Применение технологий искусственного интеллекта в процессах, которые хорошо нам известны, может оказаться очень полезным для их улучшения.

Человеческий фактор и эффективность ручного труда. Существенная часть уязвимостей кибербезопасности заключена в человеческом факторе. Компьютерная без-

опасность не перестает совершенствоваться и становиться сложнее. Применяемые инструменты помогают искать и устранять проблемы при модификациях и обновлениях систем. Оценка надежности выполнения работ вручную – достаточно ресурсозатратная задача, тогда как использование интеллектуальной автоматизации позволяет оперативно обнаруживать проблемы и получать анализ по их устранению.Одни и те же действия для решения проблемы невозможно каждый раз выполнить одинаково, тем более в постоянно меняющейся среде. Производить индивидуальные настройки устройств, обновлять и исправлять данные настройки, – достаточно трудоемкая задача. При этом вид и характер угроз непрерывно изменяется. Время реагирование человека на такие угрозы резко снижается, особенно при возникновении нештатных ситуаций. Системы же, основанные на искусственном интеллекте, работают с минимальными задержками.

Скорость реагирования на угрозу. Оперативность при возникновении угрозы – важнейший показатель эффективности обеспечения безопасности. Технологии позволяют автоматизировать кибератаки, что ускоряет процесс перехода от поиска и использования уязвимостей в системах и развертыванию. Одним из примеров таких угроз являются шифровальщики LockBit. Реакции человека зачастую недостаточно для предотвращения угрозы, несмотря на то, что отлично известно о типе атаки. Многим специалистам по безопасности приходится заниматься устранением последствий, а не предотвращением атак. Дополнительная проблема заключается в необнаруженных атаках.Технологии помогают специалистам сформировать отчеты, для упрощения обработки данных и принятия решений, а также предоставить рекомендации для уменьшения ущерба предотвращения новых атак.

Прогнозирование угроз. Определить и подготовить прогноз для новых угроз еще один фактор, оказывающий влияние на время реагирования на атаку. Программы на основе машинного обучения позволяют не только распознавать атаку, определяя схожие черты по ранее обнаруженным, но и облегчают прогнозирование таких угроз и сокращают время реагирования, благодаря работе с базой известных угроз.

Кадры. Поиск квалифицированного специалиста с требуемыми знаниями и навыками является систематической проблемой. Оплата труда такого специалиста, а также его обучение и повышение квалификации требует серьезного финансирования. Внедрение систем искусственного интеллекта позволяет существенно сократить расходы на содержание специалистов.

Адаптируемость. В сравнении с другими проблемами,проблема адаптируемости не лежит на поверхности, но может принести значительный ущерб безопасности.Сотрудники могут не обладать знаниями в работе с некоторыми методами, инструментами, либо правилами, принятыми в конкретной организации, что может привести к неэффективности выполнения работы команды в целом. Выполнение даже простой задачи может существенно затянуться. На внедрение всего нового требуется время. Для решения этой проблемы могут помочь алгоритмы машинного обучения.

7. Заключение

Защита компьютерных систем от компьютерных атак является одним из основных вопросов национальной и международной безопасности. На сегодняшний день информационная безопасность подвержена определенным трудностям: это и большие потоки событий, и снижение экспертизы, и отсутствие достаточного количества обученного персонала. Наблюдается огромный рост атак, независимо от принимаемых усилий по защите систем, что объясняет высокую значимость применения современных методик по защите информационных систем от такого вида атак. Одной из самых востребованных методик является машинное обучение. Пока для принятия решения невозможен полный отказ от участия человека, однако, существует множество разработанных моделей, которые позволяют определять новые угрозы и выявлять аномалии. Использование методов машинного обучения в сфере информационной безопасности является одним из самым перспективных способов для обеспечения защиты современных информационных систем.

В настоящей статье описана краткая история развития искусственного интеллекта в кибербезопасности, проведены исследования различных методов машинного обучения и искусственного интеллекта, показано, что искусственный интеллект и машинное обучение играют значительную роль в защите информационных систем, рассмотрено практическое применение искусственного интел-

лекта в области информационной безопасности, наиболее значимые современные научно-исследовательские задачи и некоторые примеры проблем, связанных с искусственным интеллектом в области информационной безопасности, приведены примеры использования машинного обучения в кибербезопасности, уделено внимание вкладу искусственного интеллекта в решение проблем кибербезопасности и его роли в области информационной безопасности. Дальнейшее направление исследования заключается в том, чтобы рассмотреть классы различных наборов данных, методы выявления аномалий, определить достоинства и недостаткиалгоритмов машинного обучения, выработать универсальный подходк разработке моделей, обобщить и опубликовать результаты.

Литература

1. Choi Y., Liu P., Shang Z., Wang H., Wang Z., Zhang L., Zhou J., Zou Q. Using Deep Learning to Solve Computer Security Challenges: A Survey, arXiv preprint arXiv:1912.05721, 2020.

2. Dhir N., Hoeltgebaum H., Adams N., Briers M., Burke A., Jones P. Prospective Artificial Intelligence Approaches for Active Cyber Defence, arXiv preprint arXiv:2104.09981, 2021.

3. Указ Президента Российской Федерации № 646 (2016). Доступен по ссылке: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. Доктрина информационной безопасности Российской Федерации.

4. Yavanoglu O., Aydos M. A review on cyber security datasets for machine learning algorithms. IEEE International Conference on Big Data (Big Data), 2017.

5. Dua S., Du X. Data mining and machine learning in cybersecurity. CRC press, 2016.

6. Symantec Corporation. Symantec Web Application Firewall. OWASP TOP 10 2017 COVERAGE. Available at: https://docs.broadcom.com/doc/web-application-firewall-owasp-top-10-2017-coverage-en. The Ten Most Critical Web Application Security Risks, 2017.

7. Mnih V., Kavukcuoglu K., Silver D., Rusu A.A., Veness J., Bellemare M.G., Graves A., Riedmiller M., Fidjeland A.K., Ostrovski G., Petersen S., Beattie Ch., Sadik A., Antonoglou I., King H., Kumaran Dh., Wierstra D, Legg Sh. & Hassabis D. Human-level control through deep reinforcement learning. J. Nature, 2015, V. 518. pp. 529–533.

8. Silver D., Huang A., Maddison C.J., Guez A., Sifre L., Driessche G., Schrittwieser J., Antonoglou I., Panneershelvam V., Lanctot M., Dieleman S., Grewe D., Nham J., Kalchbrenner N., Sutskever I., Lillicrap T., Leach M., Kavukcuoglu K., Graepel Th. & Hassabis D. Mastering the game of Go with deep neural networks and tree search, J. Nature, 2016, V. 529, pp. 484–489.

9. Kaspersky. Искусственный интеллект и машинное обучение в кибербезопасности – прогноз на будущее. Доступен по ссылке: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity.

10. Meshram A., Haas C. Anomaly detection in industrial networks using machine learning: a roadmap. Machine Learning for Cyber Physical Systems, 2017, pp. 65–72.

11. Feily M., Alireza S., Sureswaran R. A survey of botnet and botnet detection. Emerging Security Information, Systems and Technologies, 2009.

