ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ» РҚБ

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»

N E W S

OF THE NATIONAL ACADEMY OF
SCIENCES OF THE REPUBLIC OF
KAZAKHSTAN

SERIES OF PHYSICS AND MATHEMATICS

2 (354)

APRIL – JUNE 2025

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of Physics and Mathematics
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty).
Certificate **No. KZ20VPY00113741** on the re-registration of the periodical printed and online publication of the information agency, issued on **28.02.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«ҚР ҰҒА Хабарлары. Физика-математика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы).

Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **28.02.2025** ж. берген **№KZ20VPY00113741** Куәлік.

Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*

Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физико-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*

Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ20VPY00113741.** Дата выдачи **28.02.2025**

Тематическая направленность: *информационно-коммуникационные технологии.*

В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*

Периодичность: *4 раза в год.*

Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

INFORMATION AND COMMUNICATION TECHNOLOGIES

МАЗМҰНЫ

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

СОДЕРЖАНИЕ

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2. Namber 354 (2025). 92–106

https://doi.org/10.32014/2025.2518-1726.346

UDC 004.75

©T. Zhukabayeva[1,4], V. Desnitsky [2], Y. Mardenov[1,3], N. Karabayev[1], 2025.
[1] L.N. Gumilyov Eurasian National University, Astana, Kazakhstan;
[2]St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), Russia;
[3]Astana International University, Astana, Kazakhstan;
[4]Astana IT University, Astana, Kazakhstan.
E-mail: emardenov@gmail.com

INFORMATION SECURITY INCIDENT MANAGEMENT IN IIOT SYSTEMS WITH EDGE COMPUTING

Zhukabayeva Tamara — PhD, Professor, Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
E-mail: zhukabayeva_tk@enu.kz, ORCID ID: http://orcid.org/0000-0003-2783-186X;
Desnitsky Vasily — Senior Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), Russia,
E-mail: desnitsky@ comsec.spb.ru; ORCID 0000-0002-3748-5414;
Mardenov Yerik — research fellow, L.N. Gumilyov Eurasian National University, Astana International University, Astana, Kazakhstan,
E-mail: emardenov@gmail.com, ORCID ID: https://orcid.org/0000-0001-9284-9797;
Karabayev Nurdaulet — PhD student, research fellow, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
E-mail: 222240@astanait.edu.kz, ORCID ID: http://orcid.org/0000-0003- 2783-186X.

Abstract. *The main problem, its relevance:* This article addresses the scientific problem of improving approaches and tools for managing information security incidents in Industrial Internet of Things (IIoT) systems. The growing relevance of this topic is driven by the distributed nature of IIoT architectures, the extensive use of edge computing, and the presence of vulnerable wireless communication channels that pose threats to data integrity, service availability, and overall system stability. The proposed approach to managing information security incidents in IIoT systems is based on the edge computing concept. It covers the stages of distributed and coordinated data collection from various system devices, followed by filtering, normalization, standardization, aggregation, event correlation, and visualization of security-related data. Methods used: The research applies systems analysis, mathematical and physical modeling, machine learning–based forecasting, and visual data analytics. Key hypotheses and findings: The distinctive feature of

the proposed approach is the comprehensive consideration of incidents through the correlation of cyber-physical security events. Another important aspect is the distributed character of data processing within the IIoT infrastructure. Practical implementation: The feasibility of the approach is confirmed by a hardware-software prototype developed for managing incidents in the transport infrastructure of an industrial facility. Due to the presence of autonomous vehicles, edge computing is essential, with some control functions implemented directly within the vehicle's primary computing module. This enables effective distributed data processing and enhances security monitoring quality.

Key words: industrial internet of things (IIoT), edge computing, security monitoring, security incident, modeling

This work has been performed by the staff of the L.N. Gumilyov Eurasian National University with the financial support of the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23489127).

©Т. Жукабаева[1,4], В. Десницкий[2], Е. Марденов[1,3], Н. Карабаев[1], 2025.
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан;
[2]Ресей ғылым академиясының Санкт-Петербург федералды зерттеу орталығы (СПб ФЗО РҒА), Ресей;
[3]Астана халықаралық университеті, Астана, Қазақстан;
[4]Astana IT University, Астана, Қазақстан.
E-mail: emardenov@gmail.com

ІІОТ-ЖҮЙЕЛЕРІНДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ИНЦИДЕНТТЕРІН ШЕТКІ ЕСЕПТЕУЛЕРДІ ПАЙДАЛАНА ОТЫРЫП БАСҚАРУ

Жукабаева Тамара — PhD, профессор, Ақпараттық технологиялар факультеті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
E-mail: zhukabayeva_tk@enu.kz, ORCID ID: http://orcid.org/0000-0003-2783-186X;
Десницкий Василий — аға ғылыми қызметкер, Компьютерлік қауіпсіздік мәселелері зертханасы, Ресей Ғылым Академиясының Санкт-Петербург Федералды ғылыми орталығы (SPC RAS), Санкт-Петербург, Ресей,
E-mail: desnitsky@comsec.spb.ru, ORCID ID: 0000-0002- 3748-5414;
Марденов Ерік — ғылыми қызметкер, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана Халықаралық Университеті, Астана, Қазақстан,
E-mail: emardenov@gmail.com, ORCID ID: https://orcid.org/0000-0001-9284-9797;
Қарабаев Нұрдәулет — PhD докторанты, Л.Н. Гумилев Атындағы Еуразия Ұлттық Университетінің ғылыми қызметкері, Астана, Қазақстан,
E-mail: 222240@astanait.edu.kz, ORCID ID: http://orcid.org/0000-0003-2783-186X.

