MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ — INTERNATIONAL UNIVERSITY — SINCE 2009 — МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Published since 2020.
Volume 7. 1 (25). 2026
January–March

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

2020 жылдан бері шығарылады
Том 7. 1 (25). 2026
Қаңтар-Наурыз

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Издается с 2020 г.
Том 7. 1 (25). 2026
Январь-Март

Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан № KZ82VPY00020475, выданное от 20.02.2020 г.

Зарегистрировано в Международном центре регистрации серийных изданий ISSN (ЮНЕСКО, Париж, Франция). ISSN 2708–2032 (print), ISSN 2708–2040 (online)

Журнал входит в Перечень научных изданий, рекомендуемых КОКНВО МНВО РК для публикации основных результатов научной деятельности.

International Journal of Information and Communication Technologies
Periodicity: 4 times a year.
Languages: Kazakh, Russian, English
DOI prefix: 10.54309
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Thematic focus: "Information technology"; "Digital technologies in the development of socio-economic systems"; "Information security and communication technologies".

Journal website: https://journal.iitu.edu.kz
Owner: International Information Technology University JSC (Almaty).

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Префикс DOI: 10.54309
Мерзімділігі: жылына 4 рет.
Басылым тілі: қазақ, орыс, ағылшын.
Тақырып бағыты: "Ақпараттық технологиялар"; "Ақпараттық қауіпсіздік және коммуникациялық технологиялар"; "Әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технология".
Журнал сайты: https://journal.iitu.edu.kz

Меншік иесі: АҚ «Халықаралық ақпараттық технологиялар университеті» (Алматы қ.).

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Префикс DOI: 10.54309
Периодичность: 4 выпусков в год.
Язык издания: казахский, русский, английский.
Тематическая направленность: "Информационные технологии"; "Информационная безопасность и коммуникационные технологии"; "Цифровые технологии в развитии социо-экономических систем".
Сайт журнала: https://journal.iitu.edu.kz

Собственник: АО «Международный университет информационных технологий» (г. Алматы).

CONTENTS

DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF SOCIO-ECONOMIC SYSTEMS

INFORMATION TECHNOLOGY

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

МАЗМҰНЫ

ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМЫТУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИСОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 7. Is.1. Number 25 (2026). Pp. 270–291
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2026.25.1.017
УДК 004.056.5

EDGE COMPUTING-BASED TECHNIQUE FOR CONSTRUCTION OF ATTACK DETECTION MEANS IN CYBER-PHYSICAL SYSTEMS OF INDUSTRIAL INTERNET-OF-THINGS

T. K. Zhukabayeva[1*], D.B. Baumuratova[2], E. Benkhelifa [3], N.A. Niyetbayeva[4]
[1]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan;
[2]Astana International University, Astana, Kazakhstan;
[3]Staffordshire University, Staffordshire, United Kingdom;
[4]M.Kh. Dulaty Taraz University, Taraz, Kazakhstan.
E-mail: tamara.kokenovna@gmail.com

Tamara K. Zhukabayeva — PhD, Professor of the Department of Information Systems, Faculty of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
E-mail: tamara.kokenovna@gmail.com, https://orcid.org/0000-0001-6345-5211;
Baumuratova B. Dilaram — PhD, Senior Lecturer, Pedagogical Institute, Astana International University, Astana, Kazakhstan
https://orcid.org/0009-0009-4621-1886;
Elhadj Benkhelifa — PhD, Professor of Computer Science and Artificial Intelligence, Staffordshire University, Staffordshire, United Kingdom
https://orcid.org/0000-0001-6168-2664;
Niyetbayeva A. Nadira — PhD, Associate Professor, Department of Physics and Informatics, M.Kh. Dulaty Taraz University, Taraz, Kazakhstan
https://orcid.org/0000-0003-2921-6879.

Abstract. The article examines security issues of contemporary cyber-physical systems that use the concept of edge computing to solve problems of secure operation of industrial Internet of Things infrastructures. The main contribution of this article comprises a description and results of the analysis of the proposed technique for detecting attacks in cyber-physical systems of the Industrial Internet of Things using edge computing. The technique is aimed at application by design engineers and developers of software packages to ensure information security of cyber-physical systems of the Industrial Internet of Things, where a significant part of the target computing processes of the system is imposed on the end devices of the

system. The technique includes six main stages covering the processes of analytical and natural-simulation modeling of attacks, generation and marking of initial data sets, construction of software classifiers as means of attack detection, and visual data analysis. In general, the implementation of the technique is presumed at the following stages of the life cycle of cyber-physical systems, these are the stages of designing and testing the system, setting up and evaluating the operation quality of attack detection tools. The feasibility of the technique using an example of an industrial system in the field of incident management of transport infrastructure using software and hardware modules of the Arduino platform confirms the correctness and effectiveness of the technique for its further practical application.

Keywords: attack, detection, edge computing, analysis, technique

For citation: T.K. Zhukabayeva, D.B. Baumuratova E. Benkhelifa, N.A. Niyetbayeva (2026). Edge computing-based technique for construction of attack detection means in cyber-physical systems of industrial internet-of-things // International journal of information and communication technologies. Vol. 7. No.25. Pp. 270-291. https://doi.org/10.54309/IJICT.2026.25.1.017. (In Russ),

Conflict of interest: The authors declare that there is no conflict of interest.

ШЕКАРАЛЫҚ ЕСЕПТЕУЛЕРДІ ҚОЛДАНА ОТЫРЫП, ЗАТТАРДЫҢ ӨНЕРКӘСІПТІК ИНТЕРНЕТІНІҢ КИБЕРФИЗИКАЛЫҚ ЖҮЙЕЛЕРІНДЕГІ ШАБУЫЛДАРДЫ АНЫҚТАУ ҚҰРАЛДАРЫН ҚҰРУ ӘДІСТЕМЕСІ

Т.К. Жукабаева[1*], Д. Б Баумуратова[2], Е. Бенкхелифа[3], Н.А. Ниетбаева[4]

[1] Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан;

[2]Астана халықаралық университеті, Астана, Қазақстан;

[3] Стаффордшир университеті, Стаффордшир Ұлыбритания;

[4]М.Х. Дулати атындағы Тараз университеті, Тараз, Қазақстан.

E-mail: tamara.kokenovna@gmail.com

Жукабаева Тамара Кокеновна — PhD, ақпараттық технологиялар факультетінің Ақпараттық жүйелер кафедрасының профессоры, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
E-mail: tamara.kokenovna@gmail.com, https://orcid.org/0000-0001-6345-5211;

Баумуратова Диларам Бекбулатовна — PhD, Астана халықаралық университетінің Педагогикалық институтының аға оқытушысы, Астана, Қазақстан https://orcid.org/0009-0009-4621-1886;

Бенхелифа Эльхадж — PhD, компьютерлік ғылымдар және жасанды интеллект профессоры, Стаффордшир университеті, Стаффордшир Ұлыбритания https://orcid.org/0000-0001-6168-2664;

Ниетбаева Надира Ашировна — PhD, физика және информатика кафедрасының қауымдастырылған профессоры, М.Х. Дулати атындағы Тараз

университеті, Тараз, Қазақстан
https://orcid.org/0000-0003-2921-6879.