12. Salem M.B., Hershkop S., Stolfo S.J. A survey of insider attack detection research, Insider Attack and Cyber Security, 2008, pp. 69-90.

13. Van Der Malsburg C. Frank Rosenblatt: Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms, J. Springer, 1984, pp. 245–248.

14. Goodfellow I., Bengio Y., Courville A. Deep Learning, The MIT Press, 2016.

15. Albon C. Machine Learning with Python Cookbook Practical Solutions from Preprocessing to Deep Learning, O'Reilly Media, Inc., 2018, 366 p.

16. Watt J., Borhani R., Katsaggelos A.K. Machine Learning Refined Foundations, Algorithms, and Applications, Cambridge University Press, 2020, 301 p.

17. Goldblum M., Tsipras D., Xie C., Chen X., Schwarzschild A., Song D., Madry A., Li B., Goldstein T. Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses. CoRR abs, 2020.

18. Musser M., Garriott A. Machine Learning and Cybersecurity. Center for Security and Emerging Technology, 2021.

19. Sarker I., Kayes A., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020.

20. Чио К., Фримэн Д. Машинное обучение и безопасность, ДМКПресс, 2020, 388 с.

21. Neethu B. Adaptive Intrusion Detection Using Machine Learning, International Journal of Computer Science and Network Security, 2013, pp. 118-124.

22. Kozik R., Choras M., Renk R., Hołubowicz W. A Proposal of Algorithm for Web Applications Cyber Attack Detection, J. Springer, 2014.

23. Rashid T. Make Your Own Neural Network, CreateSpace Independent Publishing Platform, 2016, 222 p.

24. Bhuyan M., Bhattacharyya K., Kalita J. Towards Generating Real-life Datasets for Network Intrusion Detection, IJ Network Security, 2015, pp. 683-701.

25. Kato K., Klyuev V. An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine, IJICR, 2014, pp. 464-471.

26. Glassner A. Deep Learning, The Imaginary Institute, 2018.

27. Дремлюга Р.И. Основы национального регулирования применения искусственного интеллекта: опыт Сингапура, Азиатско-Тихоокеанский регион: экономика, политика, право, 2022, с. 214–224.

28. IŞiker B., SoGukpinar I. Machine Learning Based Web Application Firewall, 2021 2nd International Informatics and Software Engineering Conference (IISEC), 2021, pp. 1-6.

29. Zhu X. et al. Defuzz: Deep learning guided directed fuzzing, arXiv preprint arXiv:2010.12149, 2020.

30. Alkasassbeh M., Almseidin M. Machine learning methods for network intrusion detection, arXiv preprint arXiv:1809.02610, 2018.

31. Shahrivari V., Darabi M., Izadi M. Phishing detection using machine learning techniques, arXiv preprint arXiv:2009.11116, 2020.

32. Vartouni A., Kashi S., Teshnehlab M. An anomaly detection method to detect web attacks using Stacked Auto-Encoder, 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2018, pp. 131-134.

33. Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, 2021, pp. 1-6.

34. Lu D. et al. A GAN-based Method for Generating SQL Injection Attack Samples, 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2022, pp. 1827-1833.

35. Latchoumi T., Reddy M., Balamurugan K. Applied machine learning predictive analytics to SQL injection attack detection and prevention, European Journal of Molecular & Clinical Medicine., 2020.

36. Асяев Г.Д., Соколов А.Н. Обнаружение вторжений на основе анализа аномального поведения локальной сети с использованием алгоритмов машинного обучения с учителем, Вестник УрФО. Безопасность в Информационной Сфере, 2020, с. 77-83.

37. Соколов А.Н., Алабугин С.К., Пятницкий И.А. Применение методов одноклассовой классификации для обнаружения вторжений, Вестник УрФО. Безопасность в Информационной Сфере, 2018, с. 43-48.

38. Алабугин С.К., Соколов А.Н., Пятницкий И.А. Применение рекуррентных и сверточных нейронных сетей для выявления аномалий технологического процесса, Вестник УрФО. Безопасность в Информационной Сфере, 2019, с. 60-65.

39. Асяев Г.Д., Соколов А.Н. Модели предиктивной защиты информации автоматизированной системы управления водоснабжением на основе временных рядов с использованием технологий машинного обучения, Вестник УрФО. Безопасность в Информационной Сфере, 2021, с. 39-45.

40. Фельдман Е.В. Ручай А.Н., Чербаджи Д.Ю. Модель выявления аномальных банковских транзакций на основе машинного обучения, Вестник УрФО. Безопасность в Информационной Сфере, 2021, с. 27-35.

References

1. Choi Y., Liu P., Shang Z., Wang H., Wang Z., Zhang L., Zhou J., Zou Q. Using Deep Learning to Solve Computer Security Challenges: A Survey, arXiv preprint arXiv:1912.05721, 2020.

2. Dhir N., Hoeltgebaum H., Adams N., Briers M., Burke A., Jones P. Prospective Artificial Intelligence Approaches for Active Cyber Defence, arXiv preprint arXiv:2104.09981, 2021.

3. Ukaz Prezidenta Rossiyskoy Federatsii № 646 (2016). Dostupen po ssylke: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii.

4. Yavanoglu O., Aydos M. A review on cyber security datasets for machine learning algorithms. IEEE International Conference on Big Data (Big Data), 2017.

5. Dua S., Du X. Data mining and machine learning in cybersecurity. CRC press, 2016.

6. Symantec Corporation. Symantec Web Application Firewall. OWASP TOP 10 2017 COVERAGE.

Available at: https://docs.broadcom.com/doc/web-application-firewall-owasp-top-10-2017-coverage-en. The Ten Most Critical Web Application Security Risks, 2017.

7. Mnih V., Kavukcuoglu K., Silver D., Rusu A.A., Veness J., Bellemare M.G., Graves A., Riedmiller M., Fidjeland A.K., Ostrovski G., Petersen S., Beattie Ch., Sadik A., Antonoglou I., King H., Kumaran Dh., Wierstra D, Legg Sh. & Hassabis D. Human-level control through deep reinforcement learning. J. Nature, 2015, V. 518. pp. 529–533.

8. Silver D., Huang A., Maddison C.J., Guez A., Sifre L., Driessche G., Schrittwieser J., Antonoglou I., Panneershelvam V., Lanctot M., Dieleman S., Grewe D., Nham J., Kalchbrenner N., Sutskever I., Lillicrap T., Leach M., Kavukcuoglu K., Graepel Th. & Hassabis D. Mastering the game of Go with deep neural networks and tree search, J. Nature, 2016, V. 529, pp. 484–489.

9. Kasperskiy. Iskusstvennyy intellekt i mashinnoye obucheniye v oblasti kiberbezopasnosti – prognoz na budushcheye. Dostupen po ssylke: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity.

10. Meshram A., Haas C. Anomaly detection in industrial networks using machine learning: a roadmap. Machine Learning for Cyber Physical Systems, 2017, pp. 65–72.

11. Feily M., Alireza S., Sureswaran R. A survey of botnet and botnet detection. Emerging Security Information, Systems and Technologies, 2009.