Аннотация: Негізгі мәселе және оның өзектілігі: Мақала Өнеркәсіптік Заттар Интернеті (Industrial Internet of Things, IIoT) жүйелерінде ақпараттық

қауіпсіздік инциденттерін басқару тәсілдері мен құралдарын жетілдіру жөніндегі ғылыми мәселені шешуге арналған. IIoT жүйелерінің үлестірілген құрылымы, граничтік (перифериялық) есептеулердің кеңінен қолданылуы және осал сымсыз байланыс арналарының пайда болуы — деректердің тұтастығына, қызметтердің қолжетімділігіне және жалпы жүйенің сенімділігіне елеулі қатер төндіретін факторлар болып табылады. Жұмыста ақпараттық қауіпсіздік инциденттерін басқаруға арналған edge computing тұжырымдамасына негізделген жаңа тәсіл ұсынылады. Ұсынылып отырған тәсіл жүйенің әртүрлі құрылғыларынан деректерді үлестірілген және үйлестірілген түрде жинау, оларды сүзгілеу, нормализациялау, стандарттау, агрегаттау, қауіпсіздік оқиғаларын корреляциялау және визуализациялау кезеңдерін де қамтиды. Қолданылған әдістер: Жүйелік талдау, математикалық және натуралық модельдеу, машиналық оқытуға негізделген болжау және деректерді визуалды талдау әдістері қолданылған. Негізгі гипотезалар мен қорытындылар: Тәсілдің басты ерекшелігі — кибер-физикалық қауіпсіздік оқиғаларын корреляциялау арқылы инциденттерді жан-жақты есепке алу. Практикалық іске асырылуы: Тәсілдің тиімділігі өнеркәсіптік кәсіпорынның көлік инфрақұрылымына арналған инциденттерді басқару бойынша аппараттық-бағдарламалық стенд мысалында дәлелденген. Автономды жұмыс істейтін көлік құралдарының болуы edge computing технологияларын қолдану қажеттігін айқындайды. Бұл жағдайда көлік құралдарын басқару функцияларының бір бөлігін деректерді алғашқы жинау нүктелерінде — көлік құралының негізгі есептеу модулінде жүзеге асыру орынды. Ұсынылған тәсілді енгізу арқылы құрылғылар деңгейінде операциялық деректерді үлестірілген түрде жинау, өңдеу және талдау ұйымдастырылып, нәтижесінде, қауіпсіздікті бақылау сапасы едәуір жақсарады.

Түйін сөздер: өндірістік заттар интернеті (IIoT), шеткі есептеу (edge computing), қауіпсіздікті бақылау, қауіпсіздік инциденті, модельдеу

©Т. Жукабаева[1,4], В. Десницкий[2], Е. Марденов[1, 2], Н. Карабаев[1], 2025.
[1]Евразийский национальный университет имени Л.Н. Гумилёва,
Астана, Казахстан;
[2]Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН), Россия;
[3]Международный университет Астана, Астана, Казахстан;
[4]Astana IT University, Астана, Казахстан.
E-mail: emardenov@gmail.com

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В IIOT-СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ

Жукабаева Тамара — кандидат технических наук, профессор факультета информационных технологий Евразийского национального университета им.Л.Н. Гумилева, Астана, Казахстан, E-mail: zhukabayeva_tk@enu.kz, ORCID ID: http://orcid.org/0000-0003-2783-186X;

Десницкий Василий — старший научный сотрудник лаборатории проблем компьютерной безопасности, Санкт-Петербургский федеральный исследовательский центр Российской академии наук (НПЦ РАН), Россия,
E-mail: desnitsky@comsec.spb.ru, ORCID 0000-0002-3748- 5414;
Марденов Ерик — научный сотрудник, Евразийский национальный университет им. Л.Н. Гумилева, Международный университет «Астана», Астана, Казахстан,
E-mail: emardenov@ gmail.com, ORCID ID: https://orcid.org/0000-0001-9284-9797;
Карабаев Нурдаулет — аспирант, научный сотрудник, Евразийский национальный университет им.Л.Н. Гумилева, Астана, Казахстан,
E-mail: 222240@astanait.edu.kz, ORCID ID: http://orcid.org/0000-0003-2783-186X.

