ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 3(41) / 2021

УЧРЕДИТЕЛИ

ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

Подписной индекс 73852 в каталоге «Почта России»

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

Свидетельство ПИ № ФС77-65765 от 20.05.2016

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

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

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

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 3(41) / 2021

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

CHAIRMAN OF THE EDITORIAL BOARD

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

CHIEF EDITOR

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

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SHRABER A. E.

PROOFREADING

FEDOROV V. S.

Subscription index 73852

in the «Russian Post» catalog

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

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

Publisher: OOO « South Ural Legal Newsletter»

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

Electronic version of the magazine in the Internet:

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

16+

В НОМЕРЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

ИССЛЕДОВАНИЕ И ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ

МЕТОДЫ АНАЛИЗА ДАННЫХ

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКАЯ И ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

INFORMATION TECHNOLOGY AND COMPUTER SECURITY

RESEARCH AND DESIGN OF TECHNICAL FACILITIES

METHODS OF DATA ANALYSIS

ORGANIZATIONAL, TECHNICAL AND LEGAL PROTECTION OF INFORMATION

TOPICAL PROBLEMS OF CYBERSECURITY

УДК 004.032.26

Вестник УрФО № 3(41) / 2021, с. 5–11

Кротова Е.Л., Уразбаева Ю.В.

DOI: 10.14529/secur210301

НЕЙРОННЫЕ СЕТИ ДЛЯ ОБНАРУЖЕНИЯ ЗЛОУМЫШЛЕННИКА В РАСПРЕДЕЛЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

В работе проведено исследование расширения стандартной модели поиска злоумышленника в распределённой автоматизированной системе. Предложено дополнить систему, построенную на эвристических правилах, моделью, оценивающей отклонение поведения легального пользователя от профиля его стандартного поведения в сети. Данный метод реализован на основе перцептрона. Работа проиллюстрирована примерами реализации разработанной методики.

Ключевые слова: *компьютерная безопасность, статистическое моделирование, нейронные сети.*

Krotova E.L., Urazbaeva Yu.V.

NEURAL NETWORKS FOR DETECTING AN INTRUDER IN A DISTRIBUTED AUTOMATED SYSTEM

The paper investigates the extension of the standard model for searching for an intruder in a distributed automated system. It is proposed to supplement the system based on heuristic rules with a model that estimates the deviation of the behavior of a legal user from the profile of his standard behavior in the network. This method is implemented on the basis of a perceptron. The work is illustrated with examples of the implementation of the developed methodology.

Keywords: *computer security, statistical modeling, neural networks.*

Одна из основных направлений исследований по информационной безопасности – задача наискорейшего обнаружения злоумышленников в информационной системе и сведения к минимуму ошибок применяемых методов.

Традиционным методом обнаружения злоумышленника является использование алгоритмов на основе эвристических правил, позволяющих отличить злоумышленника от легального пользователя. Тем не менее, в настоящее время этого метода уже недостаточно для решения проблемы.

Альтернативные способы включают в себя изучение моделей активности пользователя с помощью статистических методов и их классификацию по заданному критерию. Актуальность применения статистических методов заключается в том, что, по сравнению с эвристическими методами, статистические методы позволяют в большей степени избежать ошибок при мониторинге активности пользователя, что, в свою очередь, усиливает надежность информационной системы. Анализируя реальные данные по различным действиям пользователя в информационной системе с помощью предложенного метода, мы сможем разделить пользователей на легальных и нелегальных и выявить ошибки.

Применение статистических методов для обнаружения злоумышленника в информационной системе рассматривалось такими отечественными и зарубежными учеными, как В. Столлингс, А.А. Корниенко, И.М. Слюсаренко, С.М. Доценко, Н.Н. Фимичев, Rodriguez, M.Z., Zeng L., Zhang M., Bouchachia A. [1, 2, 3]

Файлы журналов регистрации событий безопасности дают представление о состоянии информационной системы и позволяют обнаруживать аномалии в поведении пользователей и фиксировать инциденты информационной безопасности. Однако, автоматический анализ данных журналов событий безопасности затруднен, поскольку он содержит огромное количество неструктурированных данных, собранных из различных источников. Файлы журнала содержат информацию почти обо всех событиях, происходящих в информационной системе, в зависимости от уровня журнала. Для этого развернутая инфраструктура ведения журналов автоматически собирает, объединяет и хранит журналы, которые постоянно создаются большинством компонентов и устройств.

Основная проблема исследования заключается в том, что при анализе журналов инциденты обнаруживаются только задним числом. Кроме того, анализ журналов – это трудоемкая и ресурсоемкая задача, требующая знания предметной области о системе. Таким образом, обнаружение аномалий в поведении пользователей в реальном времени становится возможным благодаря постоянному мониторингу системных журналов в режиме онлайн, то есть сразу после их создания. Это позволяет своевременно реагировать на инциденты информационной безопасности и снижает вызванные ими расходы. К сожалению, эта задача вряд ли возможна для человека, поскольку данные журнала генерируются в огромных объемах и с большой скоростью. При рассмотрении крупных корпоративных систем нередко количество ежедневно создаваемых строк журнала исчисляется миллионами. Например, общедоступные журналы распределенной файловой системы Hadoop (HDFS) содержат более 4 миллионов строк журнала в день, а небольшие организации имеют дело с пиковыми значениями 22000 событий в секунду. Статистические методы позволяют анализировать большие данные журналов событий безопасности и выявлять аномалии в поведении пользователя с большей эффективностью.

При сравнении подходов нейронных сетей и других статистических методов можно увидеть, что статистические методы используют формулы, а нейронные сети – графическую интерпретацию. При использовании нейронных сетей основное время занимает обучение сетей, тогда как в статистике основное время посвящается анализу задачи, для которого требуются предшествующие знания. Нейросетевой подход, в свою очередь, в большинстве случаев может без таких знаний обойтись.

Вопрос о том, какие методы лучше использовать для обнаружения злоумышленника в информационной системе, остается открытым. Выбор метода зависит от ситуации, которая в основном определяется наличием априорной информации о данных, по которым можно выявить злоумышленника.

Мы остановимся на исследовании методов, основанных на нейронных сетях, так как это более молодая, в данный момент развивающаяся, область, доступная для применения в различных сферах деятельности. С помощью нейронных сетей можно анализировать большее количество данных и получить возможность обнаруживать злоумышленни-

ка в информационной системе за более короткое время за счет обучения [4, 5 с. 1-7].

Искусственная нейронная сеть (ИНС) – математическая модель, а также её программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма. Это понятие возникло при изучении процессов, протекающих в мозге, и при попытке смоделировать эти процессы.

ИНС представляют собой систему соединённых и взаимодействующих между собой простых процессоров (искусственных нейронов). Такие процессоры обычно довольно просты (особенно в сравнении с процессорами, используемыми в персональных компьютерах). Каждый процессор подобной сети имеет дело только с сигналами, которые он периодически получает, и сигналами, которые он периодически посылает другим процессорам. И, тем не менее, будучи соединёнными в достаточно большую сеть с управляемым взаимодействием, такие локально простые процессоры вместе способны выполнять довольно сложные задачи.

После того как нейронная сеть обучена множеством последовательных команд защищаемой системы или одной из ее подсистем, сеть представляет собой «образ» нормального поведения. Процесс обнаружения аномалий представляет собой определение показателя неправильно предсказанных команд, то есть фактически обнаруживается отличие в поведении объекта.

Преимущества:

– успех данного подхода не зависит от природы исходных данных;

– нейронные сети легко справляются с зашумленными данными;

– автоматически учитываются связи между различными измерениями, которые, несомненно, влияют на результат оценки.

При обнаружении злоумышленника в информационной системе предполагается, что его поведение отличается от поведения легального пользователя и эти различия можно оценить количественно. Невозможно будет увидеть совершенно разную работу в информационной системе нелегального пользователя по сравнению с легальным, тем не менее можно отследить в их поведении общие черты и рассчитать вероятность ошибки.

Основная задача исследования заключается в том, чтобы проанализировать большой объем данных по действиям пользователя в информационной системе и обучить нейронную сеть анализировать новые данные, что позволит определять, является пользователь легальным или нелегальным.

Входными параметрами модели является вектор, представляющий собой множество бинарных данных, характеризующих действия пользователя в информационной системе.

Ядром математической модели является нейронная сеть, обученная анализировать входные данные и выявлять в них аномалии, что будет интерпретироваться как аномальное поведение пользователя.

Выходные параметры:

– 0;

– 1,

	A	B	C	D	E	F	G	H	I	J	K	L
1	1	0	0	0	0	0	0	0	0	0	0	0
2	1	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0
4	1	0	0	0	0	0	0	0	0	0	0	0
5	1	0	0	0	0	0	0	0	0	0	0	0
6	1	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0
8	1	0	0	0	0	0	0	0	0	0	0	0
9	1	0	0	0	0	0	0	0	0	0	0	0
10	1	0	0	0	0	0	0	0	0	0	0	0
11	1	0	0	0	0	0	0	0	0	0	0	0
12	1	0	0	0	0	0	0	0	0	0	0	0
13	1	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0
15	1	0	0	0	0	0	0	0	0	0	0	0
16	1	0	0	0	0	0	0	0	0	0	0	0
17	1	0	0	0	0	0	0	0	0	0	0	0
18	1	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0
20	1	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0
22	1	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0
25	1	0	0	0	0	0	0	0	0	0	0	0
26	1	0	0	0	0	0	0	0	0	0	0	0

Рис. 1. Массив данных в MS Excel

где 0 – пользователь легальный, 1 – пользователь нелегальный.

Для дальнейшего анализа в качестве ядра модели выбран перцептрон, который является простейшей нейронной сетью, способной к обучению и решению поставленной задачи.

Для разработки тестовых заданий использован массив данных, представленных в бинарном виде, которые характеризуют действия пользователя в информационной системе.

Первый столбец представляет собой реальное положение пользователя:

0 – легальный;

1 – нелегальный.

Все последующие столбцы – данные, которые соответствуют поведению пользователя.

Часть массива представлена на рисунке 1.

Так как массив содержит более 700 видов оцениваемых данных по более 1500 пользователей, очень сложно провести его анализ.

Для того, чтобы сократить массив и составить таблицу из наиболее показательных примеров, проведена корреляция. Рассчитаны коэффициенты корреляции для каждого столбца относительно первого.

Выбраны 30 столбцов, модуль коэффициента корреляции которых наиболее приближен к 1. Фрагмент полученной таблицы представлен на рисунке 2.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
690	0	1	1	0	0	0	0	0	0	1	1	1	1	0	0	0
691	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
692	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
693	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
694	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
695	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
696	0	1	0	0	1	0	0	0	1	1	1	0	0	0	0	0
697	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0
698	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
699	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
700	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0
701	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
702	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
703	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
704	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
705	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
706	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
707	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
708	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
709	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
710	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
711	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
712	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
713	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	0
714	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
715	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
716	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
717	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
718	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
719	КОРРЕЛ	-0,08141	0,07409	-0,07723	-0,08987	0,074714	-0,07723	-0,07723	0,09866	-0,07396	-0,09839	-0,08406	-0,10922	0,085359	-0,07723	0,091926
720	МОДУЛЬ	0,08141	0,07409	0,077232	0,089874	0,074714	0,077232	0,077232	0,09866	0,073959	0,098393	0,084059	0,109218	0,085359	0,077232	0,091926

Рис. 2. Сокращенная таблица в MS Excel

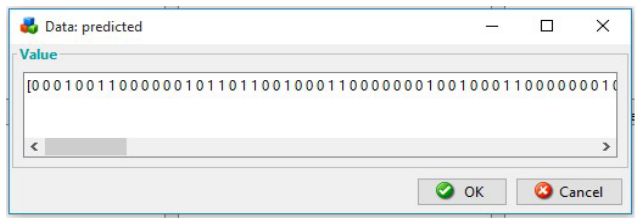


Рис. 3. Полученные выходные данные нейронной сети на персептроне

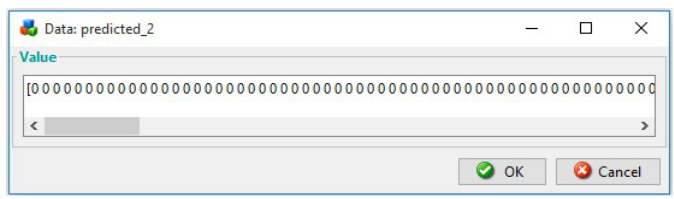


Рис. 4. Полученные выходные данные линейной нейронной сети

Полученная таблица далее использована для реализации метода в пакете MATLAB.

Полученную таблицу разделим пополам по строкам. Первую часть будем использовать для построения и обучения нейронной сети. Вторую – для реализации метода и выявления ошибок относительно реальных данных.

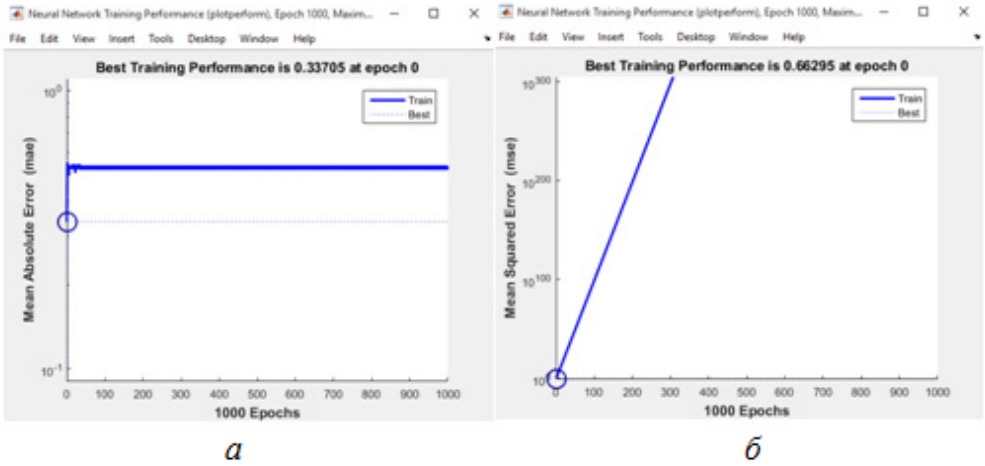
В пакете MATLAB проведено обучение нейронной сети на персептроне. На обучен-

ной нейронной сети смоделированы выходные данные для второй части таблицы с реальными данными.

Смоделированные нейронной сетью на персептроне выходные представлены на рисунке 3.

Для сравнения аналогичные действия проведены с линейной нейронной сетью. В данном случае в структуре результирующих данных преобладают нули, что говорит о том, что сеть определяет пользователя как легального в большинстве случаев. Выходные данные линейной нейронной сети представлены на рисунке 4.

Таким образом, сделан вывод, что персептрон наиболее подходит для решения поставленной задачи, так как для других сетей задача решается хуже.



а *б*

Рис. 5. Графики среднеквадратического отклонения нейронной сети на персептроне (а) и линейной нейронной сети (б)

На рисунке 5 представлены графики среднеквадратического отклонения для реализованных нейронных сетей. Среднеквадратическое отклонение для сети на персептроне меньше, чем для линейной нейронной сети, что так же свидетельствует о том, что сеть на персептроне способна точнее определить злоумышленника в информационной системе.

Далее проведено исследование уровней ошибок I-го и II-го рода для существующих методов и предложенного метода [6].

Ошибки I-го и II-го рода используются для проверки статистических гипотез и принятия решения на основе критерия, который может давать ложный результат.

H_0 – нулевая гипотеза, которая в данном случае соответствует нормальному поведению пользователя в информационной системе.

H_1 – альтернативная гипотеза, соответствующая аномальному поведению пользователя в информационной системе.

Возможны четыре варианта принятия решения:

– реальное поведение пользователя соответствует гипотезе H0, гипотеза H0 (пользователь легален) верно принята;

– реальное поведение пользователя соответствует гипотезе H0, гипотеза H0 (пользователь легален) неверно отвергнута, что представляет собой ошибку I-го рода;

– реальное поведение пользователя соответствует гипотезе H1, гипотеза H0 (пользователь легален) верно отвергнута;

– реальное поведение пользователя соответствует гипотезе H1, гипотеза H0 (пользователь легален) неверно принята, что представляет собой ошибку II-го рода.

Ошибка I-го рода возникает, когда легального пользователя принимают за злоумышленника, а ошибка II-го рода – когда злоумышленник определяется в информационной системе как легальный пользователь.

Для определения количества ошибок I-го и II-го рода было проведено сравнение реальных данных и данных, смоделированных нейронной сетью на персептроне в пакете MATLAB.

В таблице Excel было посчитано:

– количество легальных и нелегальных пользователей;

– количество ошибок I-го и II-го рода.

Ошибка I-го рода возникает, когда легального пользователя принимают за нелегального:

	A	B	C	D	E	F	G	H	I	J	K
1	Реальные данные:	1	0	1	1	0	1	1	1	0	1
2	Результаты нейронной сети:	0	0	0	1	0	0	1	1	0	0
3	Ошибки I-го рода:		0			0				0	
4	Ошибки II-го рода:	1		1	0		1	0	0		1
5											
6	Количество легальных пользователей:	108									
7	Количество нелегальных пользователей:	251									
8	Количество ошибок I-го рода	23									
9	Количество ошибок II-го рода	63									

Рис. 6. Определение количества ошибок I-го и II-го рода

– реальные данные – 0;

– результаты нейронной сети – 1.

Ошибка II-го рода возникает, когда нелегального пользователя принимают за легального:

– реальные данные – 1;

– результаты нейронной сети – 0.

В строках «Ошибки I-го рода» и «Ошибки II-го рода» использована функция ЕСЛИ соответственно для нуля или единицы в строке «Реальные данные». Если результат нейронной сети равен реальным данным в ячейку заполняется 0 – нет ошибки, если не равен – 1 – ошибка есть.

Таким образом количество ошибок I-го рода равно 23 (вероятность ошибки I-го рода – 21,3%), а количество ошибок II-го рода – 63 (вероятность ошибки II-го рода – 25,1%). Расчет ошибок представлен на рисунке 6.

При сравнении с количеством ошибок I-го и II-го рода других статистических методов был сделан вывод, что при равной вероятности ошибки I-го рода предложенный метод имеет меньшую вероятность ошибки II-го рода. Например, при заданной вероятности ошибки I-го рода равной вероятности ошибки I-го рода предложенного метода (≈20%) вероятности ошибки II-го рода для критериев Пирсона и Колмогорова равны ≈50% и ≈30% соответственно, что свидетельствует о том, что предложенный метод будет более надежным при обнаружении злоумышленника в информационной системе.

Исследование статистических методов обнаружения злоумышленника в информационной системе показало, что метод, основанный на нейронных сетях, наиболее подходит для реализации на предприятии, так как не требует большого объема памяти, обладает хорошим быстродействием, требует меньше времени на реализацию и позволяет анализировать больший объем данных. Использование метода на основе нейронных сетей позволяет более эффективно обеспечить обнаружение злоумышленника в информационной системе.

Литература

1. У. Столлингс. Современные компьютерные сети. 2–е издание. «Питер» 2003, 784 с.

2. Фергюсон, Нильс, Шнайер, Брюс. Практическая криптография.: Пер. с англ. М.: Издательский дом "Вильямс", 2005.

3. https://habr.com/ru/company/nix/blog/478286/ Выявление мошенничества с помощью алгоритмов случайного леса, нейронного автокодировщика и изолирующего леса.

4. https://www.securitylab.ru/blog/company/pt/345640.php Обнаружение веб–атак с помощью рекуррентных нейронных сетей.

5. Мустафаев А.Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика // Вопросы безопасности. – 2016. – № 2. – С. 1 – 7. DOI: 10.7256/2409–7543.2016.2.18834 URL: https://nbpublish.com/library_read_article.php?id=18834

6. Ивченко Г.И., Медведев Ю.И. Введение в математическую статистику: Учебник. М.: Издательство ЛКИ, 2010.

References

1. U. Stollings. Sovremennyye komp'yuternyye seti. 2–ye izdaniye. «Piter» 2003, 784 s.

2. Fergyuson, Nil's, Shnayyer, Bryus. Prakticheskaya kriptografiya.: Per. s angl. M.: Izdatel'skiy dom "Vil'yams", 2005.

3. https://habr.com/ru/company/nix/blog/478286/ Vyyavleniye moshennichestva s pomoshch'yu algoritmov sluchaynogo lesa, neyronnogo avtokodirovshchika i izoliruyushchego lesa.

4. https://www.securitylab.ru/blog/company/pt/345640.php Obnaruzheniye veb–atak s pomoshch'yu rekurrentnykh neyronnykh setey.

5. Mustafayev A.G. Neyrosetevaya sistema obnaruzheniya komp'yuternykh atak na osnove analiza setevogo trafika // Voprosy bezopasnosti. – 2016. – № 2. – S. 1 – 7. DOI: 10.7256/2409–7543.2016.2.18834 URL: https://nbpublish.com/library_read_article.php?id=18834

6. Ivchenko G.I., Medvedev YU.I. Vvedeniye v matematicheskuyu statistiku: Uchebnik. M.: Izdatel'stvo LKI, 2010.

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

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

УРАЗБАЕВА Юлия Владимировна, учебный мастер кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. yulyia.urazbaeva@mail.ru

URAZBAEVA Yulia Vladimirovna, training master of the Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Territory, Perm, Komsomolsky prospect, 29. yulyia.urazbaeva@mail.ru

УДК 004.056.5:519.876.5 Вестник УрФО № 3(41) / 2021, с. 12–23

Литвинов Г.А., Щерба Е.В.

DOI: 10.14529/secur210302

ПРИМЕНЕНИЕ МОДЕЛЕЙ ДОВЕРИЯ И РЕПУТАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МАРШРУТИЗАЦИИ В ДИНАМИЧЕСКИ ОРГАНИЗУЕМЫХ СЕТЯХ [1]

Репутационные модели имеют широкий спектр применения, включая системы электронной торговли и социальные сети. В статье исследована возможность их использования для обеспечения безопасности маршрутизации в динамически организуемых сетях и предложен сравнительный анализ существующих репутационных моделей доверия. Определены отличительные особенности, достоинства и недостатки рассмотренных моделей. Применение моделей для решения поставленной задачи проиллюстрировано наглядными примерами. Обозначены перспективные направления для дальнейших исследований в рамках заданной проблематики.

Ключевые слова: *самоорганизующиеся сети, многошаговые сети, безопасность маршрутизации, репутационные модели, сетевые атаки.*

Litvinov G. A., Shcherba E. V.

APPLICATION OF TRUST AND REPUTATION MODELS TO SECURE ROUTING IN DYNAMICALLY ORGANIZED NETWORKS

Reputation models have a wide variety of uses, including e-commerce and social networks. The presented paper contains a comparative survey of the existing reputation-based trust models. The possibilities of use the models to provide the security of routing in dynamically orga-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90100.

nized networks are examined. The authors highlight the differentiating features, advantages and disadvantages of the considered models. The examples presented in the paper illustrate the application of models to solve the problem. The promising directions for further research in the framework of the given problem are outlined. Acknowledgments: The reported study was funded by RFBR, project number 20-37-90100.

Keywords: *ad-hoc networks, routing security, reputation model, network attacks, MANET.*

Введение

Развитие современных цифровых технологий и их проникновение в различные отрасли деятельности привело к появлению новых способов связи и взаимодействия различных устройств. В качестве перспективной архитектуры связи можно рассматривать объединение большого количества устройств в децентрализованную сеть, где каждый узел осуществляет поиск доступных устройств в зоне его покрытия для установления подключения с целью последующего взаимодействия. При этом каждое устройство сети может участвовать в передаче данных для других устройств, т.е. выступать в качестве маршрутизатора. В различных исследованиях указанные сети именуются как многошаговые или самоорганизующиеся сети. Как правило, взаимодействие устройств такой сети осуществляется по беспроводному каналу связи. Беспроводный канал связи позволяет обеспечить мобильность устройств сети, но, вместе с тем, требует дополнительного внимания к защите передаваемой информации.

В беспроводной самоорганизующейся сети узлы имеют возможность перемещаться в пространстве, устанавливая новые связи с соседними узлами и теряя ранее имевшиеся. Таким образом, динамическая топология, множественный доступ и специфика маршрутизации пакетов в беспроводных самоорганизующихся сетях повышают сложность обеспечения их безопасной доставки до получателя.

Для обеспечения конфиденциальности и целостности пересылаемых пакетов данных могут применятся криптографические методы, но указанный подход к защите не позволяет гарантировать доступность информации при атаках типа «блэкхол» и «грейхол», связанных с полной или частичной фильтрацией сетевых пакетов вредоносными и «эгоистичными» узлами [1].

В этом случае обеспечение надёжной доставки сетевых пакетов возможно в результате выбора более безопасного маршрута от узла источника до узла назначения, исключающего маршрутизацию пакетов через вредоносные узлы. Выбор наиболее безопасного маршрута для доставки пакетов возможен на основе определения уровня доверия к узлам сети, образующим маршрут. Определение доверия в сети может происходить с помощью одной из моделей вычисления репутации узлов [2, 3].

Модели вычисления репутации широко применяются для создания доверительных отношений среди пользователей онлайн-сообществ, где участники взаимодействия не знают друг друга заранее. Основная идея использования репутации, заключается в накоплении опыта взаимодействия с оцениваемым пользователем, для принятия решения о взаимодействии с ним в будущем. Таким образом, репутация является показателем надежности объекта оценки и предоставляемых им услуг на основе его поведения в прошлом. Когда пользователю необходимо принять решение о взаимодействии с другим пользователем в сети, он может принять во внимание репутацию этого пользователя и начать взаимодействие с ним, только если репутация узла превышает некоторое пороговое значение. Таким образом, репутационная модель, которая помогает управлять репутацией (например, путем сбора, распространения и агрегирования информации о поведении пользователей), становится фундаментальным компонентом архитектуры безопасности любой платформы.

Большинство моделей вычисления репутации, разработанных к настоящему времени, предназначены для решения специализированных задач. В рамках данной работы рассматривается возможность применения некоторых репутационных моделей для определения уровня доверия к узлам и маршрутам сетевой инфраструктуры.

Исследования и разработки по имплементации репутационных моделей в динамически организуемых сетях различных типов ведутся как российскими [4–8], так и зарубежными учёными и научными группами [9–21]. При этом можно выделить ряд признаков и

свойств репутационных моделей, которые можно использовать для их классификации. Во-первых, оценка репутации либо может быть выражена в абсолютном значении, либо представлена по отношению к другим узлам. Нужно учитывать, что если модель позволяет только ранжировать узлы, то узлы, не заслуживающие доверия, могут занимать достаточно высокие позиции в рейтинге. Часть моделей позволяет учитывать различные аспекты взаимодействия узлов (контекст взаимодействия) и различать взаимодействия на основе их стоимости. Свойство транзитивности позволяет репутационным моделям устанавливать новые доверительные отношения из существующих доверительных отношений. Например, если узел i доверяет узлу j, то он так же имеет некоторое доверие к узлам, которым доверяет узел j. Однако способность узла предоставлять услугу может отличаться от его способности давать рекомендации другим узлам. В этом отношении некоторые модели различают функциональное доверие, то есть доверие к способности узла предоставлять услугу, и реферальное доверие, то есть доверие к способности узла предоставлять рекомендации.

Возможность внедрения и применения репутационной модели зависит от её способности отражать фактическую надежность узлов, участвующих в коммуникации. Очевидно, что объем информации, используемой для расчета репутационных оценок, напрямую влияет на их качество. Некоторый достаточный объем информации требуется для корректного применения любой репутационной модели. Тем не менее, определить минимальный объем данных, необходимый для оценки репутации, как правило затруднительно. Кроме того, узлы могут иметь различное управление рисками и, как следствие, поразному воспринимать репутацию. Например, некоторые узлы могут установить доверительные отношения с оцениваемым узлом, имеющим высокую репутацию на основании очень небольшого количества прошлых взаимодействий, в то время как другим узлам может потребоваться больше данных, подтверждающих положительную оценку взаимодействия.

Как правило, формальное определение репутационной модели включает в себя определение репутационной меры и математическую модель агрегирования информации о поведении узлов и вычисления значения репутации. Определение значения репутации может быть основано на простом суммировании оценок [9] или вычислении их среднего значения, на потоковых моделях [10–15], вероятностных моделях, таких как байесовские системы [16, 17], и моделях на основе субъективной логики [18–20].

Протокол маршрутизации для динамически организуемых сетей CORE представляет классический пример применения репутационной модели, основанной на взвешенном усреднении оценок [9]. Использованная модель поддерживает только положительные оценки и разделяет функциональное и реферальное доверие.

Репутационные модели, в основе которых используется потоковая модель вычисления значения репутации, используют понятие транзитивного доверия. В таких репутационных моделях оценки значения репутации, полученные от других узлов, агрегируются и нормализуются для построения цепи Маркова. Вектор репутации, включающий оценки значения репутации всех участников взаимодействия, вычисляется как вектор стационарного распределения цепи Маркова. Каждый узел начинает с вектора начальных значений репутации, а затем многократно выполняет переход, пока не будет достигнуто стационарное распределение. Это соответствует учету все большего количества косвенных свидетельств о поведении узлов сети.

Модели, основанные на субъективной логике, используют теорию Демпстера-Шафера [22]. Субъективная логика обеспечивает математическую основу для работы с мнениями других пользователей и обладает естественной способностью явно выражать неопределенность. Упрощенно, неопределенность отражает погрешность в расчете значения репутации и может возникать из-за ограниченного количества имеющейся информации о поведении узлов. Модель с использованием субъективной логики использует оператор консесуса «Å» для объединения независимых мнений и оператор дисконтирования «Ä» для вычисления транзитивного доверия. Таким образом, модель на основе субъективной логики может быть использована для вычисления значения репутации, учитывая существующие отношения доверия между узлами.

Потоковые модели

Одной из самых известных и широко используемых потоковых репутационных моде-

лей является EigenTrust [10, 11]. Применение данной модели в системах управления доверием в сети позволяет снизить воздействие вредоносных узлов и уменьшить их влияние на процесс передачи информации.

Все узлы сети взаимодействуют друг с другом для предоставления услуг, совершая так называемые транзакции. По завершении транзакции между парой узлов, участники транзакции производят оценку её качества. Узел i может оценить транзакцию с узлом j, как положительную (tr(*i, j*) = 1) или отрицательную (tr(*i, j*) = -1).

Локальное значение доверия узла *i* к узлу *j*, обозначается S_{ij} и определяется как разница между числом положительных и отрицательных транзакций соответствующих узлов:

$$S_{ij} = \mathrm{sat}(i,j) - \mathrm{unsat}(i,j).$$

Дальнейшая нормализация позволяет исключить возможность формирования произвольно высоких и произвольно низких значений локального доверия, в результате кооперации вредоносных узлов. Нормализованное локальное значение доверия Cij узла i к узлу j определяется как:

$$C_{ij} = \frac{\max(S_{ij},0)}{\sum_k \max(S_{ik},0)}, \text{ если } \sum_k \max(S_{ik},0) \neq 0. \quad (1)$$

При этом, если некоторый узел *i* ранее не потреблял услуги других узлов сети, то $S_{ij} = 0$ для любого *j*. В этом случае нормализованное значение локального доверия $C_{ij} = P_j$, где $P_j = 1/|P|$, если $j \in P$, иначе $P_j = 0$. При этом *P* представляет собой множество изначально доверенных узлов.

Нормализованное значение локального доверия может рассматриваться как вероятностная мера, поскольку:

$$0 \le C_{ij} \le 1, \ \sum_k C_{ik} = 1.$$

Свойство транзитивности доверия позволяет каждому узлу сети *i* агрегировать локальные значения репутации некоторого узла *k*, предоставленные другими узлами сети, для получения значения глобального доверия к соответствующему узлу:

$$t_{ik} = \sum_j C_{ij} C_{jk}.$$

Вектор соответствующих значений для всех узлов сети образует вектор глобального доверия. Тогда определив **C** как матрицу значений нормализованных значений $[C_{ij}]$ локального доверия между узлами сети, вектор глобального доверия можно получить следующим образом:

$$\overline{\mathbf{t}}_i = \mathbf{C}^{\mathbf{T}} \overline{\mathbf{c}}_i.$$

Благодаря свойствам **C**, при увеличении количества итераций *n*, вектор глобального доверия сходится к общему вектору для каждого узла *i* (левому собственному вектору указанной матрицы):

$$\overline{\mathbf{t}} = (\mathbf{C}^{\mathbf{T}})^n \overline{\mathbf{c}}_i.$$

Таким образом, глобальная оценка репутации узлов сети соответствует элементам полученного вектора.

Используя вектор глобального доверия, вычисленный в результате k итераций, можно вычислить значение данного вектора на следующем шаге:

$$\overline{\mathbf{t}}^{(k+1)} = (1-a)\mathbf{C}^{\mathbf{T}} \overline{\mathbf{t}}^{(k)} + a\overline{\mathbf{p}}. \quad (2)$$

Здесь $\overline{\mathbf{p}}$ – вектор априорного доверия к узлам сети, и *a* – некоторая постоянная, необходимая для противодействия кооперации узлов нарушителей, причем $0 < a < 1$.

Применение модели EigenTrust для оценки репутации узлов сети передачи данных можно продемонстрировать на следующем примере. Пусть задана полносвязная сетевая топология из четырех узлов (рис. 1).

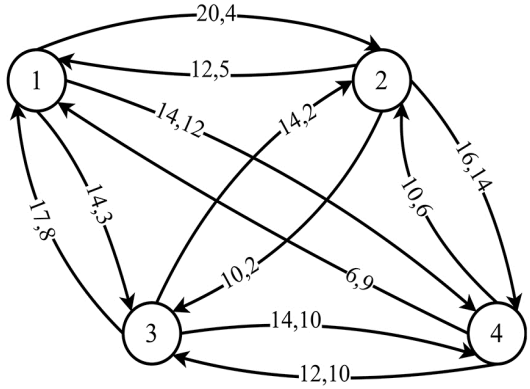


Рис. 1. Пример топологии для демонстрации модели EigenTrust с указанием числа положительных и отрицательных транзакций

Каждый узел предоставляет услуги маршрутизации, т.е. выполняет передачу пакетов для других узлов сети. Некоторые передаваемые пакеты могут быть утеряны в результате ошибок или вредоносного поведения узлов. Пусть узел 4 является нарушителем, отбрасывающим большую часть пакетов, полученных от других узлов сети.