12. Salem M.B., Hershkop S., Stolfo S.J. A survey of insider attack detection research, Insider Attack and Cyber Security, 2008, pp. 69-90.

13. Van Der Malsburg C. Frank Rosenblatt: Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms, J. Springer, 1984, pp. 245–248.

14. Goodfellow I., Bengio Y., Courville A. Deep Learning, The MIT Press, 2016.

15. Albon C. Machine Learning with Python Cookbook Practical Solutions from Preprocessing to Deep Learning, O'Reilly Media, Inc., 2018, 366 p.

16. Watt J., Borhani R., Katsaggelos A.K. Machine Learning Refined Foundations, Algorithms, and Applications, Cambridge University Press, 2020, 301 p.

17. Goldblum M., Tsipras D., Xie C., Chen X., Schwarzschild A., Song D., Madry A., Li B., Goldstein T. Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses. CoRR abs, 2020.

18. Musser M., Garriott A. Machine Learning and Cybersecurity. Center for Security and Emerging Technology, 2021.

19. Sarker I., Kayes A., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020.

20. Chio K., Frimen D. Mashinnoye obucheniye i bezopasnost', DMKPress, 2020, 388 c.

21. Neethu B. Adaptive Intrusion Detection Using Machine Learning, International Journal of Computer Science and Network Security, 2013, pp. 118-124.

22. Kozik R., Choras M., Renk R., Hołubowicz W. A Proposal of Algorithm for Web Applications Cyber Attack Detection, J. Springer, 2014.

23. Rashid T. Make Your Own Neural Network, CreateSpace Independent Publishing Platform, 2016, 222 p.

24. Bhuyan M., Bhattacharyya K., Kalita J. Towards Generating Real-life Datasets for Network Intrusion Detection, IJ Network Security, 2015, pp. 683-701.

25. Kato K., Klyuev V. An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine, IJICR, 2014, pp. 464-471.

26. Glassner A. Deep Learning, The Imaginary Institute, 2018.

27. Dremlyuga R.I. Osnovy natsional'nogo regulirovaniya primeneniya iskusstvennogo intellekta: opyt Singapura, Aziatsko-Tikhookeanskiy region: ekonomika, politika, pravo, 2022, s. 214–224.

28. IŞiker B., SoGukpinar I. Machine Learning Based Web Application Firewall, 2021 2nd International Informatics and Software Engineering Conference (IISEC), 2021, pp. 1-6.

29. Zhu X. et al. Defuzz: Deep learning guided directed fuzzing, arXiv preprint arXiv:2010.12149, 2020.

30. Alkasassbeh M., Almseidin M. Machine learning methods for network intrusion detection, arXiv preprint arXiv:1809.02610, 2018.

31. Shahrivari V., Darabi M., Izadi M. Phishing detection using machine learning techniques, arXiv preprint arXiv:2009.11116, 2020.

32. Vartouni A., Kashi S., Teshnehlab M. An anomaly detection method to detect web attacks using Stacked Auto-Encoder, 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2018, pp. 131-134.

33. Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, 2021, pp. 1-6.

34. Lu D. et al. A GAN-based Method for Generating SQL Injection Attack Samples, 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2022, pp. 1827-1833.

35. Latchoumi T., Reddy M., Balamurugan K. Applied machine learning predictive analytics to SQL injection attack detection and prevention, European Journal of Molecular & Clinical Medicine., 2020.

36. Asyayev G.D, Sokolov A.N., Obnaruzheniye vtorzheniy na osnove analiza anomal'nogo povedeniya lokal'noy seti s ispol'zovaniyem algoritmov mashinnogo obucheniya s uchitelem, Vestnik UrFO. Bezopasnost' v Informatsionnoy Sfere, 2020, c.77-83

37. Sokolov A.N., Alabugin S.K., Pyatnitskiy I.A. Primeneniye metodov odnoklassovoy klassifikatsii dlya obnaruzheniya vtorzheniy, Vestnik UrFO. Bezopasnost' v Informatsionnoy Sfere, 2018, c. 43-48.

38. Alabugin S.K., Sokolov A.N., Pyatnitskiy I.A. Primeneniere kurrentnyx i svertochnyx nejronnyx setej dlya vyyavleniya anomalij texnologicheskogo processa, Vestnik UrFO. Bezopasnost v Informacionnoj Sfere, 2019, c. 60-65.

39. Asyaev G.D., Sokolov A.N. Modeli prediktivnoj zashhity informacii avtomatizirovannoj sistemy upravleniya vodosnabzheniem na osnove vremennyx ryadov s ispolzovaniemtexnologijmashinnogoobuch eniya, Vestnik UrFO. Bezopasnost v Informacionnoj Sfere, 2021, c. 39-45.

40. Feldman E.V., Ruchay A.N., Cherbadzhi D.Yu. Model vyyavleniya anomalnyx bankovskix tranzakcij na osnove mashinnogo obucheniya, Vestnik UrFO. Bezopasnost v Informacionnoj Sfere, 2021, c. 27-35.

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

ТОКАРЕВ Игорь Вячеславович, аспирант (соискатель) математического факультета, Челябинский государственный университет. Россия, 454001, Челябинск, ул. Братьев Кашириных, 129. E-mail: tokarev_i_v@mail.ru

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

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

TOKAREV Igor Vyacheslavovich, PhD candidate of the Faculty of Mathematics, Chelyabinsk State University. Russia, 454001, Chelyabinsk, st. Brothers Kashirin, 129. E-mail: tokarev_i_v@mail.ru

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

УДК 004.384 Вестник УрФО № 4(46) / 2022, с. 88–96

Богер А.М., Соколов А.Н., Морозов И.А.

DOI: 10.14529/secur220410

ОЦЕНКА ВОЗДЕЙСТВИЙ DOS-АТАКИ НА ТРАФИК ОБМЕНА ДАННЫМИ МЕЖДУ ПРОГРАММИРУЕМЫМИ ЛОГИЧЕСКИМИ КОНТРОЛЛЕРАМИ SIMATIC 1510 И SIMATIC 1512[1]

В работе исследована эмуляция распределенного DoS-воздействия на лабораторный стенд, осуществляющий взаимодействие двух программируемых логических контроллеров: SIMATIC 1510 и SIMATIC 1512 в автоматизированной системе управления технологическим процессом. В ходе работы совершены внутреннее и внешнее DoS-воздействие, оценены продолжительность выполнения программного цикла контроллера и возможность передачи данных между контроллером и периферийными устройствами, сделан вывод о значительном влиянии DoS-воздействия на рабочий процесс контроллера.

Ключевые слова: *программируемый логический контроллер (ПЛК), сетевые атаки, кибератака, DDoS, АСУ ТП.*

Boger A.M., Sokolov A.N., Morozov I.A.

EVALUATION OF DOS ATTACK IMPACT ON DATA TRAFFIC BETWEEN SIMATIC 1510 AND SIMATIC 1512 PLCS

The paper studies the emulation of a distributed DoS impact on a laboratory stand that interacts with two programmable logic controllers: SIMATIC 1510 and SIMATIC 1512 in an automated process control system. In the course of work, internal and external DoS impacts were made, the duration of the controller program cycle and the possibility of data transfer between

[1] Исследование поддержано грантом Российского научного фонда (проект № 22-71-10095).

the controller and peripheral devices were estimated, and a conclusion was made about the significant impact of DoS impacts on the controller's workflow.