Аннотация. Основная проблема, ее актуальность: Статья направлена на решение научной проблемы совершенствования подходов и средств управления инцидентами информационной безопасности в системах промышленного Интернета вещей (IIoT). Проблематика управления инцидентами безопасности становится все более актуальной ввиду распределенного характера IIoT-систем, широкого применения граничных вычислений и появлении уязвимых беспроводных каналов связи, создающих угрозы для целостности данных, сервисов и другие актуальные угрозы функционирования системы. В работе предложен подход к управлению инцидентами информационной безопасности в системах промышленного Интернета вещей (IIoT) с использованием концепции граничных (периферийных) вычислений (edge computing). Предложенный подход охватывает этапы распределенного и координированного сбора данных на различных устройствах системы, фильтрации, нормализации, стандартизации и агрегации собранных данных, корреляции и визуализации событий безопасности. Используемые методы: в работе применяются методы системного анализа, математического и натурного моделирования, методы прогнозирования на основе машинного обучения и методы визуального анализа данных. Основные гипотезы и выводы: отличительными чертами подхода являются всесторонний учет инцидентов на основе корреляции событий кибер-физической безопасности.. Практическая реализуемость подхода подтверждена на примере разрабатываемого аппаратно-программного стенда для управления инцидентами в транспортной инфраструктуре промышленного предприятия. Наличие автономно функционирующих транспортных средств определяет необходимость применения edge computing, при этом часть функционала управления транспортом целесообразно реализовать непосредственно в точках первичного сбора данных, в пределах основного электронного вычислительного модуля транспортного средства. Умение применять результаты на практике: реализация предложенного подхода к управлению инцидентами безопасности такой инфраструктуры позволит организовать распределённый сбор, обработку и анализ операционных данных на устройствах и будет способствовать улучшению качественных показателей мониторинга безопасности.

Ключевые слова: промышленный интернет вещей (IIoT), периферийное

вычисление (edge computing), мониторинг безопасности, инцидент безопасности, моделирование

Introduction. Currently, cyber-physical systems of the Internet of Things, functioning to solve various industrial problems (IIoT infrastructures), are becoming increasingly widespread. Such infrastructures are used in telemedicine, in distributed generation and transmission networks of electric power, in transport and logistics systems, in smart city management processes and other spheres of life.

In a number of works the concept of edge computing is directly associated with the expansion of cloud computing models by extending the functionality performed in the cloud to the edges of the computer network with the involvement of end user devices in such computations (Zhao, et al, 2018; Shirazi, et al, 2017). Such systems are also referenced to as mobile edge computing, representing the integration of cloud and mobile computing (Abbas, et al, 2018). In this case, part of the functionality of such systems and its execution are transferred to end devices, i.e. directly to the places of generation, removal or receipt of primary data (Fazeldehkordi, et al, 2022). In particular this is aimed at increasing the total volume of processed data and speeding up their processing (Ahmadi, 2024). In (Garg, et al, 2018), Garg, et al. note that in systems with edge computing, peripheral devices are able to analyze data in order to obtain information before acting with it. Given the distributed nature of edge computing, Chirra claims an increase in the efficiency of processing target data during the operation and a decrease in delays in the transmission and processing of data (Chirra, 2023). At the same time, when transferring a part of the functionality from the cloud to the edge device level, it is necessary to take into account limitations on the computing and storage resources of edge devices (Lin, et al, 2018).

In addition, Rapuzzi and Repetto note the specificity of using edge computing for systems with geographical distribution and a variety of device types with multilayer horizontal and vertical architectures and the use of virtualization (Rapuzzi, et al, 2018). Thus, within the framework of the multilayer architecture of a typical cyber-physical system, an additional edge layer appears, accumulating part of the target functionality of the system, information security functions and incident monitoring (Kim, et al, 2024). Thus, in a general case, the edge layer is structurally located between the cloud layer and the user terminal layer.

At the same time, the distribution of functionality from the cloud to other devices can significantly change the security context, which should be taken into account both at the stage of designing the target system and during its operation. Thus, in particular ensuring the proper security level in systems with edge computing may require the modification and development of anomaly detection and incident management mechanisms based on security policies (Shirazi, et al, 2017). At the same time, in general, the expansion of the system in the direction of the emergence of edge computing increases the attack surface due to the greater heterogeneity of devices and the rise in the number of potential vulnerabilities in the software and

hardware of such systems (Chirra, 2023). In particular, the most important types of attacks include data leaks, Denial-of-Service attacks, and attacks of unauthorized access to sensitive information located permanently or temporarily within the system devices (Chirra, 2023).

Fazeldehkordi and Grønli consider edge computing as computations that are performed not directly within the end cyber-physical user devices, but within one hop along network channels from them (Fazeldehkordi, et al, 2022). That is, such computations are performed within small data centers close to end users. The goal of such a scheme is to increase the efficiency of access to primary data, at least in the early stages of data processing, including filtering, preprocessing and aggregation of data from IoT devices. In addition, the advantage here is the ability to use the computing and storage resources of end devices that will be in close contact with such small data centers.