Аннотация. Мақалада заттардың өнеркәсіптік интернеті инфрақұрылымдарының қорғалатын жұмысының мәселелерін шешу үшін шекаралық есептеу тұжырымдамасын қолданатын заманауи киберфизикалық жүйелердің қауіпсіздігі мәселелері қарастырылады. Мақаланың негізгі үлесі шекаралық есептеулерді қолдана отырып, заттардың өнеркәсіптік интернетінің киберфизикалық жүйелеріндегі шабуылдарды анықтаудың ұсынылған әдістемесін сипаттау мен талдау нәтижелерін қамтиды. Әдістеме инженер-дизайнерлер мен бағдарламалық жасақтама жасаушылардың өнеркәсіптік интернет заттарының киберфизикалық жүйелерінің ақпараттық қауіпсіздігін қамтамасыз ету үшін қолдануға бағытталған, онда жүйенің мақсатты есептеу процестерінің маңызды бөлігі жүйенің соңғы құрылғыларына жүктеледі. Әдістеме шабуылдаушы әсерлерді аналитикалық және заттай Имитациялық модельдеу, бастапқы деректер жиынтығын құру және белгілеу, шабуылдарды анықтау құралы ретінде бағдарламалық классификаторларды құру, деректерді визуалды талдау процестерін қамтитын алты негізгі кезеңді қамтиды. Жалпы, әдістемені орындау киберфизикалық жүйелердің өмірлік циклінің келесі кезеңдерінде – жүйені жобалау және тестілеу, шабуылдарды анықтау құралдарының жұмыс сапасын реттеу және бағалау кезеңдерінде қарастырылады. Arduino платформасының бағдарламалық-аппараттық модульдерін пайдалана отырып, көлік инфрақұрылымының инциденттерін басқару саласындағы индустриялық жүйе мысалында Әдістеменің орындылығы оны одан әрі практикалық қолдану үшін Әдістеменің дұрыстығы мен пәрменділігін растайды.

Түйін сөздер: шабуыл, анықтау, шекаралық есептеу, талдау, әдістеме

Дәйексөздер үшін: Т.К. Жукабаева, Д.ББаумуратова, Е. Бенкхелифа, Н.А. Ниетбаева (2026). Шекаралық есептеулерді қолдана отырып, заттардың өнеркәсіптік интернетінің киберфизикалық жүйелеріндегі шабуылдарды анықтау құралдарын құру әдістемесі // Халықаралық ақпараттық және коммуникациялық технологиялар журналы. Т 7. № 25. 270-291 бет. https://doi.org/10.54309/IJICT.2026.25.1.017. (Орыс тіл.);

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдейді.

МЕТОДИКА ПОСТРОЕНИЯ СРЕДСТВ ОБНАРУЖЕНИЯ АТАК В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ

Т.К. Жукабаева[1*], Д Б. Баумуратова[2], Е. Бенкхелифа[3], Н.А. Ниетбаева[4]
[1]Евразийскии национальный университет имени Л.Н. Гумилева, Астана, Казахстан;
[2]Международный университет Астана, Астана, Казахстан;
[3]Стаффордшир университет, Стаффордшир, Великобритания;
[4]Таразский университет имени М.Х. Дулати, Тараз, Казахстан.
E-mail: tamara.kokenovna@gmail.com

Жукабаева Тамара Кокеновна — PhD, профессор кафедры информационные системы, факультет информационных технологий, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан
E-mail: tamara.kokenovna@gmail.com, https://orcid.org/0000-0001-6345-5211;
Баумуратова Диларам Бекбулатовна — PhD, старший преподаватель, Педагогический институт Международного университета Астана, Астана, Казахстан
https://orcid.org/0009-0009-4621-1886;
Бенкхелифа Эльхадж — PhD, профессор компьютерных наук и искусственного интеллекта, Стаффордширский университет, Стаффордшир, Великобритания
https://0000-0001-6168-2664;
Ниетбаева Надира Ашировна — PhD, ассоцированный профессор, кафедра физики и информатики, Таразский университет имени М.Х. Дулати, Тараз, Казахстан
https://orcid.org/0000-0003-2921-6879.

Аннотация. В статье исследуются вопросы безопасности современных киберфизических систем, использующих концепцию граничных вычислений для решения задач защищенного функционирования инфраструктур промышленного интернета вещей. Основной вклад статьи включает описание и результаты анализа предложенной методики обнаружения атак в киберфизических системах промышленного интернета вещей с использованием граничных вычислений. Методика ориентирована на применение инженерами-проектировщиками и разработчиками программных комплексов для обеспечения информационной безопасности киберфизических систем промышленного интернета вещей, в которых значимая часть целевых вычислительных процессов системы возлагается на конечные устройства системы. Методика включает шесть основных стадий, охватывающих процессы аналитического и натурно-имитационного моделирования атакующих воздействий, генерации и разметки наборов исходных данных, построения программных классификаторов в качестве средств обнаружения атак, визуального анализа данных. В целом выполнение методики предусматривается на следующих этапа жизненного цикла киберфизических

систем – этапах проектирования и тестирования системы, настройки и оценивания качества работы средств обнаружения атак. Выполнимость методики на примере индустриальной системы в области управления инцидентами транспортной инфраструктуры с использованием программно-аппаратных модулей платформы Arduino подтверждает корректность и действенность методики для ее дальнейшего практического применения.

Ключевые слова: атака, обнаружение, граничные вычисления, анализ. методика

Для цитирования: Т.К. Жукабаева, Д.Б. Баумуратова, Е. Бенкхелифа, Н.А. Ниетбаева (2026). Методика построения средств обнаружения атак в киберфизических системах промышленного интернета вещей с использованием граничных вычислений // Международный журнал информационных и коммуникационных технологий. Т 7. No. 25. Стр. 270–291. https://doi.org/10.54309/IJICT.2026.25.1.017.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Финансирование. *Настоящая работа сотрудниками НАО «Евразийский национальный университет имени Л.Н. Гумилева» проводится при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан (Грант № AP23489127).*

Введение.

В настоящее время все большее распространение на практике получают различные информационно-телекоммуникационные инфраструктуры, включающие в свой состав разнородные киберфизические и мобильные устройства, автоматизированные системы управления такими инфраструктурами и интеллектуальные сервисы, предоставляемые конечным пользователям и организующие высоконадежные и защищенные межмашинные взаимодействия. Киберфизические системы и инфраструктуры, реализующие концепцию граничных вычислений (edge; edge computing) (Ilyin, 2021), представляют сетевые распределенные структуры автономно работающих встроенных и мобильных устройств интернета вещей с возможностью обработки первичных данных непосредственно на стороне конечных устройств с последующей передачей обработанных данных на централизованные сетевые хосты и облачные системы (Shirazi, 2017; Esposito, 2017). Согласно этой концепции, значительная часть вычислений и обработки данных должна выполняться либо непосредственно в местах их сбора или в непосредственной их близости. Ввиду не доверенности программно-информационного окружения таких систем, а также уязвимостей используемого программно-аппаратного обеспечения киберфизических устройств, в том числе уязвимостей нулевого дня (Anwer, 2022), а также недостаточной защищенности существующих коммуникационных протоколов, в частности, протоколов канального, сетевого и

прикладного уровней, такие инфраструктуры оказываются подверженными разнообразным атакующим воздействиям, направленным на компрометацию устройств, данных, циркулирующих по сети и хранящихся на устройствах, а также предоставляемых пользовательских сервисов (Yahuza, 2020).