Каждый узел производит накопление данных о количестве доставленных и недоставленных пакетов другими узлами сети. Пусть по результатам сетевого взаимодействия получена совокупная статистика положительных и отрицательных транзакций для каждой пары узлов. Указанные значения приписаны соответствующим дугам сети на рис.

1. Полученные данные отражают вредоносное поведение узла 4.

Используя имеющуюся статистику, каждый узел определяет нормализованное локальное значение доверия к остальным узлам сети в соответствии с (1):

$$\mathbf{C}=\begin{pmatrix} 0 & 0{,}55 & 0{,}37 & 0{,}08 \\ 0{,}41 & 0 & 0{,}47 & 0{,}12 \\ 0{,}36 & 0{,}48 & 0 & 0{,}16 \\ 0 & 0{,}66 & 0{,}34 & 0 \end{pmatrix}.$$

На основе (2) может быть предложен простой алгоритм для вычисления вектора глобального доверия с заданной точностью ε (рис. 2).

1: **procedure** EIGENTRUST($\mathbf{C}$, $\vec{t}^{(0)}$, ε)
2: **repeat**
3: $\vec{t}^{(k+1)} \leftarrow \mathbf{C}^{\mathbf{T}}\vec{t}^{(k)}$
4: $\delta \leftarrow \|\vec{t}^{(k+1)} - \vec{t}^{(k)}\|$
5: **until** $\delta < \varepsilon$
6: **return** $\vec{t}^{(k+1)}$
7: **end procedure**

Рис. 2. Алгоритм EigenTrust

Пусть, в рамках рассматриваемого примера, задано значение a = 0,5, допустимое стандартное отклонение глобального вектора доверия ε = 0,01, а также значение каждого элемента начального вектора глобального доверия принимается равным $1/|P|$.

В результате вычисления вектора глобального доверия на первом шаге алгоритма получено стандартное отклонение δ1 = 0.2175, что превышает допустимое значение. Для достижения требуемого значения стандартного отклонения необходимо выполнить четыре шага алгоритма. Значение вектора глобального доверия, полученное на четвертом шаге алгоритма представлено в табл. 1.

Анализ результатов работы алгоритма позволяет сделать вывод о том, что глобальное доверие к узлу 4 ниже, чем к остальным участникам сетевого взаимодействия. На практике, если репутация узла падает ниже некоторого порогового значения, сетевой узел может быть исключен из процесса маршрутизации или, иначе говоря, изолирован [12].

Один из недостатков модели EigenTrust заключается в том, что нормализация значений доверия не позволяет отличить узлы с отрицательной репутацией от узлов с нейтральной репутацией. Кроме того, оценка доверия в рамках модели является относительной, а не абсолютной, т.е. по сути только позволяет сформировать рейтинг надёжности узлов.

Система PeerTrust [13] представляет еще одну потоковую репутационную модель, изначально разработанную для пиринговых сетей. Хотя PeerTrust имеет много общего с EigenTrust, при оценке уровня доверия к узлам сети учитывается большее количество факторов. В модели PeerTrust репутация узла, который не взаимодействовал с другими узлами, остается неопределенной. Кроме того,

Таблица 1

Результаты работы алгоритма

Шаг	Вектор глобального доверия				δ
	1	2	3	4	
0	0,25	0,25	0,25	0,25	-
1	0,2213	0,3363	0,2725	0,17	0,2175
2	0,2430	0,3073	0,2739	0,1758	0,0578
3	0,2373	0,3156	0,2721	0,1751	0,0164
4	0,2387	0,3133	0,2728	0,1752	0,00448

PeerTrust обеспечивает поддержку контекста взаимодействия, что позволяет учитывать, например, важность транзакций при оценке уровня доверия.

Комбинированный показатель доверия объединяет сразу несколько факторов, что позволяет эффективно противодействовать вредоносному поведению узлов. Важно, что оценки, предоставляемые другими узлами, являются взвешенными по уровню надежности этих узлов. Исходя из этого, адекватность репутационной модели PeerTrust может значительно снижаться в некоторых сценариях сетевого взаимодействия. В частности, узел может обеспечивать высококачественные услуги в качестве маршрутизатора, в то же время предоставляя вредоносные оценки для других узлов сети.

Одно из возможных решений указанной проблемы было предложено в рамках репу-

тационной системы BP/P2P [14]. Для каждого узла сети определяется показатель репутации, вычисляемый на основе его качества обслуживания, и показатель достоверности, вычисляемый на основе оценок, которые предоставляет этот узел после каждой транзакции. Таким образом, модель разделяет функциональное и реферальное доверие.

Для вычисления соответствующих показателей авторы предложили специальный алгоритм распространения сообщений между вершинами фактор графа, соответствующего рассматриваемой телекоммуникационной сети. Всесторонняя оценка показала, что система BP/P2P эффективна при вычислении значений достоверности узлов, что с высокой вероятностью позволяет уменьшить ошибки при вычислении значений репутации, возникающие в результате распространения фиктивных оценок. Более того, в результате сравнения с EigenTrust, система BP/P2P продемонстрировала более высокую устойчивость к вредоносному поведению узлов при меньшем количестве накладных расходов.

В рамках полностью децентрализованной репутационной модели VectorTrust происходит построение сети доверия на базе сети передачи данных [15]. Вектор доверия (trust vector) представляет собой дугу между двумя узлами соответствующего графа, вес которой определяется по результатам прямых транзакций между соответствующими узлами. Таким образом, каждый узел определяет уровень прямого доверия к соседним узлам сети, которое хранится в локальных таблицах доверия. Модель подразумевает транзитивность доверия и позволяет быстро агрегировать вектора доверия с помощью специального алгоритма, основанного на алгоритме Беллмана-Форда. В результате формируется таблица маршрутов с максимальным уровнем доверия до всех узлов сети.

Применение модели VectorTrust для поиска наиболее безопасных маршрутов можно продемонстрировать на следующем примере. Пусть задана сетевая топология из шести узлов (рис. 3).

Каждый узел предоставляет услуги маршрутизации, при этом узел 5 является нарушителем, отбрасывающим большую часть пакетов, полученных от других узлов сети, что отражается результатами прямых наблюдений соседних узлов. Рассмотрим задачу поиска маршрута с максимальным уровнем доверия от узла 1 до узла 6.

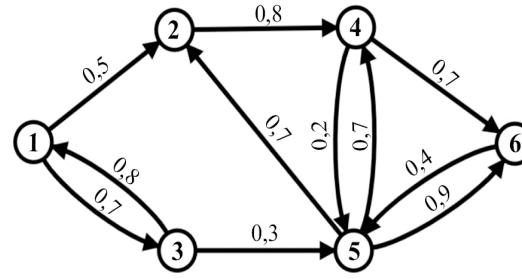


Рис. 3. Пример топологии для демонстрации модели VectorTrust с указанием прямого доверия между соседними узлами сети

На начальном этапе каждый узел формирует таблицу маршрутов исходя из локальной таблицы доверия. Далее, на каждом шаге алгоритма соседние узлы обмениваются таблицами маршрутов и агрегируют получаемую информацию. Например, на первом шаге узел 1 получает таблицу маршрутов от узла 2, в которой содержится маршрут из узла 2 до узла 4 с уровнем доверия $T_{2,4} = 0,8$. Учитывая существующий маршрут от узла 1 до узла 2 с уровнем доверия $T_{1,2} = 0,5$, в таблицу узла 1 добавляется новый маршрут до узла 4 с уровнем доверия $T_{1,4} = T_{1,2} * T_{2,4} = 0,4$.

Обмен таблицами продолжается вплоть до достижения их сходимости. В результате работы алгоритма каждый узел получил таблицу маршрутов, каждый из которых имеет максимально возможный уровень доверия. Совокупность этих данных представлена в табл. 2. Первое значение в каждой ячейке таблицы представляет узел следующего перехода, а второе – уровень доверия к маршруту.

Используя указанную таблицу, наиболее безопасный маршрут от узла 1 к узлу 6 может быть определен как «1->2->4->6».

По сравнению с другими моделями, включая EigenTrust и PeerTrust, при увеличении количества узлов модель VectorTrust эффективно масштабируется благодаря высокой скорости конвергенции и умеренной вычислительной нагрузке. Вместе с тем, по сравнению с моделью PeerTrust, модель VectorTrust не позволяет учитывать достоверность агрегируемых оценок.

Модели на основе субъективной логики

Альтернативное направление исследований по обеспечению безопасности маршрутизации в динамически организуемых сетях связано с разработкой репутационных моделей на базе субъективной логики. Субъективная логика представляет собой алгебру доверия, основанную на байесовской теории и булевой логике, и может быть использована

Таблица2

Совокупная таблица маршрутов

Узел назначения	Узел источника					
	1	2	3	4	5	6
1	1; 1	-	1; 0,8	-	-	-
2	2; 0,5	2; 1	1; 0,4	6; 0,196	2; 0,7	5; 0,28
3	3; 0,7	-	3; 1	-	-	-
4	2; 0,4	4; 0,8	1; 0,32	4; 1	4; 0,7	5; 0,28
5	3; 0,21	4; 0,4	5; 0,3	6; 0,28	5; 1	5; 0,4
6	2; 0,28	4; 0,56	5; 0,27	6; 0,7	6; 0,9	6; 1

для моделирования и анализа сетей доверия [18, 23]. Центральным понятием модели является трехэлементный кортеж, именуемый мнением. Мнение узла A о некотором узле X обозначается как:

$$\omega_X^A = (b_X^A, d_X^A, u_X^A),$$

где *b, d, u* ∈ [0, 1] и $b + d + u = 1$. Здесь *b, d* и *u* отражают уровень доверия, недоверия и неопределенности соответственно.

Трехэлементное мнение может быть расширено с помощью четвертого параметра *a* ∈ [0, 1], называемого базовым коэффициентом. Тогда прогнозируемая вероятность легитимности узла *X* по мнению узла *A* определяется как:

$$P_X^A = b_X^A + a_X^A u_X^A. \quad (3)$$

В отсутствие каких-либо конкретных свидетельств о рассматриваемой сети базовый коэффициент определяет априорное доверие, которое будет оказано любому узлу сети.

Пространство мнений можно отобразить внутри равностороннего треугольника, где для мнения $\omega_X = (b_X, d_X, u_X, a_X)$, три показателя b_X, d_X и u_X определяют положение точки, представляющий мнение в треугольнике. Оси доверия, недоверия и неопределенности представляют собой серединные перпендикуляры, которые проходят от каждой стороны треугольника к противоположной вершине, обозначенной меткой *b, d, u* соответственно. Например, полностью положительное мнение представлено правой нижней вершиной треугольника. Базовый коэффициент *a* отображается в виде указателя, а прогнозируемая вероятность формируется путем проецирования мнения на основание треугольника параллельно линии проекции базового коэффициента.

На рис. 4 представлен пример треугольника пространства мнений, внутри которого располагается значение $\omega_X = (0.6, 0.3, 0.1, 0.5)$.

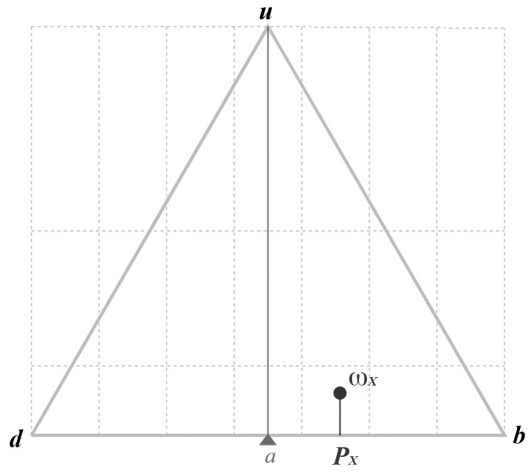


Рис. 4. Визуализация пространства мнений для репутационной модели на основе субъективной логики

Мнения основаны на свидетельствах. Свидетельства могут быть представлены в виде пары неотрицательных конечных чисел *(p, n),* где *p* - количество позитивных свидетельств, подтверждающих предположение, а n – количество негативных свидетельств, которые ему противоречат.

Одна из первых попыток применить модель на основе субъективной логики для обеспечения безопасности маршрутизации была выполнена в рамках протокола TAODV [21]. Применительно к сети передачи данных, для определения мнения узла используются данные предыдущего взаимодействия. Позитивными и негативными свидетельствами могут являться положительные и отрицательные

транзакции (доставленные и недоставленные пакеты соответственно). Как правило, в контексте сетей доверия, базовый коэффициент можно исключить из рассмотрения, потому что он не изменяется никакими вычислениями на основе мнений.

Пусть p – количественный показатель успешно доставленных узлом X пакетов, n – количественный показатель недоставленных пакетов, тогда расчет показателей доверия, недоверия, неопределенности производится следующим образом:

$$b_X = \frac{p}{p+n+2},$$
$$d_X = \frac{n}{p+n+2}, \quad (4)$$
$$u_X = \frac{2}{p+n+2}.$$

Для объединения нескольких мнений в рамках модели на основе субъективной логики предложен ряд операций. Операция дисконтирования позволяет узлу A вычислить мнение об узле C, дополнительно опираясь на мнение промежуточного узла B о целевом узле:

$$b_C^{A\otimes B} = b_B^A b_C^B,$$
$$d_C^{A\otimes B} = b_B^A d_C^B,$$
$$u_C^{A\otimes B} = d_B^A + u_B^A + b_B^A u_C^B.$$

Операция консенсуса позволяет согласовать два независимых мнения узлов *A* и *B* об узле *C*:

$$b_C^{A\oplus B} = b_C^A u_C^B + b_C^B u_C^A \Big/ u_C^A + u_C^B - u_C^A u_C^B,$$
$$d_C^{A\oplus B} = d_C^A u_C^B + d_C^B u_C^A \Big/ u_C^A + u_C^B - u_C^A u_C^B,$$
$$u_C^{A\oplus B} = u_C^A u_C^B \Big/ u_C^A + u_C^B - u_C^A u_C^B.$$

Применение репутационной модели на основе субъективной логики для выбора наиболее безопасного маршрута можно продемонстрировать на следующем примере. Пусть задана сетевая топология из шести узлов (рис. 5).

Каждый узел предоставляет услуги маршрутизации, при этом узел 5 является нарушителем, отбрасывающим большую часть пакетов, полученных от других узлов сети, что отражается результатами прямых наблюдений соседних узлов. Вес каждой дуги в представленной сети соответствует количеству позитивных и негативных свидетельств, накопленных в результате прямого взаимодействия двух узлов к некоторому моменту времени.

Рассмотрим задачу поиска маршрута с максимальным уровнем доверия от узла 1 до узла 6. Базовый коэффициент a принимается равным 0,5 для всей сети.

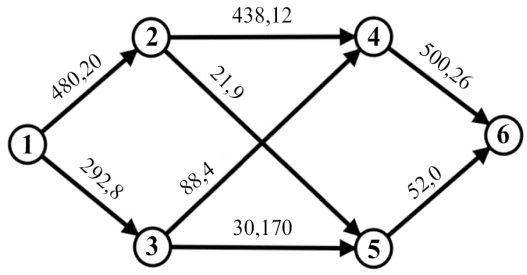


Рис. 5. Пример топологии для демонстрации модели на основе субъективной логики с указанием числа положительных и отрицательных транзакций

Используя имеющуюся историю взаимодействия, каждый узел динамически вычисляет прямое мнение о всех соседних узлах в соответствии с (3). Результаты вычислений для рассматриваемого примера представлены в табл. 3. Для агрегирования мнений узлы сети обмениваются полученными результатами. Таким образом, узел 1 получает возможность сформировать мнение о всех узлах сети.

Используя операции дисконтирования и консенсуса узел 1 вычисляет мнение об узле 4 и узле 5:

$$\omega_4^1 = \omega_4^{(1\otimes 2)\oplus(1\otimes 3)} = (0{,}94,\ 0{,}034,\ 0{,}026),$$

$$\omega_5^1 = \omega_5^{(1\otimes 2)\oplus(1\otimes 3)} = (0{,}292,\ 0{,}677,\ 0{,}031).$$

Каждый из этих узлов является прямым соседним узлом для узла 6 и может предложить маршрут до этого узла. Исходя из (3), вероятность легитимности узла 4 по мнению узла 1 превосходит соответствующую вероятность для узла 5:

$$P_4^1 = 0{,}953,\ P_5^1 = 0{,}308.$$

Таким образом построение маршрута до узла 6 производится через узел 4. Учитывая, что по мнению узла 1, вероятность легитимности узла 2 превосходит вероятность легитимности узла 3, наиболее безопасный маршрут от узла 1 до узла 6 определяется как «1->2->4->6».

Несмотря на уникальную возможность учитывать неопределенность информации, базовая модель на основе субъективной логики имеет ряд недостатков. Учитывая, что расчет репутации зависит от топологии доверительной сети и графа взаимодействий, имплементация модели в рамках протоколов маршрутизации сдерживается проблемой автоматизации вычислений.

Важно, что операция дисконтирования не имеет естественной интерпретации по отношению к учету свидетельств [19]. Кроме того, дисконтирование не является дистрибутивным по отношению к операции консенсуса.

Таблица 3

Совокупная таблица прямых мнений

Мнение	b	d	u
ω_2^1	0,956	0,04	0,004
ω_3^1	0,967	0,026	0,007
ω_4^2	0,969	0,027	0,004
ω_5^2	0,656	0,281	0,063
ω_4^3	0,936	0,043	0,021
ω_5^3	0,149	0,842	0,009
ω_6^4	0,947	0,049	0,004
ω_6^5	0,963	0	0,037

Операция дисконтирование накладывает ограничения на свидетельства, которые можно агрегировать. Требуется, чтобы свидетельства были независимыми [23]. В тоже время, четко определить понятие независимости свидетельств достаточно трудно. Таким образом, может возникнуть проблема повторного учета свидетельств. Например, рассмотрим выражение $(\omega_y \otimes \omega_x) \oplus (\omega_z \otimes \omega_x)$, где мнения об узле x сформированы из одного и того же наблюдения. Свидетельства, лежащие в основе мнения об *x*, учитываются как в левой, так и в правой части выражения. Это явный случай повторного учета свидетельств. Для предотвращения указанной проблемы в рамках моделей на основе субъективной логики требуется, чтобы сеть доверия была представлена в канонической форме [24], где все пути доверия независимы. Упрощенно, выражение сети доверия находится в канонической форме, если каждое ребро появляется в выражении только один раз. Довольно часто сеть доверия невозможно представить канонической форме. В таком случае, в соответствии с [24], можно удалить некоторые ребра из сети для решения указанной проблемы. При этом качество получаемых репутационных оценок снижается, поскольку учитывается не вся доверительная информация.

В работе [19] предпринята попытка объединить достоинства подхода на основе субъективной логики и потоковых репутационных моделей. Авторы работы предложили альтернативную операцию дисконтирования, которая вместо перемножения мнений предполагает учитывать некоторую часть доказательств узла пропорционально вероятности легитимности этого узла. В результате можно представить себе дисконтирование как физическую передачу свидетельств от узла B к узлу A, во время которой из-за недоверия и неопределенности сохраняется только некоторая их часть. В работе представлено доказательство, что предложенная операция дисконтирования является дистрибутивной относительно операции консенсуса и позволяет исключить двойной учет свидетельств.

Представленную алгебру мнений авторы работы именуют субъективной логикой, основанной на доказательствах (EBSL, Evidence Base Subjective Logic). Показано, что новая алгебра EBSL позволяет определить итерационный алгоритм для расчета репутации узлов в сетях доверия произвольного вида. Основное достоинство предложенного подхода заключается в возможности обеспечить качество агрегируемых свидетельств, поскольку удалять ребра из сети больше не требуется. Полученные результаты позволяют на базе EBSL разработку новых репутационных моделей.

Вместе с тем, предложенный подход также имеет недостатки. В частности, при формировании мнений не учитываются отрицательные свидетельства, а для получения адекватных репутационных оценок требуется корректное определение системного параметра, связанного с максимально допустимым количеством положительных свидетельств.

Заключение

В настоящее время различные репутационные системы всё чаще применяются для оценки надежности узлов и достоверности информации в сетевой инфраструктуре. Вместе с тем, репутационные модели доверия должны учитывать специфику конкретной задачи, чтобы их можно было использовать для её решения. Это требует понимания возможностей и ограничений существующих репутационных моделей.

В результате исследования был сформирован ряд требований, которым должна удовлетворять репутационная модель для решения рассматриваемой проблемы. Учитывая сложные топологии динамически организуемых сетей, используемая модель должна поддерживать передачу доверия, т.е. быть транзитивной. При этом, процедура агрегирования оценок может быть интегрирована в процесс объявления сетевых маршрутов. Для противодействия вредоносным узлам модель должна учитывать качество источника получаемых оценок, поскольку оценки, полученные от разных узлов, могут иметь различный вес. Модель должна отличать поведение эгоистичных узлов, игнорирующих объявление сетевых маршрутов. Необходимо, чтобы модель учитывала количество информации, использованной для формирования оценки (например, за счёт показателя неопределенности). Также модель должна учитывать контекст взаимодействия, различать функциональное и реферальное доверие. Кроме того, для динамически организуемых сетей важно, чтобы используемая модель обеспечивала минимальный уровень вычислительных и сетевых накладных расходов. Таким образом, разработка модели с указанными характеристиками для обеспечения безопасности маршрутизации в динамически организуемых сетях по-прежнему представляет актуальную задачу.

Литература

1. Щерба Е.В., Никонов В.И., Литвинов Г.А. Обеспечение безопасности протоколов маршрутизации для телекоммуникационных сетей с динамической топологией // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21. № 3. С. 19–29.

2. Braga D.D.S., Niemann M., Hellingrath B., Neto F.B.L. Survey on computational trust and reputation models // ACM Computing Surveys. 2018. Vol. 51, №5. P. 1–40.

3. Губанов Д.А. Обзор онлайновых систем репутации/доверия. М., ИПУ РАН, 2009. 25 с.

4. Абрамов Е.С., Басан Е.С., Басан А.С. Разработка системы управления уровнем доверия в мобильной кластерной беспроводной сенсорной сети // Известия ЮФУ. Технические науки. 2015. № 7(168). С. 41–52.

5. Басан А.С., Басан Е.С. Методика оценки доверия в беспроводной сенсорной сети // Безопасные информационные технологии (БИТ-2016): Сборник трудов Седьмой Всероссийской научно-технической конференции. М., МГТУ имени Н.Э.Баумана, 2016. С. 38–40.

6. Басан А.С., Басан Е.С., Макаревич О.Б. Анализ и разработка средств обеспечения безопасности для систем группового управления автономными мобильными роботами // Вопросы кибербезопасности. 2017. № 5(24). С. 42–49.

7. Калинин М.О., Минин А.А. Выявление угроз информационной безопасности в сетях с динамической топологией за счет контроля активности узлов // Проблемы информационной безопасности. Компьютерные системы. 2016. № 4. С. 23–31.

8. Овасапян Т.Д., Иванов Д.В. Обеспечение безопасности WSN-сетей на основе модели доверия // Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 64–72.

9. Michiardi P., Molva R. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks // Advanced communications and multimedia security. 2002. P. 107–121.

10. Kamvar S.D., Schlosser M.T., Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks // Proc. of the 12th international conference on World Wide Web, 2003. P. 640–651.

11. Kurdi H.A. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems // Journal of King Saud University: Computer and Information Sciences. Vol. 27(3). 2015. P. 315–322.

12. Proto F.S., Detti A., Pisa C., Bianchi G. A Framework for Packet-Droppers Mitigation in OLSR Wireless Community Networks // Proc. of 2011 IEEE International Conference on Communications (ICC), 2011. P. 1–6.

13. Xiong L., Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities // IEEE Transactions on Knowledge and Data Engineering. 2004. Vol. 16, №7. P. 843–857.

14. Ayday E., Fekri F. BP-P2P: Belief propagation-based trust and reputation management for P2P networks // Proc. of 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012. P. 578–586.

15. Zhao H., Li X. VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks // The Journal of Supercomputing. 2013. Vol. 64(3). P. 805–829.

16. Tavakolifard M., Knapskog S. A probabilistic reputation algorithm for decentralized multi-agent environments // Electronic Notes in Theoretical Computer Science. 2009. Vol. 244. P. 139–149.

17. Teacy W.T.L., Luck M., Rogers A., Jennings N.R. An efficient and versatile approach to trust and reputation using hierarchical bayesian modelling // Artificial Intelligence. 2012. Vol. 193. P. 149–185.

18. Jøsang A. Trust network analysis with subjective logic / A. Jøsang, R. Hayward, S. Pope // In Proc. of the Twenty-Ninth Australasian Computer Science Conference (ACSW). – 2006. – P. 85–94.

19. Škorić B., De Hoogh S.J., Zannone N. Flow-based reputation with uncertainty: evidence-based logic // International Journal of Information Security. 2016. Vol. 15(4). P. 381–402.

20. Kurdi H., Alshayban B., Altoaimy L., Alsalamah S. TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds // Wireless Communications and Mobile Computing. 2018. Vol. 2018. P. 1–13.

21. Li X, Lyu M.R., Liu J. A trust model based routing protocol for secure ad hoc networks // Proc. of Aerospace Conference. IEEE, 2004. Vol. 2. P. 1286–1295.

22. Shafer G. A mathematical theory of evidence. Princeton University Press, 1976. 298 p.

23. Jøsang A. Subjective Logic – A Formalism for Reasoning Under Uncertainty. Springer, 2016. 326 p.

24. Jøsang A., Gray E., Kinateder M. Simplification and analysis of transitive trust networks // Web Intelligence and Agent Systems: An International Journal. 2006. Vol. 4(2). P. 139–161.

References

1. Shcherba E.V., Nikonov V.I., Litvinov G.A. Securing Routing Protocols for Wireless Networks with Dynamic Topology. Proceedings of TUSUR University, 2018, vol. 21, no. 3, pp. 19–29.

2. Braga D.D.S., Niemann M., Hellingrath B., Neto F.B.L. Survey on computational trust and reputation models. ACM Computing Surveys, 2018, vol. 51, №5, pp. 1–40.

3. Gubanov D.A. Obzor onlajnovykh sistem reputatsii/doveriia [The survey of online systems of reputation/trust]. Moscow, IPU RAN Publ., 2005. 25 p.

4. Abramov E.S., Basan E.S., Basan A.S. Development of the trust management system for mobile wireless sensor network. Izvestiya SFedU. Engineering sciences, 2015, no. 7(168), pp. 41–52.

5. Basan A.S., Basan E.S. The method of the trust estimation in a wireless sensor network [Metodika ocenki doverija v besprovodnoj sensornoj seti]. Bezopasnye informacionnye tehnologii (BIT-2016): Sbornik trudov Sedmoj Vserossijskoj nauchno-tehnicheskoj konferencii [Secure information technology. Proc. of the seven AllRussian scientific conference]. Moscow, MSTU them. N.E. Bauman Publ., 2016, pp. 38–40.

6. Basan A.S., Basan E.S., Makarevich O.B. Analysis of ways to secure group control for autonomous mobile robots. Cybersecurity issues, 2017, no. 5(24), pp. 42–49.

7. Kalinin M.O., Minin A.A. Detection of information security threats in computer networks with dynamic topology using hosts activity monitoring. Information Security Problems. Computer Systems, 2016, no. 4, pp. 23–31.

8. Ovasapyan T.D., Ivanov D.V. Trust model based approach to WSN-networks information security. Information Security Problems. Computer Systems, 2017, no. 4, pp. 64–72.

9. Michiardi P., Molva R. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. Advanced communications and multimedia security, 2002, pp. 107–121.

10. Kamvar S.D., Schlosser M.T., Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks. Proc. of the 12th international conference on World Wide Web, 2003, pp. 640–651.

11. Kurdi H.A. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems. Journal of King Saud University: Computer and Information Sciences, vol. 27(3), 2015, pp. 315–322.

12. Proto F.S., Detti A., Pisa C., Bianchi G. A Framework for Packet-Droppers Mitigation in OLSR Wireless Community Networks. Proc. of 2011 IEEE International Conference on Communications (ICC), 2011, pp. 1–6.

13. Xiong L., Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 2004, vol. 16, no. 7, pp. 843–857.

14. Ayday E., Fekri F. BP-P2P: Belief propagation-based trust and reputation management for P2P networks. Proc. of 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012, pp. 578–586.

15. Zhao H., Li X. VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks. The Journal of Supercomputing, 2013, vol. 64(3), pp. 805–829.

16. Tavakolifard M., Knapskog S. A probabilistic reputation algorithm for decentralized multi-agent environments. Electronic Notes in Theoretical Computer Science, 2009, vol. 244, pp. 139–149.

17. Teacy W.T.L., Luck M., Rogers A., Jennings N.R. An efficient and versatile approach to trust and reputation using hierarchical bayesian modelling. Artificial Intelligence, 2012, vol. 193, pp. 149–185.

18. Jøsang A., Hayward R., Pope S. Trust network analysis with subjective logic. Proc. of the Twenty-Ninth Australasian Computer Science Conference (ACSW), 2006, pp. 85–94.

19. Škorić B., de Hoogh S.J., Zannone N. Flow-based reputation with uncertainty: evidence-based logic. International Journal of Information Security, 2016, vol. 15(4), pp. 381–402.

20. Kurdi H., Alshayban B., Altoaimy L., Alsalamah S. TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds. Wireless Communications and Mobile Computing, 2018, vol. 2018, pp. 1–13.

21. Li X., Lyu M.R., Liu J. A trust model based routing protocol for secure ad hoc networks. Proc. of Aerospace Conference, 2004, IEEE, 2004, vol. 2, pp. 1286–1295.

22. Shafer G. A mathematical theory of evidence. Princeton University Press, 1976, 298 p.

23. Jøsang A. Subjective Logic – A Formalism for Reasoning Under Uncertainty. Springer, 2016, 326 p.

24. Jøsang A., Gray E., Kinateder M. Simplification and analysis of transitive trust networks. Web Intelligence and Agent Systems: An International Journal, 2006, vol. 4(2), pp. 139–161.

ЛИТВИНОВ Георгий Александрович, аспирант кафедры комплексной защиты информации, Омский государственный технический университет, 644050, г. Омск, пр. Мира, 11. E-mail: georgyfunds@gmail.com

ЩЕРБА Евгений Викторович, кандидат технических наук, доцент, доцент кафедры комплексной защиты информации, Омский государственный технический университет, 644050, г. Омск, пр. Мира, 11. E-mail: evscherba@gmail.com

LITVINOV George, Graduate student, Department of Complex Information Protection, Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: georgyfunds@gmail.com

SHCHERBA Evgeny, Candidate of Engineering, Associate Professor, Department of Complex Information Protection, Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: evscherba@gmail.com

УДК 004.056 Вестник УрФО № 3(41) / 2021, с. 24–29

Чан З. Х.

DOI: 10.14529/secur210303

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Обеспечение информационной безопасности элементов киберфизических систем является необходимым условием их корректного функционирования. В мобильной распределённой киберфизической системе эта задача осложняется рядом специфических факторов, связанных, в том числе с неконтролируемым доступом к беспроводной среде передачи данных и ограничениями на применение «тяжёлой» криптографии. В статье проанализированы протоколы аутентификации типа «запрос - ответ», приведены результаты исследования различных криптографических механизмов, используемых в таких протоколах, и выявлены угрозы безопасности аутентификации. Работа будет полезна молодым ученым, разрабатывающим методы аутентификации в киберфизической системе, а также специалистам, работающим в области информационной безопасности.

Ключевые слова: *сенсорная сеть, информационная безопасность, аутентификации стороны, криптография, угроза, киберфизическая система.*

Chan Z.H.

AUTHENTICATION PROBLEMS IN WIRELESS SENSOR NETWORKS

Ensuring information security of elements of cyber-physical systems is a prerequisite for their correct functioning. In a mobile distributed cyber-physical system, this task is complicated by a number of specific factors related, including uncontrolled access to wireless data transmission medium and restrictions on the use of "heavy" cryptography. The article analyzes authentication protocols of the "challenge-response" type, presents the results of a study of various cryptographic mechanisms used in such protocols, and identifies threats to the security of authentication. The work will be useful for young scientists who develop authentication methods in a cyber-physical system, as well as specialists working in the field of information security.

Keywords: *sensor network, information security, side authentication, cryptography, threat, cyber-physical system.*

Введение

В киберфизической системе (КФС) [1] аутентификация объекта является необходимым шагом для обеспечения информационной безопасности и корректности функционального взаимодействия. Несмотря на наличие широкого спектра работ в этом направлении, задача разработки метода аутентификации в беспроводных сенсорных сетях остаётся актуальной научно-технической задачей. Причём вопросы выявления проблемы аутентификации для конкретной реализации КФС выходят на первый план с увеличением комплексных рисков эксплуатации таких систем.

Необходимость применения беспровод-

ных сенсорных сетей стала важной в настоящее время и в будущем из-за их уникальных преимуществ: низкая стоимость (установка и эксплуатация), возможность широкого развертывания с самоорганизацией, легким добавлением или исключением агента из сети. Они используются в роботах не только для обмена данными, но и для сбора информации, полученной из окружающей среды, для передачи ее центральному узлу. С точки зрения мобильных агентов к процедуре аутентификации предъявляется ряд дополнительных требований, связанных с ограничением времени и пространства взаимодействия, ограниченностью доступных вычислительных ресурсов и возможностью компрометации объекта путём получения физического доступа к нему [2,3]. Причём для КФС актуальной становится не только аутентификация информационного потока, но и аутентификация собственно агента (устройства) [4].

В зависимости от конкретных условий функционирования КФС реализуются различные механизмы аутентификации взаимодействующих сторон, как правило с сохранением конфиденциальности информации. Выделяют две основные модели аутентификации: модель с непосредственной связью пар агентов [5]; и модель с использованием доверенной третьей стороны [6], что особенно важно при отсутствии зон перекрытия коммуникаций мобильных агентов [7].

Протокол аутентификации типа «запрос – ответ»

Согласно со стандартами ISO / IEC 9798 под аутентификацией сторон понимается как процесс проверки подлинности предлагающего агента [8]. В том числе включает протоколы аутентификации на основе симметричного, асимметричного ключа, хеширование, протоколы с нулевым разглашением знаний.

Протоколы аутентификации типа «запрос – ответ» с использованием симметричных криптосхем основаны на подтверждении путём доказывания знания секрета. Этот секрет может быть создан заранее или сгенерирован доверенной третьей стороной во время сеанса связи. Протоколы аутентификации на основе асимметричного шифрования обеспечивают высокую степень безопасности, но требуют больших вычислительных ресурсов и сложности процесса генерирования ключевой пары. Протоколы аутентификации в беспроводных специальных сетях описаны в таблицах 1,2,3,4,5.