As a result, in general, edge computing provides higher computing performance in a distributed system due to some reduction in the level of centralization of data storage and processing, as well as computations. This allows for a reduction in the total latency time due to a decrease in access time to the data used. In addition, reducing the flows of transmitted data in the system allows for a descent in the number of types of data that can leak, as well as the total volumes of such sensitive data. In addition, due to possible pre-processing of data near the nodes, some of the data can be anonymized on them, thereby increasing the privacy of data when transmitting them to a central cloud or server. Thus, it becomes possible to more flexibly configure the functioning of such systems with the possibility of increasing data availability. In addition, there is less dependence on less reliable communication channels due to the expected reduction in the volume of transmitted data in such systems (Fazeldehkordi, et al, 2022).

The benefits of using edge computing to solve computationally heavy information security problems such as deep traffic inspection are also demonstrated in (Kozik, et al, 2018), where efficient traffic classification is performed using edge computing based on models pre-trained in the cloud.

Zhao, et al. propose a system that is based on edge computing technology and uses an edge cloud for organizing data collection and managing crowd social security incidents (Zhao, et al, 2018). Depending on the types of information got, including graphic, text, audio and video data, the police are able to check the current situation and respond in a timely manner. To optimize the police response and increase its efficiency, an ant colony optimization algorithm proposed by the authors is applied. Within the framework of the edge computing system server, data is collected and accumulated from individual user devices, smartphones. Besides, after that the data is processed and interpreted. In this case, the effectiveness of this algorithm is tested experimentally using software simulator Matlab. As an alternative example, in (Al-Zinati, 2020), edge computing technology is used to process and analyze medical information from user mobile devices in real time, including against biological outbreaks and epidemics.

In (Banik, et al, 2024), various machine learning methods and artificial neural networks are investigated for detecting attacks on cyber-physical systems with edge computing. The hypothesis on the potential effectiveness of such methods for detecting attacks such as intrusion, data breaches, and various other malicious actions is empirically confirmed using several datasets such as UNSW-NB15 and NSL-KDD. Based on the use of machine learning, a range of methods are also proposed in (Chirra, 2022) to improve the security of edge computing systems against attacks, as well as to enhance real-time anomaly detection, predictive analytics, and robust encryption techniques. Attack detection is also possible using cooperative approaches at several levels of edge computing system representation with improvement of a number of non-functional performance metrics of attack detection (Krishnan, et al, 2019).

In (Garg, et al, 2018), the concept of edge computing is further extended by involving unmanned aerial vehicles (UAVs) in the network. Such systems represent the next generation of intelligent transportation systems. The transmission of data from the vehicle to the edge devices for real-time analysis can be simplified by using UAVs, which can act as intermediate above-ground nodes between the vehicles and the edge nodes.

The issues of security incident management in systems using edge computing are becoming especially relevant due to the following three reasons. Namely these are, first, the importance of the correctness of target processes of cyber-physical systems in the Industrial Internet of Things, second, the distributed nature of functioning using edge computing, and, third, the presence of wireless communication channels for transmitting data between devices of such infrastructures. At the same time, wireless channels and data transmission protocols over them present vulnerabilities, and their exploitation allows attackers to successfully perform actions to compromise devices, data stored and circulated within the infrastructure, as well as information services provided to end users. The need to build mechanisms for managing information security incidents within such systems is due to the necessity for decentralized collection of primary data from sensors, operating system logs of devices, various user data, events from information security tools used, such as antiviruses, firewalls, network traffic scanning and interception tools, intrusion detection and prevention tools.

This article proposes an approach to managing information security incidents in systems using the concept of edge computing with the use of distributed and coordinated data collection on various devices of the system, filtering, normalization, standardization and aggregation of collected data, correlation and visualization of security events, as well as data mining. Unlike existing alternative published works, the novelty of this article includes a comprehensive accounting of incidents based on the correlation of information and cyber-physical security events, as well as the distributed nature of data collection and processing within an IIoT infrastructure.

The rest of the article is organised as follows. The next section includes a

description of the proposed approach to security incident management in cyber-physical systems implementing edge computing. The next section presents a description of the practical implementation in the form of an incident management test-bench for the transport infrastructure of an industrial enterprise and an analysis of the results obtained. The final section provides a summary of the results obtained and the main conclusions.

Materials and methods.

Based on the conducted analysis of the subject research field of cyber-physical security of systems using edge computing, we propose the following approach to security incident management. The approach includes the following 7 main stages, where the initial data are collected, cyber-physical security incidents are generated, processed and managed. In Fig. 1, the stages are schematically indicated by rectangles, and generally the stages are performed sequentially. Rectangles with rounded corners indicate the data that is the input and output of the stages. Arrows present control and data transmission loops, i.e. the output data of some stage in turn is the input for the next stage.