Отметим, что особенная сложность формирования надежных и защищенных механизмов киберфизической безопасности систем, реализующих концепцию граничных вычислений, возникает в результате следующих факторов, непосредственно влияющих на уровень защищенности таких систем: многошаговость, многоаспектность и многовариантность действий потенциального нарушителя информационной безопасности (ИБ). Многошаговость включает наличия типовых и узкоспециализированных сценариев действий атакующего, разделяемых логически и во временном исчислении на явно выделенные этапы, такие как

- предваряющий анализ доступного атакующему программно-технического окружения с определением перечней информационных активов, воздействия на которые могут служить достижению его целей. В частности, на данном этапе может проводиться сетевое сканирование коммуникационной инфраструктуры с использованием сканеров безопасности Nmap (Asokan, 2023), Nessus (Muin, 2022), OpenVAS (Toyin, 2023) и др., позволяющих выявить нужные уязвимости в программно-аппаратном обеспечении, незащищенные открытые порты, архитектурные слабости и другие характерные особенности инфраструктуры, влияющие на процесс подготовки несанкционированного воздействия;

- получение доступа к целевым программно-аппаратным компонентам в рамках заданной сетевой коммуникационной и/или виртуальной инфраструктуры, «продвижение» по сети с использованием метода последовательного повышения привилегий в условиях накопления данных и ресурсов, достаточных для проведения воздействия;

- осуществление несанкционированного воздействия на целевой объект приложения с модификацией его структуры или конфигурационных настроек, прослушиванием и/или перехватом его данных, нарушением его доступности и др.

- опциональное удаление следов присутствия нарушителя в рамках заданной программно-информационной инфраструктуры.

Многоаспектность атакующих воздействий состоит в возможностях нарушителя использовать в процессе атаки одновременно или последовательно нескольких целевых приложений атаки, взаимодополняющих друг друга и включающих воздействия на уровне сетевых хостов, аппаратно-физические воздействия на критически важные узлы инфраструктуры, социоинженерные воздействия и иные проявления. Так, в общем случае комбинированный характер подобного воздействия позволяет атакующему не только усилить эффект атаки, но и сократить временные затраты на проведение атаки, в том

числе сократить время поиска слабых мест и уязвимостей, которые он будет эксплуатировать в качестве своих стартовых шагов (Yang, 2024). Вытекающая из многоаспектности многовариантность действий атакующего обуславливает возможность динамического выбора им наиболее выгодных шагов в зависимости от текущего контекста атаки, осведомленности нарушителя об интересуемых его активах и условий их функционирования (Golchin, 2022). Все это определяет потребность в совершенствовании программных средств обнаружения атак и повышении защищенности киберфизических систем для улучшения показателей качества обнаружения атак и улучшения нефункциональных характеристик средств защиты за счет комплексного учета условий функционирования целевой инфраструктуры, моделирования анализа действий атакующего и особенностей технологии граничных вычислений.

Настоящая работа ориентирована на совершенствование существующих и разработку новых перспективных программных средств обнаружения атак в современных киберфизических информационно-телекоммуникационных системах и сетях, базирующихся на концепции граничных вычислений. Основной вклад данной статьи включает разработанную методику обнаружения атак в киберфизических системах промышленного интернета вещей (IIoT) с использованием граничных вычислений, а также результаты ее анализа. Характерными примерами систем промышленного интернета вещей являются индустриальные системы мониторинга периметра производства и контроля качества индустриального процесса; различные транспортные киберфизические системы, организующие автоматизированные сценарии сортировки, хранения и доставки производственных деталей при их изготовлении; системы безопасных и эффективных интеллектуальных процессов генерации и распределения электроэнергии для индустриальных предприятий –так называемые, умные сети электроснабжения (Smart Grid). При этом передача части значимого функционала таких систем на сторону географически распределенных и удаленных устройств не только расширяет функциональность устройств и предоставляемых сервисов, а также улучшает нефункциональные характеристики, но и представляет далеко идущую тенденцию в совершенствовании и повышении целевых показателей качества таких систем в целом. Вместе с тем во всех указанных примерах проблематика безопасности функционирования киберфизичекой инфраструктуры, а также отдельных входящих в ее состав устройств, узлов, действующих пользователей представляется крайне актуальной, в особенности в условиях потенциально не доверенного и ненадежного окружения устройств.

Выделим следующие основные факторы, определяющие актуальность и практическую значимость задач по разработке методик по построению средств обнаружения атак в IIoT-системах с использованием граничных вычислений. К ним относятся в первую очередь разнородность IIoT-систем и их уязвимость к широкому классу несанкционированных воздействий, а также

атаки непосредственно на граничные устройства и функции граничных вычислений. В частности, в настоящее время наблюдается существенная разнородность существующих систем промышленного интернета вещей, включающих в свой состав отличающиеся наборы конечных и промежуточных устройств, сенсоров, исполнительных механизмов, различные сетевые конфигурации, виды аппаратных архитектур и протоколов сетевого взаимодействия. Поэтому Разнообразие IIoT-систем обуславливает потребность в унификации и построении средств обнаружения атак в таких системах с учетом, вариативности действий потенциального нарушителя, его практических возможностей, доступных ресурсов и инструментов (Vankayalapati, 2023).

Ввиду распределенного характера IIoTсистем, наличия ограничений ресурсопотребления их устройств, открытости существующих сетевых протоколов, наличия слабых мест в используемом программном обеспечении, такие системы оказываются уязвимыми к актуальным угрозам информационной безопасности. В том числе это касается воздействий, представляющим, в частности, такие атаки как сетевые атаки DoS, MitM, различные фишинговые атаки; атаки на конкретные устройства, включающие атаки подбора пароля методом направленного перебора и эксплуатацию уязвимостей программных прошивок устройств; атаки на модификацию данных от сенсоров; атаки уровня приложений, такие как XSS-атаки, SQL-инъекции и др.(Xiao, 2019).

Поэтому разнообразие возможных видов атак, а также их взаимосвязанность обуславливают потребность в комплексном выявлении атак в IIoT-системах, которое должно охватывать различные аспекты обеспечения безопасности: моделирование атак, построение программных классификаторов и визуализацию данных, что способствует обеспечению всестороннего анализа возможных угроз безопасности (Roman, 2018). Кроме того, отметим, что использование IIoT-системой граничных вычислений позволяет устройствам эффективно обрабатывать данные непосредственно на конечных устройствах, что повышает оперативность реагирования на угрозы. Вместе с тем возможность несанкционированной эксплуатации функций граничных вычислений позволяет потенциальному злоумышленнику осуществлять воздействия непосредственно на граничные устройства системы, в том числе атаки утечки данных с устройств, backdoor-атаки и атаки нарушения аутентификации.

Поэтому, указанные выше особенности IIoT-систем позволяют подтвердить, что предлагаемая методика является важным инструментом для повышения уровня информационной безопасности киберфизических систем промышленного интернета вещей, базирующихся на использовании граничных вычислений, что особенно актуально в условиях растущего числа угроз, увеличивающейся сложности современных технологических решений. Таким образом, своевременное обнаружение инцидентов безопасности в таких инфраструктурах с высоким качеством представляется крайне важной задачей.