Проблема качества криптографических примитивов

Применение криптографических методов аутентификации обеспечивает более высокий уровень безопасности. Однако облечённый протокол требует небольшого времени обработки оператором для уменьшения задержки. Мы протестировали время отработки некоторых операторов (рисунок 1) с использованием Raspberry Pi3 b +, 1,4 ГГц ЦП, 1024 RAM LPDDR2, Micro SD 8GB. Размер ключа выбирается в соответствии с требованием безопасности [9].

Как показано на рисунке, время обработ-

Таблица 1

Протокол аутентификации на основе пароля

Агент А	*к* - общий секретный ключ	Агент В
$M = D_k(C)$ Если { $P_b^{'} = P_b$ } то {В аутентифицирован}	<|= [C]	P_b – пароль $C = E_k(P_b)$

Таблица 2

Протокол взаимной аутентификации, основанной на симметричном шифровании

Агент А	*к* - общий секретный ключ	Агент В
	<|= [N_b]	N_b – случайное число
N_a - случайное число $C_1 = E_k(N_a, N_b, B)$	[C_1] =|>	$M_1 = D_k(C_1)$ Если {$N_b^{'} = N_b$}и{$B^{'} = B$} то {А аутентифицирован}
$M_2 = D_k(C_2)$ Если {$N_a^{'}$=N_a}и{$N_b^{''} = N_b$} то {В аутентифицирован}	<|= [C_2]	$C_2 = E_k(N_a, N_b)$

Таблица 3

Протокол взаимной аутентификации, основанной на асимметричном шифровании

Агент А		Агент В
Генерация пары ключей sk_a, pk_a	$[pk_a]=\|>$ $<\|=[pk_b]$	Генерация пары ключей sk_b, pk_b
	$<\|=[N_b]$	N_b – случайное число
N_a - случайное число $C_1 = E_{pk_b}(N_a, N_b, B)$	$[C_1]=\|>$	$M_1 = D_k(C_1)$ Если $\{N_b^{'} = N_b\}$и$\{B^{'} = B\}$ то {А аутентифицирован}
$M_2 = D_k(C_2)$ Если $\{N_a^{'} = N_a\}$и$\{N_b^{"} = N_b\}$ то {В аутентифицирован}	$<\|=[C_2]$	$C_2 = E_{pk_a}(N_a, N_b)$

Таблица 4

Протокол взаимной аутентификации, основанной на основе сертификатов, и цифровой подпись

Агент А		Агент В
Генерация пары ключей sk_a, pk_a Получение сертификат cer_a	$[pk_a]=\|>$ $<\|=[pk_b]$	Генерация пары ключей sk_b, pk_b Получение сертификат cer_b
Получение t_a - метка времени $S_1 = Sign_{sk_a}(t_a, B)$	$[S_1, t_a, B, cer_a]=\|>$	$Ver_{pk_a}(S_1) \overset{?}{=} \{0/1\}$ Если $\{Ver_{pk_a}(S_1) == 1\}$ то {А аутентифицирован}
$Ver_{pk_b}(S_2) \overset{?}{=} \{0/1\}$ Если $\{Ver_{pk_b}(S_2) == 1\}$ то {В аутентифицирован}	$<\|=[S_2, t_b, A, cer_b]$	Получение t_b - метка времени $S_2 = Sign_{sk_b}(, t_b, A)$

Таблица 5

Протокол взаимной аутентификации на основе ключевой хеш-функции

Агент А	k - общий секретный ключ	Агент В
	$<\|=[N_b]$	N_b – случайное число
N_a - случайное число $H_1 = h_k(N_a, N_b, B)$	$[N_a, H_1]=\|>$	$H_1^{'} = h_k(N_a, N_b, B)$ Если $H_1^{'} = H_1\}$, то {А аутентифицирован}
$H_2^{'} = h_k(N_a, N_b, A)$ Если $\{H_2^{'} = H_2\}$, то {В аутентифицирован}	$<\|=[H_2]$	$H_2 = h_k(N_a, N_b, A)$

Разъяснение обозначений

$E_k()$	Шифрование с общим ключом
$D_k()$	Дешифрование с общим ключом
sk	Секретный ключ
pk	Публичный ключ
$Sign_{sk}$	Подпись секретным ключом
Ver_{pk}	Верификация публичным ключом
$h_k()$	Хэш-функция
$E_{pk}()$	Шифрование публичным ключом
$D_{sk}()$	Дешифрование секретным ключом

ки DSA является самым высоким, а время обработки MD5 - самым низким, составляющим всего 0,125 мс. Значительная разница во времени отработки показывает возможность

Рис. 1. Примитивное время для криптографической операции

Таблица 6

Сравнение степени использования методов аутентификации в беспроводных сенсорных сетях

Аутентификации в беспроводной сенсорной сети	Уровень вычисления	Уровень безопасности	Уровень ресурсов
Аутентификация на основе пароля	средняя	низкая	средняя
Аутентификация на основе сертификатов и цифровая подпись	высокая	высокая	высокая
Аутентификация, основанная на симметричном шифровании	средняя	высокая	средняя
Аутентификация, основанная на асимметричном шифровании	высокая	высокая	высокая
Аутентификация на основе хеша	низкая	высокая	средняя

применения аутентификация на основе односторонней хеш-функции требует наименьших вычислительных затрат. Ключевая хеш-функция использует общий секретный ключ для вычисления хэш-значения, но необходимо периодически изменять секретный ключ для защиты от некоторых атак. Чтобы решить эту проблему, используется общий секретный ключ в качестве аргумента хэш-функции. Выводы о степени применения методов аутентификации в беспроводных сенсорных сетях представлены в таблице 6.

Специфика аутентификации в беспроводных сенсорных сетях

Используя централизованный подход, агенты должны связываться с сервером, когда требуется аутентификация. Это очень неудобно для динамичного киберпространства, как воздушного аппарата. Более того, серверу аутентификации будет сложно избежать перегрузки при выполнении взаимной аутентификации для агентов в группе. Что касается децентрализованного подхода, проблема распределения групповых секретных ключей должна быть решена, потому что должна быть точка доверия, такая как центральный сервер аутентификации.

Основными проблемами аутентификации в беспроводных сенсорных сетях являются динамичность (часто меняется состояние элементов); ограниченный ресурс, запас энергии, время автономной работы устройств и наличие информационных угроз. В открытых средах злоумышленникам доступны данные сеансов связи, что позволяет осуществлять сбор коммуникационной информации и проводить типовые атаки на протоколы аутентификации, такие как подмена одного

Таблица 7

Угроз аутентификации в беспроводных сенсорных сетях

Причина	Вид воздействия
Несовпадение предъявленного секрета	- Сбой техники (аппаратный или программный) - Попытка злоумышленника (нарушители)
Превышено время аутентификации	- DoS- атака (интенсивность потока заявок) - Внутренний нарушитель
Недостаточно времени для завершения процессы	- Динамичный агент (не завершил процесс аутентификации, находясь в области взаимодействия)
Не выявил обман при проверке ID	- Атака класса «маскарад» (подделка на имя легального агента)
Потеря аутентичный секрет	- Атака злоумышленника

агента другим, сохранение и задержка передачи сообщения, повторение сеансового сообщения, отражение сообщения и комбинированные. Наличие уязвимостей в системе и угроз приводит к тому, что, с одной стороны, необходимо решить проблему сохранения целостности данных, с другой стороны, обеспечить нормальный доступ для легальных агентов на этих данных. Проблема информационных угроз представлена в таблице 7.

Существуют нарушители (законные агенты) и злоумышленники (неавторизованные агенты), влияющие на качество аутентификации. Нарушители могут выявлять «личность» другого агента и отправлять сообщения для обнаружения соседей, «сговориться» и использовать общий секретный ключ с аутентичными агентами. Злоумышленник может стараться идентифицировать секретный ключ и взломать схему аутентификации. Для повышения эффективности процесса обеспечения информационной безопасности во время аутентификации необходимо дифференцировать вредоносные объекты, что позволит разработать специфические механизмы противодействия.

Заключение

В статье проанализирован протокол аутентификации типа «запрос-ответ». Проведен результат исследования криптографических операторов, используемых в таких протоколах, выявлены угрозы процессу аутентификации. Исследование потенциальных проблем аутентификации в беспроводных сенсорных сетях способствует улучшению способности обрабатывать методы и протоколы аутентификации в зависимости от поставленных задач.

Перспективными направлениями исследований являются: разработка методики автоматизированной генерации протоколов аутентификации в группировках агентов – беспилотных транспортных средств в зависимости от условий и требований к функционированию КФС; и, связанное с этим формирование библиотек (шаблонов) примитивов, содержащих верифицированные компоненты протоколов взаимодействия таких агентов.

Литература

1. A. Humayed, J. Lin, F. Li and B. Luo. Cyber-Physical Systems Security—A Survey // IEEE Internet of Things Journal, Dec. 2017, vol. 4, no. 6, pp. 1802-1831, DOI: 10.1109/JIOT.2017.2703172.

2. Комаров И. И., ЮРЬЕВА Р. А., ДРАННИК А.Л., МАСЛЕННИКОВ О. С. Постановка задачи обеспечения информационной безопасности роевых робототехнических систем //Наука и бизнес: пути развития. – 2015. – №. 3. – С. 53.

3. Чан З., Комаров И. И., Швед В.Г. Аутентификация агентов в группе БПЛА на основе социальных механизмов // Защита информации. Инсайд - 2019. - № 6(90). - С. 66-71.

4. А. В. Черемушкин, "Криптографические протоколы: основные свойства и уязвимости // прикладная дискретная математика, 2009, приложение № 2, ст.115–150. DOI: 10.1016/j.procs.2016.06.038.

5. A. H. Moon, U. Iqbal, and G. M. Bhat. Mutual entity authentication protocol based on ECDSA for WSN // Procedia Computer Science, 2016, vol. 89, pp. 187–192.

6. Ullah, S., Li, XY. & Lan, Z. A novel trusted third party based signcryption scheme // Multimedia Tools and Applications, 2020, vol. 79, p. 22749 – 22769, DOI: 10.1007/s11042-020-09027-w.

7. M. N. Aman, U. Javaid, and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles // IEEE Internet of Things Journal, 2020 DOI: 10.1109/JIOT.2020.3010893.

8. ISO/IEC 9798:2010 Information technology – Security techniques – Entity authentication.

9. Рекомендация по размеру криптографического ключа. Интернетный ресурс – [Режим доступно] https://www.keylength.com/en/compare/

References

1. A. Humayed, J. Lin, F. Li and B. Luo. Cyber-Physical Systems Security — A Survey // IEEE Internet of Things Journal, Dec. 2017, vol. 4, no. 6, pp. 1802-1831, DOI: 10.1109 / JIOT.2017.2703172.

2. Komarov I. I., YUR'YEVA R. A., DRANNIK A.L., MASLENNIKOV O. S. Postanovka zadachi obespecheniya informatsionnoy bezopasnosti royevykh robototekhnicheskikh sistem //Nauka i biznes: puti razvitiya. – 2015. – №. 3. – S. 53.

3. Chan Z., Komarov I. I., Shved V.G. Autentifikatsiya agentov v gruppe BPLA na osnove sotsial'nykh mekhanizmov // Zashchita informatsii. Insayd - 2019. - № 6(90). - S. 66-71.

4. A. V. Cheremushkin, "Kriptograficheskiye protokoly: osnovnyye svoystva i uyazvimosti // prikladnaya diskretnaya matematika, 2009, prilozheniye № 2, st.115–150. DOI: 10.1016/j.procs.2016.06.038.

5. A. H. Moon, U. Iqbal, and G. M. Bhat. Mutual entity authentication protocol based on ECDSA for WSN // Procedia Computer Science, 2016, vol. 89, pp. 187-192.

6. Ullah, S., Li, XY. & Lan, Z. A novel trusted third party based signcryption scheme // Multimedia Tools and Applications, 2020, vol. 79, p. 22749 - 22769, doi: 10.1007 / s11042-020-09027-w.

7. M. N. Aman, U. Javaid, and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles // IEEE Internet of Things Journal, 2020 DOI: 10.1109 / JIOT.2020.3010893.

8. ISO / IEC 9798: 2010 Information technology – Security techniques – Entity authentication.

9. Rekomendatsiya po razmeru kriptograficheskogo klyucha. Internetnyy resurs – [Rezhim dostupno] https://www.keylength.com/en/compare/

ЧАН Зуи Хань, инженер, аспирант факультета безопасности информационных технологий, университет информационных технологий, механики и оптики (национальный исследовательский университет). 197101, г. Санкт-Петербург, Кронверкский проспект, д. 49-А. Email: viewtheworld93@gmail.com.

CHAN Zui Han, engineer, PhD student of the Faculty of Secure Information Technologies, University of Information Technologies, Mechanics and Optics (National Research University). 197101, St. Petersburg, Kronverkskiy prospect, 49-A. Email: viewtheworld93@gmail.com.

УДК 621.372.543.2 Вестник УрФО № 3(41) / 2021, с. 30–37

Фомин Д. Г., Дударев Н. В., Даровских С. Н.

DOI: 10.14529/secur210304

СВЕРХШИРОКОПОЛОСНЫЙ ПОЛОСНО-ПРОПУСКАЮЩИЙ ФИЛЬТР НА ОСНОВЕ МИКРОПОЛОСКОВОГО ПЕРЕХОДА ДЛЯ ОБЕСПЕЧЕНИЯ ВЫСОКОГО УРОВНЯ СКРЫТНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

В работе представлен структурно-параметрический синтез сверхширокополосного полосно-пропускающего фильтра на основе микрополоскового перехода, предназначенного для использования в качестве частотно-селективного устройства на входе/выходе приемо-передающих модулей инфокоммуникационных систем, направленных на повышение скрытности приема-передачи информации. Результаты исследования S-параметров получены двумя способами: 1) методом моделирования эквивалентной схемы фильтра в программе MATLAB, а также 2) методом численного электродинамического моделирования в программе ANSYS HFSS. Они имеют хорошее качественное и количественное совпадение друг с другом. Так согласно результатам проведенного исследования сверхширокополосный полосно-пропускающий фильтр на основе микрополоскового перехода характеризуется следующими электрическими параметрами: 1) полоса пропускания по уровню коэффициента передачи -3 дБ составляет 994 МГц (от 483 МГц до 1477 МГц), 2) коэффициент затухания на центральной частоте составляет 0,7 дБ, 3) коэффициент прямоугольности равен 1,26.

Ключевые слова: *микрополосковый переход, S-параметры, сверхширокополосный полосно-пропускающий фильтр, скрытность.*

ULTRA-WIBEBAND BAND PASS FILTER BASED ON MICROSTRIP TRANSITION FOR PROVIDING A HIGH LEVEL OF SECURITY OF INFOCOMMUNICATION SYSTEMS

The paper presents a structural-parametric synthesis of an ultra-wideband band-pass filter based on a microstrip transition. The presented filter intended for application as a frequency-selective device at the input/output of transceiver modules of infocommunication systems that aimed for increasing the secrecy of information transmission and reception. The results of the presented study obtained in two ways: 1) by the method of simulation the equivalent filter circuit in MATLAB software, and 2) by the method of numerical electrodynamics simulation in ANSYS HFSS software. The dependencies of the S-parameters in the frequency range obtained by the two presented methods have a good qualitative and quantitative agreement with each other. According to the results of the study the ultra-wideband band pass filter based on a microstrip transition is characterized by the following electrical parameters: 1) the passband at the level of the transmission coefficient of -3 dB is 994 MHz (from 483 MHz to 1477 MHz), 2) the insertion loss at the center frequency is 0,7 dB, 3) the squareness factor is 1,26.

Keywords: *microstrip transition, S-parameters, ultra-wideband band pass filter, secrecy.*

Введение. Одной из основных характеристик специализированных инфокоммуникационных систем является скрытность, направленная на затруднение обнаружения передаваемых сигналов системами радиочастотной разведки. В настоящее время известно несколько технических решений, позволяющих обеспечить заданный уровень скрытности радиосигналов. Одним из таких способов является применение сигналов со сверхширокополосным спектром (с шириной спектра более 500 МГц или 50 % от значения центральной частоты [1]), амплитуда которых во всем диапазоне частот сопоставима с амплитудой радиошумов. В результате радиоприемные устройства «обычных» узкополосных систем воспринимают СШП сигнал как случайные помехи и не детектируют его.

Одним из элементов «классического» построения приемо-передающих модулей сверхширокополосных систем является полосно-пропускающий фильтр, основной функцией которого является подавление внеполосного и побочного спектра, а также пропускание спектра в заданной полосе частот без потерь мощности. В настоящее время известны методы реализации сверхширокополосных полосно-пропускающих фильтров на основе микрополосковых схем [2 — 6], основным недостатком которых являются значительные габаритные характеристики. Целью данной работы является структурно-параметрический синтез и обоснование нового подхода к реализации сверхширокополосного полосно-пропускающего фильтра, конструкция которого основана на применении микрополоскового перехода.

1. Микрополосковый переход. Конструкция микрополоскового перехода представляет собой две диэлектрические подлож-

ки 1, 2, разделенные металлическим экраном 3. На каждой из подложек расположена микрополосковая линия 4. В металлическом экране вырезан щелевой резонатор П-образной формы 5, электрическая длина которого на центральной частоте составляет половину длины волны. Применение П-образной формы щелевого резонатора обеспечивает уменьшение потерь вследствие излучения щелевого резонатора. Микрополосковые линии перекрещиваются с щелевым резонатором и заканчиваются обрывом на расстоянии четверти длины волны на центральной частоте от места перекрещивания. Участок микрополосковой линии от места перекрещивания с щелевым резонатором до обрыва будем называть микрополосковым резонатором 6 (Рис. 1.).

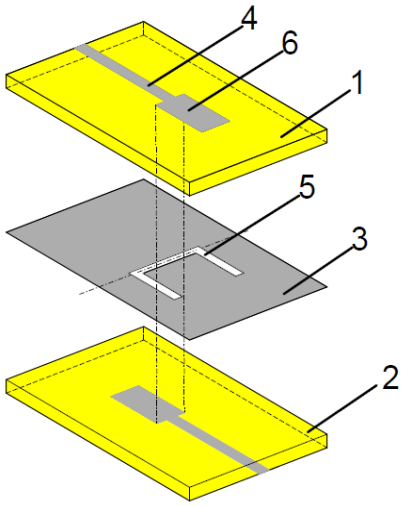


Рис. 1. Конструкция микрополоскового перехода

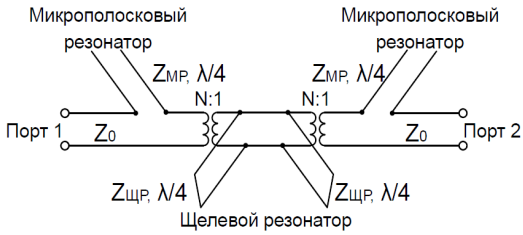


Рис. 2. Эквивалентная схема микрополоскового перехода

На представленной эквивалентной схеме введены следующие условные обозначения: 1) микрополосковые резонаторы представлены как отрезки линий передачи с обрывом на конце (волновое сопротивление ZMP, электрическая длина λ/4), 2) щелевой резонатор представлен как два параллельно включенных отрезка линии передачи с коротким замыканием на конце (волновое сопротивление $Z_{ЩР}$, электрическая длина λ/4), 3) трансформатор N:1 представляет собой связь микрополоскового и щелевого резонаторов за счет магнитного поля, при этом коэффициент трансформации определяет потери, 4) Z_0 – волновое сопротивление 50 Ом. Проведем схемотехническое моделирование представленной эквивалентной схемы в программе MATLAB при этом зададимся следующими параметрами: 1) центральная частота f = 1000 МГц, 2) волновое сопротивление микрополосковых линий 50 Ом, 3) волновое сопротивление микрополосковых резонаторов 50 Ом, 4) волновое сопротивление щелевого резонатора 50 Ом, 5) в качестве материала диэлектрических подложек взят Arlon AD1000 толщиной 1,5 мм и относительной диэлектрической проницаемостью εr = 10,2. В результате моделирования получили зависимости S-параметров микрополоскового перехода (Рис. 3) в диапазоне частот, а также зависимости реальной и мнимой части его входного сопротивления в диапазоне частот (Рис. 4).

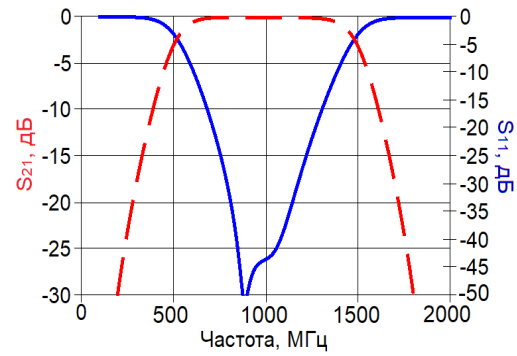


Рис. 3. Зависимости S-параметров микрополоскового перехода в диапазоне частот, полученные при схемотехническом моделировании

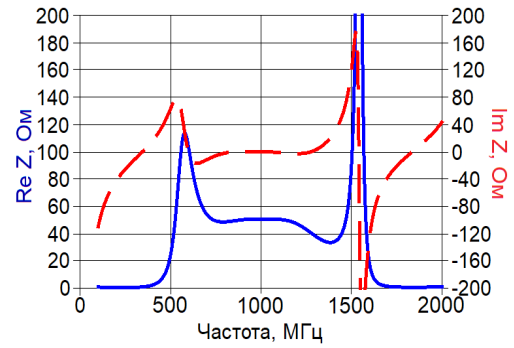


Рис. 4. Зависимости реальной и мнимой части входного сопротивления микрополоскового перехода в диапазоне частот, полученные при схемотехническом моделировании

Из полученных в результате схемотехнического моделирования зависимостей S-параметров следует, что полоса пропускания по уровню коэффициента передачи -3 дБ составляет 960 МГц (от 520 МГц до 1480 МГц). Коэффициент прямоугольности по уровню -20 дБ равен 1,5 (Δf_{-20} дБ от 280 МГц до 1720 МГц). Реальная часть входного сопротивления изменяется от 25 Ом до 116 Ом. Мнимая часть входного сопротивления изменяется от -18 Ом до 120 Ом. Таким образом, при расчете фильтра, состоящего из каскадного включения двух и более микрополосковых переходов необходимо выполнение дополнительных операций по согласованию.

Аналогичным образом проведем численное моделирование микрополоскового перехода в строгой формулировке электродинамической задачи. в программе ANSYS HFSS Результаты моделирования представлены в виде зависимости коэффициента передачи (S_{21}) в диапазоне частот (Рис. 5).

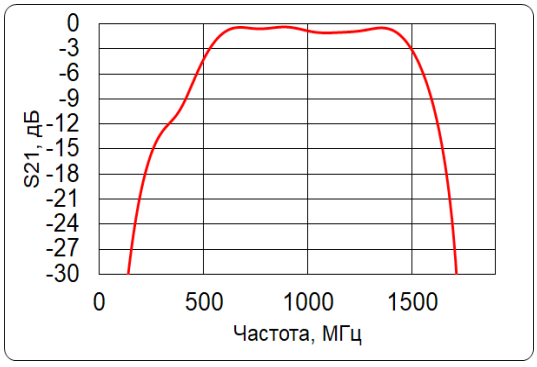


Рис. 5. Зависимость коэффициента передачи (S_{21}) микрополоскового перехода в диапазоне частот, полученная при численном моделировании

Так согласно результатам численного электродинамического моделирования следует, что полоса пропускания микрополоскового перехода по уровню коэффициента передачи -3 дБ составляет 970 МГц (от 527 МГц до 1497 МГц). Коэффициент прямоугольности по уровню -20 дБ равен 1,52 (Δf_{-20} дБ от 200 МГц до 1675 МГц). Потери на центральной частоте составляют 0,9 дБ и обусловлены излучением концов микрополосковых резонаторов, а также излучением щелевого резонатора.

2. Сверхширокополосный полосно-пропускающий фильтр

При исследовании сверхширокополосного полосно-пропускающего фильтра будем отдельно рассматривать два варианта конструкции, в каждом из которых используется по два микрополосковых перехода. Электрическая связь между микрополосковыми переходами (далее - звеньями) осуществляется: 1) микрополосковой линией, 2) полосковой линией.

2.1. Микрополосковая связь. Конструкция полосно-пропускающего фильтра, где электрическая связь между звеньями (микрополосковыми переходами) осуществляется за счет микрополосковой линии (Рис. 6) была рассчитана при использовании эквивалентной схемы в программе MATLAB (Рис. 7), а также путем численного электродинамического моделирования в программе ANSYS HFSS. В состав конструкции фильтра входят две диэлектрические подложки, разделенные металлическим основанием. При этом входная и выходная микрополосковые линии расположены на верхней диэлектрической подложке, связующая микрополосковая линия расположена на нижней диэлектрической подложке. В металлическом основании прорезаны два П-образных щелевых резонатора. Из результатов синтеза эквивалентной схемы следует, что для обеспечения согласования фильтра с волновым сопротивление 50 Ом, расстояние между щелевыми резонаторами должно составлять 0,22λ на центральной частоте, при этом волновое сопротивление микрополосковых резонаторов должно составлять 24 Ом. В связи с этим микрополосковые резонаторы имеют Т-образную форму, причем параллельно включенные отрезки с холостым ходом на конце имеют волновое сопротивление 48 Ом.

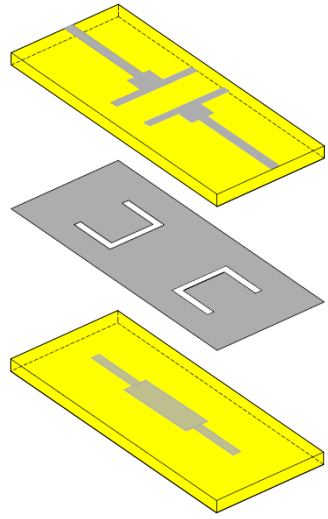


Рис. 6. Конструкция полосно-пропускающего фильтра со связью между звеньями за счет микрополосковой линии

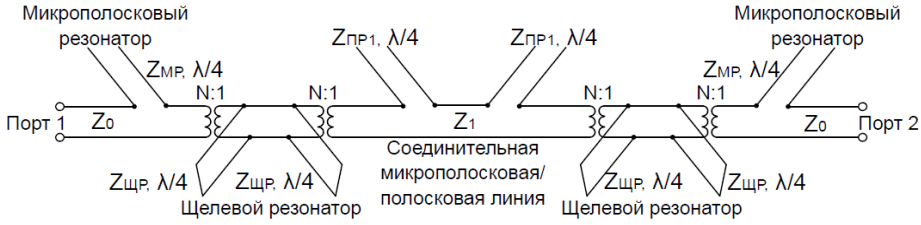


Рис. 7. Эквивалентная схема полосно-пропускающего фильтра со связью между звеньями за счет микрополосковой/полосковой линии передачи

Результаты численного электродинамического моделирования представленной конструкции полосно-пропускающего фильтра, полученные в программе ANSYS HFSS (Рис. 6), а также результаты схемотехнического моделирования его эквивалентной схемы, полученные в программе MATLAB (Рис. 7) представлены в виде зависимостей S-параметров в диапазоне частот (Рис. 8, 9).

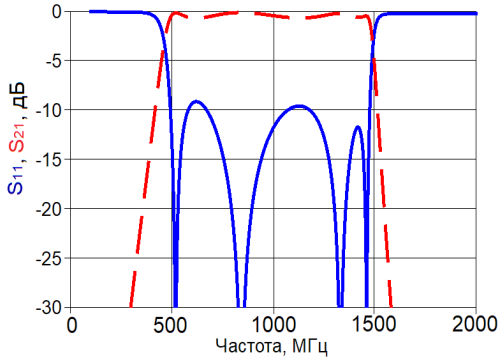


Рис. 8. Зависимости S-параметров сверхширокополосного полосно-пропускающего фильтра со связью между звеньями за счет микрополосковой линии в диапазоне частот, полученные при схемотехническом моделировании

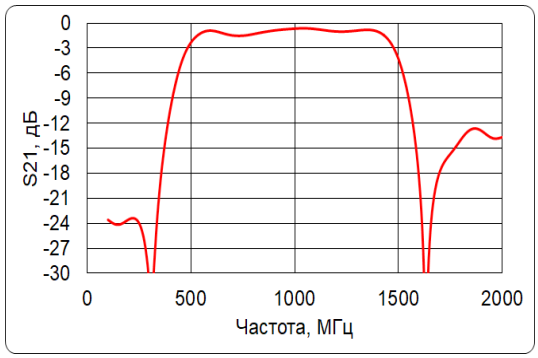


Рис. 9. Зависимость коэффициента передачи сверхширокополосного полосно-пропускающего фильтра со связью между звеньями за счет микрополосковой линии в диапазоне частот, полученная при численном моделировании

Из представленных зависимостей (Рис. 8, 9) следует, что результаты схемотехнического моделирования эквивалентной схемы фильтра имеют хорошее качественное и количественное совпадение с результатами, полученными при численном моделировании. Так согласно результатам численного моделирования следует, что полоса пропускания по уровню коэффициента передачи -3 дБ составляет 994 МГц (от 483 МГц до 1477 МГц). Коэффициент прямоугольности по уровню -20 дБ равен 1,26 (Δf_{-20} дБ от 350 МГц до 1602 МГц). Потери на центральной частоте составляют 0,7 дБ и обусловлены излучением концов микрополосковых резонаторов, а также излучением щелевого резонатора. Также из результатов моделирования эквивалентной схемы фильтра следует, что коэффициент отражения в рабочем диапазоне частот не превышает -9,4 дБ.

2.2. Полосковая связь. Конструкция полосно-пропускающего фильтра, где электрическая связь между звеньями осуществляется за счет полосковой линии передачи, была рассчитана при использовании эквивалентной схемы в программе MATLAB, а также путем численного электродинамического моделирования в программе ANSYS HFSS. Основное преимущество данной конструкции заключается в возможности ее вертикального построения. При этом с увеличением числа звеньев фильтра возрастает сложность его сверхширокополосного согласования. В состав конструкции фильтра (Рис. 10) входят четыре диэлектрические подложки, разделенные двумя металлическими основаниями. Входная микрополоковая линия расположена на верхней диэлектрической подложке, выходная микрополосковая линия расположена на нижней диэлектрической подложке. Связующая полосковая линия расположена между второй и третьей диэлектрическими подложками. В металлических основаниях

прорезаны П-образные щелевые резонаторы. Волновое сопротивление микрополосковых резонаторов составляет 23 Ом.

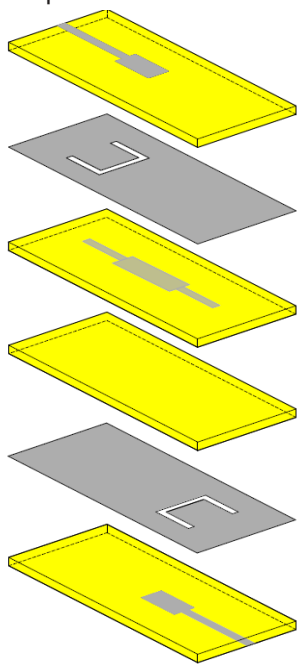


Рис. 10. Конструкция полосно-пропускающего фильтра со связью между звеньями за счет полосковой линии

Эквивалентная схема полосно-пропускающего фильтра со связью между звеньями за счет полосковой линии аналогична ранее представленной (Рис. 7).

Из представленной зависимости (Рис. 11) следует, что полоса пропускания по уровню коэффициента передачи -3 дБ составляет 864 МГц (от 574 МГц до 1438 МГц). Коэффициент

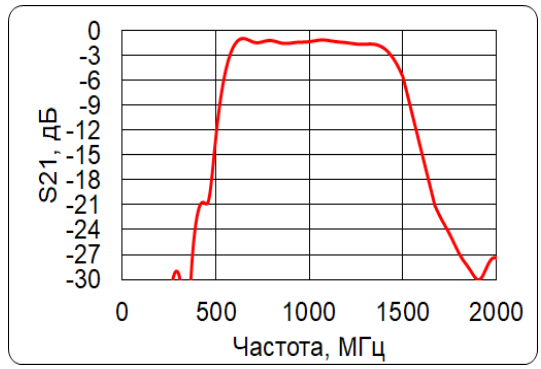


Рис. 11. Зависимость коэффициента передачи сверхширокополосного полосно-пропускающего фильтра со связью между звеньями за счет полосковой линии, полученная при численном моделировании

прямоугольности по уровню -20 дБ равен 1,38 (Δf_{-20} дБ от 466 МГц до 1659 МГц). Потери на центральной частоте составляют 1,3 дБ.

3. Обсуждение результатов. Полученные в результате исследования S-параметры подтверждают возможность реализации сверхширокополосного полосно-пропускающего фильтра на основе микрополоскового перехода. Для наглядного сравнения полученных результатов объединим их в Таблице 1.

Из представленных (Таблица 1) результатов следует, что наилучшие параметры сверхширокополосного полосно-пропускающего фильтра наблюдаются при его исполнении с электрической связью между звеньями за счет микрополосковой линии. При этом наблюдается лучшие показатели по всем оцениваемым электрическим параметрам: коэффициент прямоугольности, полоса пропускания, затухание на центральной частоте. Ухудшенные характеристики фильтра с электрической связью между звеньями за счет полосковой линии обусловлены увеличением диэлектрических потерь по причине возросшего количества диэлектрических подложек.