Keywords: *programmable logic controller (PLC), network attacks, cyberattack, DDoS, ICS.*

Стабильность сетевого взаимодействия между программируемыми логическими контроллерами (далее ПЛК) является очень важной частью работоспособности производственных линий заводов и фабрик. Отсутствие стабильности может привести к невозможности обмена управляющими данными между контроллерами и их периферией. А это в свою очередь может привести к потере прибыли и авариям на производстве.

Для проверки возможности сетей уровня контроля автоматизированными системами управления технологическими процессами (АСУ ТП) поддерживать собственную стабильность было принято решение подвергнуть сетевое соединение двух ПЛК нагрузке в виде эмуляции DoS-атаки. Данный тип атаки был выбран как один из наиболее легко осуществимых и наиболее вероятных [1].

В работе использовался лабораторный стенд, осуществляющий сетевое взаимодействие двух ПЛК. Состав стенда:

- ПЛК-1, SIMATIC 1512;
- ПЛК-2, SIMATIC 1510;
- Коммутатор Scalance XC208;
- АРМ инженера, содержащая ПО для программирования ПЛК;
- HMI- панель для визуализации и управления.

Основной рабочей программой ПЛК является управление машиной непрерывного литья заготовок. На АРМ инженера находится симуляция машины, созданная в среде Unity, которая по протоколу PROFINET передает сигналы датчиков, принимает управляющие сигналы и симулирует работу механизмов машины. Управление исполнительными механизмами машины распределено между двумя ПЛК. В процессе работы ПЛК-1 регулярно осуществляет проверку данных, которые обрабатывает ПЛК-2, сравнивая текущие данные датчиков с данными тех же датчиков, но хранящимися в памяти ПЛК-2. Для создания распределенного воздействия к стенду подключен ноутбук, исполняющий роль компьютера нарушителя и/или закладного устройства (рис. 1).

В качестве источника трафика для DoS-воздействия было выбрано ПО Low Orbit Ion Cannon (LOIC). Этот выбор был сделан по следующим критериям: свободное распространение, открытый код, удобство использования [2].

До начала работы со стендом была произведена оценка воздействия LOIC на персональный компьютер. В результате DoS-воздействия было отмечено увеличение требуемой памяти для системных процессов, связанных с сетевым взаимодействием, более чем в 50 раз (до 15% от возможностей центрального процессора), что говорит о работоспособности приложения LOIC.

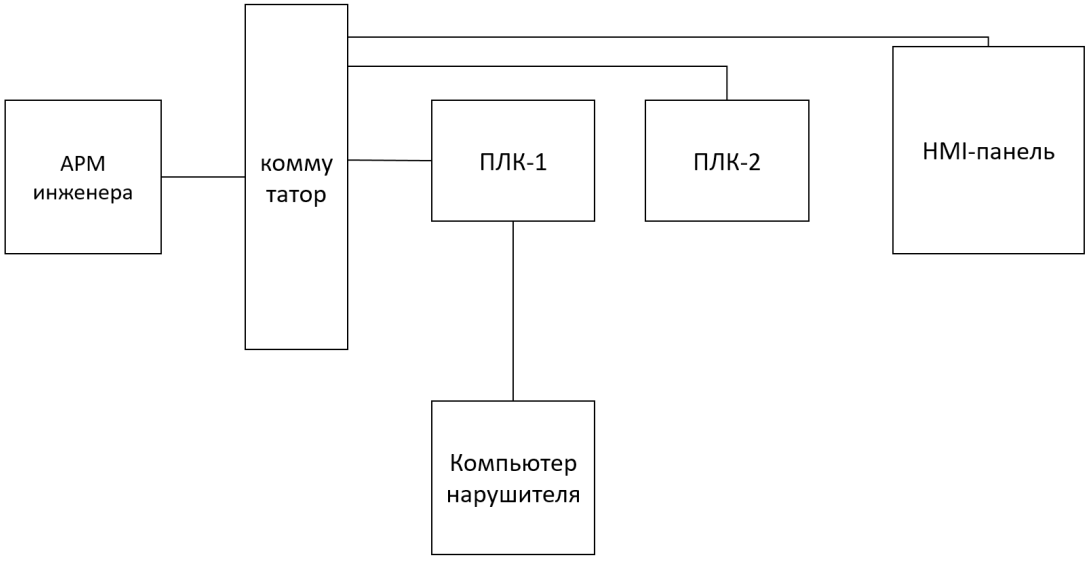


Рис.1. Схема сетевых соединений лабораторного стенда

В качестве метода DoS-воздействия были выбраны UDP-запросы по IP-адресу ПЛК-1 (рис.2). Активность воздействия – около 100000 запросов в секунду. В качестве источников DoS-воздействия были выбраны 2 хоста: ранее упомянутый компьютер нарушителя, представляющий собой внешнее воздействие, и АРМ инженера АСУ ТП, представляющий собой воздействие внутри самой сети АСУ ТП.

В процессе испытаний каждый из хостов по отдельности генерировал DoS-воздействие с интенсивностью до 100000 запросов в секунду. Также было проверено влияние одновременного DoS-воздействия с обоих хостов.

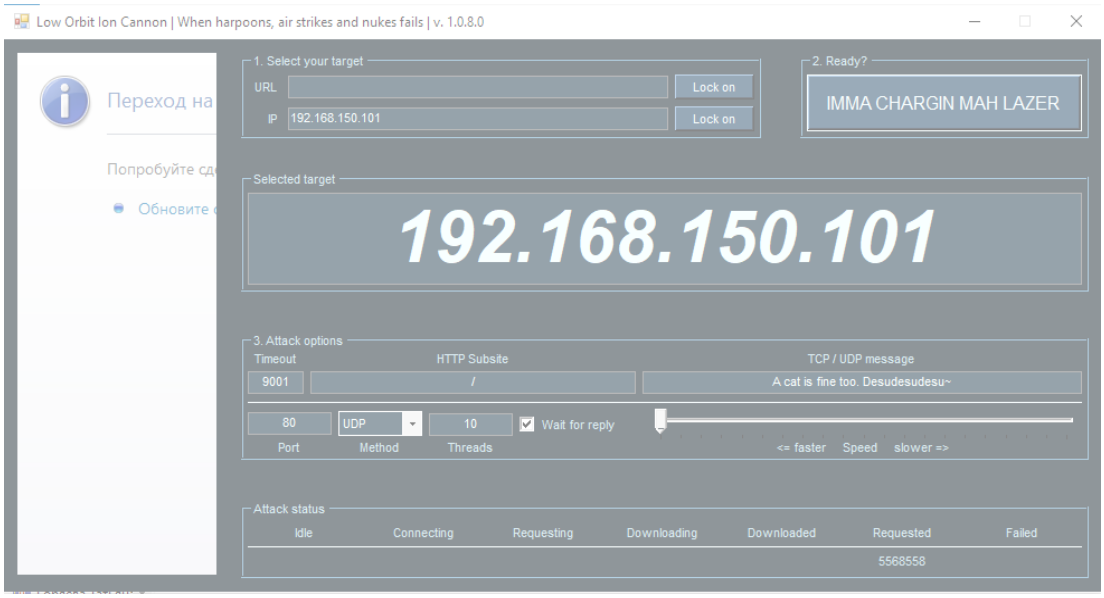


Рис.2. Интерфейс и настройки ПО LOIC

Первоначально тесты проводились при прямом подключении хоста-источника атаки к порту сетевого интерфейса ПЛК-1.