Оставшаяся часть статьи организована следующим образом. Следующий раздел статьи включает обзор и анализ существующих механизмов информационной безопасности и обнаружения атак в киберфизических системах индустриального интернета вещей в рамках концепции граничных вычислений. Далее в статье раскрываются сущность и особенности предложенной методики обнаружения атак. Последующий раздел статьи посвящен вопросам применения и анализу данной методики. Статья завершается заключением и списком основных использованных источников научно-технической литературы.

Граничные вычисления, называемые также периферийными вычислениями, представляют концепцию распределенных вычислений, которые осуществляются в границах некоторого множества конечных устройств, функционирующих в заданной киберфизической инфраструктуре (Lin, 2020). Другими словами, граничные вычисления предполагают организацию хранения данных, вычисления и их фактическое расположение в некоторой окрестности имеющихся устройств и источников первичных данных. Это в свою очередь способствует снижению временных задержек при передаче данных в таких инфраструктурах, а также увеличивает пропускную способность сетевых коммуникационных каналов связи. Таким образом, к основным преимуществам систем граничных вычислений можно отнести следующие:

- снижение объемов, передаваемых данных;
- повышение оперативности функционирования системы за счет принятия решений по управлению системой непосредственно на устройствах (узлах сети) и снижению коммуникационных задержек;
- повышение надежности и бесперебойности работы системы, в том числе за счет повышения степени автономности отдельных устройств и их сегментов в условиях временных нарушений связности используемой коммуникационной сети, а также уменьшения критичности централизованных модулей обработки данных;
- повышение уровня безопасности системы за счет возможностей по отслеживанию аномалий и выявлению атак непосредственно на устройствах сети.

Научная проблема, на исследование и решение которой направлена настоящая работа, состоит в недостаточной защищенности систем, реализующих концепцию граничных вычислений, и их подверженности сложным для выявления комбинированным многошаговым информационным воздействиям, направленным на некорректное и нецелевое использование таких систем, нарушение корректного функционирования таких систем, причинение ущерба их инфраструктуре и пользователям. Отметим также, что понятие граничных вычислений введено для выделения подкласса систем интернета вещей, для которых действия по обработке данных могут выполняться в пределах локального сетевого контура некоторой группы пользовательских устройств (Dolui et al., 2018). В частности, в системах, реализующих концепцию граничных вычислений,

информационные сервисы могут располагаться на конечных пользовательских устройствах или устройствах, представляющих точки доступа к связи с устройствами пользователей. При этом процедуры такой распределенной инфраструктуры граничных вычислений выполняются на вычислительных модулях, максимально приближенных к местам расположения считываемым с сенсоров данных о людях, процессах, вещах. То есть, фактически, такой набор вычислительных узлов позволяет реализовать функциональность облачных вычислений (cloud computing), но не централизованно на высокопроизводительных серверах, а «приближенную к земле», формируя более быстрые ответы на информационные импульсы со стороны собираемых в IoT-системе данных (Nam, 2023).

Отметим также, что граничные и облачные вычисления могут применяться совместно. При этом граничные вычисления формируют дополнительный слой управления между сенсорами, как источниками данных, и облаком, как вычислительным слоем, отвечающим за обработку и хранение больших массивов данных. Облачные вычисления освобождают организации от решения множеств технологических вопросов, таких как вопросы хранения данных, вычислительных и сетевых ограничений, при этом они в текущем их виде с большим трудом позволяют справляться с требованиями на поддержку мобильности, осведомленность о местонахождении и низкие коммуникационные задержки, предъявляемыми со стороны пользовательских приложений (Qing, 2018).

К особенностям проблематики информационной безопасности систем граничных вычислений можно отнести зачастую опосредованный и отложенный характер несанкционированного воздействия, выражаемый, в том числе, в постепенной деградации каналов связи за счет разрастающегося вовлечения имеющихся edge-узлов в botnet-атаку (Gulatas, 2023). Это способно приводить к постепенному перераспределению вычислений и связанному с этих ухудшению скорости связи и показателей корректности доставки сообщений (показатели Quality-of-Service). Кроме того, сложность обнаружения атак в таких системах связана с нехваткой централизации при сборе данных, которые могут содержать важные признаки, необходимые для обнаружения атак.

В (Gulatas, 2023) отмечается, что помимо того, что системы граничных вычислений наследуют классы уязвимостей от предшествующих коммуникационно-вычислительных технологий, таких как распределенные P2P-системы и беспроводные сенсорные сети, за счет многоуровневой структуры граничных вычислений и ограниченности ресурсов устройств такие системы обладают дополнительными наборами уязвимостей, опирающимися на изъяны отдельных edge-узлов и их взаимодействия. Кроме того, в (Alwarafy, 2019) обосновывается важность вопросов обеспечения защищенности и приватности данных в системах граничных вычислений.

На примере нескольких практических сценариев, таких как системы электронной медицина и умных городов, в (Caprolu, 2020) освещаются основные вопросы безопасности граничных вычислений, связанные, в том числе, с

применением технологий виртуализации к edge-системам, как с применением уязвимостей контейнерных инфраструктур, так и без них. В частности, показано, что архитектурные особенности инфраструктуры таких сценариев формируют наборы характерных им специфических программно-аппаратных уязвимостей, которые могут быть успешно эксплуатированы потенциальным нарушителем в рамках таких атакующих воздействий как удаленное выполнение кода, DoS-атаки и различные атаки переполнение (flooding-атаки), атаки сканирования портов и уязвимостей, атаки повышение привилегий, утечки данных и др.

Таким образом, в условиях отсутствия унифицированных средств обнаружения атак в киберфизических системах промышленного интернета вещей с использованием граничных вычислений, а также необходимой адаптивности таких механизмов под требования и условия функционирования конкретных сценариев выполнения конкретных систем с использованием граничных вычислений возникает необходимость разработки комплексной методики построения средств обнаружения атак, которая должна учитывать основные архитектурные и сценарные особенности граничных вычислений. К основным отличиям предлагаемой в настоящей работе методики можно отнести учет специфики граничных вычислений на всех основных стадиях методики, включающих проведение аналитического моделирования, натурно-имитационного моделирования, генерацию тестовых и обучающих наборов данных и проведение визуального анализа данных.

Материалы и Методы.

Методика построения средств обнаружения атак. Предлагаемая методика ориентирована на построение механизмов обнаружения атак в киберфизических системах промышленного интернета вещей с использованием граничных вычислений с учетом специфики структуры и особенностей функционирования таких инфраструктур. Предлагаемая методика включает выполнение следующих основных шести стадий, осуществление которых обеспечивает решение задач построения средств обнаружения атак в киберфизических системах промышленного интернета вещей с использованием граничных вычислений (Рис. 1). Данная методика предназначена для инженеров-проектировщиков и разработчиков программных комплексов для обеспечения информационной безопасности киберфизических систем промышленного интернета вещей, в которых значимая часть вычислительных процессов бизнес-логики системы возлагается на конечные устройства системы. Выполнение методики предполагается на этапах проектирования, тестирования, настройки и оценивания качества работы средств обнаружения атак. На рисунке 1 обозначены основные входные и выходные данные, при этом стадии методики представлены в виде прямоугольников, тогда как стрелки между ними формируют контуры управления и передачи данных между стадиями.