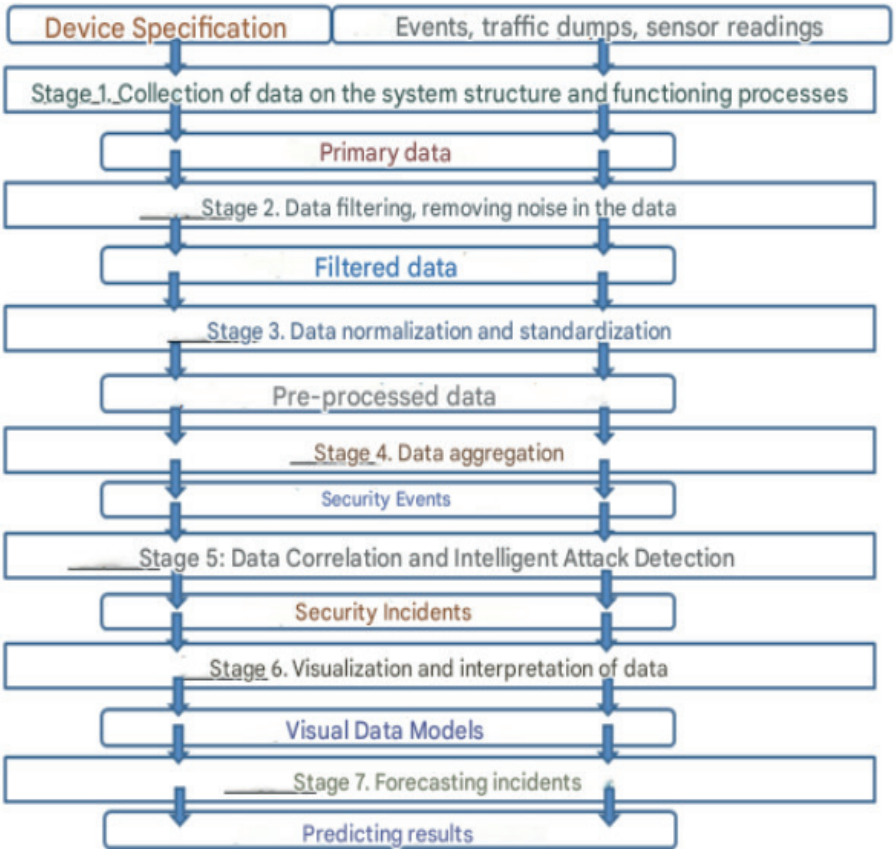

Fig. 1. An approach to managing security incidents in edge computing systems

In the framework of the proposed approach, the input data are, first, static data on the network structure and devices included in it in the form of specifications presented using CSV and JSON formats, as well as in the form of text descriptions and links to standards and open vulnerability databases, and, second, dynamic data generated directly during the network operation. Dynamic data characterize the processes of device operation and user behavior. An example of such data is streaming records of traffic between network devices and traffic outside and from outside the network. Another example is the logs of device operating systems, intrusion detection tools, antivirus and other tools presented in heterogeneous formats, different units of measurement and with different semantic features. Also, the initial data can include readings from the sensors of the system devices, data from user interfaces, data on the current states of device actuators.

At stage 1, the above-mentioned types of source data are collected and written to a single distributed storage, which generally can be divided among the system devices. The distribution of data among the devices during their storage can be performed taking into account, first, the data source devices and, second, the places of their direct target use. Note that according to the concept of edge computing, it is preferable to process such data near the end devices, including to minimize the number of operational calculations and improve the values of resource consumption indicators. A NoSQL database such as MongoDB, which is necessary when processing large data arrays, as well as traditional relational databases, can be used as a data storage technology. In addition, at stage 1 one can use security scanners, such as Nmap for building a network map, and Nessus for identifying specific vulnerabilities in the software used on the system devices. The result of stage 1 is so-called primary data, which can be used for further processing, analysis, visualization, interpretation, forecasting and making any management decisions regarding the functioning of the system and its information security.

At stage 2, data filtering is performed. It involves extracting the most significant data fragments only, for example, those one related to information security. The data filtering is performed using rules of the following type x^((n)) (t)→{0,1,… ,k}, where x^((n)) specifies the value of the next input vector of size n of data entering the filtering at time t, while the resulting values 0, 1, ... k indicate the need to discard (0) and leave this vector in the output data stream with redirection to computing units 1,2,...,k, respectively. Within the framework of this type of rules, regular expressions can also be used, specifying the need to fulfill certain properties for the rule to be triggered, for example, describing the network addresses of devices to which the rule in question is applicable, the time intervals for the rule to be triggered, restrictions on the types and volumes of data, and other characteristics. In addition, at stage 2, noise in the data is removed if necessary, for example, using Kalman filters (Thuraisingham, 2020) or other relevant digital signal processing methods. As a result of data filtering, the flow size can be significantly reduced. In addition, in case of large arrays of filtered data, parallelization is applied using Map-Reduce paradigm by Apache Hadoop framework within a computing cluster

integrated into the cyber-physical system (Apache Hadoop, 2024). Thus, the output of stage 2 presents filtered data and, if necessary, divided into several flows, where each one is supposed to be processed separately.