Для предварительного расчета стабильности работы ПЛК под DoS-воздействием было произведено обращение к теории массового обслуживания (ТМО). Согласно ей ПЛК, принимающий сетевые запросы можно представить, как одноканальную систему массового обслуживания (СМО) с ограниченной длиной очереди. Это обуславливается одним процессором и ограниченными оперативной памятью, и сетевым буфером.

Согласно ТМО, существует возможность рассчитать вероятность отказа в обслуживании новому пакету данных, приходящему по сети. Эта вероятность равна

$$\rho_{отк} = \rho^{m+1}\rho_0, \quad (1)$$

где $\rho_{отк}$ – вероятность отказать новому пакету данных в обслуживании, ρ – коэффициент загрузки СМО, m – максимальное количество пакетов, принятых в обработку (число мест в очереди), ρ_0 – вероятность отсутствия пакета данных на обработку.

Коэффициент загрузки системы ρ вычисляется по формуле

$$\rho = \lambda/\mu, \quad (2)$$

где λ – интенсивность поступления пакетов данных или же интенсивность DoS-воздействия, μ – интенсивность обслуживания пакетов данных.

Вероятность отсутствия пакета данных на обработку высчитывается по формуле

$$\rho_0 = \frac{1-\rho}{1-\rho^{m+2}}. \quad (3)$$

Согласно технической документации на ПЛК Siemens 1512C-1 PN, он способен хранить до 1 Мб принятых данных и реагировать на аналогичный объем данных в секунду. С одного хоста LOIC создает около 100000 UDP-запросов в секунду, объем пакета данных каждого запроса равен 48 байтам. Отсюда можно подсчитать, что ПЛК может хранить и обслуживать до 20834 пакетов(m=μ=20834).

Таким образом, используя (1), (2), (3) и описанные данные, можно вывести зависимость вероятности отказа в обслуживании нового пакета данных ротк от интенсивности DoS-воздействия λ:

$$\rho_{отк} = \left(\frac{\lambda}{20834}\right)^{20835} * \frac{1-\lambda/20834}{1-(\lambda/20834)^{20836}}. \quad (4)$$

Очевидно, что при λ<μ вся формула стре-

мится к 0, что означает, что воздействие менее 20000 запросов в секунду не окажет существенного влияния.

При λ>μ единица, стоящая в знаменателе дроби в (4), несущественна и все выражение обращается в следующее уравнение:

$$\rho_{отк} = \frac{1-\lambda/20834}{-\lambda/20834} . \qquad (5)$$

На рис. 3 изображен график зависимости вероятности отказа в обработке от интенсивности DoS-воздействия при λ>μ.

При интенсивности атаки в 100000 запросов в секунду с одного хоста вероятность отказа составит около 79%, при добавлении еще одного хоста вероятность повысится до 89%.

Оценка последствий DoS-воздействия проводилась по следующим категориям:

- продолжительность (время выполнения) программного цикла контроллера;
- возможность передачи данных с контроллера на периферийные устройства.

Замеры времени выполнения программного цикла производились путем использования встроенных инструментов ПО для программирования ПЛК TIAPortal. Как показали

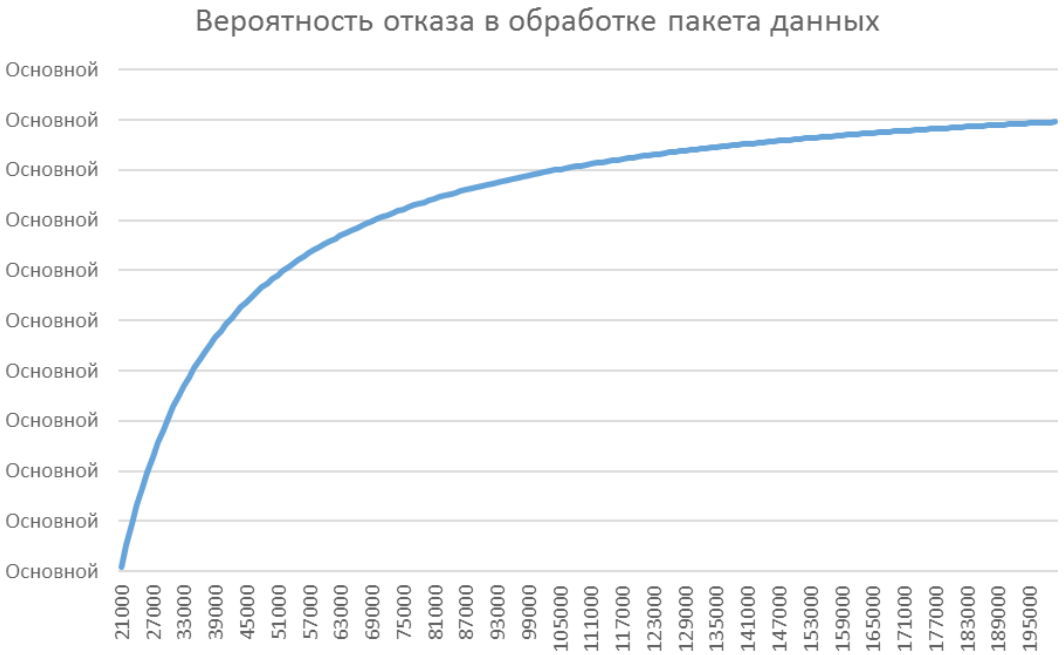


Рис.3. Вероятность отказа в обработке пакета данных при различных интенсивностях DoS-воздействия