Входом методики являются формальная спецификация анализируемой

IIoT-системы, включающая набор функциональны требований и нефункциональных ограничений, а также перечень угроз информационной безопасности, связанных с ожидаемыми разновидностями атак, которые необходимо детектировать в процессе защищенного функционирования IIoT-системы.

Выходом методики является реализованный программный компонент, корректность функционирования которого подтверждается на основе эмпирических проверок – тестирования качества программных классификаторов и экспертного оценивания с использованием средств визуального анализа данных о работе построенных программных классификаторов.

На стадии 1 производится построение аналитической модели атакующих воздействий на IIoT-систему, реализующую концепцию граничных вычислений. На основе имеющихся спецификаций и перечня актуальных угроз для целевой системы такое моделирование предполагает получение результатов анализа по определению предполагаемых целей и мотивов нарушителя. При этом в общем случае нарушитель способен эксплуатировать как свойства распределенного сбора и обмена информацией между периферийными устройствами IIoT-системы, так и уязвимости самих устройств. Также определяются типовые сценарии нарушителя с уточнением отдельных шагов, включающих, воздействия, как физического характера, так и программно-информационного. Отметим, что идентифицируются также доступные ресурсы и используемые атакующим программно-аппаратные средства. Кроме того, в процессе проводимого анализа также выясняются стартовые возможности нарушителя и завязанные на это устройства и программно-аппаратные интерфейсы – места осуществления доступа, атакующего к системе.

В целях учета динамических особенностей функционирования целевой системы стадия 2 методики предполагает использованием методов натурного и имитационного моделирования. В частности, для получения исходных данных, адекватным образом описывающих одну или несколько различных видов атак, проанализированных на стадии 1 методики, закладывается формирование физической полнофункциональной или до определенной степени ограниченной натурной модели сети, включающей ряд целевых и обеспечивающих электронно-вычислительных и периферийных устройств, датчиков, связующего сетевого оборудования и других электронных компонентов. Ввиду возможной практической сложности подобного моделирования часть функциональности модели предполагается возможной к реализации за счет имитационного представления.

Стадия 2 предлагаемой методики включает также возможность поиска существующих наборов данных, включающих описание логов индустриальной системы интернета вещей. Такие наборы данных могут применяться, как для обогащения данных, формируемых в рамках методики, так и в качестве положительных примеров для формирования новых наборов данных с использованием имеющейся натурно-имитационной модели.

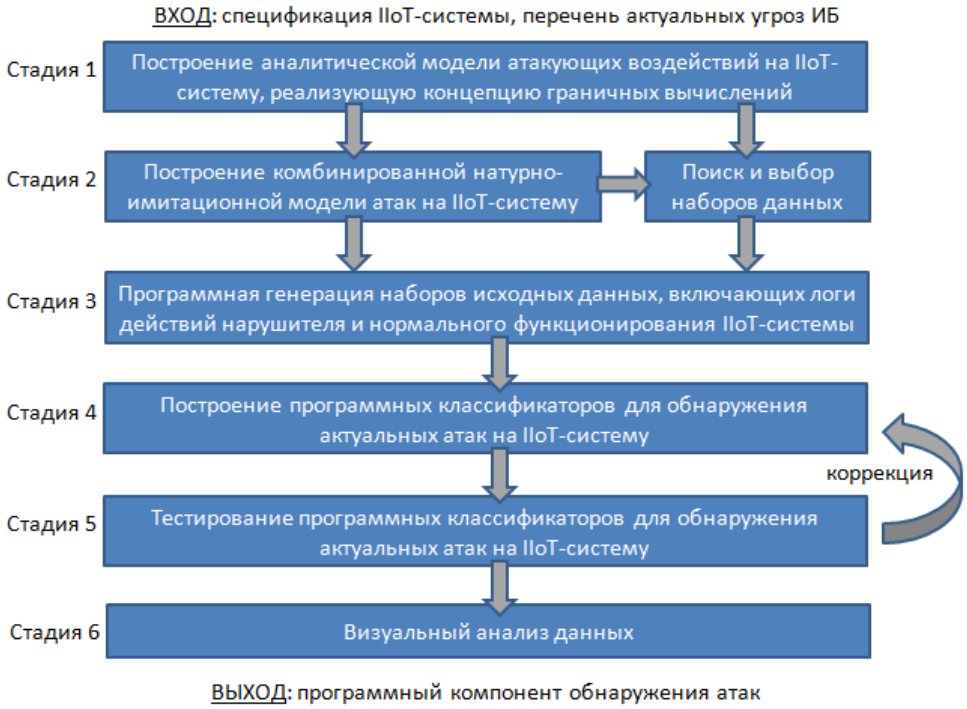

Рис.1. Схема методики построения средств обнаружения атак.

На стадии 3 осуществляется программная генерация наборов исходных данных, включающих логи действий нарушителя и нормального функционирования IIoT-системы. Формируемые на этой стадии исходные данные требуются для построения программных модулей обнаружения атак, а также для осуществления разметки данных по классам атак. Искомые наборы данных предполагается построить в рамках экспериментов с использованием натурно-имитационной модели, как в случае нахождения IIoT-системы под атакой, так и в случае ее нормального функционирования. Фактически, основой для такой генерации является запуск сценариев функционирования натурно-имитационной модели на наборах стартовых параметров модели с использованием правил управления устройствами граничных вычислений. На данной стадии также производится задание разметки в рамках генерируемых наборов исходных данных, которая в общем случае включает указание временных периодов моделирования атаки, а также физических и/или сетевых адресов устройств, вовлеченных в моделируемый сценарий в зависимости от используемых канальных, сетевых и прикладных протоколов, по которым происходит взаимодействие устройств граничных вычислений. Примером актуального вида атак на устройства граничных вычислений являются атаки отказа в обслуживании (Gulatas, 2023), атаки ransomware-шифрования (Job, 2021), botnet-атаки, как например Mirai (Febro, 2022), DSN poisoning-атаки

(Gulatas, 2023).

Стадия 4 охватывает построение программных классификаторов для обнаружения актуальных видов атак на IIoT-систему с использованием методов машинного обучения с учителем, включающих, в том числе, следующие методы: случайный лес, деревья решений, k-ближайших соседей, adaboost-классификатор, машина опорных векторов, LSTM и другие. На данной стадии возможно также применение дополнительных алгоритмов комбинирования классификаторов, включающих стекинг, мажоритарное голосование, а также алгоритмов сэмплинга – в случае необходимости балансировки обучающих и тестовых выборок. В частности, комбинирование бинарных классификаторов позволяет организовать эффективный мульти-классификатор по различным классам атакующих воздействий.

Стадия 5 включает проверку корректности построенных на стадии 4 программных классификаторов на тестовых выборках данных с вычислением значений точности, полноты, F1-меры и других классификационных показателей. В случае невыполнимости требований на показатели качества классификации производится возврат к стадии 4 с измененными значениями гипер-параметров классификационных методов и/или уточнением самих методов.

Стадия 6 включает проведение экспертного анализа построенных классификаторов на имеющихся наборах данных с использованием визуального анализа исходных данных и интерпретации результатов работы классификаторов. В частности, данная стадия методики предполагает использование методов уменьшения объемов и размерности анализируемых данных с применением алгоритма главных компонент (PCA) и алгоритма независимого компонентного анализа (ICA).