Stage 3 includes standardization and normalization of data, which involves their unification according to a single specification format. Also, if necessary, data can be standardized by converting to a given range, for example (0,1) while maintaining the statistical distribution. Thus, the output of stage 3 is pre-processed data suitable for subsequent generalization, transformations, and analysis.

At stage 4, data is aggregated, including data related to one or more devices, i.e. data sources. In particular at this stage some statistical transformations can be applied, such as formation of time series, as well as convolution of a range of information fields into one field. The result of this stage is the generated flows of security events, where each of them has a single presentation format. Such a format assumes, in fact, data in one of the existing formats (for example, JSON) with a specified list of metadata describing their sources, time of creation and last modification, and, if necessary, any other crucial characteristics.

At stage 5, individual security events are correlated into an incident that covers several events, such as a network event, an operating system event, and an event of the physical infrastructure of the system. In particular, linking an information security event, e.g. direct user access to the operating system of the on-board computer of a vehicle via a local hardware-software interface, and a physical security event, e.g. loading a vehicle with cargo in excess of the permitted weight, forms a cyber-physical security incident with a number of attributes describing the user, location of the vehicle, its speed, actual weight, etc. In addition, this stage uses trained software classifiers built using supervised machine learning methods, which are capable of identifying attacks of certain types based on the analysis of existing events. Thus, the output of this stage is a list of security incidents and some relevant types of attacks.

Stage 6 involves visualization of security events and incidents using various visual representations, including structured and unstructured graphical data models, such as scatter plots, tabular representations, planar graphs, tree maps, Chord diagrams, and trilinear coordinates (Kolomeets, et al, 2023). In combination with quantitative and qualitative data on the current functioning of the system, suitable visual models can be used to quickly assess the cyber-physical security of the system and identify anomalous data based on the overall situation and changing trends observed expertly.

At stage 7, forecasting of subsequent cyber-physical security incidents is performed taking into account the current behavioral characteristics of the functioning and the history of security events and incidents for the analyzed period. In particular, this stage involves the use of a recurrent neural network LSTM for sequential forecasting of security incidents with their iterative refinement as the time of their forecasting approaches.

Distinctive features of this approach include comprehensive accounting of

incidents based on the correlation of information and cyber-physical security events, which are performed at stages 4–7 of this approach. The peculiarities of this approach also include the distributed nature of the implemented processes of data collection and processing within the IIoT infrastructure. It should be noted that within the framework of the proposed approach, edge computing can be used primarily at stage 1 when collecting data directly on the devices of the cyber-physical system, at stages 2, 3 and 4 in the process of their filtering, pre-processing and aggregation, using decentralized methods of information presentation and processing. In this case, in general, stages 5, 6 and 7 are advisable to be fulfilled within the centralized network entities and devices, as well as within the cloud infrastructure.

Results

The practical part of the work includes the construction of a hardware/software test-bench implementing a laboratory research prototype of a fragment of an industrial system using the concept of edge computing with microcircuits. Besides it includes testing of the proposed approach to incident management using this tesn-bench. In fact, this prototype represents a full-scale model of a specialized service of the industrial Internet of Things for managing cyber-physical incidents of a transport infrastructure.

The modeled object presents a rectangular industrial place with two transport vehicles (T1 and T2) moving along specified routes around the place for loading and unloading materials or products of some industrial production. The vehicles move along the perimeter of the place. Loading and unloading points for materials are also located along the perimeter. The vehicles are 4 wheeled robotic models of cars with an engine that allows them to move in two directions (forward and backward) and turn 90 degrees, both when moving forward and backward (Fig. 2).

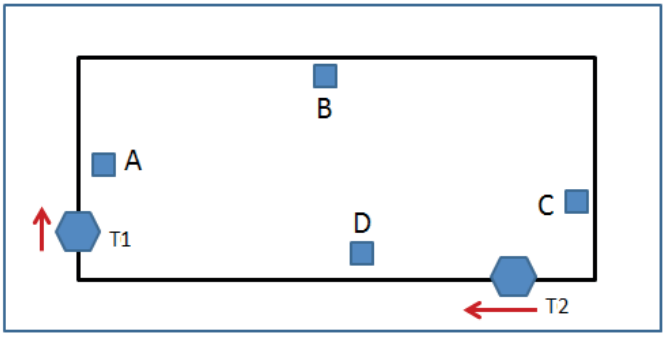

Fig. 2. Schematic of a fragment of the test-bench of the transport infrastructure system for modeling cyber-physical security incidents

The test-bench includes a control server. Using it the system operator can assign tasks to the vehicles. For example, a task may be as follows, it is necessary to drive to point A → accept cargo → move to point B → unload cargo. Both vehicles (T1

and T2) have a permanent network connection to the server via a wireless channel, and both vehicles can also communicate to each other via a wireless channel. The hardware/software test-bench currently being implemented is based on the use of Arduino microcontrollers, a wheeled platform, several sensors and a Wi-Fi channel. Using a wireless channel, control of physical models of the vehicles is realized.