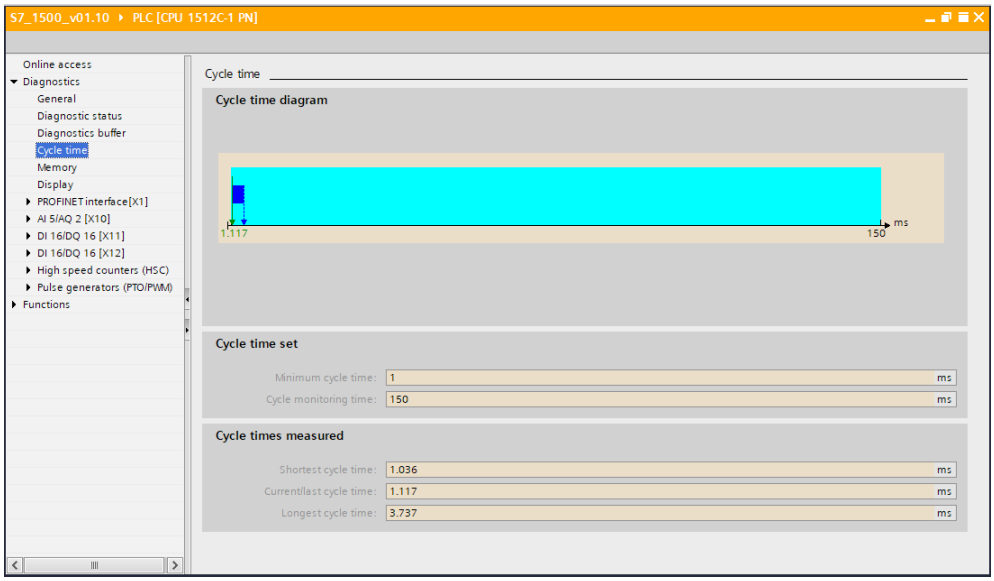


Рис.4. Базовое время цикла

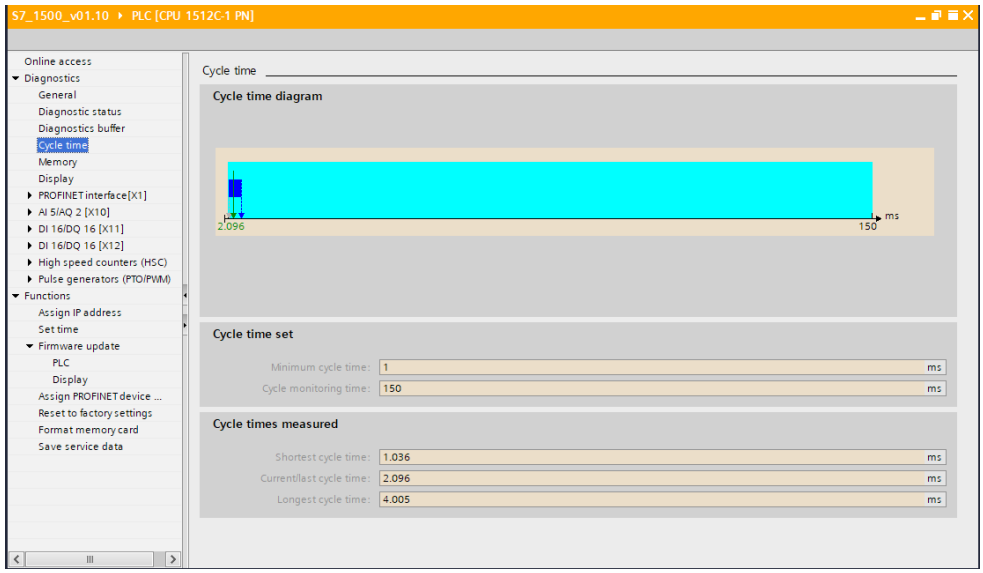


Рис.5. Время цикла под нагрузкой

измерения, среднее время выполнения программного цикла до начала воздействия составляло около 1,1 – 1,2 миллисекунд (рис.4). После подключения DoS-воздействия время выполнения программного цикла увеличивалось до среднего значения около 2,1 – 2,2 миллисекунд, увеличиваясь практически вдвое (рис.5).

Возможность передачи данных с контроллера на периферийные устройства оценивалась несколькими способами:

• наличие соединения с отслеживающим модулем TIAPortal;

• наличие соединения с HMI-панелью и вторым контроллером;

• наличие отклика сети (команда ping).

Несколько запусков LOIC показали, что в течение 7–10 секунд после начала DoS-воздействия пропадала связь ПЛК с отслеживающим модулем (рис. 6).