Таблица 1

S-параметры представленных в работе конструкций фильтров

Конструкция	Наименование параметра		
	Полоса пропускания, МГц	Потери на центральной частоте, дБ	Коэффициент прямоугольности
Микрополосковый переход	970	0,9	1,52
Полосно-пропускающий фильтр со связью между звеньями за счет микрополосковой линии	994	0,7	1,26
Полосно-пропускающий фильтр со связью между звеньями за счет полосковой линии	864	1,3	1,38

Заключение. В работе представлены результаты структурно-параметрического синтеза сверхширокополосного полосно-пропускающего фильтра на основе микрополоскового перехода. Результаты исследования S-параметров получены двумя способами: 1) методом моделирования эквивалентной схемы фильтра в программе MATLAB, а также 2) методом численного электродинамического моделирования в программе ANSYS HFSS. Рассчитаны S-параметры и входное сопротивление микрополоскового перехода в диапазоне частот, по результатам которых следует, что при каскадном включении двух и более микрополосковых переходов требуется проведение дополнительных операций по их согласованию. Рассмотрены два варианта конструкции сверхширокополосного полосно-пропускающего фильтра в каждом из которых используется по два микрополосковых перехода. При этом электрическая связь между микрополосковыми переходами осуществляется за счет: 1) микрополосковой линии, 2) полосковой линии. Так в результате исследования установлено, что предпочтительные электрические характеристики имеет фильтр со связью между звеньями за счет микрополосковой линии. При этом он характеризуется следующими электрическими параметрами: 1) полоса пропускания по уровню коэффициента передачи -3 дБ составляет 994 МГц (от 483 МГц до 1477 МГц), 2) коэффициент затухания на центральной частоте составляет не более 0,7 дБ, 3) коэффициент прямоугольности равен 1,26. Представленный в работе полосно-пропускающий фильтр может быть использован в качестве частотно-селективного устройства на входе/выходе приемо-передающих модулей инфокоммуникационных систем, предназначенных для повышения скрытности приема-передачи информации.

Литература

1. Разиньков С.Н. Основные направления развития и базовые технологии создания систем радиосвязи со сверхширокополосными сигналами. Воздушно-космические силы. Теория и практика, 2019, № 11, с. 38 – 44.

2. Shome P. P., Khan T. A Compact Design of Circular Ring-Shaped MMR Based Bandpass Filter for UWB Applications. 2019 IEEE Asia-Pacific Microwave Conference (APMC), 2019, pp. 962 – 964.

3. S. Parvez, Md. Nurunnabi M. Quarter Wavelength Open Stub Band Pass Filter Based on Dumbbell Annular Ring Resonator For UWB Applications. 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017, pp. 827 – 830.

4. Sandip K., Ravi Dutt Gupta, Manoj Singh Parihar. Multiple Band Notched Filter Using C-Shaped and E-Shaped Resonator for UWB Applications. IEEE Microwave and Wireless Components Letters, Vol. 26, No. 5, May 2016, pp. 340 – 342.

5. Wang L. T., Yang X., Ming H. Review on UWB Bandpass Filters [online]. IntechOpen, 2019. URL: https://www.intechopen.com/chapters/68017 (Дата обращения: 02.09.2021 г.)

6. Gao X., Feng W., Che W. Compact Ultra-Wideband Bandpass Filter With Improved Upper Stopband Using Open/Shorted Stubs. IEEE Microwave and Wireless Components Letters, 2017, vol. 27, pp. 123 – 125.

7. Фомин Д.Г., Дударев Н.В., Даровских С.Н., Баранов В.К. Исследование объемного полосково-щелевого перехода с П-образным щелевым резонатором. Ural Radio Engineering Journal, 2020, 4(3), с. 277 – 292.

8. Fomin D.G., Dudarev N.V., Darovskikh S.N. Scattering matrix simulation of the volumetric strip-slot transition and estimation of its frequency properties. Journal of Physics: Conference Series, 2020, Vol. 1679, No. 2, pp. 1 – 6.

References

1. Razin'kov S.N. Osnovnyye napravleniya razvitiya i bazovyye tekhnologii sozdaniya sistem radiosvyazi so sverkhshirokopolosnymi signalami. Vozdushno-kosmicheskiye sily. Teoriya i praktika, 2019, № 11, s. 38 – 44.

2. Shome P. P., Khan T. A Compact Design of Circular Ring-Shaped MMR Based Bandpass Filter for UWB Applications. 2019 IEEE Asia-Pacific Microwave Conference (APMC), 2019, pp. 962 – 964.

3. Shakhawat P., Md. Nurunnabi M. Quarter Wavelength Open Stub Band Pass Filter Based on Dumbbell Annular Ring Resonator For UWB Applications. 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017, pp. 827 – 830.

4. Sandip K., Ravi Dutt Gupta, Manoj Singh Parihar. Multiple Band Notched Filter Using C-Shaped and E-Shaped Resonator for UWB Applications. IEEE Microwave and Wireless Components Letters, Vol. 26, No. 5, May 2016, pp. 340 – 342.

5. Wang L. T., Yang X., Ming H. Review on UWB Bandpass Filters [online]. IntechOpen, 2019. Available at: https://www.intechopen.com/chapters/ 68017 (accessed: 02.09.2021).

6. Gao X., Feng W., Che W. Compact Ultra-Wideband Bandpass Filter With Improved Upper Stopband Using Open/Shorted Stubs. IEEE Microwave and Wireless Components Letters, 2017, Vol. 27, pp. 123 – 125.

7. Fomin D.G., Dudarev N.V., Darovskikh S.N., Baranov V.K. Issledovaniye ob"yemnogo poloskovo-shchelevogo perekhoda s P-obraznym shchelevym rezonatorom. Ural Radio Engineering Journal, 2020, 4(3), s. 277 – 292.

8. Fomin D.G., Dudarev N.V., Darovskikh S.N. Scattering matrix simulation of the volumetric strip-slot transition and estimation of its frequency properties. Journal of Physics: Conference Series, 2020, Vol. 1679, No. 2, pp. 1 – 6.

ФОМИН Дмитрий Геннадьевич, аспирант кафедры «Инфокоммуникационные технологии», младший научный сотрудник, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: Fomin95@ya.ru

ДУДАРЕВ Николай Валерьевич, кандидат технических наук, старший научный сотрудник кафедры «Инфокоммуникационные технологии», ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: dudarevnv@susu.ru

ДАРОВСКИХ Станислав Никифорович, доктор технических наук, доцент, заведующий кафедрой «Инфокоммуникационные технологии», ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: darovskikhsn@susu.ru

FOMIN Dmitry Gennadievich, Post-graduate student of the Department «Infocommunication Technologies», Junior Researcher, South Ural State University (National Research University). 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: Fomin95@ya.ru

DUDAREV Nikolay Valerievich, Candidate of Technical Sciences, Senior Researcher, Department «Infocommunication Technologies», South Ural State University (National Research University). 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: dudarevnv@susu.ru

DAROVSKIKH Stanislav Nikiforovich. Doctor of Technical Sciences, Associate Professor, Head of the Department «Infocommunication Technologies», South Ural State University (National Research University). 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: darovskikhsn@susu.ru

УДК 004.896 + 004.056.5 Вестник УрФО № 3(41) / 2021, с. 38–48

Алабугин С.К., Соколов А.Н.

DOI: 10.14529/secur210305

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ С ИСПОЛЬЗОВАНИЕМ АНСАМБЛЯ МОДЕЛЕЙ РЕКУРРЕНТНОЙ И ДВУНАПРАВЛЕННОЙ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНОЙ НЕЙРОННЫХ СЕТЕЙ[1]

В работе рассмотрены генеративно-состязательные и рекуррентные архитектуры нейронных сетей, а также практика их применения для обнаружения вторжений в автоматизированных системах управления технологическими процессами. Для проведения экспериментов использован набор данных Secure Water Treatment, описывающий работу водоочистного сооружения. В ходе экспериментальных исследований на примерах, соответствующих нормальному состоянию технологического процесса, были обучены рекуррентная и двунаправленная генеративно-состязательная нейронные сети. Для улучшения метрик качества проведено ансамблирование сетей. Применение ансамбля нейронных сетей позволило улучшить точность и полноту обнаружения вторжений.

Ключевые слова: *автоматизированная система управления технологическим*

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта № 16/2020.

процессом, ансамблирование, выявление аномалий, глубокое обучение, двунаправленная генеративно-состязательная нейронная сеть, информационная безопасность, обнаружение вторжений, реккурентная нейронная сеть.

Alabugin S.K., Sokolov A.N.

INTRUSION DETECTION IN INDUSTRIAL CONTROL SYSTEMS USING THE ENSEMBLE OF MODELS OF RECURRENT AND BIDIRECTIONAL GENERATIVE ADVERSARIAL NEURAL NETWORKS

The paper considers generative adversarial and recurrent neural network architectures, as well as their application for intrusion detection in industrial control systems. For the experiments, the Secure Water Treatment dataset was used. This dataset describes the operation of the wastewater treatment plant. In the course of experimental studies, on examples corresponding to the normal state of the industrial process, recurrent and bidirectional generative-adversarial neuronal networks were trained. To improve the quality metrics, both networks were ensembled. The use of an ensemble of neural networks has improved the precision and recall.

Keywords: *industrial control systems, ensemble, anomaly detection, deep learning, bidirectional generative adversarial neural network, information security, intrusion detection, recurrent neural network.*

Обнаружение вторжений является одним из наиболее приоритетных направлений исследований в области информационной безопасности (ИБ). Важность решения этой задачи обусловлена постоянным ростом количества и разнообразия угроз ИБ, реализация которых может приводить к финансовым и репутационным потерям организации, подвергшейся атаке. В случае, когда речь идёт об информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), к возможным последствиям успешной атаки добавляются человеческие жертвы и ущерб экологии, вплоть до техногенной катастрофы. Это обусловлено тем, что АСУ ТП часто размещаются на индустриальных объектах, от работы которых зависит качество жизни значительного числа граждан и/или экономическое благополучие отдельного региона или страны. Примерами успешных атак на АСУ ТП являются сетевой червь Stuxnet [1], использованный для совершения диверсии на предприятиях ядерной промышленности Ирана в 2010, вредоносное программное обеспечение BlackEnergy [2], использованное для атаки на энергетический сектор Украины в 2015, атака на предприятия энергетической промышленности Израиля в 2016 [3], атаки на объекты водоснабжения и водоочистки Израиля в 2020 [4] и др.

В течение длительного времени такие системы были изолированы от внешних сетей, и, в особенности от сети Интернет. В настоящее время наблюдается тенденция к объединению индустриальных и корпоративных сетей [5]. Это позволяет более эффективно экс-

плуатировать АСУ ТП легитимным пользователям, при этом делает подобные системы более уязвимыми для действий злоумышленников. Технологии, используемые в АСУ ТП, часто разработаны без учета требований информационной безопасности, – как правило, к ним относятся проприетарные средства [6]. Для отрасли в целом характерен низкий уровень культуры информационной безопасности [7], в частности, это касается оперативной разработки обновлений безопасности производителями и своевременной установки этих обновлений на объекте. Вышеперечисленные факторы характеризуют причины, по которым АСУ ТП в целом уязвимы для злоумышленника и обосновывают необходимость повысить уровень защищенности АСУ ТП. Для своевременного обнаружения вторжений, в частности, для обнаружения таргетированных атак, предлагается использовать метод обнаружения вторжений, основанный на выявлении аномалий.

В качестве данных для анализа использованы данные состояния технологического процесса (значения сигналов сенсоров и актуаторов в конкретный момент времени). Исходя из предположения, что большая часть аномалий технологического процесса является следствием действий злоумышленника, выявленная аномалия технологического процесса позволяет установить факт вторжения. Нужно отметить, однако, что при такой постановке задачи, в случае, если аномалия является следствием программной ошибки, сбоя технического оборудования или действий оператора – она будет свидетельствовать о ложном вторжении.

При использовании методов машинного обучения для анализа состояния технологического процесса можно выделить несколько подходов. В частности, для выявления аномалий технологического процесса применимы методы классификации и кластеризации. В [8] представлены результаты работы некоторых классических алгоритмов машинного обучения (K-means, Naive Bayesian, GMM, PCA-SVD) на наборе данных Gas Pipeline. В [9, 10] проведен анализ практической применимости классических методов машинного обучения (линейная регрессия, решающие деревья, SVM) и нейронной сети классификатора для выявления аномалий технологического процесса. В [11] безопасность сетевой инфраструктуры АСУ ТП обеспечивается с помощью полносвязной нейронной сети и автокодировщика для выявления атак в сетевом трафике. В [12] нейронная сеть использована для выявления атак типа False Data Injection на основе анализа показаний сенсоров АСУ ТП. В [13] рассмотрено применение метода оптимизации Particle Swarm при обучении нейронной сети, обнаруживающей атаки. Предложенный метод позволяет обучать сеть за меньшее количество итераций и обеспечивает более высокую точность. В [14] авторы предложили систему, состоящую из нейронной сети и Lyapunov-based model predictive controller (LMPC). Нейронная сеть анализирует показания сенсоров химического процесса и производит обнаружение факта атаки. В случае атаки LMPC используется для смягчения деструктивного влияния атаки и рестабилизации системы. В [15] для выявления аномалий авторы использованы полносвязные нейронные сети, построенные при помощи генетических алгоритмов (Evolutionary based Neural Networks), в частности, они предложили применять для оптимизации весов сети алгоритм Grey Wolf Optimizer с целью увеличения скорости обучения сети. В [16] авторы применили алгоритмы Random Forest и Support Vector Machine для выявления аномалий, а также исследовали способы обработки пропусков в данных и нормализации данных для улучшения качества работы алгоритмов. В [17] авторы предложили использовать для выявления аномалий новый подход в рамках одноклассовой классификации, основанный на импульсных нейронных сетях с целью получения практически применимого алгоритма, который не нуждается в данных об аномальном состоянии АСУ ТП.

Использование нейронных сетей-классификаторов имеет несколько недостатков: на стадии обучения требуется достаточное количество примеров, репрезентирующих вторжения (как правило, получить и корректно разметить такие примеры – отдельная трудоёмкая задача). Кроме того, сеть-классификатор, при обработке принципиально новых данных, соответствующих атаке, не представленной в обучающей выборке, вполне может отработать неправильно. Методы, использующие обучение без учителя, в частности, кластеризация, зачастую не позволяют получить результат, который был бы применим на практике. Кроме того, результаты работы методов классификации и кластеризации часто не интерпретируемы: получив сообщение о выявленной аномалии, пользова-

тель не сможет определить причину ее возникновения. С целью преодоления описанных недостатков рассмотрены модели на основе двух архитектур искусственных нейронных сетей:

1. Рекуррентные нейронные сети, позволяющие анализировать последовательности данных и предсказывать их дальнейшую динамику.

2. Генеративно-состязательные сети, конструирующие из сырых данных внутреннее представление и выделяющие наиболее характерные признаки.

Для проведения экспериментальных исследований использован набор данных Secure Water Treatment (SWaT) [18], разработанный исследователями из Singapore University of Technology and Design с целью использования для создания и оценки механизмов защиты киберфизических систем. При его разработке был построен испытательный стенд, который представляет собой уменьшенную полнофункциональную копию реального водоочистного сооружения.

Стенд Secure Water Treatment включает 6 стадий технологического процесса, который реализован в водоочистном сооружении: забор воды (P1), оценка качества неочищенной воды (P2), механическая фильтрация воды (P3), дехлоризация (P4), обратный осмос (P5), перегонка очищенной воды в хранилище или на ещё один цикл очистки (P6).

Данные содержат дамп сетевого трафика SWaT и данные, описывающие показания 25 сенсоров и 26 актуаторов стенда. Набор данных содержит 964722 записи, которые разделены на две части:

• данные, собранные в течение 7 дней нормальной работы стенда, без каких-либо сбоев (первая часть);

• данные, собранные за 4 дня, во время которых проводились атаки (вторая часть).

Рекуррентные нейронные сети (recurrent neural networks, RNN) – это разновидность архитектур нейронных сетей, которые обладают обратной (рекуррентной) связью. Для анализа последовательностей использованы рекуррентные нейронные сети, так как благодаря наличию обратной связи, они могут запоминать внутреннее состояние, то есть помнить данные, которые были представлены в последовательности. С помощью рекуррентной нейронной сети прогнозируется состояние технологического процесса. Из существующих архитектур рекуррентных сетей была выбрана ячейка Long Short-Term Memory (LSTM) [19]. В модели также использован одномерный сверточный слой, позволяющий извлекать из сырого состояния технологического процесса признаки, которые подаются на вход LSTM слоям. Структура сети, используемой в работе, представлена на рис. 1.

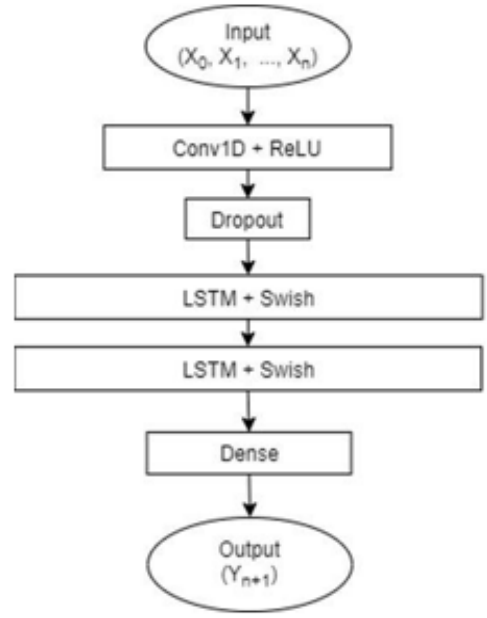


Рис. 1. Структура рекуррентной нейронной сети, используемой для выявления аномалий технологического процесса

Сеть состоит из одномерной свертки с функцией активации ReLU (Conv1D + ReLU), Dropout-слоя, который используется, чтобы избежать переобучения, двух слоев LSTM и полносвязного слоя (Dense) на выходе. В качестве функции активации LSTM-слоев была использована функция Swish [20].

Сеть принимает на вход последовательность из состояний технологического процесса SWaT, описываемого 51 признаком, в моменты времени X_0, X_1, …, X_n, и выдает в качестве результата работы состояние технологического процесса в следующий момент времени Y_{n+1}.

С помощью библиотеки машинного обучения Tensorflow реализована рекуррентная нейронная сеть. Для обучения и тестирования реализованной модели использованы данные из набора SWaT. Обучающая выборка включала данные, соответствующие нормальной работе системы. Контрольная выборка состояла из данных, полученных в период проведения атак. Данные были нормализованы и разбиты на последовательности, описывающие состояние системы в течение

30 секунд. Таким образом, на вход модели подавались многомерные тензоры, имеющие форму [M,30,51], где M – размер батча. Для обучения модели в качестве функции потерь использовалась средняя квадратичная ошибка (mean square error, MSE), а в качестве алгоритма градиентного спуска – алгоритм Adam [21]. Модель обучалась в течение 200 эпох и достигла значения MSE равного 2.7301. Показатель средней абсолютной ошибки (mean absolute error, MAE) при этом составил 0.7267.

После этого к контрольной выборке применена обученная модель. Разница вычислялась между предсказанным и фактическим состоянием технологического процесса. В качестве метрики аномальности использована максимальная разница среди всех признаков.

Для метрики аномальности был эмпирически подобран подходящий порог, обеспечивающий наилучшие результаты работы. ROC-кривая, с помощью которой был подобран порог для метрики аномальности, представлена на рис. 2.

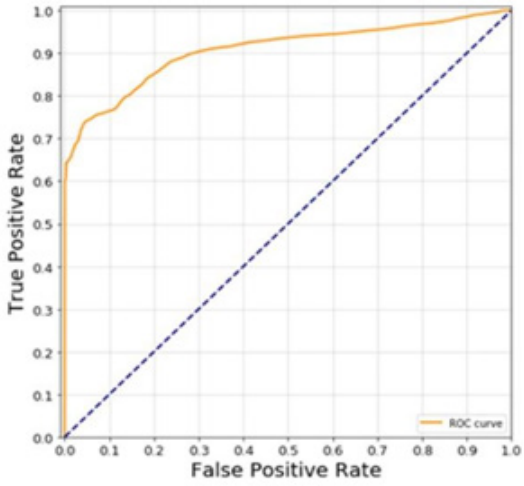


Рис.2. ROC-кривая метода выявления аномалий, основанного на применении рекуррентной сети

Генеративно-состязательные сети (Generative Adversarial Net, GAN) – это класс нейронных сетей, используемый для генерации новых синтетических данных на основе реальных. Концептуально генеративно-состязательные сети основаны на идее состязательного обучения и впервые были описаны в [22].

Архитектура GAN включает две модели: генератор G, порождающий на основе вектора шума новые, похожие на настоящие, объекты в пространстве данных, и дискриминатор D, целью которого является отличить порождаемые генератором объекты от реальных данных, – поэтому архитектура и называется генеративно-состязательной. Для применения генеративно-состязательных сетей в задаче обнаружения аномалий использована двунаправленная генеративно-состязательная сеть (Bidirectional Generative Adversarial Net, BiGAN) [17], схема которой представлена на рис. 3.

По сравнению с базовой архитектурой генеративно-состязательной сети, в архитектуре BiGAN дополнительно задействована сеть-кодировщик (encoder) E, что добавляет структуру автокодировщика (автокодировщиком является пара генератор – кодировщик) в очную генеративно-состязательную сеть.

Автокодировщик (autoencoder) [23] — это архитектура искусственной нейронной сети, позволяющая применять обучение без учителя при использовании метода обратного распространения ошибки. Наиболее простая архитектура автокодировщика — сеть прямого распространения, без наличия рекуррентных связей и содержащая входной, промежуточный и выходной слои. В отличие от перцептрона, выходной слой автокодировщика должен содержать столько же нейронов, сколько и входной слой.

Основной принцип работы и обучения сети автокодировщика — получить на выходе вектор, как можно более близкий к входному. Для того, чтобы решение не было тривиальным (идентичное преобразование вектора), на промежуточный слой сети накладываются ограничения некоторые ограничения, в частности: промежуточный слой должен быть или меньшей размерности, чем входной и выходной слои, или искусственно ограничивается количество одновременно активных нейронов промежуточного слоя (применяется разрежённая активация). Эти ограничения заставляют кодировщик искать обобщения и корреляцию в поступающих во входных данных, а также выполнять их сжатие. Таким образом, сеть обучается выделять из входных данных общие признаки, которые кодируются в значениях весов искусственной нейронной сети. Так, после обучения сети на наборе различных входных изображений, кодировщик может научиться распознавать отдельные линии и полосы под различными углами.

В архитектуре BiGAN, кодировщик E осуществляет преобразование из пространства реальных данных в пространство скрытых

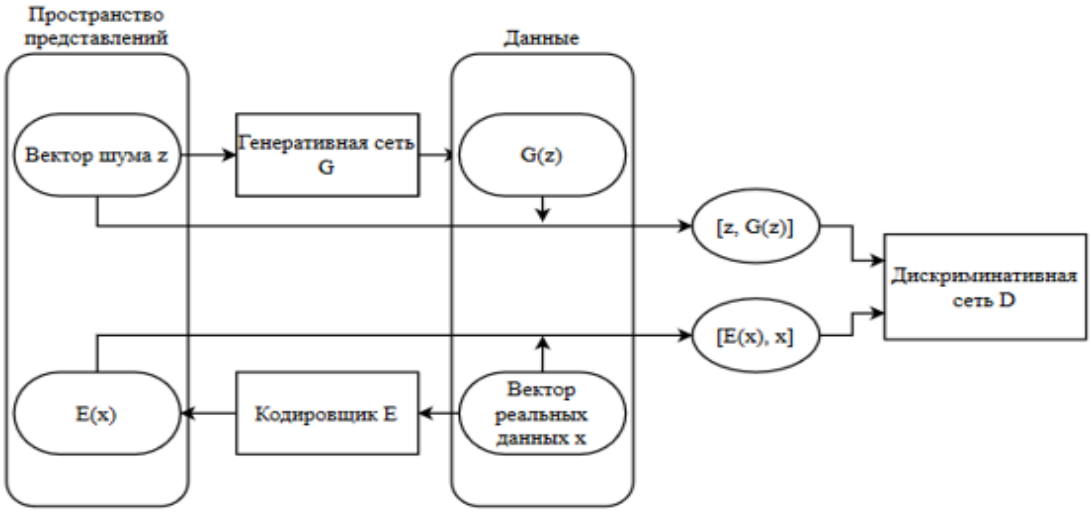


Рис.3. Схема двунаправленной генеративно-состязательной нейронной сети (BiGAN)

переменных, из которого берётся вектор шума для генератора. Формально это действие можно представить в виде функции:

$$E = E(x ; \theta_e) : X \longrightarrow Z, \quad (1)$$

где θ_e – параметры сети-кодировщика.

Таким образом, сеть-кодировщик в процессе обучения учиться делать преобразование, обратное генератору. Кроме того, в архитектуре BiGAN, сеть-дискриминатор обучается различать не только порожденные генератором объекты и объекты из реальных данных, но и векторы из пространства скрытых переменных z (используемые для порождения объектов) и результат отображения кодировщика E(x). Формальное доказательство того, что в описанной схеме кодировщик после обучения сети BiGAN, реализует функцию, обратную функции генератора, приведено в [23]. Процесс обучения сети BiGAN аналогичен процессу обучения обычной генеративно-состязательной сети: веса каждой сети обновляются попеременно.

Добавления сети-кодировщика в архитектуру генеративно-состязательной сети, который каждому объекту из пространства данных x ставит в соответствие вектор z из пространства скрытых переменных, позволяет непосредственно извлекать представления (representations) этих объектов. С точки зрения семантики, вектор z репрезентирует признаки объекта x, выявленные в процессе обучения BiGAN. Именно это свойство позволяет использовать BiGAN для выявления аномалий [24].

Один из подходов к использованию BiGAN для обнаружения аномалий состоит в построении метрики A аномальности объекта, основанной на выпуклой комбинации (convex combiantion) функции потерь реконструкции и функции потерь дискриминатора

$$A(x) = aL_G(x) + (1\text{-}a)L_D(x), \quad (2)$$

где $L_G(x)$ – функция потерь реконструкции, определяемая как модуль разности исходного вектора, репрезентирующего объект, и вектора, полученного последовательным преобразованием объекта кодировщиком и генератором:

$$L_G(x) = ||x - G(E(x))||. \quad (3)$$

$L_D(x)$ – функция потерь дискриминатора:

$$LD(x) = \sigma(D(x,(E(x)),1), \quad (4)$$

где σ – кросс-энтропия (логарифмическая функция потерь) дискриминатора, при условии, что объект x является настоящим, а не порожден генератором.

Таким образом, сеть BiGAN, обученная на данных, соответствующих нормальному состоянию, применяется к новому объекту, после чего вычисляется значение метрики аномальности A для объекта. Чем выше значение этой метрики, тем более вероятно, что объект является аномальным.

Для обучения и тестирования сети BiGAN были также использованы данные из набора SWaT. Обучающая выборка включает в себя данные соответствующие нормальной работе системы. Контрольная выборка состоит из данных, полученных в период проведения атак. Данные были приведены к одному масштабу, после чего BiGAN обучалась исключительно на данных соответствующих нормальной работе системы. После этого к контрольной выборке применена обученная модель, а для каждого объекта контрольной выборки построена метрика аномальности. Качество

работы обученной модели определяется не только ее возможностями аппроксимировать распределение данных, соответствующих нормальной работе системы, но и конкретным значением порога метрики аномальности. На рис. 4 представлена зависимость метрик точности и полноты при изменении порогового значения. Из рисунка видно, что при увеличении порогового значения увеличивается точность и уменьшается полнота. Это свойство позволяет настроить желаемое поведение модели в каждом конкретном случае.

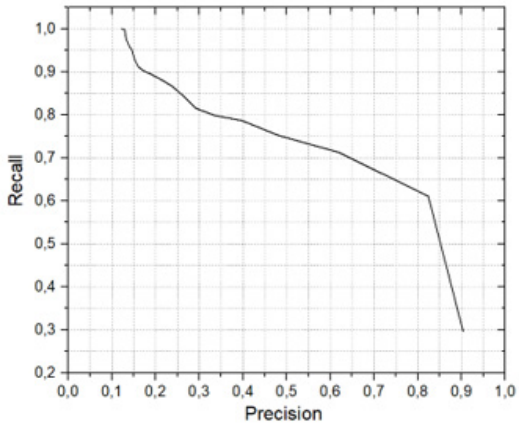


Рис. 4. Зависимость метрик точности (Precision) и полноты (Recall) при из-менении порогового значения для метода выявления аномалий технологического процесса с помощью сети BiGAN

С целью повышения результативности выявления аномалий разработана модель машинного обучения, включающая генеративно-состязательную и рекуррентную архитектуры с использованием ансамблирования моделей [25]. При таком подходе состояние технологического процесса анализируется как с помощью рекуррентной сети (прогнозирования состояния), так и с помощью двунаправленной генеративно-состязательной сети BiGAN (оценка аномальности состояния в моменте). Такой подход, как правило, используется при решении сложных задач, когда ни один из применяемых алгоритмов не показывает желаемого уровня точности. Смысл применения голосования состоит в том, чтобы взаимно компенсировать ошибки, допущенные каждой моделью. Эффективность такого подхода, как правило, определяется природой решаемой задачи, используемыми признаками и алгоритмами.

Основным решателем предложенной модели является рекуррентная сеть. Для обеспечения высокого уровня точности (Precision) для генеративно-состязательной сети архитектуры BiGAN выбран достаточно высокий порог по метрике аномальности. В предложенной ансамблевой модели оценкам генеративно-состязательной сети корректируют решения, полученные путем прогнозирования рекуррентной сети: состояние технологического процесса признается аномальным только в том случае, когда оценки, полученные с помощи обеих моделей, совпадают. Схема применения ансамбля нейронных сетей для обнаружения вторжений в АСУ ТП на основе обнаружения аномалий технологического процесса приведена на рис. 5.

Рис. 5. Схема ансамблирования моделей нейронных сетей для обнаружения вторже-ний в АСУ ТП

В таблице представлены результаты применения ансамбля моделей для набора данных SWaT в сравнении с результатами, полученными при использовании только рекуррентной сети и другими методами.

Таким образом, предложенная модель достаточно результативно справляется с выявлением аномалий технологического процесса, порожденных вторжениями злоумышленника, и может быть использована при разработке систем обнаружения вторжений. Достоинствами метода на основе ансамбля нейронных сетей являются его быстродействие и

Таблица

Результаты работы методов для набора данных SWaT

Метод	Precision	Recall	F1-Score
1D CNN [26]	0.968	0.791	0.871
MLP [27]	0.967	0.696	0.812
CNN [27]	0.952	0.702	0.808
RNN [27]	0.936	0.692	0.796
DNN [28]	0.982	0.678	0.802
OCSVM [28]	0.925	0.699	0.796
Метод на основе прогнозирования состояния технологического процесса с использованием рекуррентной сети	0.934	0.820	0.865
Метод на основе ансамбля нейронных сетей	0.981	0.890	0.933

отсутствие необходимости использовать данные, описывающие аномальное состояние технологического процесса. В случае применения ансамблевой модели на наборе данных SWaT на компьютере с процессором Intel Core i7-9750H и видеокартой NVIDIA GeForce RTX 2070 среднее время одной итерации составило 0.65 секунды.

Литература

1. Kushner D. The real story of stuxnet //ieee Spectrum. – 2013. – Т. 50. – №. 3. – С. 48-53.

2. Khan R. et al. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid //4th International Symposium for ICS & SCADA Cyber Security Research 2016 4. – 2016. – С. 53-63.

3. Li, Zhong-wei, Weiming Tong, and Xianji Jin. "Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel." Automation of Electric Power Systems 40.8 (2016): 147-151.

4. Israel Government Tells Water Treatment Companies to Change Passwords [Электронный ресурс]. — URL: https://www.zdnet.com/article/israel-says-hackers-are-targeting-its-water-supply-and-treatment-utilities/ (visited on 6/11/2020).

5. Xu H. et al. A survey on industrial Internet of Things: A cyber-physical systems perspective //IEEE Access. – 2018. – Т. 6. – С. 78238-78259.

6. Баринов А. Е., Скурлаев С. В., Соколов А. Н. Методика оценки рисков, вызванных уязвимостями в программном обеспечении автоматизированных систем управления технологическими процессами //Вестник УрФО. Безопасность в информационной сфере. – 2017. – №. 3 (25). – С. 34-42.

7. Luiijf E. Cyber (in-) security of industrial control systems: A societal challenge //International Conference on Computer Safety, Reliability, and Security. – Springer, Cham, 2014. – С. 7-15.

8. Shirazi S. N. et al. Evaluation of anomaly detection techniques for scada communication resilience //2016 Resilience Week (RWS). – IEEE, 2016. – С. 140-145.

9. Sokolov A. N., Pyatnitsky I. A., Alabugin S. K. Research of classical machine learning methods and deep learning models effectiveness in detecting anomalies of industrial control system //2018 Global Smart Industry Conference (GloSIC). – IEEE, 2018. – С. 1-6.

10. Sokolov A. N., Pyatnitsky I. A., Alabugin S. K. Applying methods of machine learning in the task of intrusion detection based on the analysis of industrial process state and ICS networking //FME Transactions. – 2019. – Т. 47. – №. 4. – С. 782-789.

11. Muna A. L. H., Moustafa N., Sitnikova E. Identification of malicious activities in industrial internet of things based on deep learning models //Journal of information security and applications. – 2018. – Т. 41. – С. 1-11.

12. Potluri S., Diedrich C., Sangala G. K. R. Identifying false data injection attacks in industrial control systems using artificial neural networks //2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). – IEEE, 2017. – С. 1-8.

13. Yang H. et al. Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm //2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). – IEEE, 2017. – С. 957-961.

14. Wu Z. et al. Detecting and handling cyber-attacks in model predictive control of chemical processes //Mathematics. – 2018. – Т. 6. – №. 10. – С. 173.

15. Davahli A., Shamsi M., Abaei G. Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks //Journal of Ambient Intelligence and Humanized Computing. – 2020. – Т. 11. – №. 11. – С. 5581-5609.

16. Perez R. L. et al. Machine learning for reliable network attack detection in SCADA systems //2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). – IEEE, 2018. – С. 633-638.

17. Demertzis K., Iliadis L., Spartalis S. A spiking one-class anomaly detection framework for cyber-security on industrial control systems //International Conference on Engineering Applications of Neural Networks. – Springer, Cham, 2017. – С. 122-134.

18. Mathur A. P., Tippenhauer N. O. SWaT: a water treatment testbed for research and training on ICS security //2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater). – IEEE, 2016. – С. 31-36.

19. Hochreiter S., Schmidhuber J. Long short-term memory //Neural computation. – 1997. – Т. 9. – №. 8. – С. 1735-1780.

20. Ramachandran P., Zoph B., Le Q. V. Searching for activation functions //arXiv preprint arXiv:1710.05941. – 2017.

21. Kingma D. P., Ba J. Adam: A method for stochastic optimization //arXiv preprint arXiv:1412.6980. – 2014.

22. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – С. 2672-2680.

23. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

24. Baldi P. Autoencoders, unsupervised learning, and deep architectures //Proceedings of ICML workshop on unsupervised and transfer learning. – 2012. – С. 37-49.