In general, based on data on the movement and operation of the vehicles, as well as any additional data characterizing the technological process of a given industrial facility, incidents of information and physical security can be generated on the server. But as a result of the possibility of direct data exchange between two vehicles, it becomes possible to process some of the incidents directly on the vehicles, that is, at the data collection points. This is essentially the edge computing that is of primary interest in the modeling being performed.

The modeled incidents include the following two types of transport infrastructure incidents.

– Information security incidents. An example of such an incident is a transfer of some false information from a vehicle to the server, for example, incorrect data on the state of the vehicle, i.e. an illegitimately modified information field that determines whether the vehicle is currently loaded or unloaded.

– Physical security incidents. An example of such one is an incident of a collision between two vehicles or their dangerous approach to each other.

It should be noted that in general, some complex, composite incidents may arise, including manifestations at the information level and at the physical level at the same time.

Discussion

The feasibility of the proposed approach to information security incident management is confirmed by an example of a currently developed hardware/software test-bench for incident management of the transport infrastructure of an industrial enterprise. The scenario under study includes modeling an incident of dangerous approach of vehicles during modeled movement along specified trajectories in accordance with specified rules. Table 1 discloses the security incident management process for this case study in the form of data generated and processed within the stages of the proposed approach in compliance with the scheme shown in Fig. 1.

Table 1. Incident management using the example of a fragment of the transport infrastructure of an industrial enterprise

Stage	Incident of dangerous approach of the vehicles
1	Vehicle location event chains T_1 and T_2 $\{al_{\{i\}}(T_1)(t_i)\}_{\{i\in I\}}$, $\{al_{\{i\}}(T_2)(t_i)\}_{\{i\in I\}}$, where I – index for designating discrete time moments of occurrence of events *al* for vehicles T_1 and T_2
2	Eliminate duplication in data, including events of position of vehicle T_1 and T_2 in a state of no movement for some period of time $\{al_{\{i\}}(T_1)(t_i)\}_{\{i\in I\}} \rightarrow \{al_{\{i\}}(T_1)(t_i)\}_{\{i\in I'\}}$, where $I' \subseteq I$

3	Transformation of local positioning values of a specific vehicle based on a black line scanner (one-dimensional value $al_{\{i\}}$) into global location values on the industrial place (two-dimensional vector value $(al^{(1)}_{\{i\}}, al^{(2)}_{\{i\}})$) $\{al_{\{i\}}(T_1)(t_i)\}_{\{i\in I'\}} \rightarrow \{(al^{(1)}_{\{i\}}, al^{(2)}_{\{i\}})(T_1)(t_i)\}_{\{i\in I'\}}$
4	Formation of vehicle trajectories $\{al_{\{i\}}(T_1)(t_i)\}_{\{i\in I\}} \rightarrow \{tr_{\{i\}}\}$ and $\{al_{\{i\}}(T_2)(t_i)\}_{\{i\in I\}} \rightarrow \{tr_{\{i\}}\}$, necessary to identify a close-in incident
5	Checking conditions $\bigcup_{i\in I'}(\{\mid al_{\{i\}}(T_1)(t_i) - al_{\{i\}}(T_2)(t_i) \mid < d\})$
6	Expert selection of the most effective visual means for displaying identified incidents, including a graphical two-dimensional map of the physical place and a traffic light model
7	Using LSTM recurrent neural networks to form chains of *n* previous events to iteratively predict future $(n+1)^{th}$, $(n+2)^{th}$,..., $(n+k)^{th}$ events with the issuance of forecasts *(type(in), t_i, P_i)* as a result, where t_i means predicted time of incident *in* of type *type(in)* with probability P_i

The feasibility of the developed test-bench and the modeled scenario of movement of two models of vehicles is confirmed experimentally. During the testing, the attack and anomaly detection component generated security incidents using calculations on vehicle microcontrollers, thereby implementing edge computing.

The advantages of the proposed approach include flexibility in the use of computing resources of the cyber-physical system by transferring part of the calculations to the end devices, i.e. cyber-physical models of the vehicles. In addition, in conditions of possible communication failures, it becomes possible to process part of the data and make some operational decisions locally directly on the side of the vehicles. This helps to increase the reliability and uninterrupted operation. This circumstance is especially relevant for transport systems, when the connection of the vehicle with the server or cloud can occasionally deteriorate or disappear due to the limited range of the wireless signal and possible electromagnetic interference.

Conclusion. This article proposes an approach to managing information security incidents in IIoT systems using edge computing. The approach allows for the formation of mechanisms for collecting and processing initial data, generating security events and incidents, identifying attacks and providing information about them to the operator in an interpretable form within the framework of solving transport infrastructure problems. As a direction for further research on this topic, we are planning experiments to calculate indicators of efficiency, reliability and resource consumption on a fully functional implementation of the proposed hardware/software test-bench.