Обсуждение и результаты.

Применение методики и дискуссия. Обобщим основные полученные результаты данной работы. Конечной целью данного исследования является разработка эффективных методов управления производственными процессами для повышения качества продукции и оптимизации затрат. Работа предлагает целостный подход к обеспечению безопасности в киберфизических системах, интегрируя методы машинного обучения и экспертный анализ для повышения надежности и устойчивости к атакам. Статья посвящена разработке методики обнаружения атак в киберфизических системах промышленного интернета вещей, основанных на концепции граничных вычислений. В работе подчеркиваются актуальные проблемы безопасности в таких системах, обусловленные сложностью и разнообразием возможных атак, а также необходимостью учитывать распределенный характер инфраструктуры граничных вычислений.

Таким образом, предложена новая методика обнаружения атак, включающая, в частности, генерацию релевантных наборов данных, построение программных классификаторов и их проверку с использованием показателей качества классификации, экспертный анализ и интерпретация результатов с

использованием методов снижения размерности данных. Методика включает комбинацию различных алгоритмов машинного обучения для построения эффективного мульти-классификатора, способного обнаруживать широкий спектр атак. Разработанная методика предназначена для унифицированного подхода к защите разнородных IIoT-систем, учитывая разнообразие устройств, протоколов и атак.

В рамках данного исследования используются комплексный подход, включающий следующие основные методы: статистический анализ — проводится сбор и обработка данных о основных показателях IIoT-системы; методы аналитического и натурно-имитационного моделирования для представления и анализа процессов IIoT-системы и возможных атак на ее устройства; методы машинного обучения и визуального анализа данных в качестве основы комбинированного обнаружения атак.

Научная новизна методики заключается в комплексном подходе к обнаружению атак в IIoT-системах с использованием граничных вычислений, применении натурно-имитационной модели для генерации данных и комбинировании различных методов машинного обучения для создания универсального мульти-классификатора. Также учитывается разнородность систем и применяются методы снижения размерности данных для повышения точности и интерпретируемости результатов. Результаты исследований могут быть применены для улучшения безопасности промышленных киберфизических систем, минимизируя риски несанкционированного доступа и потери данных.

Отметим, что конкретный практический результат заключается в разработке методики, которую инженеры и разработчики смогут использовать для защиты IIoT-инфраструктуры от различных видов атакующих воздействий. Данная методика охватывает широкий спектр задач: от анализа потенциальных угроз до реализации механизмов их предотвращения. Она применима на этапе проектирования и тестирования систем, а также при настройке и оценке работы защитных средств.

Важным аспектом является использование натурно-имитационного моделирования, которое позволяет моделировать атаки и исследовать их воздействие на систему. Такой подход повышает точность и надежность методик защиты, поскольку он учитывает разнообразные сценарии атак.

Применение предложенной в работе методики производится на примере IIoT-системы в области управления инцидентами транспортной инфраструктуры, где устройствами граничных вычислений являются автономные программно-аппаратные модели дистанционно управляемых колесных робототехнических устройств на основе модулей платформы Arduino и совместимых с ней электронных компонентов. К отличительным особенностям методики, отличающей ее от альтернативных наработок и решений в предметной области комплексный учет граничных вычислений на протяжении методики и ее основных стадий. Это выражается, в том числе, в свойствах мобильности устройств граничных

вычислений, возможности их пространственного перемещения, изменчивости способов коммуникации и статистического распределения характера процессов сетевого взаимодействия (Ray, 2020; Goel, 2020). В свою очередь, это обуславливает наличие на таких устройствах узкоспециализированных уязвимостей, связанных с недостаточной защищенностью edge-устройства, и подверженностью актуальным видам атак на него. Таким образом, статья предлагает не только теоретическую основу, но и проверенную на практике методологию, готовую к внедрению в реальных проектах. Ниже приведен псевдокод, иллюстрирующий обобщенный алгоритм, лежащий в основе предложенной методики обнаружения атак с использованием граничных вычислений. Данный код специфицирует структуру методики и последовательность шагов, которые необходимы для выполнения методики с учетом специфики конкретной IIoT-системы, ее устройств и используемого инструментария. Алгоритм записан в процедурном виде императивного стиля программирования, символ # означают текст комментария, поясняющего конкретную команду и для удобства выделенный курсивом.

```
def simulate_attacks(): # Шаг 1: Аналитическое и натурно-имитационное моделирование атак
    simulated_attacks = generate_attack_scenarios() # Генерация типов атак (DDoS, Man-in-the-Middle и др.)
    simulation_results = run_simulation(simulated_attacks) # Моделирование атак на тестируемой системе
    return simulation_results
def prepare_datasets(): # Шаг 2: Генерация и разметка наборов данных
    raw_data = collect_sensor_data() # Сбор данных с датчиков и систем мониторинга
    labeled_data = label_data(raw_data) # Разметка данных: нормальные данные и аномальные (данные и описывающие атаки)
    return labeled_data
def build_classifier(data): # Шаг 3: Построение классификатора для обнаружения атак
    model_type = select_model_algorithm() # Выбор подходящего алгоритма машинного обучения
    trained_model = train_model(model_type, data) # Обучение модели на размеченных данных
    return trained_model
def visualize_data(data): # Шаг 4: Визуальный анализ данных
    plots = create_plots_and_diagrams(data) # Создание графиков и диаграмм для наглядного представления данных
    analysis_results = analyze_visualizations(plots) # Анализ визуальных данных для выявления аномалий
    return analysis_results
def evaluate_classifier(model, test_data): # Шаг 5: Настройка и оценка каче-
```

ства работы классификатора

```
    accuracy = calculate_accuracy(model, test_data) # Оценка точности классификатора на тестовых данных
    thresholds = set_thresholds(accuracy) # Определение пороговых значений для классификации атак
    return thresholds
def integrate_and_test(system, classifier): # Шаг 6: Интеграция и тестирование в промышленной среде
    integrated_system = deploy_classifier(classifier, system) # Интеграция классификатора в существующую систему
    test_results = perform_real_world_tests(integrated_system) # Тестирование интегрированной системы в реальных условиях
    return test_results
def main(): # Основная функция выполнения методики
    attack_simulations = simulate_attacks()
    datasets = prepare_datasets(attack_simulations)
    classifier = build_classifier(datasets)
    visual_analysis = visualize_data(datasets)
    evaluation_results = evaluate_classifier(classifier, datasets)
    integration_results = integrate_and_test(existing_system, classifier)
    print(«Методика выполнена. Результаты:», integration_results)
```

Предлагаемое в рамках методики натурно-имитационное моделирование может проводиться в рамках заданных начальных параметров устройств и/или процессов с применением системы правил, учитывающих возможные состояния системы и переходы между ними. Также проводится запуск такой имитационной модели на некотором множестве входных данных, зависящих от фактического выполнения используемой натурной составляющей модели. В частности, имитационная компонента такого моделирование позволяет упростить формирование распределенной функциональности сбора и обмена данными между устройствами граничных вычислений с минимизацией организационно-технических усилий по настройке и обработке функций граничных вычислений. Таким образом, в целом натурно-имитационные представления позволяют более точно и с ограниченными объемами ресурсов моделировать функционал целевой IIoT-системы, наиболее существенные поведенческие особенности устройств и пользователей системы.