Связь с периферийными устройствами также была нарушена: отмечена нестабиль-

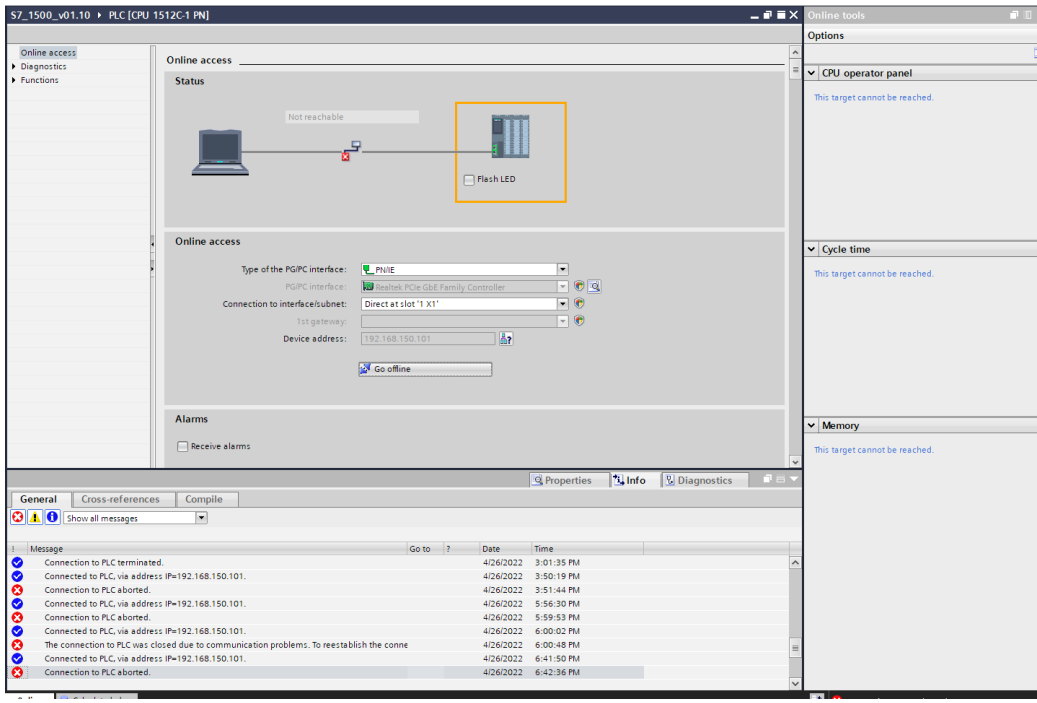


Рис.6. Пропавшее соединение с ПЛК

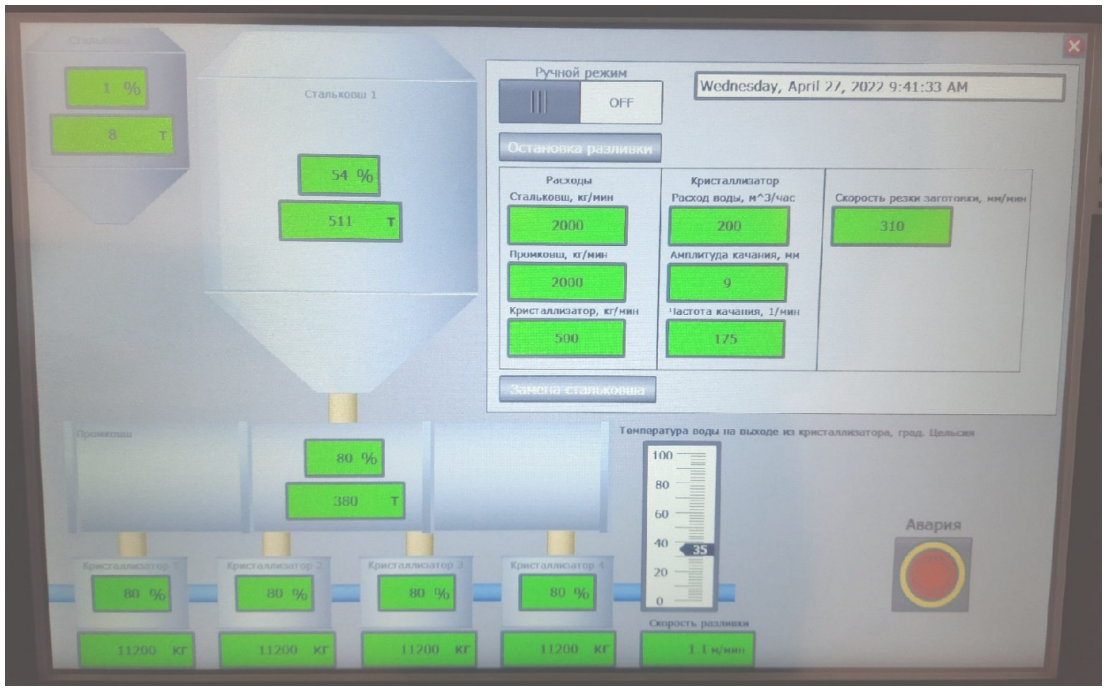


Рис.7. Базовая работа HMI-панели. Данные с контроллера приходят нормально

Рис.8. Работа HMI-панели под нагрузкой. Данные с контроллера не приходят и заменяются на символы «#»

ность поступления данных на HMI-панель и второй ПЛК (рис. 7 и 8).

Дополнительная проверка с помощью команды ping подтвердила сильную нестабильность соединения: увеличение времени отклика в разы и потерю значительной части (около 75%) пакетов данных (рис. 9). Подключение второго атакующего хоста увеличивало эту долю до приблизительного значения в 90%.

Дальнейшим шагом было повторение вышеописанных процедур, но была изменена точка подключения хоста нарушителя с сетевого интерфейса самого ПЛК на маршрутизатор.

Стандартный трафик в сети лабораторного стенда при выполнении проекта составляет около 4-5 килобайт в секунду. 2 хоста, создающие по 100000 запросов в секунду, как было показано ранее, создают поток данных

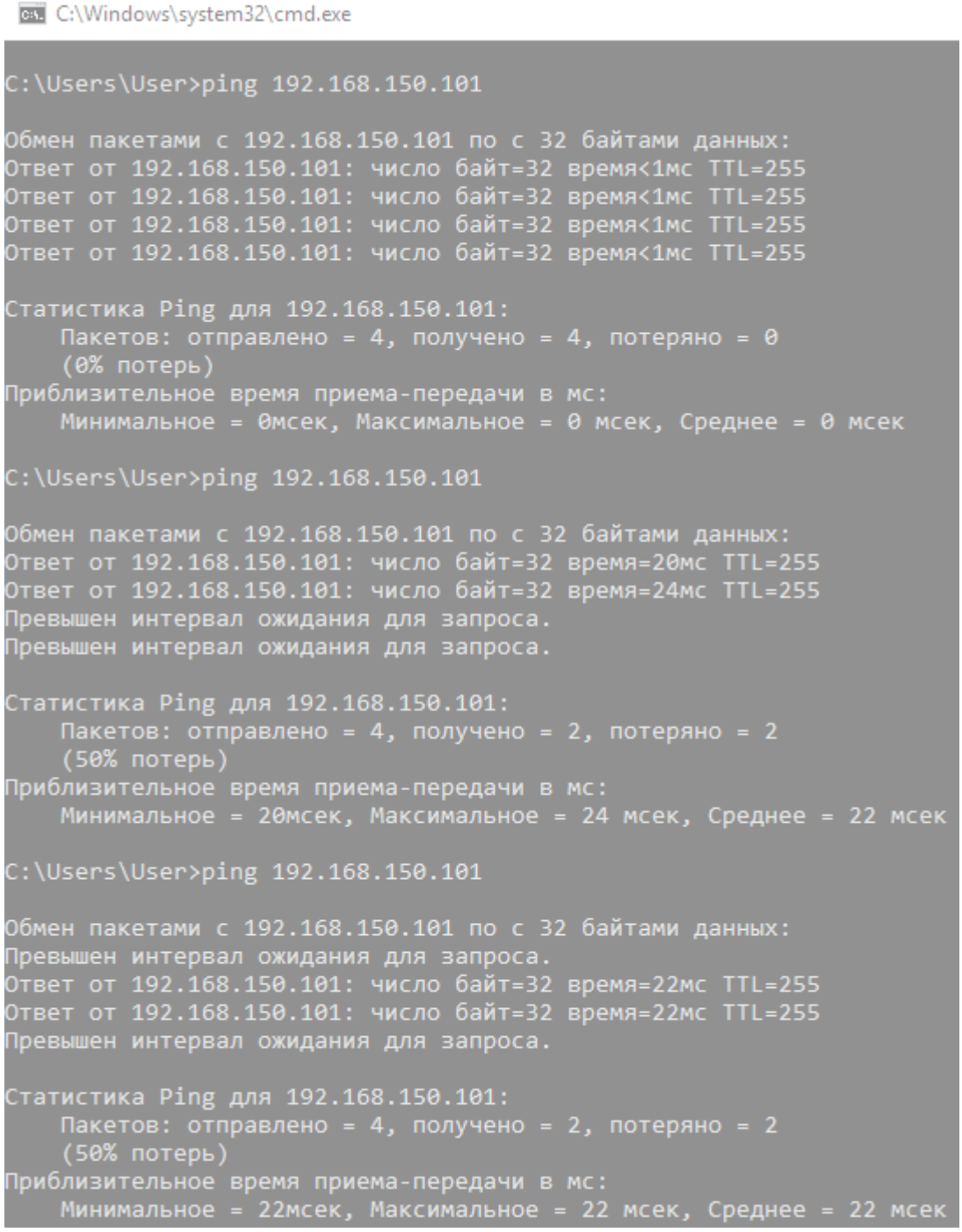


Рис.9. Исполнение команды ping: первый запрос выполнен при нормальной работе, второй и третий – под нагрузкой

приблизительно равный 5 мегабайтам в секунду с одного хоста. Таким образом, трафик данных через маршрутизатор должен увеличиваться до 10 МБ/с.

Для сканирования трафика удаленного маршрутизатора была использована программа Multi Router Traffic Grapher (MRTG) [3], которая позволяет осуществлять сканирование трафика с помощью SNMP, а именно количество байт, проходящих через определенный порт коммутатора в секунду, независимо от их источника, и предоставляет данные в графическом виде. Показания MRTG показаны на рис. 10.