25. Zenati H. et al. Efficient gan-based anomaly detection //arXiv preprint arXiv:1802.06222. – 2018.

26. Lueckenga J., Engel D., Green R. Weighted vote algorithm combination technique for anomaly based Smart Grid Intrusion Detection systems //2016 International Joint Conference on Neural Networks (IJCNN). – IEEE, 2016. – С. 2738-2742.

27. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks //Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. – 2018. – С. 72-83.

28. Shalyga D., Filonov P., Lavrentyev A. Anomaly detection for water treatment system based on neural network with automatic architecture optimization //arXiv preprint arXiv:1807.07282. – 2018.

29. Inoue J. et al. Anomaly detection for a water treatment system using unsupervised machine learning //2017 IEEE International Conference on Data Mining Workshops (ICDMW). – IEEE, 2017. – С. 1058-1065.

References

1. Kushner D. The real story of stuxnet //ieee Spectrum. – 2013. – Т. 50. – №. 3. – С. 48-53.

2. Khan R. et al. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid //4th International Symposium for ICS & SCADA Cyber Security Research 2016 4. – 2016. – С. 53-63.

3. Li, Zhong-wei, Weiming Tong, and Xianji Jin. "Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel." Automation of Electric Power Systems 40.8 (2016): 147-151.

4. Israel Government Tells Water Treatment Companies to Change Passwords [Электронный ресурс]. — URL: https://www.zdnet.com/article/israel-says-hackers-are-targeting-its-water-supply-and-treatment-utilities/ (visited on 6/11/2020).

5. Xu H. et al. A survey on industrial Internet of Things: A cyber-physical systems perspective //IEEE Access. – 2018. – Т. 6. – С. 78238-78259.

6. Barinov A. E., Skurlaev S. V., Sokolov A. N. Metodika otsenki riskov, vyzvannykh uyazvimostyami v programmnom obespechenii avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2017. – no. 3. – pp. 34-42. Luiijf E. Cyber (in-) security of industrial control systems: A societal challenge //International Conference on Computer Safety, Reliability, and Security. – Springer, Cham, 2014. – С. 7-15.

7. Luiijf E. Cyber (in-) security of industrial control systems: A societal challenge //International Conference on Computer Safety, Reliability, and Security. – Springer, Cham, 2014. – С. 7-15.

8. Shirazi S. N. et al. Evaluation of anomaly detection techniques for scada communication resilience //2016 Resilience Week (RWS). – IEEE, 2016. – С. 140-145.

9. Sokolov A. N., Pyatnitsky I. A., Alabugin S. K. Research of classical machine learning methods and deep learning models effectiveness in detecting anomalies of industrial control system //2018 Global Smart Industry Conference (GloSIC). – IEEE, 2018. – С. 1-6.

10. Sokolov A. N., Pyatnitsky I. A., Alabugin S. K. Applying methods of machine learning in the task of intrusion detection based on the analysis of industrial process state and ICS networking //FME Transactions. – 2019. – Т. 47. – №. 4. – С. 782-789.

11. Muna A. L. H., Moustafa N., Sitnikova E. Identification of malicious activities in industrial internet of things based on deep learning models //Journal of information security and applications. – 2018. – Т. 41. – С. 1-11.

12. Potluri S., Diedrich C., Sangala G. K. R. Identifying false data injection attacks in industrial control systems using artificial neural networks //2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). – IEEE, 2017. – С. 1-8.

13. Yang H. et al. Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm //2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). – IEEE, 2017. – С. 957-961.

14. Wu Z. et al. Detecting and handling cyber-attacks in model predictive control of chemical processes //Mathematics. – 2018. – Т. 6. – №. 10. – С. 173.

15. Davahli A., Shamsi M., Abaei G. Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks //Journal of Ambient Intelligence and Humanized Computing. – 2020. – Т. 11. – №. 11. – С. 5581-5609.

16. Perez R. L. et al. Machine learning for reliable network attack detection in SCADA systems //2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). – IEEE, 2018. – С. 633-638.

17. Demertzis K., Iliadis L., Spartalis S. A spiking one-class anomaly detection framework for cyber-security on industrial control systems //International Conference on Engineering Applications of Neural Networks. – Springer, Cham, 2017. – С. 122-134.

18. Mathur A. P., Tippenhauer N. O. SWaT: a water treatment testbed for research and training on ICS security //2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater). – IEEE, 2016. – С. 31-36.

19. Hochreiter S., Schmidhuber J. Long short-term memory //Neural computation. – 1997. – Т. 9. – №. 8. – С. 1735-1780.

20. Ramachandran P., Zoph B., Le Q. V. Searching for activation functions //arXiv preprint arXiv:1710.05941. – 2017.

21. Kingma D. P., Ba J. Adam: A method for stochastic optimization //arXiv preprint arXiv:1412.6980. – 2014.

22. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – С. 2672-2680.

23. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

24. Baldi P. Autoencoders, unsupervised learning, and deep architectures //Proceedings of ICML workshop on unsupervised and transfer learning. – 2012. – С. 37-49.

25. Zenati H. et al. Efficient gan-based anomaly detection //arXiv preprint arXiv:1802.06222. – 2018.

26. Lueckenga J., Engel D., Green R. Weighted vote algorithm combination technique for anomaly based Smart Grid Intrusion Detection systems //2016 International Joint Conference on Neural Networks (IJCNN). – IEEE, 2016. – С. 2738-2742.

27. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks //Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. – 2018. – С. 72-83.

28. Shalyga D., Filonov P., Lavrentyev A. Anomaly detection for water treatment system based on neural network with automatic architecture optimization //arXiv preprint arXiv:1807.07282. – 2018.

29. Inoue J. et al. Anomaly detection for a water treatment system using unsupervised machine learning //2017 IEEE International Conference on Data Mining Workshops (ICDMW). – IEEE, 2017. – С. 1058-1065.

АЛАБУГИН Сергей Константинович, инженер кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sergei_alabugin@mail.ru.

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru.

ALABUGIN Sergei, engineer of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sergei_alabugin@mail.ru.

SOKOLOV Alexander, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru.

УДК 004.056.2; 316.334.3:324(470+571) Вестник УрФО № 3(41) / 2021, с. 49–56

Поршнев С.В., Рябко Н.Ю., Уксусников Н.А.

DOI: 10.14529/secur210306

ОБЕСПЕЧЕНИЕ ДОСТОВЕРНОСТИ РЕЗУЛЬТАТОВ ЭКЗИТ-ПОЛЛОВ КАК ЗАДАЧА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье проведен анализ проблем, связанных с обеспечением достоверности данных экзит-поллов, результаты которого позволили сделать обоснованный вывод о том, что эта задача по своей постановке изоморфна задачам информационной безопасности, поэтому для ее решения целесообразно использовать методы защиты информации. Выбраны соответствующие методы защиты.

Обоснована необходимость в дополнительном правовом регулировании, определяющем и уточняющем порядок проведения экзит-поллов, установления правил поведения и пределов их соблюдения для его участников, также разработки моделей угроз безопасности данным социологических опросов на выходе избирательных участков, модели нарушителей и модели защиты, разработки оптимальных средств и способов обеспечения достоверности, целостности, доступности информации экзит-поллов для каждого из этапов данного социологического исследования.

Ключевые слова: *экзит-полл, достоверность результатов экзит-поллов, защита информации, информационная безопасность.*

Porshnev S.V., Ryabko N.Yu., Uksusnikov N.A

ENSURING THE VALIDITY OF EXIT-POLLS RESULTS AS A TASK OF INFORMATION SECURITY

The analysis of the problems associated with the insurance of the data reliability of exit polls was conducted. These results have provided the basis that this task is isomorphic to information security tasks in its formulation, therefore, to solve it, it is advisable to use information protection methods. Appropriate protection methods have been selected.

There was justified the need for additional legal regulation that defines and clarifies the procedure for the organization of exit polls, establishing rules of conduct and limits of their

compliance for participants, as well as developing models of security threats to the data of sociological surveys at the output of polling stations, violators and protection models, developing optimal means and methods to ensure the reliability, integrity, availability of exit poll information for each stage of this sociological research.

Keywords: *exit poll, reliability results of exit polls, information protection, information security.*

Введение

Сегодня изучение общественного мнения (экзит-полл (exit poll) – опрос избирателей на выходе с избирательных участков непосредственно после процедуры голосования) является важным компонентом каждой избирательной кампании [1]. Данный способ сбора социологических данных, предложенный У. Митофски, применяется на практике с 60х гг. XX в. [2]. Его популярность обусловлена возможностью получать ценную первичную социологическую информацию о «профиле» избирателя, голосующего за ту или иную партию или кандидата, о степени доверия граждан к выборам, о ходе голосования и явке избирателей.

Экзит-полл, целью которого является исследование электоральных процессов, с учетом особенностей цели, задач, специфику изучаемых ситуаций, особенности подготовки и процесса сбора информации, анализа данных, выводов, а также итоговых рекомендаций, разработанных на основе полученных материалов, традиционно относят к одному из особых направлений социологических и политологических наук. *Объект электоральных исследований* – характер и направленность действий субъектов политического поля (политическая элита, органы власти и оппозиция, поддерживающие их политические партии, движения и блоки, а также рядовые избиратели) в борьбе за власть. *Предмет исследования* – особенности их взаимодействия, зафиксированные в ходе электоральных замеров таких параметров, как политическое влияние, политическая культура, политическая активность, политический выбор, политическое участие и т. п.

Данная система электоральных исследований, рассматриваемая политическими силами, как одно из эффективных средств в борьбе за власть, а также как способ реализации потребности демократического общества в объективной, надежной и непрерывной информации о функционировании политического поля, призвана обеспечивать выполнение следующих основных функций: *информационную, корригирующую, прогностическую и пропагандистскую.*

Информационная функция, являющаяся одной основных целей электоральных исследований, состоит в обеспечении политических институтов общества достоверными сведениями об электоральной ситуации, которые позволяют принимать управленческие решения, направленные на ее оптимизацию в интересах конкретных субъектов политического поля.

Функция коррегирования реализуется использованием результатов электоральных исследований для проверки эффективности реализации принятых ранее управленческих решений в целях корректировки используемых методов и направлений деятельности соответствующих политических сил, в том числе, психологического воздействия на электорат.

Прогностическая функция состоит в составлении прогноза дальнейшего развития изучаемых процессов и явлений в рамках политического поля на основе анализа данных электоральных замеров. При этом прогноз должен базироваться на результатах анализа временных рядов (ВР) – серий замеров, проведенных с определенным временным интервалом по воспроизводимой методике и на базе одной и той же выборки в рамках единой генеральной совокупности.

Пропагандистская функция электоральных исследований заключается в опубликовании результатов социологических замеров, проведенных в ходе предвыборной кампании, и ознакомлении с ними избирателей, что, как ожидается, повысит их осведомленность о перипетиях политической борьбы и интерес к предстоящим выборам.

Анализ Федерального закона «Об информации, информационных технологиях и о защите информации» (149-ФЗ) [3], который в соответствие со статьей 1 регулирует отношения, возникающие при:

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

2) применении информационных технологий;

3) обеспечении защиты информации.

Он также устанавливает принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации [3, ст. 3], в том числе, принцип «достоверности информации и своевременности ее предоставления». Следовательно, перечисленные выше функции электральных исследований находятся в юрисдикции 149-ФЗ.

При этом, принимая во внимание, что обеспечение «достоверности информации» является одной из задач информационной безопасности (ИБ), к которой в соответствие с [4] относятся все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки, можно высказать гипотезу о том, что задача выявления причин возникающих расхождений между данными экзит-поллов и официальными результатами выборов относится к задачам обеспечения ИБ. В статье приведено обоснование высказанной выше гипотезы.

2. Роль экзит-поллов в современной политической жизни

За прошедшие шестьдесят лет социологическими службами и фондами постоянно совершенствовались методы и приемы проведения экзит-поллов, внедрялись новые технологии передачи и обработки полученных данных, обсуждались различные аспекты проблемы повышения точности результатов проводимых опросов (см, например, [5]).

Вместе с тем ряд специалистов высказывают мнение, что в последнее десятилетие применительно к экзит-поллам на передний план начинает выходить проблема контрольной функции экзит-поллов и возможности их использования для проверки честности выборов. Так, по мнению Ю.М Баскаковой, восприятие экзит-полла можно рассматривать как проекцию отношения населения к политической системе, в которой одним из ключевых вопросов является вопрос о доверии населения результатам выборов, уровень этого доверия определяет легитимность действующей власти [6]. Следует также отметить точку зрения В.И. Паниотто, который считает, что в ситуации, когда общество не доверяет официальным результатам, экзит-поллы могут выполнять контрольную функцию, хотя она и не присуща этому виду исследований изначально [7].

Представляется, что выход на первый план проблемы валидности экзит-поллов обусловлен тем, что этот вид социологических исследований все чаще применяется не только в научных и общественно-значимых целях, но и становится непосредственным инструментом политической борьбы, способом активизации протестных настроений в обществе и дестабилизации общественно-политической обстановки. Данная проблема характерна не только для экзит-поллов. Опросы населения по самому широкому спектру вопросов (оценки социально-экономической ситуации и материального благополучия, степени защищенности от террористических угроз, уровне доверия к органам власти) постоянно используются оппозиционными силами для формирования отрицательного отношения к органам власти и повышения уровня социальной напряженности в обществе, при этом активно применяются приемы искажения или интерпретации итоговых результатов для формирования негативной повестки, а сам процесс проведенного исследования может быть объявлен «сфабрикованным» (см. например, [8]).

Необходимо отметить, что экзит-полл, в отличие от «классического» социологического исследования, обладает целым рядом специфических качеств, сформулированных Л.В. Львовым [9]:

– «удобство» выборки и отсутствие необходимости скрининга, что повышает оперативность получения данных;

– вовлеченность и непосредственный «контакт» респондента предметом исследования;

– отсутствие «проблемы» забывания респондентами сущности и деталей предмета интервью;

– отсутствие влияния референтных источников на мнение респондента;

– сопоставимость данных с результатами исследований в других целевых аудиториях, аудиториях с малой степенью вовлеченности, в потенциальных аудиториях.

Перечисленные качества, с учетом высокой степени вовлеченности опрашиваемых респондентов, совершивших активное избирательное действие и заинтересованных в победе своей партии или кандидатов (а, значит, и в том, чтобы результаты опроса и выбо-

ров совпали с их ожиданиями) существенно повышают потенциал экзит-полла как инструмента политической борьбы. Следует учитывать и то, что в ходе самого опроса его предварительные результаты могут использоваться заказчиками и политтехнологами как повод для вмешательства в ход процедуры голосования и применения «грязных» политических технологий (использование административного ресурса, подкуп избирателей, вброс бюллетеней, оказание давления на избирательные комиссии).

Анализ методов и задач проведения экзит-поллов, а также возможностей их использования для оказания влияния на общественные настроения позволяет сделать вывод, что опросы на выходе с избирательных участков могут преследовать как общественно-значимые (научные, информационные и контрольные), так и явно антиобщественные цели, в том числе:

– отслеживающую (использование оперативной информации о ходе голосования для влияния различными способами на его результат);

– имитационную (проведение экзит-полла и использование его результатов для оправдания проигрыша кандидата в результате «фальсификации выборов»);

– дестабилизирующую (публикация и использование результатов опроса, отличающихся от официальных результатов, для создания предпосылок к общественной дискуссии о законности прошедшего голосования).

Проблема использования экзит-поллов как инструмента влияния на ход голосования и способа политической борьбы становится все более актуальной, причем не только в России, но и на постсоветском пространстве. Например, во время выборных кампаний в Украине, Армении и Белоруссии результаты экзит-поллов распространялись через социальные сети и мессенджеры для мобилизации электората, а также использовались для активизации и радикализации протестных настроений в среде оппозиционно настроенных к действующей власти граждан. Более того, в Украине результаты проведенного в 2004 г. так называемого «национального экзит-полла», опубликованные до объявления официальных результатов выборов, оппозиция использовала как прямое доказательство победы В. Ющенко над В. Януковичем (см., например, [10] и другие ссылки, приведенные на данной странице). Также напомним о массовых акциях протестов после выборов в Государственную Думу VI созыва (декабрь 2011 г.) и выборов Президента Российской Федерации (март 2012 г.) организаторы и участники которых, заявляя о «фальсификации» выборов, также ссылались на данные неких «альтернативных» экзит-поллов (см., например, [11]).

Исследуя проблему повышения качества проведения экзит-поллов и их достоверности, эксперты указывают, что доказать фальсификацию экзит-полла при применяемых технологиях практически невозможно. Например, Ю.М. Баскакова отмечает, что в условиях экзит-полла процедуры контроля находятся в руках организации, непосредственно проводящей исследование, а возможности внешнего контроля сведены к минимуму [2]. Предложенные Н.В. Паниной критерии валидности данных экзит-полла (соответствие результатов опроса данным избирательных комиссий, соответствие результатов опроса результатам параллельного подсчета голосов, согласованность результатов опросов, проведенных разными центрами) [12], а также дополнительные критерии, разработанные В.И. Паниотто (логическая валидность и участие социологических служб в предыдущих выборах с соответствием данных опроса итогам этих выборов) [2], не исключают возможных обвинений организаций, проводящих экзит-поллы, в политической ангажированности. Кроме того, оппозиционно настроенная часть общества не склонна критически относиться к опубликованным данным «альтернативных» экзит-поллов, доверяя им в противовес уже сформировавшегося негативного отношения к официальным источникам информации. По мнению экспертов, решение вышеуказанных проблем невозможно без привлечения внешних аудиторов, а также использования технологий, обеспечивающих как «прозрачность» процедуры проведения опроса для наблюдателей, так и необходимой защиты информации.

3. Выбор методов защиты информации, получаемой при проведении экзит-полла

Любое социологическое исследование, в том числе и экзит-полл, может быть декомпозировано на следующие основные этапы:

– подготовительный этап;

– этап проведения опроса;

– этап передачи данных в центр обработки;

– обработка данных;

– публикация и последующее хранение результатов опроса.

В процессе проведения экзит-полла лицо, проводящее опрос, осуществляет сбор и хранение первичной информации, имеющей важное общественно-политическое значение (особенно результаты проведенных опросов), а также ее анализ с целью получения интегрированных данных по кандидатам, участвующим в выборах за выбранный период времени. Таким образом, существует очевидная аналогия между действиями, выполняемыми при организации и проведении опросов на выходе с избирательных участков, и действия, выполняемые информационными системами (ИС), осуществляющими сбор, хранение и обработку информации. В этой связи целесообразно рассмотреть методы защиты информации, используемые в ИС для обеспечения достоверности, целостности и доступности, с точки зрения возможности их использования для обеспечения достоверности данных экзит-поллов на каждом из этапов их проведения.

На подготовительном этапе экзит-полла (особенно в ходе федеральных избирательных кампаний) в целях защиты информации целесообразно применять организационные меры, например, установление определенных квалификационных требований к социологическим службам, планирующим проведение опроса (наличие необходимого количества обученных интервьюеров, опыта проведения соответствующих социологических исследований на федеральном или региональном уровнях, достаточная материально-техническая база и т.д.). При этом можно ожидать, что применение этих мер позволит исключить или существенно ограничить появление в публичном доступе сфабрикованных результатов «имитационных» опросов, а также будет способствовать формированию критического восприятия данных подобных исследований.

Следует отметить, что частью 2 статьи 46 Федерального закона от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» установлено, что при опубликовании (обнародовании) результатов опросов общественного мнения, связанных с выборами и референдумами, редакции средств массовой информации, граждане и организации, публикующие (обнародующие) эти результаты, обязаны указывать организацию, проводившую опрос, время его проведения, число опрошенных (выборку), метод сбора информации, регион, где проводился опрос, точную формулировку вопроса, статистическую оценку возможной погрешности, лицо (лиц), заказавшее (заказавших) проведение опроса и оплатившее (оплативших) указанную публикацию (обнародование).

Таким образом, сведения, необходимые для первичного анализа и контроля качества проведения экзит-полла, в настоящее время могут стать доступны только после проведения опроса. В этой связи для обеспечения возможности оценивания экспертным и профессиональным сообществами планируемый опрос с научной точки зрения (например, объема планируемой выборки, места проведения, метода сбора информации, формулировок вопросов), а также контроля соответствия заявленных мест проведения экзит-поллов представляется целесообразным принятие на федеральном уровне нормативного документа, обязывающего организации, проводящие экзит-полл, предоставлять свободный доступ к требуемым сведениям до начала опроса.

Защита информации на этапе проведения социологического опроса также может обеспечиваться организационными мерами – контролем качества его проведения, в том числе – сохранения анонимности респондентов, соответствия содержания анкеты, формулировок вопросов и действий интервьюеров методике проведения опроса. Отметим, что высказанное нами предложение также подтверждается З.И. Корякиной и Ю.И. Жегусовым, которые считают, что с учетом современного состояния законодательства о выборах процедура экзит-полла нуждается в дополнительном правовом регулировании, определяющем и уточняющем порядок его проведения, установления определенных правил поведения и пределов их соблюдения для его участников [13].

На этапе передачи данных и их последующей обработки могут применяться разнообразные средства защиты, обеспечивающие достоверность, целостность и сохранность информации – процедуры аутентификации отправителя и получателя информации, доверенные или защищенные каналы связи, криптографическая защита информации, средства разграничения доступа, доверен-

ная среда обработки или сертифицированное программное обеспечение. Независимым внешним аудиторам на этих этапах должна быть предоставлена возможность частичного доступа к обрабатываемым данным для проведения выборочного контроля достоверности информации. Средства защиты на данных этапах должны выбираться и применяться сообразно с масштабом и значимостью проводимого опроса, поскольку небольшие социологические службы и фонды могут не обладать достаточными финансовыми ресурсами для приобретения необходимых программно-аппаратных продуктов и организации каналов связи.

В отношении этапа публикации данных экзит-полла необходимо отметить, что объем прав и обязанностей как организаций, проводивших экзит-полл, так и непосредственно заказчика опроса при публикации итоговых результатов, нуждаются в дополнительном правовом регулировании, которое должно предусматривать внедрение практики предоставления каждым организатором или заказчиком опроса доступа независимых аудиторов ко всему накопленному массиву информацию, а не только к интегрированным результатам экзит-полла. Это позволит проводить независимую проверку качества проведенных опросов и выявлять (при их наличии) факты фальсификации результатов, допущенные конкретными экспертами, проводящими опрос на выходе из избирательного участка, так и организациями, как отвечающими за проведение опросов, так и его заказчиками, а также сравнивать результаты опроса, вызывающие недоверие, с результатами, полученными другими авторами. При этом представляется целесообразным использовать как известные методы прикладной статистики, традиционно применяемые для анализа результатов социологических опросов, в которых, как правило, проводится сравнение распределений различных выборок, так и разработать математические модели, описывающие динамику процесса голосования, наличие которых позволит использовать методы анализа и прогнозирования временных рядов.

4. Заключение

Проведенный анализ проблем оценивания адекватности результатов экзит-поллов позволяет сделать вывод о необходимости комплексной всесторонней системы защиты информации, получаемой во время проведения опросов на выходе с избирательных участков, которая должна обеспечить:

а) соответствие выборки генеральной совокупности;

б) соблюдение методики проведения опроса

в) анонимность респондентов;

г) доверенную (защищенную) среду передачи информации в центр обработки;

д) достоверность, целостность и сохранность данных при обработке;

е) конфиденциальность полученных результатов (до окончания процедуры голосования).

При этом в зависимости от сложности и масштабности проводимого опроса, должны быть разработаны различные модели угроз данным экзит-поллам, модели нарушителей и модели защиты, предложены оптимальные средства и способы обеспечения достоверности, целостности, доступности информации для каждого из этапов данного социологического исследования.

Внедрение подобной системы защиты потребует дополнительного правового регулирования экзит-поллов на федеральном уровне, а также разработка правил проведения таких исследований, определяющих порядок взаимодействия и объем прав и обязанностей всех субъектов экзит-полла – заказчика, организатора (интервьюера) и избирателя.

Решение вопросов обеспечения информационной безопасности экзит-поллов, применение в ходе таких опросов «прозрачных» и в то же время надежных систем защиты информации, несомненно, позволит повысить степень общественного доверия как к результатам социологических исследований, так и официальным результатам выборов.

Литература

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

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

3. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации».

4. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». –М.: Стандартинформ, 2014. 106 с.

5. Винославская С., Чурилов Н. Социология: теория, методы, маркетинг, 2008, № 1. С. 189–196.

6. Баскакова Ю.М. Экзит-полл и его задачи// Мониторинг общественного мнения. № 4 (104), июль-август 2011 С. 37–41.

7. Паниотто В.И., Харченко Н. Социологические исследования как способ контроля за результатами выборов и референдумов//Социология: теория, методы, маркетинг, 2002. № 1. С. 155–170.

8. Паниото В. Невыносимая легкость журналистских суждений. Как достичь взаимопонимания между СМИ и социологами?// http:https://day.kyiv.ua/ru/article/nota-bene/nevynosimaya-legkost-zhurnalistskih-suzhdeniy (дата обращения 29.08.2021)

9. Львов С.В. Опросы на выходе: перспективы метода // Мониторинг общественного мнения: экономические и социальные перемены. 2011. № 4. С. 42–46.

10. http://lenta.ru/articles/2004/11/26/letter/ (дата обращения 29.08.2021)

11. Хронология протестного движения в России (2011—2013)// https://ru.wikipedia.org/wiki/%D0%A5%D1%80%D0%BE%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%D0%BF%D1%80%D0%BE%D1%82%D0%B5%D1%81%D1%82%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B4%D0%B2%D0%B8%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_(2011%E2%80%942013) (дата обращения 29.08.2021)

12. Панина Н.В. Экзит-полл в Украине 2004 года: социология или политика?: доклад [на Круглом столе «Научное знание и власть: социологические исследования и политическая практика» (Киев, 17 марта 2005 г.)]. https://mognovse.ru/lmv-doklad-kruglij-stol-nauchnoe-znanie-i-vlaste-sociologiches.html (дата обращения 29.08.2021)

13. Корякина З.И., Жегусов Ю.И. Правовое регулирование опроса общественного мнения на выходе из избирательного участка после голосования (экзит-полла) //Мониторинг общественного мнения: экономические и социальные перемены. 2020. № 6. С. 97–112.

References

1. Rotmand D.G., Pravdivec V.V., Belov A.A. Elektoral'nye sociologicheskie issledovaniya: organizaciya oprosov v den' vyborov (ekzit-poll)// Sociologiya, 2015. № 3. S. 122–132.

2. Baskakova YU.M. Ekzit-poll i ego zadachi // Monitoring obshchestvennogo mneniya: ekonomicheskie i social'nye peremeny. 2011. № 4. S. 37-41.

3. Federal'nyj zakon ot 27.07.2006 N 149-FZ (red. ot 02.07.2021) «Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii».

4. GOST R ISO/MEK 27002-2012 «Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informacionnoj bezopasnosti». –.M.: Standartinform, 2014. 106 s.

5. Vinoslavskaya S., CHurilov N. Sociologiya: teoriya, metody, marketing, 2008, № 1. S. 18–196.

6. Baskakova YU.M. Ekzit-poll i ego zadachi// Monitoring obshchestvennogo mneniya. № 4 (104), iyul'-avgust 2011 S. 37–41.

7. Paniotto V.I., Harchenko N. Sociologicheskie issledovaniya kak sposob kontrolya za rezul'tatami vyborov i referendumov//Sociologiya: teoriya, metody, marketing, 2002. № 1. S. 155–170.

8. Panioto V. Nevynosimaya legkost' zhurnalistskih suzhdenij. Kak dostich' vzaimoponimaniya mezhdu SMI i sociologami?// http:https://day.kyiv.ua/ru/article/nota-bene/nevynosimaya-legkost-zhurnalistskih-suzhdeniy (data obrashcheniya 29.08.2021)

9. L'vov S.V. Oprosy na vyhode: perspektivy metoda // Monitoring obshchestvennogo mneniya: ekonomicheskie i social'nye peremeny. 2011. № 4. C. 42–46.

10. http://lenta.ru/articles/2004/11/26/letter/ (data obrashcheniya 29.08.2021)

11. Hronologiya protestnogo dvizheniya v Rossii (2011—2013)// https://ru.wikipedia.org/wiki/%D0%A5%D1%80%D0%BE%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%D0%BF%D1%80%D0%BE%D1%82%D0%B5%D1%81%D1%82%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B4%D0%B2%D0%B8%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_(2011%E2%80%942013) (data obrashcheniya 29.08.2021)

12. Panina N.V. Ekzit-poll v Ukraine 2004 goda: sociologiya ili politika?: doklad [na Kruglom stole «Nauchnoe znanie i vlast': sociologicheskie issledovaniya i politicheskaya praktika» (Kiev, 17 marta 2005 g.)]. https://

mognovse.ru/lmv-doklad-kruglij-stol-nauchnoe-znanie-i-vlaste-sociologiches.html (data obrashcheniya 29.08.2021)

13. Koryakina Z.I., Zhegusov YU.I. Pravovoe regulirovanie oprosa obshchestvennogo mneniya na vyhode iz izbiratel'nogo uchastka posle golosovaniya (ekzit-polla) //Monitoring obshchestvennogo mneniya: ekonomicheskie i social'nye peremeny. 2020. № 6. S. 97–112.

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

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

УКСУСНИКОВ Николай Алексеевич, магистрант 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:

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:

UKSUSNIKOV Nikolay Alekseevich, Master's 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:

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

УДК 004.056.53

Вестник УрФО № 3(41) / 2021, с. 57–64

Баранкова И.И., Афанасьева М.В., Федорова А.Р.

DOI: 10.14529/secur210307

МОДЕЛЬ ЗРЕЛОСТИ БЕЗОПАСНОСТИ АСУ ТП ДОМЕННОЙ ПЕЧИ №10 ПАО «ММК»

В статье рассматриваются понятия зрелости безопасности, модель и целевой профиль зрелости безопасности, приводятся требования к построению модели зрелости безопасности и шкала оценки уровней полноты практик безопасности. В ходе работы представляется текущий профиль безопасности АСУ ТП доменной печи, определяется целевой профиль зрелости безопасности по уровням полноты, а также дается оценка наиболее значимым практикам модели зрелости безопасности. Завершающим этапом работы является анализ текущего и целевого профилей безопасности для выявления пробелов.

Ключевые слова: *информационная безопасность, АСУ ТП, модель зрелости безопасности, целевой профиль зрелости безопасности.*

Barankova I.I., Afanasyeva M.V., Fedorova A.R.

MMK PJSC BLAST FURNACE NO. 10 AUTOMATED PROCESS CONTROL SYSTEM SAFETY MATURITY MODEL

The article discusses the concepts of security maturity, the model and the target profile of security maturity, the requirements for building a model of security maturity and a scale for assessing the levels of completeness of security practices. In the course of the work, the current safety profile of the blast furnace automated process control system is presented, the target safety maturity profile is determined by completeness levels, and the most significant practices of the safety maturity model are evaluated. The final stage of the work is the analysis of the current and target security profiles to identify gaps.

Keywords: *information security, automated control system, security maturity model, target profile of security maturity.*

Нарастающая сложность технологий, применяемых в промышленных системах, расширяет поверхность атак, создавая новые риски там, где раньше использовались некомпьютеризированные подходы или отсутствовало постоянное сетевое взаимодействие с внешним миром. Поэтому одной из основных задач в эпоху цифровизации на промышленных предприятиях является разработка стратегии защиты от киберугроз, которая проходит следующие стадии: проектирование, разработка, интеграция, использование и сопровождение. Участие в вышеперечисленных процессах сопровождается наличием большого количества участников и оценка рисков, связанных с атаками, у всех осуществляется по-разному. Существует две точки зрения в отношении безопасности для бизнеса – увеличение времени выхода на рынок или безопасный продукт, у которого есть преимущество на рынке. При автоматизации технологических процессов, производители информационных продуктов перекладывают свою ответственность на клиентов под предлогом того, что продукт должен быть изолирован от внешнего воздействия, что вовсе не может быть достижимо. Предприятия же аналогичным образом зачастую не могут полностью пользоваться продуктом автоматизации с точки зрения обеспечения безопасности без подтверждения со стороны производителя продукта [1]. Таким образом, важной и актуальной задачей на данный момент является выработка стратегически правильного подхода к управлению уязвимостями, грамотного инвестирования в механизмы безопасности, отвечающие требованиям предприятия, без чрезмерных вложений в ненужных механизмах безопасности, а также предоставить концептуальную основу для помощи в выборе и реализации соответствующих меры безопасности из бесчисленного множества вариантов.

Так как не все системы требуют одинаковой силы защитных механизмов или процедур, чтобы соответствовать их требованиям безопасности, то организационное руководство определяет приоритеты, которые движут процесс повышения безопасности, что позволяет механизмам и процедурам соответствовать цели организации, не выходя за рамки необходимого. Реализации механизмов безопасности считаются зрелыми, если ожидается, что они будут эффективны в достижении этих целей. Соответствие механизмов безопасности достижению поставленных целей, т.е. зрелость, определяется не их объективной силой. Следовательно, зрелость безопасности – это мера понимания текущего уровня безопасности, ее необходимости, преимущества и стоимости ее поддержки.

Модель зрелости безопасности представляет собой иерархию практик обеспечения безопасности, сгруппированные по ожидаемому эффекту от их применения, описанные в [2]. Для упрощения понимания модели зрелости на самом верхнем уровне практик они объединены в так называемые домены.

Три верхнеуровневых домена безопасности включают:

1. управление безопасностью и организационные меры (Управление);

2. обеспечение безопасности в силу конструкции (Внедрение);

3. укрепление безопасности (Укрепление).

Приоритет того или иного домена перед другим определяется потребностями бизнеса и особенностями системы.

На втором уровне каждый из доменов делится на три поддомена, которые классифицируют практики безопасности в соответствии с проблемой, на решение которой они нацелены. И наконец, каждый поддомен ссылается на 2 практики, каждая из которых решает некоторую задачу (рисунок 1).

Существуют два ортогональных аспекта оценки зрелости: полнота и специфичность. Полнота отражает степень глубины, последовательности и обеспечение мер безопасности, которые поддерживают домены зрелости безопасности, субдомены или практики. Например, более высокий уровень полноты моделирования угроз подразумевает большее автоматизированный системный и разносторонний подход. Специфика отражает степень соответствия отрасли или системным потребностям. Это отражает степень настройки мер безопасности, поддерживающих домены зрелости безопасности, поддомены или практики. Такие настройки обычно требуются для устранения отраслевых или системных ограничений АСУ ТП. Полнота и специфичность помогают оценивать и расставлять приоритеты в практике зрелости безопасности [3,4].