Поэтому моделирование осуществляется с меньшими ресурсными и временными затратами, как в условиях нормального функционирования IIoT-системы, так и в условиях функционирования при нахождении системы под одной или одновременно несколькими атаками. При этом по результатам аналитического моделирования предполагается ранжировать установленные виды атак по степени их критичности для данного вида систем и выбрать наиболее актуальные виды несанкционированных воздействий для их последующего анализа. Отме-

тим, в частности, что комбинированный характер модели выражается в расширении натурной модели за счет применения имитационного моделирования части напрямую сложно моделируемых/конфигурируемых стадий определенной атаки.

В общем случае для проведения такого анализа данных в рамках предложенной методики, в зависимости от структуры и особенностей анализируемых данных может потребоваться применение дополнительных предваряющих методов предварительной обработки данных, включающих стандартизацию данных, нормализацию, фильтрацию и устранение пропущенных и/или ошибочных значений отдельных полей. Отметим, что потребность в подобной фильтрации может возникать, в том числе, по причинам возможного спонтанного динамического характера функционирования устройств граничных вычислений, доступность которых может нарушаться на определенные периоды времени в рамках штатной работы IIoT-системы.

Отметим также, что в результате применения граничных вычислений, несмотря на возможность снижения объемов, пересылаемых по сети данных, тем не менее, поверхность атаки IIoT-системы с реализацией граничных вычислений может в целом увеличиться по сравнению с системами, базирующимися на концепции облачных вычислений. В частности, концентрация данных на удаленно обрабатывающих edge-узах может способствовать повышению рисков утечки таких данных (Qiang, 2021). В частности, такие утечки могут происходить не только на фазе непосредственной их обработки, но также и в дальнейшей работе при их последующем хранении для обеспечения целей кэширования данных (Ghosh, 2021).

Кроме того, отметим, что использование имитационной составляющей в процессе моделирования позволяет осуществить генерацию данных и следующее за этим интеллектуальное обнаружение атак с изолированных edge-узлов централизовано, без вов, лечения таких вычислительных концепций, как федеративное вычисление и другие (Singh, 2023; Fenanir et al., 2023; Yang, 2023).

Выводы.

В рамках проведённого исследования разработана комплексная методика построения средств обнаружения атак в киберфизических системах промышленного интернета вещей, функционирующих на основе концепции граничных вычислений. Предложенный подход направлен на системное повышение уровня информационной безопасности IIoT-инфраструктур за счёт интеграции аналитического моделирования угроз, натурно-имитационного воспроизведения сценариев атак, методов машинного обучения и экспертной интерпретации результатов. В отличие от фрагментарных решений, ориентированных исключительно на применение отдельных алгоритмов обнаружения или анализ ограниченного набора атак, представленная методика формирует целостную технологическую цепочку построения и верификации механизмов защиты.

Одним из ключевых результатов работы является обоснование необходимости учёта архитектурной специфики граничных вычислений при

разработке средств обнаружения атак. В условиях переноса значительной части вычислительной нагрузки на периферийные устройства возрастает роль локального анализа данных и оперативного реагирования на инциденты. Вместе с тем расширяется поверхность атаки за счёт распределённости узлов и ограниченности их вычислительных ресурсов. Предложенная методика учитывает данные особенности и ориентирована на построение адаптивных механизмов обнаружения, способных функционировать в условиях динамически изменяющейся сетевой среды.

Существенное значение имеет включение в структуру методики стадии аналитического моделирования действий потенциального нарушителя. Это позволяет формализовать возможные сценарии атак с учётом их многошагового и комбинированного характера, определить критические точки воздействия и сформировать требования к будущим средствам обнаружения. Такой подход обеспечивает проактивный характер защиты, при котором средства обнаружения разрабатываются не только на основе уже известных инцидентов, но и с учётом потенциальных эволюционных изменений угроз.

Натурно-имитационное моделирование, являющееся центральным элементом методики, позволяет воспроизводить реальные условия функционирования IIoT-систем и моделировать поведение как легитимных пользователей, так и нарушителей. Формирование экспериментальной среды с использованием программно-аппаратных модулей, включая устройства на базе платформы Arduino, обеспечивает практическую применимость методики и приближает экспериментальные результаты к реальным условиям эксплуатации. Имитационная составляющая позволяет масштабировать моделирование без значительного увеличения затрат, что особенно важно при анализе распределённых систем с большим числом устройств.

Важным вкладом работы является формирование процедуры генерации и разметки наборов данных для обучения и тестирования программных классификаторов. В условиях недостатка публичных датасетов для IIoT-среды данный этап имеет принципиальное значение. Разработанная процедура обеспечивает формирование сбалансированных выборок, отражающих как нормальное состояние системы, так и различные типы атакующих воздействий. Это создаёт основу для построения устойчивых моделей машинного обучения, способных выявлять аномалии в распределённых средах.

Применение методов машинного обучения, включая алгоритмы ансамблирования, позволяет повысить точность обнаружения атак и обеспечить мультиклассовую классификацию угроз. Комбинирование различных моделей способствует снижению вероятности ложноположительных и ложноотрицательных срабатываний, что критически важно для промышленных систем, где ошибки обнаружения могут привести к существенным экономическим и технологическим последствиям. При этом учёт ограничений вычислительных ресурсов граничных устройств позволяет

адаптировать модели к реальным условиям эксплуатации без чрезмерного роста энергопотребления и задержек обработки.

Проведённая апробация методики на примере системы управления инцидентами транспортной инфраструктуры продемонстрировала её применимость и масштабируемость. Полученные результаты подтверждают, что интеграция интеллектуальных механизмов обнаружения атак на уровне граничных устройств способствует повышению устойчивости системы к распределённым сетевым и прикладным воздействиям. Методика может быть использована как на этапе проектирования и тестирования IIoT-систем, так и при модернизации уже функционирующих инфраструктур, что соответствует принципам безопасной разработки и эксплуатации (Security-by-Design и Security-by-Default).

Дополнительно следует отметить перспективность дальнейшего развития методики в направлении интеграции федеративных подходов к обучению моделей, повышения интерпретируемости решений классификаторов и расширения экспериментальной базы за счёт использования реальных промышленных данных. Перспективным представляется исследование вопросов устойчивости моделей к атакам на сами алгоритмы машинного обучения, включая adversarial-воздействия, а также разработка механизмов динамической перенастройки классификаторов в процессе эксплуатации.

Таким образом, разработанная методика формирует унифицированную, адаптивную и практически ориентированную основу для построения средств обнаружения атак в киберфизических системах промышленного интернета вещей с использованием граничных вычислений. Её внедрение способствует повышению надёжности и устойчивости распределённых промышленных инфраструктур, снижению рисков компрометации граничных узлов и обеспечению безопасного функционирования критически важных технологических процессов в условиях усложняющейся киберугрозной среды.

REFERENCES

Anwer M., Ahmed G., Akhunzada A., Amin R. (2022). Comparative Analysis of Soft Computing Approaches of Zero-Day-Attack Detection // Proceedings of the 2022 IEEE International Conference on Emerging Trends in Smart Technologies (ICETST). Pakistan. Vol. 1–5. 10.1109/ICETST55735.2022.9922937.