На графике изображен сетевой трафик через порт коммутатора, соединенный с ПЛК-1, выраженный в байтах в секунду. Хорошо заметны 2 пиковых значения, достигающие не-

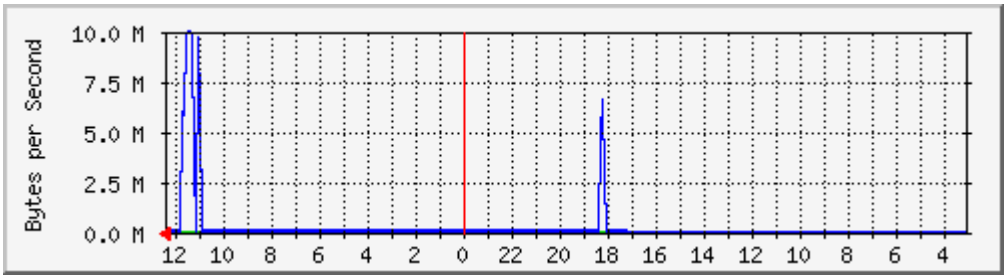


Рис. 10. Сетевой трафик, проходящий через маршрутизатор

скольких мегабайт в секунду. В эти моменты проводилась DDoS-атака. Стандартное сетевое взаимодействие ПЛК в 1000 раз менее активное, поэтому теряется на фоне всплесков. Т.к. основное предназначение DDoS-атаки – заполнение канала передачи, а ширина канала маршрутизатора стенда достигает лишь 100 мегабит в секунду, то очевидно, что 2 атакующих хоста практически полностью занимают канал передачи и не дают ПЛК стабильного доступа к легитимным сигналам. Сетевой трафик через остальные порты маршрутизатора остался неизменным. Поведение ПЛК в свою очередь ничем не отличалось от предыдущего этапа проверки. ПЛК-2 под DoS-воздействием показал поведение, аналогичное ПЛК-1: замедление программного цикла, невозможность приема/передачи данных по сетевому протоколу. Проверка данных, которую осуществляет ПЛК-1, заканчивается провалом, при этом система выдает соответствующее предупреждение.

Последним этапом работы стала проверка работы ПЛК под нагрузкой при отсутствии сетевых соединений. В результате было отмечено, что ПЛК работает в штатном режиме без явного замедления и может передавать данные через дискретные и аналоговые модули ввода/вывода.

В заключение необходимо отметить некоторые методы защиты от подобных воздействий:

1. Изоляция сети АСУ ТП. Если изолировать АСУ ТП от Интернета и от основной локальной сети предприятия, внешние воздействия становятся невозможны. Однако остаются осуществимы атаки изнутри самой сети АСУ ТП. Также подобный вариант отбрасывается с расчетом повышения удобства работы с самой промышленной сетью.

2. Фильтрация трафика. Настроенные межсетевые экраны и/или списки доступа позволят не допустить вредоносный трафик до управляющих узлов. Недостатки этого метода состоят в том, что лишь малая часть ПЛК имеют встроенные механизмы для настройки фильтрации. Фильтрации определенных сетевых протоколов в свою очередь создает необходимость тщательного подбора комплектующих и разработки архитектуры.

3. Мониторинг целостности сети. Позволит отслеживать изменение состава АСУ ТП с целью поиска недоверенных хостов. Но это метод не предупредит о DoS-воздействии с одного из доверенных элементов сети.

4. Сервисы по защите от DDoS-атак. Основной недостаток состоит в том, что подобные сервисы не способны работать с ПЛК, но вполне применимы для компьютерной части.

По результатам эксперимента можно сделать вывод о том, что сеть ПЛК не может сохранять стабильную работу под сравнительно слабым воздействием в 200000 запросов в секунду. В случае, если программа ПЛК имеет прием/передачу данных через TCP/IP соединение, происходит замедление работы программы, что может сказаться на синхронизации процессов. Соединение контроллеров с отслеживающим модулем и человеко-машинный интерфейс при тестовом испытании перестали работать в штатном режиме. Время выполнения программного цикла автономной работы ПЛК при этом не изменяется, возможность управления исполнительными механизмами и датчиками через модули ввода/вывода ПЛК сохраняется.

Также стоит отметить, что в этой работе исследовалась АСУ ТП, построенная на протоколе PROFINET со стандартным управлением потоком данных TCP, и одно из дальнейших направлений исследований - проверка при использовании АСУ ТП режима реального времени.

Литература

1. Классификация сетевых атак [Электронный ресурс]. –– URL: https://www.internet-technologies.ru/articles/newbie/klassifikaciya-setevyh-atak.html#header-8116-7 (Дата обращения: 20.04.2022).

2. Adeyemo, A. A. A study of denial-of-service attack with its tools and possible mitigation techniques / A. A. Adeyemo, K. A. Ganiyu // Computer Sciences and Telecommunications. – 2019. – № 2(57). – С. 36 - 45. –– URL: https://www.elibrary.ru/item.asp?id=45620382 (Дата обращения: 20.04.2022).

3. Теория систем массового обслуживания: учеб. пособие / И. В. Сол- нышкина. – Комсомольск-на-Амуре: ФГБОУ ВПО «КнАГТУ», 2015. – 76 с. – URL: https://knastu.ru/media/files/page_files/page_421/posobiya_2015/_Teoriya_sistem_massovogo_obsluzhivaniya.pdf

4. Tobi Oetiker's MRTG – The Multi Router Traffic Grapher [Электронный ресурс]. – URL: https://oss.oetiker.ch/mrtg/ (Дата обращения: 20.07.2022).

References

1. Klassifikacija setevyh atak –– URL: https://www.internet-technologies.ru/articles/newbie/klassifikaciya-setevyh-atak.html#header-8116-7

2. Adeyemo, A. A. A study of denial-of-service attack with its tools and possible mitigation techniques / A. A. Adeyemo, K. A. Ganiyu // Computer Sciences and Telecommunications. – 2019. – № 2(57). – S. 36-45. –– URL: https://www.elibrary.ru/item.asp?id=45620382

3. Teorija sistem massovogo obsluzhivanija: ucheb. posobie / I. V. Sol- nyshkina. – Komsomol'sk-na-Amure: FGBOU VPO «KnAGTU», 2015. – 76 s.–URL: https://knastu.ru/media/files/page_files/page_421/posobiya_2015/_Teoriya_sistem_massovogo_obsluzhivaniya.pdf

4. Tobi Oetiker's MRTG – The Multi Router Traffic Grapher [Jelek-tronnyj resurs]. – URL: https://oss.oetiker.ch/mrtg/

БОГЕР Александр Максимович, преподаватель кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, 76. E-mail: bogeram@susu.ru

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

МОРОЗОВ Игорь Александрович, младший научный сотрудник НОЦ «Информационная безопасность» ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, 76. E-mail: morozovia@susu.ru.

BOGER Aleksandr Maksimovich, Lecturer of Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: bogeram@susu.ru

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

MOROZOV Igor Alexandrovich, Junior researcher of Information Security Research and Education Centre, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: morozovia@susu.ru.

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

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

ВЕСТНИК УрФО
Безопасность в информационной сфере № 4(46) / 2022
Подписано в печать 23.12.2022. Дата выхода в свет 26.12.2022.
Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 8,75. Тираж 50 экз.
Заказ 0/0.
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(46) / 2022
Signed to print March 28, 2022. Date of publication of the 30.03.2022.
Format 70×108 1/16. Screen printing. Conventional printed sheet 8,75. Circulation – 50 issues.
Order 0/0.
Open price.

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