Полнота реализации практики оценивается по следующей шкале:

– нулевой уровень (уровень 0): нет единого понимания того, как применяется практи-

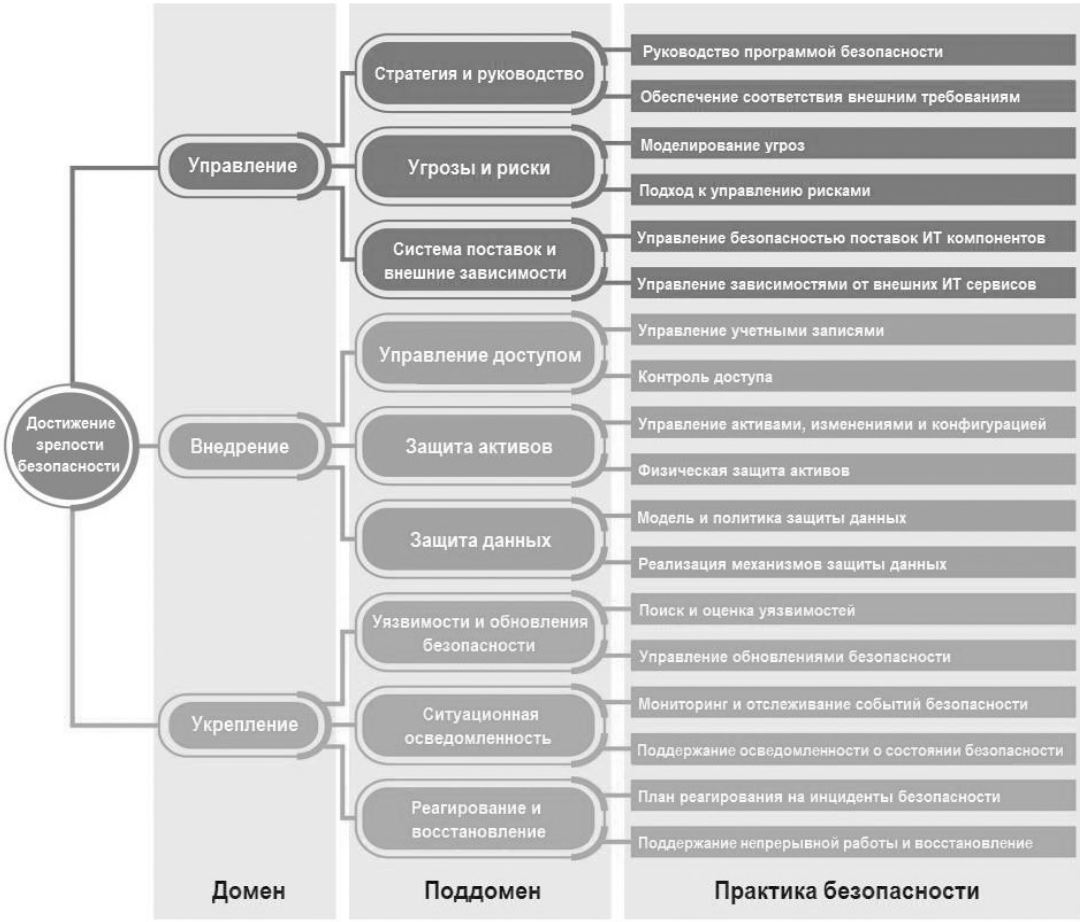


Рис. 1. Иерархия доменов, субдоменов и практик в модели зрелости безопасности

ка безопасности, и нет соответствующих требований, которые необходимо реализовать

– минимальный уровень (уровень 1): соблюдены минимальные требования практики безопасности.

– специальный уровень (уровень 2): требования к практике охватывают основные варианты использования и общеизвестные инциденты безопасности в аналогичных средах. Требования повышают точность и уровень детализации для рассматриваемой среды.

– постоянный уровень (уровень 3): требования учитывают передовой опыт, стандарты, правила, классификации, зарекомендованное программное обеспечение и другие инструменты. Инструменты устанавливают последовательный подход к практике развертывания системы защиты. Гарантия проверяет реализацию на соответствие шаблонам безопасности.

– формализованный уровень (уровень 4): хорошо отлаженный процесс формирует основу для практической реализации, обеспечения постоянной поддержки и повышения безопасности. Гарантия реализации фокусируется на удовлетворении потребностей в безопасности и своевременном решении проблем, которые несут угрозу для системы.

Из вышеперечисленного следует, что большие числа указывают на более высокую степень полноты. Каждый уровень полноты покрывает все требования, установленные нижними уровнями, расширяя их.

В свою очередь, специфичность реализации практики можно оценить следующим образом:

– неспецифичный уровень (уровень 1): это самый широкий диапазон. Практика безопасности реализована без какой-либо оценки актуальности для конкретной отрасли и системы. Возможности и методы безопасности применяются так, как они были реализованы повсеместно.

– уровень специфичный для отросли (уровень 2): сфера применения сужена от общего случая к отраслевому сценарию. Практика безопасности реализуется с учетом отраслевых проблем, в частности, которые ка-

саются компонентов и процессов, которые подвержены определенным типам атак и известны уязвимости и произошедшие инциденты, присущие конкретной отрасли.

– уровень специфичный для системы (уровень 3): это самая узкая область. Реализация практики безопасности согласованы с конкретными организационными потребностями и рисками рассматриваемой системы, определены границы доверия, компоненты, технологии, процессы и сценарии использования.

В зависимости от контекста, возможно, что некоторые из практик могут оказаться неприменимыми. В этом случае они могут быть помечены как «Неприменима».

Для разработки модели зрелости безопасности АСУ ТП доменной печи необходимо оценить текущее состояние безопасности на объекте. Определение своей текущей зрелости безопасности и ее сравнение с целевым профилем дает возможность определить, что необходимо реализовать для перехода к более высокому состоянию зрелости, а также произвести адекватную оценку реализованных средств защиты и трезво оценить текущую ситуацию на объекте..

На рисунке 2 представлен текущий профиль безопасности АСУ ТП доменной печи ПАО «ММК» по полноте реализации практик.

Рассмотрим наиболее значимые практи-

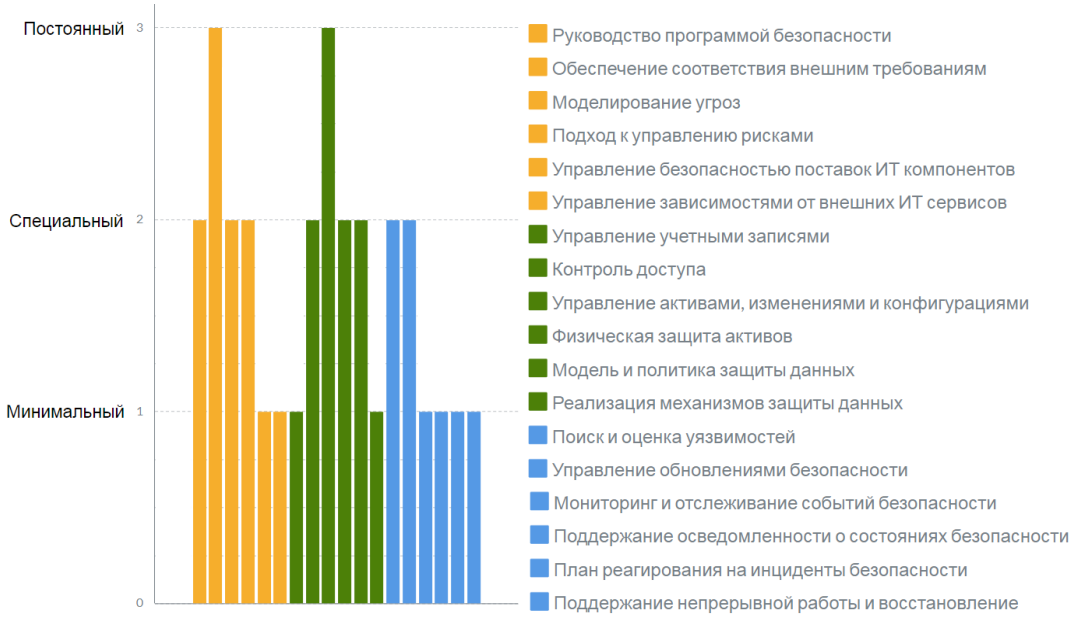


Рис. 2. Текущий профиль безопасности АСУ ТП доменной печи ПАО «ММК» по уровням полноты практик безопасности

ки для данной системы, которым был присвоен 3 уровень полноты.

1. Практика «Обеспечение соответствия внешним требованиям – постоянный уровень. Политика безопасности согласована со ФСТЭК России, объект категорирован и выполнены все требования законодательства в обеспечении безопасности на объекте критической информационной инфраструктуры.

2. Практика «Управление активами, изменениями и конфигурациями» - постоянный уровень. Классифицированы и маркированы физические и информационные активы, Политика управления изменениями включает в себя выявление значительных изменений в конфигурации системы и ПО. Разработаны руководящие принципы для защиты программного обеспечения, в том числе его целостности (внедрение антивирусных программ, реализация комплекса мероприятий по защите информации и обеспечению необходимым лицензионным ПО).

Модель зрелости помогает не только описать зрелость безопасности с разных точек зрения, в том числе с точки зрения бизнеса, но помогает согласовать и стимулировать сотрудничество среди всех заинтересованных сторон, которые работают над повышением зрелости безопасности. В то время как целевой профиль зрелости безопасности – это та цель предприятия, к которой необходимо стремиться для достижения зрелости безопасности с учетом текущих потребностей и производственных мощностей [5].

Составляя целевой профиль зрелости безопасности АСУ ТП, необходимо задавать следующие вопросы:

• Учитывая требования организации и ландшафт угроз, какова цель вашего решения?

• Каков текущий уровень зрелости безопасности на предприятии?

• Какие механизмы и процессы повлияют на переход текущего состояния безопасности в целевое состояние?

Уровень зрелости определяется с учетом полноты реализации практики безопасности и специфики ее реализации для АСУ ТП. Каждая организация, система, отдельное решение требует разной полноты и специфичности. Значит, и целевой уровень зрелости для разных случаев будет разным.

Переходы между уровнями определяются конкретными проблемами отрасли и системы, конкретными потребностями и рисками, выявленными при определении целевого уровня зрелости безопасности. Следовательно, перед оценкой зрелости безопасности заинтересованные стороны должны согласовать точные определения уровней полноты и охвата в соответствии с рисунком 3.

Из вышесказанного следует, что при уче-

Рис. 3. Состояния и переходы между уровнями полноты и специфичности реализации практик

те мощности бизнеса и потребности, не всегда присвоение 4 уровня как наилучшего будет рационально и осуществимо в ближайшей перспективе.

На рисунке 4 представлен целевой профиль безопасности АСУ ТП по полноте реализации практик.

Наиболее значимым практикам для данной системы был присвоен 4 уровень полноты. Это было сделано на основе следующих особенностей системы и приоритетов организации:

1. В силу того, что данный объект относится к критической информационной инфраструктуре (КИИ), необходимо постоянное совершенствование систем безопасности и соответствие нормативным документам по обеспечению безопасности КИИ. Поэтому целесообразно определить целевой уровень полноты практики «Обеспечение соответствия внешним требованиям» как формализованный.

2. Металлургическое производство зависит от непрерывной работы критически важных агрегатов, в работе оборудования могут возникать простои в связи с непредвиденными инцидентами информационной безопасности. Это влечет за собой большие экономические потери. Также следует отметить, что кибератака на АСУ ТП доменной печи может

Рис. 4. Целевой профиль зрелости безопасности по уровням полноты системы мониторинга состояния кожуха доменной печи ПАО «ММК»

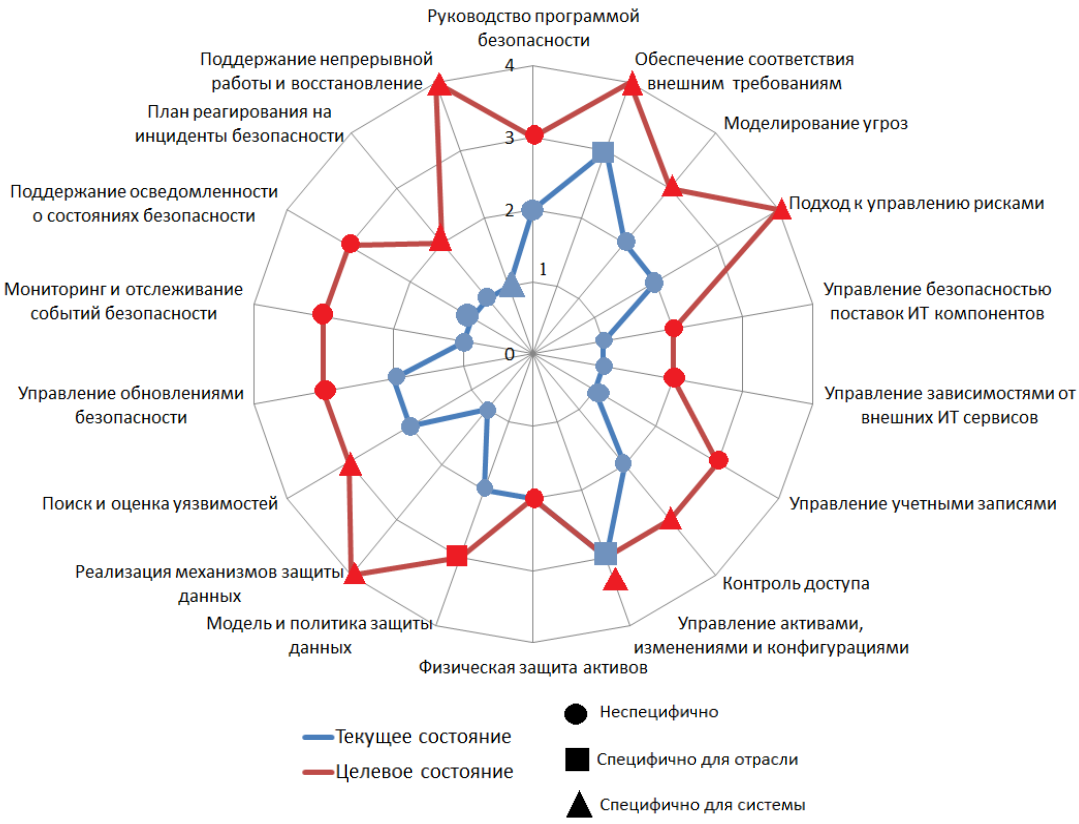


Рис. 5. Визуализация анализа расхождений текущего и целевого профиля зрелости безопасности при помощи паутинной диаграммы

привести к большим человеческим потерям, например, вследствие прорыва расплавленной шихты, а также повышает экологические риски. Согласно годовому отчету ММК [6] за 2020 год, в карте рисков ММК производственному и экологическому рискам присвоен высокий уровень. Поэтому для их снижения необходимо непрерывно управлять рисками и

разработать дорожную карту для их периодической переоценки. Поэтому следует практике «Управление рисками» присвоить 4 уровень полноты.

3. На основании вышесказанных пунктов для комплексной защиты информации выбранной системы необходимо реализовывать механизмы защиты на каждом этапе жизненного цикла системы, в том числе на этапе уничтожения. В связи с этим полнота практики «Реализация механизмов защиты» устанавливается на 4 уровне.

4. Обеспечение безотказной работы и непрерывности технологического процесса – самая приоритетная задача для производства [7]. Поэтому практика «Поддержание непрерывной работы и восстановление» должна стремиться к уровню 4.

Зная целевое состояние и текущее состояние, организация может выполнить анализ пробелов, чтобы определить подходящие области для улучшения безопасности и инвестиций. Для тех элементов управления, где есть разница между двумя состояниями, следует обратить внимание на размер разрыва, чтобы помочь при расстановке приоритетов в дорожной карте организации. Также необходимо обратить внимание на любые ситуации, в которых конкретный элемент управления может не соответствовать целевому состоянию, но потенциальный последующий риск смягчается другим средством контроля. Этот процесс должен дать список мер безопасности в организации, которые не соответствуют целевому состоянию.

На основе сравнения целевого и текущего состояния, заинтересованные стороны могут измерять прогресс и согласовывать шаги по повышению зрелости безопасности.

На рисунке 5 показана паутинной диаграмма, сравнивающая целевой и текущий профиль безопасности по полноте реализации практик. Маркеры на вершинах дают представление о специфичности реализации практик.

Пробелы в профилях определяются пробелами по полноте и специфичности. Если есть пробелы для конкретной (текущая зрелость практики ниже, чем хотелось бы), то эта практика должна быть улучшена. Если пробелов нет (одинаковые показатели уровня по практикам или текущее состояние выше целевого), то зрелость организации достаточна или опережает потребность.

Литература

1. Рудина, Е. Концепция nudge в обеспечении зрелости безопасности интернета вещей [Текст] / Е. Рудина // Технологическая перспектива в рамках Евразийского пространства: новые рынки и точки экономического роста: сб. науч. тр. – СПб.: Изд-во Центр научно-производственных технологий «Астерион», 2019. – Вып. 5 – С. 476-480.

2. Industrial Internet Consortium. IoT Security Maturity Model: Description and Intended Use Whitepaper. V1.1 of 2019-Feb-15. URL: https://iiconsortium.org/pdf/SMM Description and Intended Use FINAL Updated V1.1.pdf

3. Модель зрелости безопасности интернета вещей: толчок к развитию безопасных систем [Электронный ресурс] / Kaspersky ICS CERT - Электрон. дан. – М., 2019. – Режим доступа: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity, свободный. — Загл. с экрана.

4. Федорова А.Р., Казаков О.А., Афанасьева М.В. Модель зрелости безопасности промышленного интернета вещей // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 79-й междун. науч.-технич. конф. 2021. С. 403.

5. Афанасьева М.В., Федосеев Н.А. Определение целевого профиля безопасности промышленного интернета вещей // Безопасность информационного пространства. Сборник трудов XIX Всерос. науч.-практич. конф. студентов, аспирантов и молодых ученых. Уральский государственный экономический университет. Екатеринбург, 2021. С. 197-200.

6. Годовой отчет ПАО «Магнитогорский металлургический комбинат» за 2019 год [Электронный ресурс] / Сайт группы ПАО «ММК» - Электрон. дан. – Магнитогорск, 2020. – Режим доступа: http://mmk.ru/for_investor/annual_reports/

7. Баранкова И.И., Михайлова У.В., Афанасьева М.В., Афанасьев М.Ю. Принципы построения модели надежности системы защиты информации АСУ ТП доменной печи // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 77-й междун. науч.-технич. конф. 2019. С. 424.

References

1. Rudina, Ye. Kontseptsiya nudge v obespechenii zrelosti bezopasnosti interneta veshchey [Tekst] / Ye. Rudina // Tekhnologicheskaya perspektiva v ramkakh Yevraziyskogo prostranstva: novyye rynki i tochki ekonomicheskogo rosta: sb. nauch. tr. – SPb.: Izd-vo Tsentr nauchno-proizvodstvennykh tekhnologiy "Asterion", 2019. – Vyp. 5 – S. 476-480.

2. Industrial Internet Consortium. IoT Security Maturity Model: Description and Intended Use Whitepaper. V1.1 of 2019-Feb-15. URL: https://iiconsortium.org/pdf/SMM Description and Intended Use FINAL Updated V1.1.pdf

3. Model' zrelosti bezopasnosti interneta veshchey: tolchok k razvitiyu bezopasnykh sistem [Elektronnyy resurs] / Kaspersky ICS CERT - Elektron. dan. – M., 2019. – Rezhim dostupa: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity, svobodnyy. — Zagl. s ekrana.

4. Fedorova A.R., Kazakov O.A., Afanas'yeva M.V. Model' zrelosti bezopasnosti promyshlennogo interneta veshchey // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. Tezisy dokladov 79-y mezhdun. nauch.-tekhnich. konf. 2021. S. 403.

5. Afanas'yeva M.V., Fedoseyev N.A. Opredeleniye tselevogo profilya bezopasnosti promyshlennogo interneta veshchey // Bezopasnost' informatsionnogo prostranstva. Sbornik trudov XIX Vseros. nauch.-praktich. konf. studentov, aspirantov i molodykh uchenykh. Ural'skiy gosudarstvennyy ekonomicheskiy universitet. Yekaterinburg, 2021. S. 197-200.

6. Godovoy otchet PAO «Magnitogorskiy metallurgicheskiy kombinat» za 2019 god [Elektronnyy resurs] / Sayt gruppy PAO "MMK" - Elektron. dan. – Magnitogorsk, 2020. – Rezhim dostupa: http://mmk.ru/for_investor/annual_reports/

7. Barankova I.I., Mikhaylova U.V., Afanas'yeva M.V., Afanas'yev M.YU. Printsipy postroyeniya modeli nadezhnosti sistemy zashchity informatsii ASU TP domennoy pechi // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. Tezisy dokladov 77-y mezhdun. nauch.-tekhnich. konf. 2019. S. 424.

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

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

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

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

ФЕДОРОВА Анастасия Романовна, студент группы АИБ-19-2 кафедры информатики и информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: anastasia.43ag@gmail.com

FEDOROVA Anastasia Romanovna, student of the AIB-19-2 group of the Department of computer science and information security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: anastasia.43ag@gmail.com

УДК 004.896 + 004.056.57 Вестник УрФО № 3(41) / 2021, с. 65–87

Соколов А.Н., Рагозин А.Н., Баринов А.Е., Уфимцев М.С., Пятницкий И.А., Бухарев Д.А.

DOI: 10.14529/secur210308

РАЗРАБОТКА МОДЕЛЕЙ И МЕТОДОВ РАННЕГО ОБНАРУЖЕНИЯ КИБЕРАТАК НА ОБЪЕКТЫ ЭНЕРГЕТИКИ МЕТАЛЛУРГИЧЕСКОГО ПРЕДПРИЯТИЯ[1]

Необходимость реагирования на киберинциденты в энергетических комплексах металлургических предприятий приводит к серьезным последствиям, таким как простои и дорогостоящие перезапуски производства. Поэтому актуальной является задача реализации концепции защиты информации «предотвращать» вторжения, а не «предупреждать» о них, согласно которой поиск киберугроз становится постоянной фоновой деятельностью. В работе представлена система раннего обнаружения воздействия кибератак, разработанная с использованием технологий интеллектуальной обработки данных на основе модели системы динамических процессов, отражающих функционирование (поведение) информационной системы объекта. Разработана методика, позволяющая получать численную оценку необходимости улучшения параметров мониторинга для различных зон технологического процесса. В качестве примера использования методики приведен расчет на основе подсистемы технологического процесса металлургического предприятия, на основании которого выбраны наиболее важные информативные точки сбора данных для реализации мониторинга. Показано, что применение аппарата искусственных нейронных сетей (ИНС) автокодировщиков, генеративно-состязательных и рекуррентных ИНС полностью соответствует концепции построения диагностической поведенческой модели технологического процесса. Представленные результаты исследования моделей показали их высокую эффективность, поскольку позволяют не только обнаруживать аномалии в корпоративной сети, вызванные кибератаками, но и реализовать их локализацию. Персонал предприятия получает возможность принимать превентивные меры с целью устранения угроз информационной безопасности на производстве. В результате использования предложенных подходов ожидается значительное снижение потенциального ущерба, который могут понести металлургические предприятия в результате реализации киберинцидентов.

Ключевые слова: *автокодировщик, автоматизированная система управления технологическим процессом, генеративно-состязательная нейронная сеть, динамический процесс, зона технологического процесса, кибератака, кибервторжение, киберинцидент, киберугроза, машинное обучение, металлургическое предприятие, мони-*

[1] Исследование выполнено при финансовой поддержке РФФИ и Челябинской области в рамках научного проекта № 20-47-740006

торинг информационной системы, обнаружение аномалий, поведенческая модель, раннее обнаружение кибератак, рекуррентная нейронная сеть, энергосетевая система.

Sokolov A.N., Ragozin A.N., Barinov A.E., Ufimtcev M.S., Pyatnitskiy I.A., Bukharev D.A.

DEVELOPMENT OF MODELS AND METHODS FOR EARLY DETECTION OF CYBER ATTACKS ON ENERGY FACILITIES OF A METALLURGICAL ENTERPRISE

The need to respond to cyber incidents in the energy systems of metallurgical enterprises leads to serious consequences, such as downtime and costly restarts of production. Therefore, it is important to implement the concept of information security to "prevent" intrusions, and not "warn" about them, according to which the search for cyber threats becomes a constant background activity. This paper presents a system for the early detection of the impact of cyberattacks, developed using intelligent data processing technologies based on a model of a system of dynamic processes that reflect the behavior of an object's information system. A technique has been developed that makes it possible to obtain a numerical assessment of the need to improve the monitoring parameters for various zones of the technological process. As an example of using the methodology, a calculation based on a subsystem of the technological process of a metallurgical enterprise is given, on the basis of which the most important informative data collection points for monitoring are selected. It is shown that the use of the apparatus of artificial neural networks (ANNs) of autoencoders, generative adversarial and recurrent ANNs fully corresponds to the concept of constructing a diagnostic behavioral model of a technological process. The presented results of the study of the models showed their high efficiency, since they allow not only detecting anomalies in the corporate network caused by cyber attacks, but also their localization. The staff of the enterprise gets the opportunity to take preventive measures in order to eliminate threats to information security in production. As a result of using the proposed approaches, a significant reduction in the potential damage that can be incurred by metallurgical enterprises as a result of the implementation of cyber incidents is expected.

Keywords: *autoencoder, industrial control systems, generative adversarial neural network, dynamic process, process zone, cyber attack, cyber intrusion, cyber incident, cyber threat, machine learning, metallurgical enterprise, information system monitoring, anomaly detection, behavioral model, early detection of cyber attacks, recurrent neural network, power grid system.*

Введение.

Энергетический комплекс для металлургического производства – чрезвычайно важный элемент, от которого зависит функционирование как отдельных промышленных объектов, так и обеспечение энергоносителями

инфраструктуры, находящейся поблизости. Самая простая энергосетевая система состоит из немалого количества резервных линий, обслуживанием которых занимается большой объем оборудования, в состав которого входят коммутационные и распределительные устройства, силовые и измерительные приборы, генераторное оборудование, автоматические компенсаторы реактивной мощности и т.д. Любое из перечисленных устройств подключается к промышленной сети предприятия и управляется сложной системой, большинство действий в которой автоматизировано.

Энергетические системы, как правило, являются открытыми системами, так как взаимодействуют с другими энергосистемами, как в части учёта потреблённой электроэнергии, так и в части взаимного мониторинга нагрузки с целью её оптимального перераспределения. Поэтому площадь поверхности кибератаки на энергосетевые системы закономерно большая, и, в связи с этим, возникает необходимость мониторинга таких систем на предмет возможных кибератак. Помимо промышленного оборудования, подобные энергосетевые системы могут обеспечивать энергоснабжение ближайших промышленных объектов, жилых комплексов и социально значимых объектов. Реализация кибератаки занимает несколько минут, при этом средний показатель её идентификации составляет более ста дней. Необходимость реагирования на произошедшие инциденты в подобных энергетических комплексах приводит к серьезным последствиям, таким как простои и дорогостоящие перезапуски производства. В связи с этим для металлургических предприятий актуальной является задача реализации концепции защиты информации – «предотвращать» вторжения, а не «предупреждать» о них, согласно которой поиск киберугроз становится постоянной фоновой деятельностью. Поэтому задача разработки моделей и методов раннего обнаружения кибератак на объекты энергетики металлургического предприятия является важной.

Под «ранним» обнаружением кибератаки понимается её обнаружение в рассматриваемой системе до реализации последствий кибератаки, т.е. до необходимости реагирования на инцидент путем остановки и перезапуска системы. В предложенной работе представлена система раннего обнаружения воздействия кибератак, разработанная с использованием технологий интеллектуальной обработки данных на основе модели системы динамических процессов, отражающих функционирование (поведение) информационной системы объекта. Такая система позволяет обнаруживать ранние признаки изменения в поведении наблюдаемых динамических процессов объекта, то есть обнаруживать начало раннего развития аномалий в динамических процессах, распределённых в виде потока данных в информационной системе объекта.

В работе предложен подход, основанный на применении ИНС автокодировщиков, генеративно-состязательных и рекуррентных ИНС для анализа состояния всей автоматизированной системы управления объектами энергетики металлургических предприятий. Метод, основанный на использовании ИНС автокодировщиков, генеративно-состязательных и рекуррентных ИНС является новым в задаче обнаружения аномалий в поведении наблюдаемых динамических процессов автоматизированных систем управления при использовании машинного обучения без учителя. Модель объекта, подвергающегося воздействию кибератак, основанная на рассматриваемых в работе методах, относится к поведенческим моделям динамических процессов информационной системы. В результате использования подходов, основанных на моделях и методах раннего обнаружения кибератак, ожидается значительное снижение потенциального ущерба, который могут понести металлургические предприятия в результате реализации киберинцидентов.

Системы энергетического комплекса, обеспечивающие работу металлургического производства, обладают достаточно большим количеством контрольных точек для регистрации информативных параметров при проведении мониторинга, а также сложным зонированием исследуемой системы по важности тех или иных регистрируемых параметров. Важным является решение вопроса о том, какие данные, в каком объеме, и с какой периодичностью необходимо регистрировать, чтобы обеспечить превентивное обнаружение кибератак. Поэтому, при решении поставленной задачи важно дать описание наиболее актуальных способов регистрации информативных данных в контрольных точках исследуемой информационной системы (точки входа для мониторинга), а также разработать методику поиска наиболее приори-

тетных для мониторинга зон распределения контрольных точек исследуемой информационной системы. Как правило, при анализе имеется возможность использовать лишь ограниченный набор параметров, имеющих максимальную информативность в обеспечении безопасности технологических процессов. Задача по выбору анализируемых параметров, обладающих максимальной информативностью, сводится к необходимости выбора способа их регистрации, от которого зависит скорость получения значений, задержки фиксации параметров, стоимость получения параметров.

Задачами представленной работы являются:

1) построение концепции поведенческой модели динамических процессов информационной системы объектов энергетики металлургического предприятия, применяемой для реализации предотвращения последствий вторжений;

2) построение методики выбора контрольных точек исследуемой информационной системы и регистрации в контрольных точках параметров, обладающих максимальной информативностью, используемых при решении задачи обнаружения аномалий в наблюдаемых процессах, вызванных воздействием кибератак;

3) разработка и исследование поведенческой модели для обнаружения аномалий (обнаружения признаков кибератак) в наблюдаемых процессах информационной системы, с использованием технологий машинного обучения и ИНС автокодировщиков, а также ИНС с генеративно-состязательной и рекуррентной архитектурами.

1. Поведенческая модель динамических процессов информационной системы объектов энергетики металлургического предприятия, реализующая концепцию предотвращения последствий вторжений.

Информационная система объектов энергетики металлургического предприятия относится к сложным системам, поэтому, построение модели подобной системы базируется на принципах системного анализа [1].

В [2] отмечено, что построение адекватной модели для сложной системы невозможно, теория сложных систем должна состоять из простейших моделей нарастающей сложности, то есть грубая модель более сложной системы может быть проще точной модели более простой системы. Отмечается, что возможность построения теории сложных систем связана с возможностью построения их простых оптимизационных моделей [2]. В [3] отмечено, что при построении модели сложной системы следует руководствоваться главной целью и главным свойством исследуемой системы.

Таким образом, для построения математической модели сложной системы необходимо пойти на ослабление требований к математическому описанию исследуемой системы. При этом целесообразно использовать подход, связанный с построением диагностической модели исследуемой сложной системы, то есть модели, позволяющей достоверно оценить состояние исследуемой сложной системы. Построение диагностической модели предполагает в определённой форме идентификацию связи измеряемого вектора признаков с некоторым тестируемым свойством [4]. При этом от диагностической модели не требуется максимальной адекватности описания исследуемой системы в целом, диагностическая модель лишь предполагает описание степени отклонения технического состояния исследуемой системы от состояния, соответствующего «норме» [4].

Одной из форм построения диагностической модели является моделирование функционирования сложной системы в виде одно- или многомерных временных рядов, при этом оценка отклонения состояния исследуемой системы от «нормы» основывается на принятых допущениях о характере наблюдаемых временных рядов. В современных исследованиях оценка отклонения состояния исследуемой системы от «нормы», формируемая на основе анализа наблюдаемых временных рядов, отражающих процессы, протекающие в системе, связывается с понятием «аномалии» наблюдаемого временного ряда.

На принятых допущениях о характере наблюдаемых временных рядов, соответствующих понятию нормы исследуемой системы, строится модель временного ряда, характеризующего наблюдаемые процессы, протекающие в системы в состоянии нормы. Мера рассогласования наблюдаемого временного ряда исследуемой системы и модели временного ряда, соответствующей состоянию нормы исследуемой системы, отражает неожидаемое изменение в поведении наблюдаемых процессов, то есть аномальные изменения в динамике наблюдаемых временных рядов

данных, протекающих в исследуемой технической системе. Методы обнаружения аномалий в процессах исследуемой системы, отражаемых в виде временных рядов данных относят к поведенческим методам [5, 6].

В настоящее время методы обнаружения аномалий применяются для решения задач обнаружения кибератак как на информационном, так и на кибернетическом уровнях в сложных технических системах [7].

Кибератаки вызывают аномалии (то есть, неожидаемые изменения) в поведении наблюдаемых процессов (в динамике наблюдаемых временных рядов данных) при работе сложных технических систем. При этом задача обнаружения аномалий состоит в обнаружении расхождений между текущим (наблюдаемым) процессом работы сложной технической системы и процессом работы, который является эталонным для сложной технической системы (то есть, для системы, работающей в штатном режиме). Любое обнаруженное несоответствие наблюдаемого процесса и эталонного процесса, протекающего в сложной технической системе, рассматривается как аномалия (или кибервторжение).

Информационная система объектов энергетики металлургического предприятия относится к сложным техническим системам. Поэтому модель для раннего обнаружения кибератак и предотвращения последствий вторжений на объекты энергетики металлургического предприятия необходимо определить как диагностическую поведенческую модель процессов, протекающих в исследуемой технической системе. При этом модель процесса строится на основе временных рядов данных, наблюдаемых в исследуемой технической системе. Преимущество диагностической поведенческой модели данного типа – возможность обнаружения новых кибератак без модификации или обновления параметров модели.