References

Apache Hadoop. Official web cite. https://hadoop.apache.org (accessed on 2024.11.25). (in English)

B. Thuraisingham, "Cyber Security and Artificial Intelligence for Cloud-based Internet of Transportation Systems," 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). — New York, NY, USA, 2020, — P. 8-10, doi: 10.1109/CSCloud-EdgeCom49738.2020.00011. (in English)

B.R. Chirra. Securing Edge Computing: Strategies for Protecting Distributed Systems and Data. International Journal of Advanced Engineering Technologies and Innovations. (2023) — Volume 1. — Issue 01. — P. 354-373. (in English)

D.R. Chirra. Secure Edge Computing for IoT Systems: AI-Powered Strategies for Data Integrity and Privacy. Revista de Inteligencia Artificial en Medicina. — Volume 13. — Issue 01 (2022). — P. 485-508. (in English)

E. Fazeldehkordi, T-M Grønli. A Survey of Security Architectures for Edge Computing-Based IoT. IoT. 2022; 3(3):332-365. https://doi.org/10.3390/iot3030019 (in English)

F. Lin, Y. Zhou, X. An, I. You and K. -K. R. Choo, "Fair Resource Allocation in an Intrusion-Detection System for Edge Computing: Ensuring the Security of Internet of Things Devices," in IEEE Consumer Electronics Magazine, vol. 7. — no. 6. — P. 45-50. — Nov. 2018, doi: 10.1109/MCE.2018.2851723. (in English)

H. Kim, J. Choi. Recommendations for Responding to System Security Incidents Using Knowledge Graph Embedding. — Electronics, 2024. — 13. — 171 p. https://doi.org/10.3390/electronics13010171 (in English)

M. Al-Zinati, T. Almasri, M. Alsmirat, Y. Jararweh. Enabling multiple health security threats detection using mobile edge computing. Simulation Modelling Practice and Theory. — Volume 101, 2020. — 101957, https://doi.org/10.1016/j.simpat.2019.101957. (in English)

M. Kolomeets, V. Desnitsky, I. Kotenko, A. Chechulin. Graph Visualization: Alternative Models Inspired by Bioinformatics. — Sensors, 2023. — 23. — 3747p. https://doi.org/10.3390/s23073747 (in English)

N. Abbas, Y. Zhang, A. Taherkordi and T. Skeie, "Mobile Edge Computing: A Survey," in IEEE Internet of Things Journal. — vol. 5. — no. 1, — P. 450-465, Feb. 2018, doi: 10.1109/JIOT.2017.2750180 (in English)

P. Krishnan, S. Duttagupta, K. Achuthan. SDNFV Based Threat Monitoring and Security Framework for Multi-Access Edge Computing Infrastructure. Mobile Netw Appl 24, — P.1896–1923 (2019). https://doi.org/10.1007/s11036-019-01389-2. (in English)

R. Kozik, M. Chora´s, M. Ficco, F. Palmieri, A scalable distributed machine learning approach for attack detection in edge computing environments, J. Parallel Distrib. Comput. (2018), https://doi.org/10.1016/j.jpdc.2018.03.006. (in English)

R. Rapuzzi, M. Repetto, Building situational awareness for network (in English)

S. Ahmadi. (2024) Security Implications of Edge Computing in Cloud Networks. Journal of Computer and Communications, 12, — P.26-46. doi: 10.4236/jcc.2024.122003. (in English)

S. Banik, P.R. Kothamali, S.M.S. Dandyala. (2024). Strengthening Cybersecurity in Edge Computing with Machine Learning. Revista de Inteligencia Artificial en Medicina. — Volume 15. — Issue 01. — P. 332-364. (in English)

S. Garg, A. Singh, S. Batra, N. Kumar and L. T. Yang, "UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles," in IEEE Network. — Vol. 32. — no. 3, — P. 42-51, May/June 2018, doi: 10.1109/MNET.2018.1700286. (in English)

S. Garg, A. Singh, S. Batra, N. Kumar and L. T. Yang, "UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles," in IEEE Network. — Vol. 32. — no. 3. — P. 42-51, May/June 2018, doi: 10.1109/MNET.2018.1700286. (in English)

S. N. Shirazi, A. Gouglidis, A. Farshad and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective," in IEEE

Journal on Selected Areas in Communications. — Vol. 35. — no. 11. — P. 2586-2595, Nov. 2017, doi: 10.1109/JSAC.2017.2760478. (in English)

threats in fog/edge computing: Emerging paradigms beyond the security perimeter model, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.04.007. (in English)

Y. Zhao, Z. Li, X. Chen and Y. Chen, "Mobile Crowd Sensing Service Platform for Social Security Incidents in Edge Computing," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS. — Canada, 2018. — P. 568-574, doi: 10.1109/Cybermatics_2018.2018.00118. (in English)

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 20.06.2025.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
20,0 п.л. Заказ 2.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19