Asokan J. et al. (2023). A Case Study Using Companies to Examine the Nmap Tool's Applicability for Network Security Assessment // Proceedings of the 2023 IEEE 12th International Conference on Advanced Computing (ICoAC). India. Vol. 1–6. 10.1109/ICoAC59537.2023.10249544.

Alwarafy A. et al. (2021). A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things // IEEE Internet of Things Journal. Vol. 8(6). Pp. 4004–4022. 10.1109/JIOT.2020.3015432.

Caprolu M. et al. (2019). Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues // Proceedings of the 2019 IEEE International Conference on Edge Computing (EDGE). Vol. 116–123. DOI: 10.1109/EDGE.2019.00035.

Dolui K., Datta S.K. (2017). Comparison of Edge Computing Implementations: Fog Computing, Cloudlet and Mobile Edge Computing // Proceedings of the 2017 Global Internet of Things Summit (GIoTS). Switzerland. Vol. 1–6.10.1109/GIOTS.2017.8016213.

Esposito C., Castiglione A., Pop F., Choo K.-K.R. (2017). Challenges of Connecting Edge and Cloud Computing: A Security and Forensic Perspective // IEEE Cloud Computing. Vol. 4(2). Pp. 13–17. 10.1109/MCC.2017.30.

Febro A. et al. (2022). Edge Security for SIP-Enabled IoT Devices with P4 // Computer Networks. Vol. 203 // Article 108698. 10.1016/j.comnet.2021.108698.

Fenanir S., Semchedine F. (2023). Smart Intrusion Detection in IoT Edge Computing Using Federated Learning // Revue d'Intelligence Artificielle. Vol. 37(5). Pp. 1133–1145. 10.18280/ria.370505.

Golchin P. et al. (2022). Improving DDoS Attack Detection Leveraging a Multi-Aspect Ensemble Feature Selection // Proceedings of the 2022 IEEE/IFIP Network Operations and Management Symposium (NOMS). Hungary. Vol. 1–5. 10.1109/NOMS54207.2022.9789763.

Gulatas I. et al. (2023). Malware Threat on Edge/Fog Computing Environments from Internet of Things Devices Perspective // IEEE Access. Vol. 11. Pp. 33584–33606. 10.1109/ACCESS.2023.3262614.

Goel K. et al. (2020). Reliability Analysis of Edge Scenarios Using Pedestrian Mobility // Proceedings of the 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks – Supplemental Volume (DSN-S). — Spain. Vol. 61–62. 10.1109/DSN-S50200.2020.00033.

Ghosh S. et al. (2021). A High Performance Hierarchical Caching Framework for Mobile Edge Computing Environments // Proceedings of the 2021 IEEE Wireless Communications and Networking Conference (WCNC). Nanjing, China. Vol. 1–6. 10.1109/WCNC49053.2021.9417323.

Ilyin P.A. (2021). Osnovnye napravleniya primeneniya oblachnykh, granichnykh, tumannykh vychisleniy {Main Directions of Application of Cloud, Edge and Fog Computing} // StudNet. Vol. 4(6). Pp. 250–257.

Job G.K. et al. (2021). Impacts of Ransomware Attacks on Edge Computing Devices: Challenges and Research Opportunities // *International Journal of Engineering Research & Technology* (IJERT). Vol. 10(4). Pp. 665–670. 10.17577/IJERTV10IS040297.

Lin Z. et al. (2020). A Survey: Resource Allocation Technology Based on Edge Computing in IIoT // Proceedings of the 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI). United Arab Emirates. Vol. 1–5. 10.1109/CCCI49893.2020.9256663.

Muin M. et al. (2022). Campus Website Security Vulnerability Analysis Using Nessus // International Journal of Computer and Information System (IJCIS). Vol. 2(3). Pp. 79–82. 10.29040/ijcis.v3i2.72.

Nam D.H. (2023). A Comparative Study of Mobile Cloud Computing, Mobile Edge Computing, and Mobile Edge Cloud Computing // Proceedings of the 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE). NV, — USA. Vol. 1219–1224. 10.1109/CSCE60160.2023.00204.

Qiang W. et al. (2021). Defending CNN Against Privacy Leakage in Edge Computing via Binary Neural Networks // Future Generation Computer Systems. Vol. 125. — Pp. 460–470. 10.1016/j.future.2021.06.037.

Qing L. et al. (2018). Research on Key Technology of Network Security Situation Awareness of Private Cloud in Enterprises // Proceedings of the 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). —China. Pp. 462–466. 10.1109/ICCCBDA.2018.8386560.

Roman R. et al. (2018). Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges // Future Generation Computer Systems. Vol. 78(2). Pp. 680–698. 10.1016/j.future.2016.11.009.

Ray K. et al. (2020). Proactive Microservice Placement and Migration for Mobile Edge Computing // Proceedings of the 2020 IEEE/ACM Symposium on Edge Computing (SEC). CA, USA. Vol. 28–41. 10.1109/SEC50012.2020.00010.

Singh M.P. et al. (2023). Trusted Federated Learning Framework for Attack Detection in Edge Industrial Internet of Things // Proceedings of the 2023 IEEE Eighth International Conference on Fog and Mobile Edge Computing (FMEC). Tartu, Estonia . Pp. 64–71. 10.1109/FMEC59375.2023.10305910.

Shirazi S.N., Gouglidis A., Farshad A., Hutchison D. (2017). The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective // *IEEE Journal on Selected Areas in Communications*. Vol. 35(11). Pp. 2586–2595. 10.1109/JSAC.2017.2760478.

Toyin S. (2023). Comparative Analysis of Security Vulnerability Scanners (Nessus and OpenVAS) in Cloud Environment. Master's Project. Deane Road, Bolton. Vol. 89. 10.13140/RG.2.2.32627.71206.

Vankayalapati R.K. et al. (2023). Unifying Edge and Cloud Computing: A Framework for Distributed AI and Real-Time Processing // *Journal for ReAttach Therapy and Developmental Diversities*. Vol. 6. No. 9s(2). Pp. 1913–1926. 10.2139/ssrn.5048827.

Xiao Y. et al. (2019). Edge Computing Security: State of the Art and Challenges // Proceedings of the IEEE. 2019. Vol. 107(8). Pp. 1608–1631. 10.1109/JPROC.2019.2918437.

Yahuza M. et al. (2020). Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities // IEEE Access. Vol. 8. Pp. 76541–76567. 10.1109/ACCESS.2020.2989456.

Yang X. et al. (2024). Multi-Aspect Edge Device Association Based on Time-Series Dynamic Interaction Networks // Proceedings of the IEEE INFOCOM 2024 Workshops. Canada. Pp. 1–6. 10.1109/INFOCOM-

WKSHPS61880.2024.10620902.

Yang R. et al. (2023). Computers & Security // Computers & Security. Vol. 132 // Article 103381. 10.1016/j.cose.2023.103381.

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Собственник:
АО «Международный университет информационных технологий» (Казахстан, Алматы)

Главный редактор:
Колесникова Катерина Викторовна

Ответственный редактор:
Мрзабаева Раушан Жалиевна

Компьютерная верстка:
Калабай Замзагуль Ертугановна

Сайт журнала: https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Подписано в печать 30.03.2026.
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание АО "Международного университета информационных технологий"