Для построения диагностической поведенческой модели процессов, протекающих в информационных системах объектов энергетики металлургического предприятия целесообразно использовать интеллектуальный анализ данных, а также технологии машинного обучения, позволяющие выделять новую значимую информацию из большого объёма данных.

Значимую роль в технологическом обеспечении интеллектуального анализа данных с использованием технологии машинного обучения, в настоящее время играет аппарат искусственных нейронных сетей (ИНС). ИНС для обнаружения аномалий обучаются в течение некоторого периода времени, когда всё наблюдаемое поведение исследуемой системы считается нормальным [8, 9, 10]. После обучения нейронная сеть запускается в режиме распознавания. В ситуации, когда во входном потоке не удается распознать нормальное поведение, фиксируется аномалия, то есть факт кибератаки. В случае использования репрезентативной обучающей выборки нейронные сети дают хорошую устойчивость в пределах заданной системы.

ИНС, используемые для обнаружения аномалий в наблюдаемых процессах, можно рассматривать в контексте обнаружения аномальных образов, то есть в качестве детектора аномалий. Реализуемость детектора аномалий базируется на таком свойстве ИНС, как умение восстанавливать входную информацию на выходе. Для создания детектора аномалий необходимо составить обучающую выборку, состоящую из нормальных данных, и обучить ИНС воспроизводить на выходе нормальные данные. Тогда, если после обучения подать на вход ИНС нормальный образ, то ошибка реконструкции для входного нормального образа будет меньше, чем для входного аномального образа. При превышении ошибки реконструкции входного образа некоторого порогового значения принимается решение о принадлежности входного образа к классу аномальных образов, то есть фиксируется факт кибератаки. Для обнаружения аномальных образов наиболее подходят ИНС – автокодировщики (автоэнкодеры) [11, 12, 13, 14, 15] и генеративно-состязательные ИНС [16, 17, 18, 19].

Применение аппарата ИНС автокодировщиков, генеративно-состязательных и рекуррентных ИНС полностью соответствует концепции построения диагностической поведенческой модели, предполагающей описание степени отклонения технического состояния исследуемой системы от состояния нормы, используемой для раннего обнаружения кибератак и предотвращения последствий вторжений на объекты энергетики металлургического предприятия.

Разработанную диагностическую поведенческую модель можно отнести к технологиям, основанным на раннем обнаружении аномалий в динамических процессах, распределенных в информационной системе ис-

следуемого объекта. Поиск киберугроз, направленных на информационные системы объектов энергетики металлургического предприятия, становится постоянной фоновой деятельностью, позволяющей экономить значительные средства за счет оперативного реагирования на возникающие киберугрозы с целью предотвращения вторжений. Экономия средств также достигается за счет исключения из «ручной» обработки событий, которые не выводят качество управления объектом за пределы заданных значений [20].

2. Методика выбора контрольных точек для регистрации параметров, обладающих максимальной информативностью при решении задачи обнаружения аномалий в наблюдаемых процессах информационной системы, вызванных воздействием кибератак.

Идеальный подходом по организации мониторинга информационной системы объекта можно назвать подход, который заключается в мониторинге каждого отдельного параметра объекта. Но, при этом требуется организация сбора огромного количества данных и их оптимизация программными средствами для последующего анализа. Подобный подход является финансово затратным, поскольку требует сформированной и отлаженной системы мониторинга, где методы регистрации информативных данных оптимизированы по степени важности. Например, для получения информации с OPC-сервера (Open Platform Communications – сервера на основе программных технологий, предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами) не требуется больших финансовых вложений, если сервер уже функционирует. Однако этот подход создает гораздо большую задержку при регистрации параметров, чем, например, использование подхода на основе зеркалирования трафика с помощью TAP-устройств или коммутаторов со SPAN-портами. Такие решения требуют дополнительных финансовых затрат, однако создают меньшие задержки при регистрации информации. Это особенно важно, когда требуется высокая частота фиксации параметров технологического процесса.

В представленной работе предложена методика, позволяющая:

1) определять информативные точки для системы мониторинга с учетом специфики рассматриваемого параметра технологического процесса;

2) оценивать наиболее критичные контрольные точки фиксации информационных параметров автоматизированной системы управления технологическим процессом (АСУ ТП);

3) создавать, либо модернизировать систему мониторинга информационных процессов производственных объектов с целью повышения ее эффективности.

Для построения методики предварительно выделяются все считываемые параметры p_i технологического процесса. Для оценки каждого параметра p_i рассчитан следующий набор характеристик:

1. Нормированные значения среднеквадратической ошибки

$$RRMSE_{p_i} = \frac{\sqrt{\frac{1}{N} MSE_{p_i}}}{\max(p_i) - \min(p_i)},$$

где MSE_{p_i} – среднеквадратическая ошибка параметра p_i, N – количество измерений, используемых для расчета ошибки.

Параметр MSE_{p_i} определяет, насколько величина p_i отклоняется от усредненного значения на заданном временном интервале.

2. По рассчитанным значениям параметра $RRMSE_{p_i}$ вычисляется вес параметра $RRMSE_{p_i}$ – w_{RRMSE} [21] (табл. 1).

Таблица 1

Таблица весов нормированных значений среднеквадратической ошибки считываемых параметров технологического процесса

Значения $RRMSE_{p_i}$	**Вес w_{RRMSE}**
RRMSE > 0.5	0.1
0.5 > RRMSE > 0.25	0.5
0.25 > RRMSE > 0.1	0.75
0.1 > RRMSE > 0	1

3. Величина *FTTI* – промежуток времени от возникновения аномального состояния наблюдаемого информационного процесса (от выхода величины из нормального диапазона значений) до наступления аварийной ситуации в технологическом процессе [22].

Параметр *FTTI* устанавливается экспертным путем и вычисляется в секундах. Параметр *FTTI* необходимо нормализовать в пределах от 0 до 1 относительно остальных параметров p_i и вычислить итоговый вес параметра $w_{FTTI}=1\text{-}FTTI_{norm}$. В итоге получим величину, отражающую, насколько критичны быстрые изменения параметра вне нормального диапазона изменения величины p_i, характеризующего технологический процесс.

4. Величина w_r отражает релевантность параметра для модели машинного обучения. Типовая АСУ ТП на большом производстве может характеризоваться большим количеством параметров, при этом не все параметры могут быть информативными при обнаружении аномалий средствами машинного обучения. Для расчета параметра w_r рассчитывается метрика релевантности для каждого параметра p_i. Для этого используется один из методов отбора признаков с дальнейшим получением показателя важности параметра.

5. Величина w_k – доля полезной информации в информационном потоке [23]. Величина w_k отражает процентное соотношение информации, которую возможно использовать для получения сведений о структуре системы.

6. Величина w_m – соотношение генерируемых данных ко всем данным. Корректная работа моделей машинного обучения обеспечивается наборами данных, в которых отсутствуют пустые значения, появившиеся, например, из-за задержек при съеме состояния параметра технологического процесса. Недостающие значения генерируются с использованием статистических методов. Параметр w_m вычисляется как

$$w_m = 1 - \frac{d_{gen}}{d_{tot}},$$

где d_{gen} – количество сгенерированных значений, d_{tot} – общее количество данных.

7. Величина w_f – вес частота съема сигнала: отражает, насколько быстро изменяются значения параметра технологического процесса. Задается экспертным путем (табл. 2).

Таблица 2

Таблица весов частоты съема сигнала

Характеристика частоты съема сигнала	w_f
Очень медленная	0.1
Медленная	0.4
Средняя	0.7
Быстрая	0.9
Очень быстрая	1

Необходимо отметить, что оценка влияния каждого (считываемого при мониторинге) параметра p_i на технологический процесс выполняется исходя из соображений критичности с использованием различных риск-ориентированных моделей, внедряемых обычно в различных государствах на законодательном уровне. В приведенном примере расчета использована четырехуровневая модель категорирования.

8. Кроме параметров критичности с каждым технологическим объектом обычно сопоставляют меры функциональной безопасности [24], для этого используют понятие уровня полноты безопасности SIL, который представляет собой величину, отражающую способность системы обеспечивать выполнение функций безопасности. Всего существует 5 уровней SIL со значениями от 0 (минимальная функциональная безопасность) до 4 (максимальная функциональная безопасность).

9. Величина w_t – параметр влияния. Обозначим требуемый уровень защищённости как SL_T (определяемый исходя из моделей рисков [25, 26]), а достигнутый как SL_A. Уровни SL нормируются от 0 до 4, где 0 – отсутствие требуемых или применённых мер защиты. Тогда для каждого параметра p_i параметр влияния вычисляется как

$$w_i = 0{,}16 \times \frac{SIL+1}{C} \times \frac{SL_T+1}{SL_A+1},$$

где C – уровень критичности в зависимости от степени ущерба. В методике использованы категории безопасности объектов критической информационной инфраструктуры, применяемые в российском законодательстве, где 1 – самый высокий уровень критичности, 3 – самый низкий. Для удобства расчётов введен уровень 4 (отсутствие критичности) для объектов, не соответствующих критериям даже минимального уровня 3.

Коэффициент 0,16 применяется для нормирования значения w_i в диапазоне [0; 1].

10. Итоговый вес важности параметра p_i, определяемый как W_{pi} вычисляется по формуле

$$W_{p_i} = \frac{(w_{RRMSE}+w_{FTTI}+w_r+w_m+w_f+w_i+w_k)}{7}.$$

Зная итоговый вес важности W_{pi} параметра p_i, определим необходимый способ мониторинга сигнала p_i.

11. Обозначим способ получения информации индексом j, который может принимать следующие значения: 4 – отсутствие мониторинга, 3 – получение параметра технологического процесса путем выгрузки из базы данных, 2 – подключение напрямую к SCADA или OPC-серверу, 1 – получение данных с минимальными задержками с использованием SPAN-портов и TAP-устройств. Время получения выгрузки обозначим безразмерной величиной t_j.

Величина R_Z – относительное улучшение мониторинга, которое определяется как

$$R_Z = t_{Aj}/t_{Tj},$$

где t_{Aj} – текущее время, t_{Tj} – прогнозируемое время после добавления средства мониторинга.

Пусть в зоне (или тракте) Z обрабатывается Z_n параметров АСУ ТП, тогда рассчитав итоговый вес W_{pzi} для каждого параметра p_{Zi}, можно выразить общий ранг улучшения (для зоны или тракта), как

$$R_Z = \frac{t_{AjZ}}{t_{TjZ}} \times \sum_{i=1}^{n_Z} W_{pZi}.$$

В качестве примера расчет параметра W_{pi} выполнен для АСУ ТП электрометаллургического предприятия, контролирующей 6 параметров. Схема АСУ ТП приведена на рис. 1. АСУ ТП разделена на условные 4 зоны, обозначенные на схеме как *Z1, Z2, Z3* и *Z4*. Эти зоны требуются для расчета ранга улучшения. При этом параметры в зоне *Z1* собираются путем выгрузки из базы данных, в зонах *Z2* и *Z3* постоянный мониторинг отсутствует, а в зоне *Z4* параметры получаются путём сбора со SCADA-сервера.

Параметры исследуемого технологического процесса и их описание представлены в табл. 3.

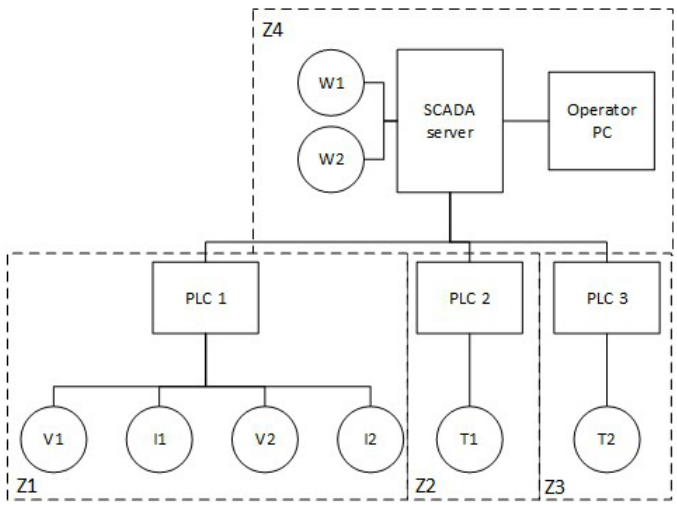


Рис. 1. Схема исследуемой АСУ ТП

Таблица 3

Параметры исследуемой АСУ ТП

Зоны	SIL	C	SL_T	SL_A	Обозначение параметра	Значение (описание) параметра
Z1	2	2	3	2	V1	Напряжение индукционной печи №1
					I1	Ток индукционной печи №1
					V2	Напряжение индукционной печи №2
					I2	Ток индукционной печи №2
Z2	2	2	4	2	T1	Температура в индукционной печи №1
Z3	2	2	4	2	T2	Температура в индукционной печи №2
Z4	2	2	3	2	W1	Мощность индукционной печи №1
					W2	Мощность индукционной печи №2

В табл. 4 приведены результаты расчетов характеристик модели. При расчете параметра w_i были использованы значения *SIL, C,* SL_T и SL_A из табл. 3.

Таблица 4

Значения характеристик модели для параметров АСУ ТП

p	w_{RRMSE}	w_{ETTI}	w_r	w_k	w_m	w_f	w_i	W_p
V1	1.00	0.08	0.04	0.40	0.85	0.70	0.32	0.48
I1	0.50	0.12	0.09	0.50	0.95	0.40	0.32	0.41
V2	1.00	0.09	0.07	0.30	0.80	0.70	0.32	0.47
I2	0.75	0.08	0.04	0.50	0.90	0.40	0.32	0.43
T1	0.75	0.29	0.49	0.80	1.00	0.70	0.40	0.63
T2	0.10	0.37	0.24	0.90	0.80	0.90	0.40	0.53
W1	0.75	0.06	0.04	0.50	1.00	1.00	0.32	0.52
W2	0.75	0.07	0.03	0.50	1.00	1.00	0.32	0.52

Далее для каждой из трех зон рассчитан прогнозируемый ранг улучшений R_Z. С учётом финансовых возможностей предприятия сделано предположение, что имеется возможность установки средств мониторинга на один уровень выше для зон *Z1 – Z3*, а в зоне *Z4* улучшения провести невозможно.

Результаты расчета ранга улучшения для каждой зоны приведены в табл. 5.

Таким образом, при распределении бюджета на выполнение соответствующих улучшений в АСУ ТП возможно применять существующее ранжирование, бюджет может распределяться пропорционально полученным рангам, или же некоторые зоны и тракты могут игнорироваться по порогу. В нашем случае зона может считаться самой приоритетной при мониторинге технологического про-

Таблица 5

Значения для зон АСУ ТП

Зона	t_{Aj}/t_{Tj}	$\sum W_{pz_i}$	R_z
Z1	1.5	1.79	2.685
Z2	1.33	0.63	0.838
Z3	1.33	0.53	0.705
Z4	1	1.04	1.040

цесса по части оптимизации программно-аппаратных средств контроля параметров технологического процесса.

Представленная в методике модель позволяет получать численную оценку необходимости улучшения мониторинга для разных зон технологического процесса. Технически это дает возможность оптимизировать систему мониторинга для существующих производств, где требуется внедрение решений по поиску аномалий, либо выбрать только наиболее критичные точки съема информации для оптимизации входного набора данных для дальнейшего исследования методами машинного обучения. В качестве примера использования методики приведен расчет на основе части технологического процесса металлургического предприятия, на основании которого выбраны наиболее важные точки регистрации данных для системы мониторинга.

3. Методы обнаружения и классификации нехарактерных состояний (аномальных изменений в динамических процессах) АСУ ТП.

Для разработки диагностической поведенческой модели исследованы методы обнаружения и классификации аномальных состояний информационных процессов с использованием ИНС автокодировщиков, генеративно-состязательных и рекуррентных ИНС [27, 28, 29].

Первый представленный метод – обнаружение аномалий с использование ИНС автокодировщиков. Автокодировщики представляют собой нейронные сети, обладающей особой архитектурой, позволяющей применять обучение без учителя, используя метод обратного распространения ошибки. Простейшая архитектура автокодировщика представляет собой сеть прямого распространения без обратных связей, и содержащая входной слой, промежуточный слой и выходной слой. Выходной слой автокодировщика должен содержать столько же нейронов, сколько и входной слой. Основ-

ной принцип работы и обучения сети автокодировщика — получить на выходном слое отклик, наиболее близкий к входному. Чтобы решение не оказалось тривиальным, на промежуточный слой автокодировщика накладывают ограничения: промежуточный слой должен быть или меньшей размерности, чем входной и выходной слои, или искусственно ограничивается количество одновременно активных нейронов промежуточного слоя — разрежённая активация. Эти ограничения заставляют ИНС искать обобщения в поступающих на вход данных, выполнять их сжатие. Таким образом, ИНС автоматически обучается выделять из входных данных общие признаки.

Автокодировщик состоят из двух частей: кодировщика и декодировщика. Кодировщик *g* переводит входной сигнал *x* в его представление (код) *h*:

$$h=g(x),$$

а декодер *f* восстанавливает сигнал *x* по его коду *h*:

$$x=f(h).$$

Автокодировщик, изменяя декодер *f* и кодировщик *g*, стремится выучить тождественную функцию $x=f(g(x))$, минимизируя некоторый функционал ошибки

$$L(x, f((g(x)))).$$

При этом семейства функций кодировщика и декодера ограничены, чтобы автокодировщик был вынужден отбирать наиболее важные свойства сигнала.

Для проведения вычислительных экспериментов был использован набор данных Power System Attack Dataset. Данный набор сгенерирован из различных наборов, содержащих 37 сценариев аномальных ситуаций, происходивших на объектах энергетики. Схема конфигурации, задействованной в данном наборе, приведена на рис. 2. Исходный набор данных был разделен на две части – тренировочный набор (80% данных) и контрольный набор (20% данных). Перед применением метода была проведена предварительная обработка данных, включая удаление строк с пустыми данными и нормализацию значений.

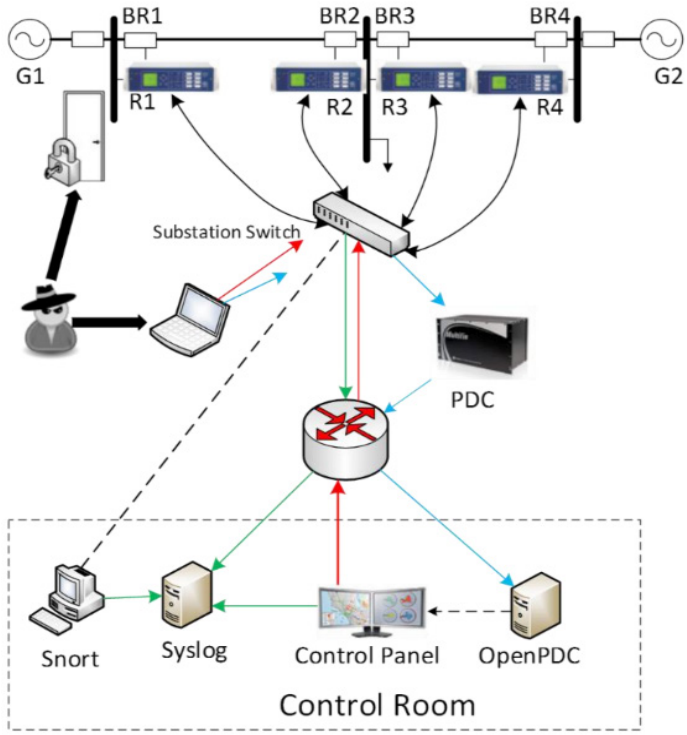


Рис. 2. Конфигурация энергетической системы Power System Attack Dataset

Архитектура ИНС автокодировщика, которая была использована для проведения вычислительных экспериментов, представлена на рис. 3.

Некоторые экспериментальные значения представлены в табл. 6.

Обозначения, использованные в табл. 6:

Bottleneck size – число нейронов в самом малом слое автокодировщика (чем меньше значение, тем больше потеря информации);

epochs – максимальное количество эпох при обучении;

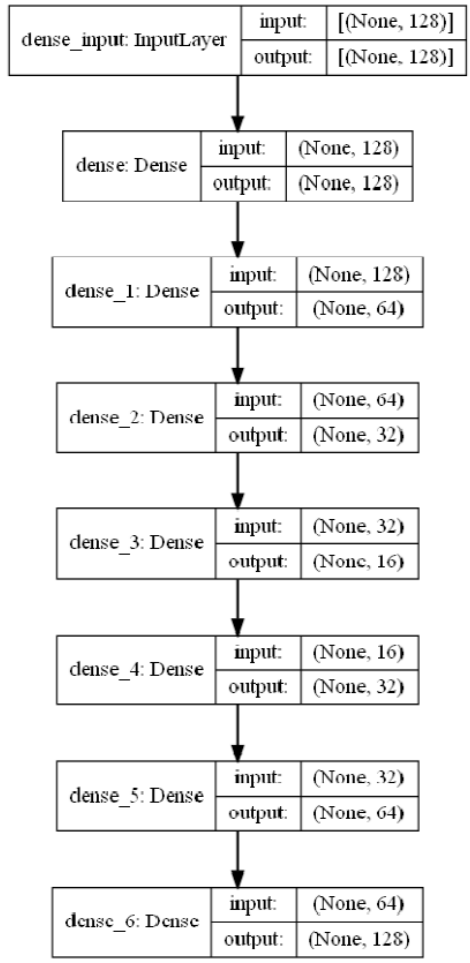


Рис. 3. Архитектура ИНС автокодировщика

Таблица 6

Результаты работы ИНС автокодировщика

Bottleneck Size	epochs	batch size	Naturals percent, %	id
16.0	50.0	16.0	95	POW1-60
16.0	50.0	16.0	90	POW1-61
16.0	50.0	16.0	85	POW1-62
16.0	50.0	16.0	80	POW1-52
16.0	50.0	16.0	75	POW1-63
16.0	50.0	16.0	70	POW1-64
16.0	50.0	16.0	65	POW1-53
16.0	50.0	16.0	60	POW1-54
16.0	50.0	16.0	55	POW1-77
16.0	50.0	16.0	50	POW1-78

batch size – число точек, используемых при обучении за момент времени (чем больше количество, тем меньше влияет на результат отдельная точка);

naturals percent – соотношение «нормальных» точек к их общему количеству;

id – идентификатор данных.

На рис. 4, 5 и 6 показаны, соответственно, зависимости метрик точности (precision), полноты (recall) и значения F_1-меры от порога отсечения. Точность (precision) интерпретируется как доля значений данных, названных автокодировщиком аномальными и при этом действительно являющимися аномальными,

а полнота (recall) показывает, какую долю аномальных данных из всего множества аномальных данных обнаружил автокодировщик. F_1-мера представляет собой агрегированный критерий качества, объединяющий precision и recall:

$$F_\beta = (1 + \beta^2) \frac{precision \cdot recall}{(\beta^2 \cdot precision) + recall}, \quad (1)$$

где β – вес точности в метрике, при $\beta = 1$ F_1 – это среднее гармоническое с множителем 2, чтобы в случае precision = 1 и recall = 1 иметь $F_1 = 1$.

Порог отсечения является настраиваемым параметром и определяет чувствительность метода по обнаружению аномальных данных. Оператор системы в зависимости от ситуации может изменять порог отсечения, получая большее количество сообщений об аномалиях, но с меньшей точностью, или наоборот, получая меньшее количество сообщений об аномалиях, но с большей точностью.

Из табл. 6 и рисунков видно, что представленный подход обладает достаточно хо-

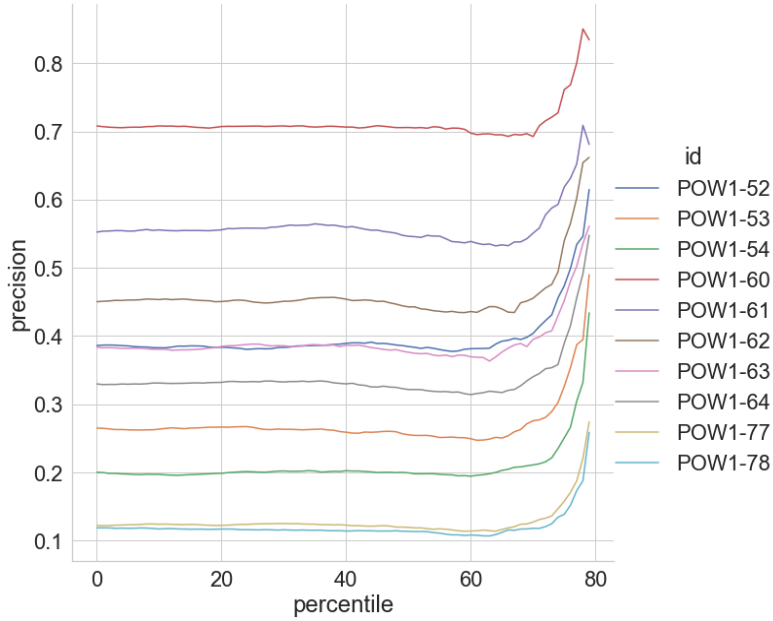


Рис. 4. Зависимость метрики точности от порога отсечения

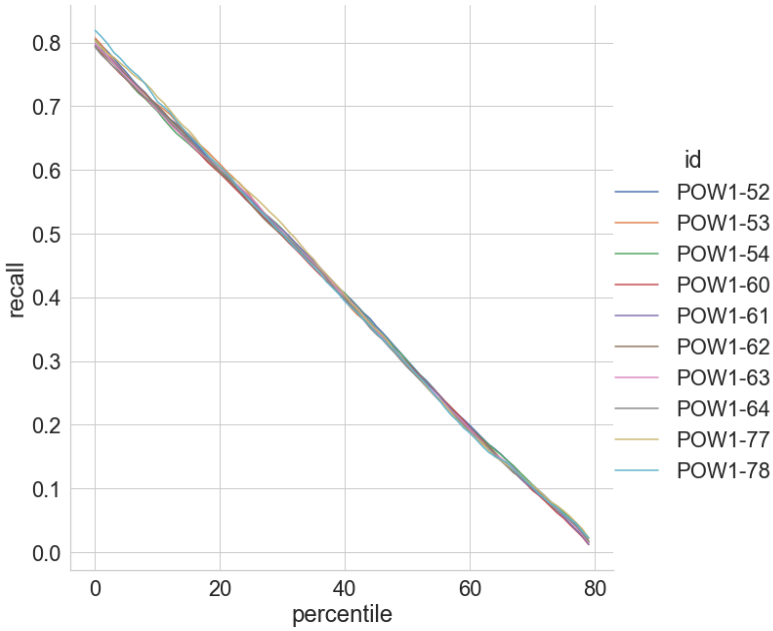


Рис. 5. Зависимость метрики полноты от порога отсечения

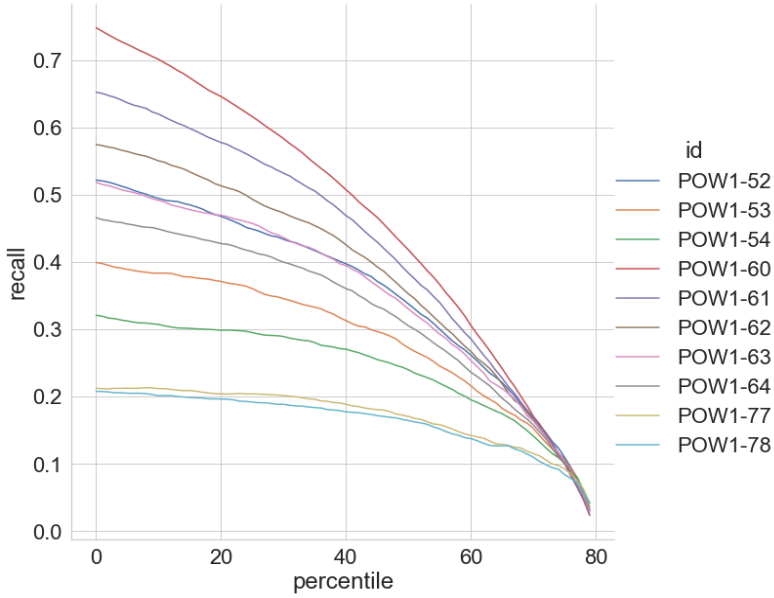


Рис. 6. Зависимость значения F1-меры от порога отсечения

рошей точностью (>0.6) при большом пороге отсечения (>95%), но наиболее оптимальные результаты достигаются тогда, когда количество аномальных состояний составляет не более 10% в общем объёме данных. При достижении данного условия, точность метода возрастает до 0.85.

Результаты, полученные при помощи автокодировщика, показывают, что данный метод возможно использовать для обнаружения аномалий в объектах энергетики, при учете того, что количество аномальных состояний в общем объёме регистрируемых данных будет не более 10%.

Второй представленный метод – обнаружение аномалий с использованием генеративно-состязательных нейронных сетей (Generative adversarial network, GAN). Генеративно-состязательные нейронные сети – это класс ИНС, который используется для генерации новых синтетических данных, основанных на имеющихся данных. Концептуально генеративно-состязательные сети основаны на идее состязательного обучения. На сегодняшний день, сети GAN используются для генерации изображений [30, 31, 32], звука [33], текста [34]. Кроме того, говоря о применении генеративно-состязательных сетей в контексте информационной безопасности, нужно отметить, что по сравнению с другими моделями глубокого обучения, GAN обладают преимуществом в случае атаки (adversarial attack) [35] со стороны злоумышленника: благодаря своей состязательной природе, обмануть такие сети сложнее, чем обычные дискриминативные модели.

Архитектура GAN включает две модели: генератор *G*, порождающий на основе вектора шума новые, похожие на настоящие, объекты в пространстве данных, и дискриминатор *D*, целью которого является отличить порождаемые генератором объекты от реальных данных – поэтому архитектура и называется генеративно-состязательной. Схема генеративно-состязательной сети представлена на рис. 7.

Генератору *G* на вход подаётся вектор, состоящий из случайного шума – вектор из некоторого пространства скрытых переменных (latent space) *Z*, на котором задано априорное распределение $p_z(z)$. На выходе генератор выдаёт новый объект из пространства данных *X*. Формально сеть-генератор можно описать в виде функции

$$G=G(z;\theta_g):Z\rightarrow X,$$

где θ_g – параметры сети-генератора. В ходе обучения генератор аппроксимирует распределение p_{data} выборки реальных данных *X*. Следовательно, по окончании обучения распределение порождаемых генератором объектов p_{gen} должно быть приближенно к распределению реальных объектов p_{data}.

Для того, чтобы генератор с каждой итерацией обучения обладал лучшей аппроксимацией распределения p_{data}, используется сеть дискриминатор. Дискриминатор, как правило, является обычным бинарным классификатором, на вход которому подаётся

Рис. 7. Схема ИНС с генеративно-состязательной архитектурой (GAN)

объект *x* из пространства данных *X*. На выходе дискриминатор выдаёт вероятность принадлежности объекта к тому или иному классу: реальный объект или объект, порождённый дискриминатором. Формально дискриминатор определяется выражением

$$D=D(x;\theta_d):X\rightarrow[0,1],$$

где θ_d – параметры сети-дискриминатора. Чтобы аппроксимировать распределение p_{data}, генератору нужно научиться обманывать дискриминатор: научиться порождать такие объекты, которые дискриминатор не в состоянии отличить от настоящих.

Для использования генеративно-состязательных сетей для решения задачи обнаружения аномалий необходимо обладать возможностью получать информацию о прообразах реальных объектов в пространстве шума, представленном найденными сетью признаками. Такая возможность реализована в двунаправленной генеративно-состязательной сети (Bidirectional GAN, BiGAN) [36]. Схема такой генеративно-состязательной сети представлена на рис. 8.

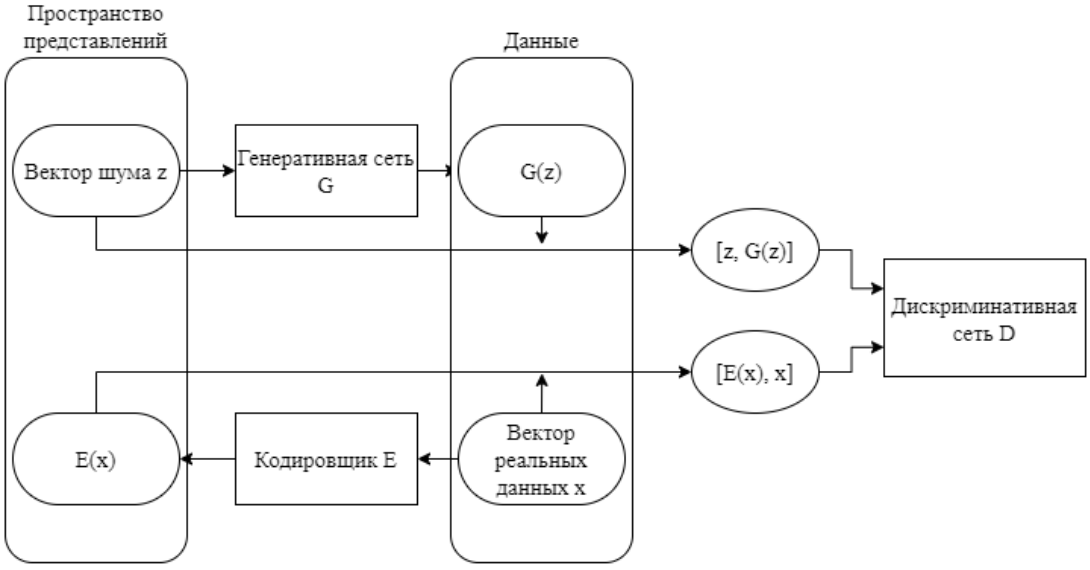


Рис. 8. Схема двунаправленной генеративно-состязательной сети (BiGAN)

По сравнению с базовой архитектурой генеративно-состязательной сети, архитектура BiGAN дополнительно использует кодирующую сеть E, которая осуществляет преобразование из пространства реальных данных в пространство скрытых переменных (из которого берётся вектор шума для генератора). Формально это действие можно представить в виде функции:

$$E=E(x;\theta_e):X\rightarrow Z,$$

где θ_e – параметры сети-кодировщика.

Таким образом, сеть-кодировщик в процессе обучения учиться выполнять преобразование, обратное генератору. Также в архитектуре BiGAN сеть-дискриминатор обучается различать не только порожденные генератором объекты и объекты из реальных дан-

ных, но и векторы из пространства скрытых переменных Z (используемые для порождения объектов) и результат отображения кодировщика $E(x)$.

Добавление сети-кодировщика в архитектуру генеративно-состязательной сети, которая каждому объекту из пространства данных x ставит в соответствие вектор z из пространства скрытых переменных, позволяет непосредственно извлекать представления этих объектов. С точки зрения семантики, вектор z репрезентирует признаки объекта , выявленные в процессе обучения BiGAN. Именно это свойство позволяет использовать BiGAN для выявления аномалий [37].

Один из подходов к использованию BiGAN для обнаружения аномалий состоит в построении метрики аномальности объекта A, основанной на выпуклой комбинации (convex combiantion) функции потерь реконструкции и функции потерь дискриминатора:

$$A(x)=aL_G(x)+(1-a)L_D(x),$$

где $L_G(x)$ – функция потерь реконструкции, определяемая как модуль разности исходного вектора, репрезентирующего объект, и вектора, полученного последовательным преобразованием объекта кодировщиком и генератором:

$$L_G(x)=||x-G(E(x))||.$$

$L_D(x)$ – функция потерь дискриминатора:

$$L_D(x)=$$

где σ – кросс-энтропия (логарифмическая функция потерь) дискриминатора, при условии, что объект x является настоящим, а не порожден генератором.

Таким образом, обученная на данных, соответствующих нормальному состоянию, сеть BiGAN применяется к новому объекту, после чего вычисляется значение метрики аномальности A для объекта. Чем выше значение этой метрики, тем более вероятно, что объект является аномальным.

Для применения генеративно-состязательной сети BiGAN были реализованы модели генератора, дискриминатора и кодировщика. Каждая из этих моделей является обычной полносвязной сетью. Разработанная генеративно-состязательная нейронная сеть испытана на наборе данных, полученных с лабораторного стенда Secure Water Treatment (SWaT) [38], схема которого представлена на рис. 9. Каждая запись набора состоит из 51 значения сенсора или привода, всего в наборе содержалось 964722 записи, записанных за 11 дней. Имитационные атаки проводились в течение 4 дней.

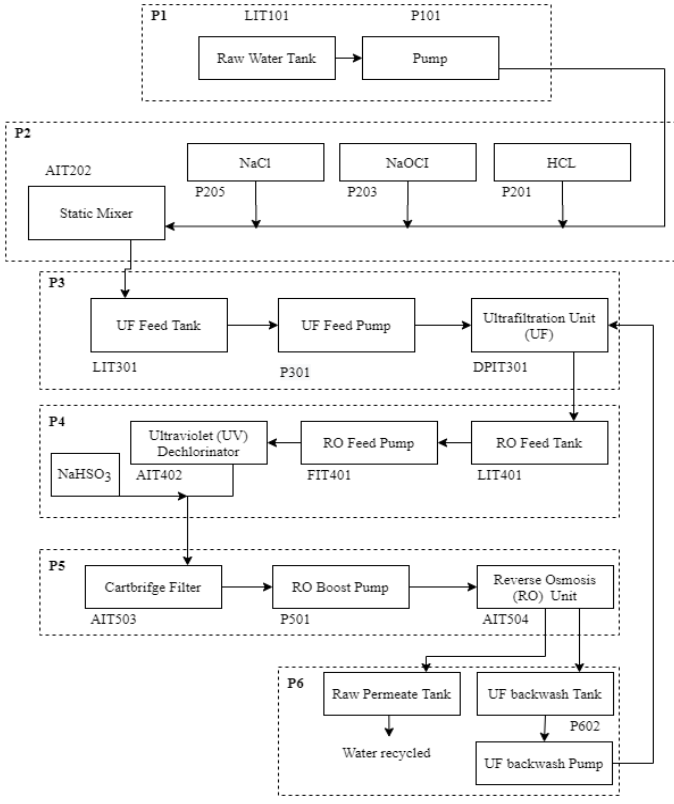


Рис. 9. Схема стенда SWaT

Обучающая выборка включает в себя данные, соответствующие нормальной работе системы. Контрольная выборка состоит из данных, полученных в период проведения атак. Данные были приведены к одному масштабу, после чего BiGAN обучалась исключительно на данных, соответствующих нормальной работе системы. После этого, к контрольной выборке применялась обученная модель, для каждого объекта контрольной выборки строилась метрика аномальности. В ходе проведения эксперимента, модели обучались в течение 20 эпох. На рис. 10, 11 и 12 представлены графики функций потерь каждой из моделей.

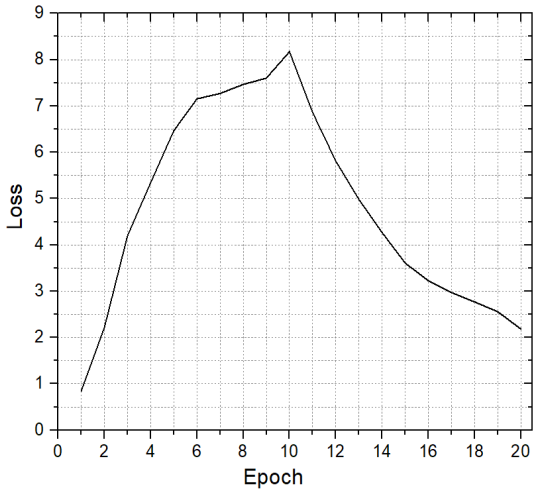


Рис. 10. Функция потерь генератора

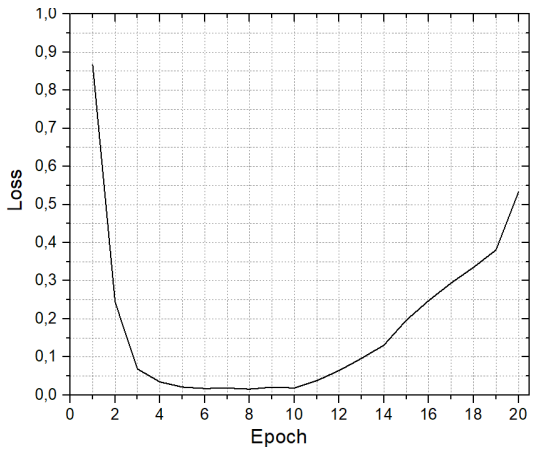


Рис. 11. Функция потерь дискриминатора

Графики функций потерь генератора, дискриминатора и кодировщика, представленные на рис. 10 – 12, отражают процесс обучения модели BiGAN: чем лучше работает дискриминатор, тем хуже работают генератор и кодировщик, и наоборот. Точка, в которой

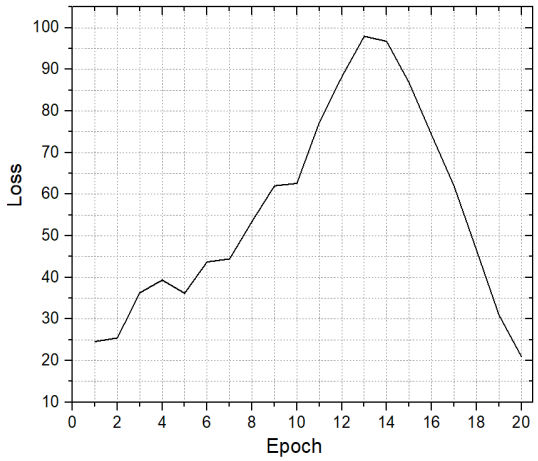


Рис. 12. Функция потерь кодировщика

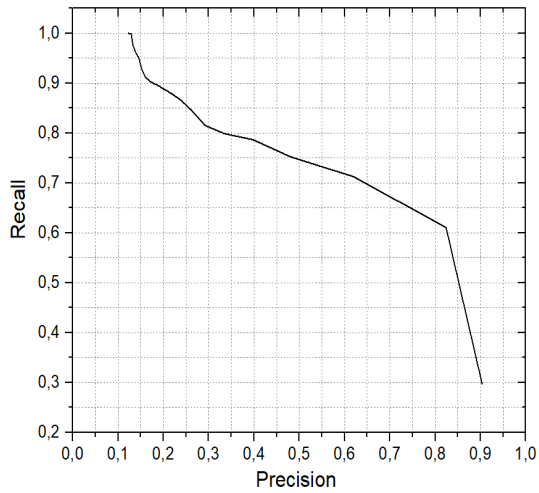


Рис. 13. Зависимость метрик точности (precision) и полноты (recall)

был остановлен момент обучения (20 эпоха), соответствует состоянию модели, при котором кодировщик и генератор работают лучше дискриминатора. Дальнейшее обучение позволяет ещё больше снизить значения функций потерь генератора и кодировщика, однако в этом случае, модель BiGAN утрачивает свою эффективность на стадии тестирования.

Качество работы обученной модели на практике во многом определяется не только тем, насколько хорошо модель научилась аппроксимировать распределение данных, соответствующих нормальной работе системы, но и конкретным значением порога метрики аномальности. Так, на рис. 13 представлена зависимость метрик точности и полноты в зависимости от порогового значения. При увеличении порогового значения увеличивается точность и уменьшается полнота. Это свой-

ство позволяет настроить желаемое поведение модели в каждом конкретном случае.

Для оценки качества работы модели использовались метрики точность (precision) и полнота (recall). Конкретные значения метрик качества определяются величиной порога для метрики аномальности. Как показано на рис. 13, при увеличении порога увеличивается значение метрики precision и уменьшается значение метрики recall.

По полученным результатам видно, что разработанная сеть может использоваться для обнаружения аномальных состояний. При этом генеративно-состязательные сети не требуют примеров данных, соответствующих аномальной работе системы, что повышает их эффективность в практическом использовании.

Третий представленный метод – обнаружение аномалий с использованием рекуррентных нейронных сетей, реализующих прогнозирование входного наблюдаемого временного ряда данных. Рекуррентные нейронные сети – это тип нейронных сетей, которые имеют соединения с обратной связью (рекуррентные соединения). Преимущества наличия таких связей состоит в том, что они позволяют запоминать предыдущее состояние и учитывать его при подсчете весов. Все рекуррентные сети имеют цепную структуру: повторяющуюся клетку. Клеткой может быть единственный нейрон или последовательность нескольких. Рассмотрим простую Recurrent Neural Network (RNN) клетку. Она имеет очень простую структуру: только один слой с функцией активации *than* (гиперболический тангенс). Пусть имеется последовательность входных данных $\{x_t\}_{t=1}^{T}$. В данном случае $x_t = (x_1^t, \dots, x_n^t)$ – векторное представление *t*-ого объекта во временном ряде. В каждый момент времени *t*, клетка анализирует объект x_t и предсказание прошлого объекта H_{t-1}. Именно в этом и проявляется рекуррентность сети.

Для целей данной работы использована ИНС Long Short Term Memory (LSTM). Сеть LSTM – особый вид рекуррентной нейронной сети, способный находить долго- и краткосрочные зависимости. LSTM также имеют цепную структуру, но повторяющаяся клетка имеет более сложное строение: она состоит из четырех нейронов, соединенных специальным образом. Структурная схема сети LSTM представлена на рис. 14.

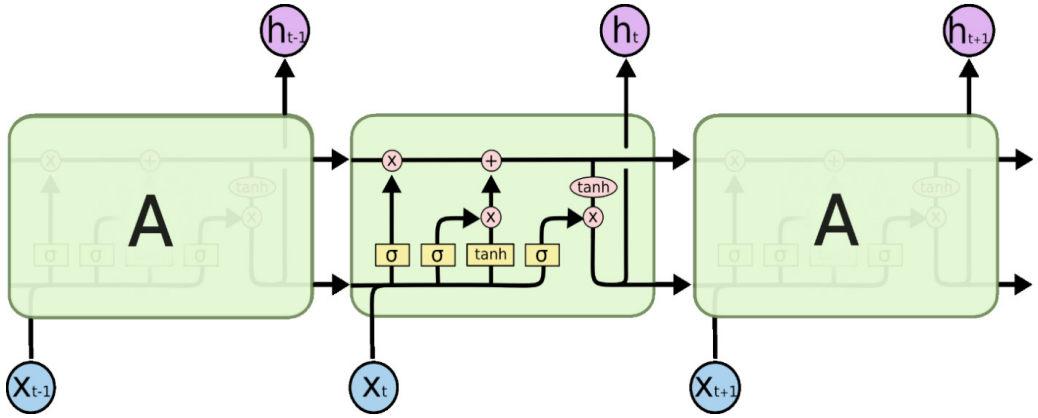


Рис. 14. Структурная схема ИНС LSTM

В работе было использована архитектура рекуррентной нейронной сети, состоящей из одномерного сверточного слоя, слоя отсева (для избегания переобучения), двух слоев LSTM и полносвязного выходного слоя. Функция Swish была использована в качестве функции активации для слоев LSTM. Предложенная сеть обрабатывает поданные на вход данные о состоянии объекта и на выходе выдает состояние объекта в следующий момент времени. Схема архитектуры ИНС представлена на рис. 15.

Разработанная нейронная сеть испытана на наборе данных, полученных с лабораторного стенда Secure Water Treatment (SWaT), который был уже описан ранее.

Результаты сравнения представленного метода обнаружения аномалий с другими методами приведены в табл. 7. Сравнение проводилось по метрикам точности (precision), отзыва (recall) и показателя F_1 (F_1-Score), определяемого формулой (1). По данным таблицам видно, что предложенный метод обладает достаточно высоким показателем F_1, усту-

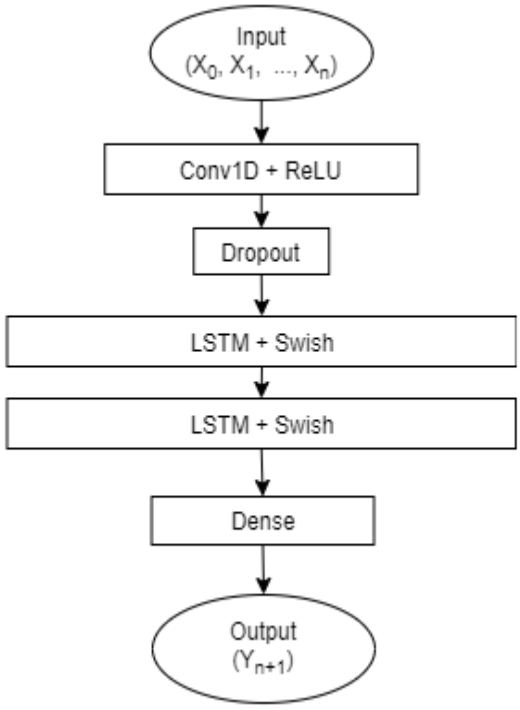


Рис. 15. Схема архитектуры ИНС LSTM

пая только методу 1D CNN. Относительно показателей точности и отзыва, предложенный метод обладает сравнимыми характеристиками и его использование возможно с целью обнаружения аномалий. Предложенный метод позволяет определить, в каком конкретном датчике произошла аномальная ситуация, что позволяет операционному персоналу объекта оперативно проанализировать ситуацию и принять необходимые превентивные меры для обеспечения информационной безопасности.

Для демонстрации качества работы представленной модели построена ROC-кривая, отображающая связь между истинно-положительными и ложноположительными результатами при разных порогах отсечки (рис. 16). О хорошей эффективности метода ИНС LSTM свидетельствует значительная отдаленность ROC-кривая от диагональной линии.

Заключение

Информационные системы объектов энергетики металлургического предприятия относится к сложным техническим системам. Поэтому модель для раннего обнаружения кибератак и предотвращения последствий вторжений на такие объекты определена как диагностическая поведенческая модель процессов, протекающих в исследуемой технической системе, которая строится на основе наблюдаемых временных рядов данных. Преимущество диагностической поведенческой модели такого типа заключается в возможности обнаружения новых кибератак без модификации или обновления параметров модели.

Таблица 7

Сравнение метода с применением ИНС LSTM с другими методами обнаружения аномалий

Метод	Precision	Recall	F_1-Score
1D CNN	0.968	0.791	0.871
MLP	0.967	0.696	0.812
CNN	0.952	0.702	0.808
RNN	0.936	0.692	0.796
DNN	0.982	0.678	0.802
OCSVM	0.925	0.699	0.796
LSTM	0.934	0.820	0.865

С целью выбора контрольных точек для регистрации параметров временных рядов данных, обладающих высокой информативностью при решении задачи обнаружения аномалий в наблюдаемых процессах информационной системы, вызванных воздействием кибератак, разработана соответствующая методика. Представленная в методике модель позволяет получить численную оценку необходимости улучшения для различных зон технологического процесса. Технически это позволяет сформировать такую систему мониторинга для производства, которую можно было бы считать достаточной для решения задач поиска аномалий наблюдаемых процессов и выбирать наиболее критичные точки регистрации данных для оптимизации входного набора данных для дальнейшего

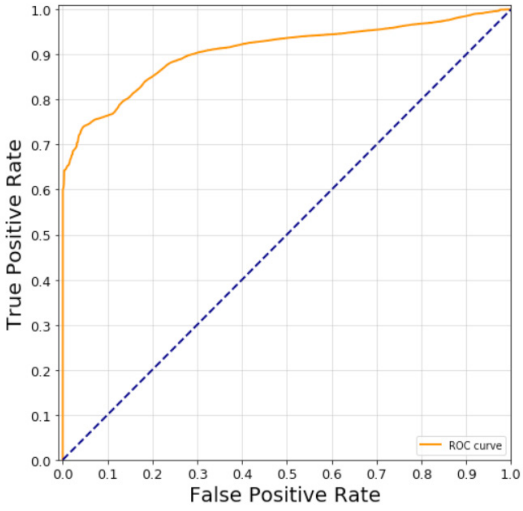


Рис. 16. ROC-кривая метода ИНС LSTM

исследования методами машинного обучения.

В ходе проведённого исследования показано, что применение аппарата ИНС автокодировщиков, генеративно-состязательных и рекуррентных ИНС полностью соответствует концепции построения диагностической поведенческой модели, предполагающей описание степени отклонения технического состояния исследуемой системы от состояния нормы, используемой для раннего обнаружения кибератак и предотвращения последствий вторжений на объекты энергетики металлургического предприятия.

Результаты, полученные авторами в ходе представленных исследований, обсуждены на международных конференциях «2021 IEEE Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology» (USBEREIT-2021, 13 – 14 мая 2021 г., г. Екатеринбург) и «International Russian Automation Conference» (RusAutoCon-2021, 5 – 11 сентября 2021 г., г. Сочи). Группой авторов выполнены также исследования, связанные с разработкой перспективных технологий иерархического кластерного анализа данных информационных процессов АСУ ТП, подвергающихся воздействию кибератак. Выполненные исследования представлены на международной конференции «International Multi-Conference on Industrial Engineering and Modern Technologie FarEastCon-2021» (FarEastCon-2021, 5 – 8 октября, 2021 г., г. Владивосток).

Литература

1. Волкова В.Н. Основы теории систем и системного анализа / В.Н. Волкова, А.А. Денисов. – СПб: Изд-во СПбГТУ, 1999. – 512 с.

2. Флейшман Б.С. Основы системологии / Б.С. Флейшман. – М.: Радио и связь. 1982. – 368 с.

3. Тырсин А.Н. О математическом моделировании сложных организационных систем // Организация и управление эффективностью и производительностью производственных и социальных систем: Матер. межд. научно-практ. конф. – Новочеркасск: ЮРГТУ (НПИ), 2005. – С. 49 – 50.

4. Биргер И.А. Техническая диагностика. – М.: Наука, 1978. – 239 с.

5. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems // Computer Networks. 1999. vol. 31. Issue 8. pp. 805 – 822.

6. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак. – Труды СПИИРАН. – 2016. – Вып. 45 – С. 207 – 244.

7. Абдулин А.А., Соколов А.Н. Исследование программных решений для обеспечения информационной безопасности промышленных сетей автоматизированных систем управления технологическими процессами //Вестник УрФО. Безопасность в информационной сфере. – 2021. № 1(39). – С. 43 – 53.

8. Herve Debar, Monique Becker, and Didier Siboni. A neural network omponent for an intrusion detection system //Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy, pages 240–250, Oakland, CA, USA, May 1992.

9. Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari. Detection of Distributed Denial of Service Attacks Using Statistical Pre- Processor and Unsupervised Neural Networks // Lecture notes in computer science, 2005.

10. Смелянский Р.Л., Качалин А.И. Применения нейросетей для обнаружения аномального поведения объектов в компьютерных сетях //Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва, 2004.

11. Neural network and artificial immune systems for malware and network intrusion detection / V. Golovko [et al.] // Studies in computational intelligence. – Heidelberg, 2010. – Vol. 263 : Advances in machine learning II. – P. 485 – 513.

12. Muna A.H., Moustafa N. & Sitnikova E.. Identification of malicious activities in industrial internet of things based on deep learning models //Journal of Information Security and Applications. – 2018. – № 41. – P. 1 – 11.

13. Sung Jin Kim, Woo Yeon Jo, Taeshik Shon. APAD: Autoencoder-based Payload Anomaly Detection for industrial IoE. December 2019 Applied Soft Computing 88:106017. DOI: 10.1016/j.asoc.2019.106017.

14. Baldi P. Autoencoders, unsupervised learning, and deep architectures //Proceedings of ICML workshop on unsupervised and transfer learning. – 2012. – С. 37 – 49.

15. Schmidhuber J. Deep learning in neural networks: An overview //Neural networks. – 2015. – № 61. – P. 85 – 117.

16. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – P. 2672 – 2680.

17. Madry A. et al. Towards deep learning models resistant to adversarial attacks //arXiv preprint arXiv:1706.06083. – 2017.

18. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

19. Алабугин С.К., Соколов А.Н. Использование генеративно-состязательных нейронных сетей при выявлении аномалий технологического процесса //Вестник УрФО. Безопасность в информационной сфере. – 2020. № 4(38). – С. 64 – 68.

20. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты //Вопросы кибербезопасности. – 2019. – № 3(31). – С. 30 – 36.

21. Quilot B., Génard M., Lescourret F., Kervella J. Simulating genotypic variation of fruit quality in an advanced peach×Prunus davidiana cross // Journal of Experimental Botany, Volume 56, Issue 422, December 2005, Pages 3071–3081, https://doi.org/10.1093/jxb/eri304.

22. Martin H., Tschabuschnig K., Bridal O., Watzenig D. (2017) Functional Safety of Automated Driving Systems: Does ISO 26262 Meet the Challenges?. In: Watzenig D., Horn M. (eds) Automated Driving. Springer, Cham. https://doi.org/10.1007/978-3-319-31895-0_16.

23. Баринов А.Е., Скурлаев С.В., Соколов А.Н. Методика оценки рисков, вызванных уязвимостями в программном обеспечении автоматизированных систем управления технологическими процессами //Вестник УрФО. Безопасность в информационной сфере. – 2017. № 3(25). – С. 34 – 42.

24. Parts 1 – 7 IEC 61508, Functional safety of electrical/electronic/ programmable electronic safety-related systems.

25. Braband J. Towards an IT security risk assessment framework for rail- way automation //CoRR abs/1704.01175, http://arxiv.org/abs/1704.01175, 2017.

26. Maidl M., Kröselberg D., Christ J. and Beckers K. A Comprehensive Framework for Security in Engineering Projects - Based on IEC 62443. // 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2018, pp. 42-47, doi: 10.1109/ISSREW.2018.00.

27. Pyatnitsky I.A., Sokolov A.N. Determination of the Optimal Ratio of Normal to Anomalous Points in the Problem of Detecting Anomalies in the Work of Industrial Control Systems // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2021, pp. 0478-0480, doi: 10.1109/USBEREIT51232.2021.9455010.

28. Alabugin S.K., Sokolov A.N. Applying of Generative Adversarial Networks for Anomaly Detection in Industrial Control Systems // 2020 Global Smart Industry Conference (GloSIC), 2020, pp. 199-203, doi: 10.1109/GloSIC50886.2020.9267878.

29. Alabugin S.K., Sokolov A.N. Applying of Recurrent Neural Networks for Industrial Processes Anomaly Detection // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2021, pp. 0467-0470, doi: 10.1109/USBEREIT51232.2021.9455060.

30. Radford A., Metz L., Chintala S. Unsupervised representation learning with deep convolutional generative adversarial networks //arXiv preprint arXiv:1511.06434. – 2015.44.

31. Ledig C. et al. Photo-realistic single image super-resolution using a generative adversarial network //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2017. – С. 4681-4690.

32. Odena A., Olah C., Shlens J. Conditional image synthesis with auxiliary classifier gans //Proceedings of the 34th International Conference on Machine Learning-Volume 70. – JMLR.org, 2017. – С. 2642-2651.

33. Engel J. et al. Gansynth: Adversarial neural audio synthesis //arXiv preprint arXiv:1902.08710. – 2019.

34. Subramanian S. et al. Towards text generation with adversarially learned neural outlines //Advances in Neural Information Processing Systems. – 2018. – P. 7551 – 7563.

35. Madry A. et al. Towards deep learning models resistant to adversarial attacks //arXiv preprint arXiv:1706.06083. – 2017.

36. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

37. Zenati H. et al. Efficient gan-based anomaly detection //arXiv preprint arXiv:1802.06222. – 2018.

38. J. Goh, S. Adepu, K. N. Junejo and A. Mathur, "A dataset to support research in the design of secure water treatment systems", Proc. International Conference on Critical Information Infrastructures Security (CRITIS 2016), 2016.

References

1. Volkova V.N. Osnovy teorii sistem i sistemnogo analiza / V.N. Volkova, A.A. Denisov. – SPb: Izd-vo SPbGTU, 1999. – 512 s.

2. Fleyshman B.S. Osnovy sistemologii / B.S. Fleyshman. – M.: Radio i svyaz'. 1982. – 368 s.

3. Tyrsin A.N. O matematicheskom modelirovanii slozhnykh organizatsionnykh sistem // Organizatsiya i upravlenie effektivnost'yu i proizvoditel'nost'yu proizvodstvennykh i sotsial'nykh sistem: Mater. mezhd. nauchno-prakt. konf. – Novocherkassk: YuRGTU (NPI), 2005. – S. 49 – 50.

4. Birger I.A. Tekhnicheskaya diagnostika. – M.: Nauka, 1978. – 239 s.

5. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems // Computer Networks. 1999. vol. 31. Issue 8. pp. 805 – 822.

6. Branitskiy A.A., Kotenko I.V. Analiz i klassifikatsiya metodov obnaruzheniya setevykh atak. – Trudy SPIIRAN. – 2016. – Vyp. 45 – S. 207 – 244.

7. Abdulin A.A., Sokolov A.N. Issledovanie programmnykh resheniy dlya obespecheniya informatsionnoy bezopasnosti promyshlennykh setey avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami //Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2021. № 1(39). – C. 43 – 53.

8. Herve Debar, Monique Becker, and Didier Siboni. A neural network omponent for an intrusion detection system //Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy, pages 240–250, Oakland, CA, USA, May 1992.

9. Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari. Detection of Distributed Denial of Service Attacks Using Statistical Pre- Processor and Unsupervised Neural Networks // Lecture notes in computer science, 2005.

10. Smelyanskiy R.L., Kachalin A.I. Primeneniya neyrosetey dlya obnaruzheniya anomal'nogo povedeniya ob"ektov v komp'yuternykh setyakh //Fakul'tet Vychislitel'noy Matematiki i Kibernetiki, MGU im. M. V. Lomonosova, Moskva, 2004.

11. Neural network and artificial immune systems for malware and network intrusion detection / V. Golovko [et al.] // Studies in computational intelligence. – Heidelberg, 2010. – Vol. 263 : Advances in machine learning II. – P. 485 – 513.

12. Muna A.H., Moustafa N. & Sitnikova E.. Identification of malicious activities in industrial internet of things based on deep learning models //Journal of Information Security and Applications. – 2018. – № 41. – P. 1 – 11.

13. Sung Jin Kim, Woo Yeon Jo, Taeshik Shon. APAD: Autoencoder-based Payload Anomaly Detection for industrial IoE. December 2019 Applied Soft Computing 88:106017. DOI: 10.1016/j.asoc.2019.106017.

14. Baldi P. Autoencoders, unsupervised learning, and deep architectures //Proceedings of ICML workshop on unsupervised and transfer learning. – 2012. – S. 37 – 49.

15. Schmidhuber J. Deep learning in neural networks: An overview //Neural networks. – 2015. – № 61. – P. 85 – 117.

16. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – P. 2672 – 2680.

17. Madry A. et al. Towards deep learning models resistant to adversarial attacks //arXiv preprint arXiv:1706.06083. – 2017.

18. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

19. Alabugin S.K., Sokolov A.N. Ispol'zovanie generativno-sostyazatel'nykh neyronnykh setey pri vyyavlenii anomaliy tekhnologicheskogo protsessa //Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2020. № 4(38). – C. 64 – 68.

20. Garbuk S.V., Pravikov D.I., Polyanskiy A.V., Samarin I.V. Obespechenie informatsionnoy bezopasnosti ASU TP s ispol'zovaniem metoda prediktivnoy zashchity //Voprosy kiberbezopasnosti. – 2019. – № 3(31). – S. 30 – 36.

21. Quilot B., Génard M., Lescourret F., Kervella J. Simulating genotypic variation of fruit quality in an advanced peach×Prunus davidiana cross // Journal of Experimental Botany, Volume 56, Issue 422, December 2005, Pages 3071–3081, https://doi.org/10.1093/jxb/eri304.

22. Martin H., Tschabuschnig K., Bridal O., Watzenig D. (2017) Functional Safety of Automated Driving Systems: Does ISO 26262 Meet the Challenges?. In: Watzenig D., Horn M. (eds) Automated Driving. Springer, Cham. https://doi.org/10.1007/978-3-319-31895-0_16.

23. Barinov A.E., Skurlaev S.V., Sokolov A.N. Metodika otsenki riskov, vyzvannykh uyazvimostyami v programmnom obespechenii avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2017. № 3(25). – C. 34 – 42.

24. Parts 1 – 7 IEC 61508, Functional safety of electrical/electronic/ programmable electronic safety-related systems.

25. Braband J. Towards an IT security risk assessment framework for rail- way automation //CoRR abs/1704.01175, http://arxiv.org/abs/1704.01175, 2017.

26. Maidl M., Kröselberg D., Christ J. and Beckers K. A Comprehensive Framework for Security in Engineering Projects - Based on IEC 62443. // 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2018, pp. 42-47, doi: 10.1109/ISSREW.2018.00.

27. Pyatnitsky I.A., Sokolov A.N. Determination of the Optimal Ratio of Normal to Anomalous Points in the Problem of Detecting Anomalies in the Work of Industrial Control Systems //2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2021, pp. 0478-0480, doi: 10.1109/USBEREIT51232.2021.9455010.

28. Alabugin S.K., Sokolov A.N. Applying of Generative Adversarial Networks for Anomaly Detection in Industrial Control Systems // 2020 Global Smart Industry Conference (GloSIC), 2020, pp. 199-203, doi: 10.1109/GloSIC50886.2020.9267878.

29. Alabugin S.K., Sokolov A.N. Applying of Recurrent Neural Networks for Industrial Processes Anomaly Detection // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2021, pp. 0467-0470, doi: 10.1109/USBEREIT51232.2021.9455060.

30. Radford A., Metz L., Chintala S. Unsupervised representation learning with deep convolutional generative adversarial networks //arXiv preprint arXiv:1511.06434. – 2015.44.

31. Ledig C. et al. Photo-realistic single image super-resolution using a generative adversarial network //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2017. – C. 4681-4690.

32. Odena A., Olah C., Shlens J. Conditional image synthesis with auxiliary classifier gans //Proceedings of the 34th International Conference on Machine Learning-Volume 70. – JMLR.org, 2017. – C. 2642-2651.

33. Engel J. et al. Gansynth: Adversarial neural audio synthesis //arXiv preprint arXiv:1902.08710. – 2019.

34. Subramanian S. et al. Towards text generation with adversarially learned neural outlines //Advances in Neural Information Processing Systems. – 2018. – P. 7551-7563.

35. Madry A. et al. Towards deep learning models resistant to adversarial attacks //arXiv preprint arXiv:1706.06083. – 2017.

36. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

37. Zenati H. et al. Efficient gan-based anomaly detection //arXiv preprint arXiv:1802.06222. – 2018.

38. J. Goh, S. Adepu, K. N. Junejo and A. Mathur, "A dataset to support research in the design of secure water treatment systems", Proc. International Conference on Critical Information Infrastructures Security (CRITIS 2016), 2016.

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, д. 76. E-mail: sokolovan@susu.ru.

РАГОЗИН Андрей Николаевич, кандидат технических наук, доцент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ragozinan@susu.ru.

БАРИНОВ Андрей Евгеньевич, старший преподаватель кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследователь-

ский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: barinovae@susu.ru.

УФИМЦЕВ Максим Сергеевич, преподаватель кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ufimtcevms@susu.ru.

ПЯТНИЦКИЙ Илья Альбертович, аспирант кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: iamKane@mail.ru.

БУХАРЕВ Дмитрий Александрович, аспирант кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: bukharevdmitrii@gmail.com.

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the Department of Information Security, South Ural State University (national research university). 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru.

RAGOZIN Andrey Nikolaevich, Ph.D., Associate Professor of the Department of Information Security, South Ural State University (national research university). 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: ragozinan@susu.ru.

BARINOV Andrey Evgenievich, Senior Lecturer of the Department of Information Security, South Ural State University (national research university). 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: barinovae@susu.ru.

UFIMTCEV Maxim Sergeevich, Lecturer of the Department of Information Security, South Ural State University (national research university). 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: ufimtcevms@susu.ru.

PYATNITSKIY Ilya Albertovich, Post-graduate student of the Department of Information Security, South Ural State University (national research university). 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: iamKane@mail.ru.

BUKHAREV Dmitriy Aleksandrovich, Post-graduate student of the Department of Information Security, South Ural State University (national research university). 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: bukharevdmitrii@gmail.com.

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

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

ВЕСТНИК УрФО
Безопасность в информационной сфере № 3(41) / 2021
Подписано в печать 30.09.2021.
Дата выхода в свет 28.10.2021. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 7.7. Тираж 100 экз. Заказ 304/364.
Цена свободная.

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

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 3(41) / 2021
Signed to print September 30, 2021.
Date of publication of the 28.10.2021. Format 70×108 1/16. Screen printing.
Conventional printed sheet 7.7. Circulation – 100 issues. Order 304/364. Open price.

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