REPUBLIC OF AZERBAIJAN

On the right of the manuscript

A B S T R A C T

of the dissertation for the degree of Doctor of Science

DEVELOPMENT OF METHODS AND ALGORITHMS FOR CYBER RESILIENCE OF CYBER-PHYSICAL SYSTEMS

Specialty:	3338.01 – System analysis, control and information processing (information technology)
Field of science:	Technical sciences
Applicant:	**Sukhostat Lyudmila Valentinovna**

Baku – 2025

The work was performed at the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

Scientific supervisor: Full member of ANAS,
Doctor of Technical Sciences, Prof.
Rasim Mahammad oglu Alguliyev

Official opponents: Doctor of Technical Sciences, Prof.
Naila Fuad gizi Musayeva
Doctor of Technical Sciences, Prof.
Valeh Azad oglu Mustafayev
Doctor of Technical Sciences, Assoc. Prof.
Zarifa Gasim gizi Jabrayilova
Doctor of Technical Sciences, Prof.
Balami Qasim oglu Ismailov

Dissertation Council ED 1.35 of Supreme Attestation Commission under the President of the Republic of Azerbaijan operating at the Institute of Information Technology of the Ministry of Science and Education

Chairman of the Dissertation Council:
Full member of ANAS,
Doctor of Technical Sciences, Prof.
Rasim Mahammad oglu Alguliyev

Scientific Secretary of Dissertation Council:
Doctor of Philosophy in Technical Sciences,
Assoc. Prof.
Fargana Jabbar gizi Abdullayeva

Chairman of the scientific seminar:
Doctor of Technical Sciences
Mutallim Mirzaahmed oglu Mutallimov

GENERAL CHARACTERISTICS OF THE WORK

The relevance of the topic and the degree of development. Modern information technologies are an important means of development for the government and society. Cyber-physical systems (CPS) are the foundational technology for implementing the Industry 4.0 concept and a key component of intelligent objects widely used in various fields of human activity.

Key technology trends underlying CPS include the Internet of Things, smart power grids, intelligent manufacturing systems, and cloud computing, among others. The cyber-physical system is the foundation for the development of the following areas: smart manufacturing, smart medicine, smart buildings and infrastructures, intelligent transportation systems, mobile systems, defense systems, and weather monitoring systems [4].

CPS systems are a combination of two technologies: information technology (IT) at the cyber level and operational technology (OT) at the physical level. The cyber level comprises servers, database systems, hosts, and other related components. The physical level consists of sensors, actuators, feedback systems, among other components, which are responsible for managing production facilities.

The CPS system requires the connection of many devices and systems to collect and exchange huge amounts of data across OT and IT platforms. To achieve this, there are various automation protocols that need to be connected to achieve the set goals. ISO 22301:2019 standard is crucial for increasing the resilience of organizations to various unexpected failures, ensuring the continuity of operations and services.

Additionally, the importance of ensuring their cybersecurity has increased dramatically in recent years following a series of cyberattacks.

Cyberattacks on the CPS system pose a significant risk to human health and safety and threaten serious damage to the environment. Interest in ensuring the information security of CPS has increased dramatically since the 2010 Stuxnet computer virus cyberattacks. Due

to the constantly changing cyber threats, it is necessary to develop a higher-level methodology that requires the detection of embedded and hidden cyberattacks, ensuring more cyber-resilient and secure cyber infrastructures.

On March 12, 2024, the European Parliament approved the proposed Cyber Resilience Act (CRA). It will apply to all products with digital elements presented on the European market that involve a direct or indirect logical or physical connection of data to a device or network.

Disruption of the CPS system and the failure of its components can lead to serious damage, highlighting the importance of considering the cybersecurity of CPS as a priority.

The transition to Industry 4.0 has created new tasks and challenges for the Republic of Azerbaijan, as well as for the whole world. The Republic of Azerbaijan has all the opportunities for the development of the Fourth Industrial Revolution. The country is constantly developing advanced technologies. On March 19, 2025, the "Artificial Intelligence Strategy for 2025-2028" was approved.

Today, all Industry 4.0 technologies are applied in various critical infrastructures across the Republic of Azerbaijan, including oil and gas platforms, transportation systems, and other key sectors.

Active cooperation with the World Economic Forum led to the establishment of the Center for Analysis and Coordination of the Fourth Industrial Revolution in Baku in accordance with the decree of the President of the Republic of Azerbaijan dated January 6, 2021. The activities of the center are designed to ensure the development of artificial intelligence and machine learning, as well as to serve citizens, the development of the digital economy, and further improve various research areas in the country.

On April 17, 2021, a decree "On Certain Measures to Ensure the Security of Critical Information Infrastructure" was signed.

Thus, according to the Law of the Republic of Azerbaijan on Amendments to the Law of the Republic of Azerbaijan "On Information, Informatization and Information Protection" dated May 27, 2022, the concepts of "critical information infrastructure," its

object and subject, as well as the legal basis for ensuring its security are added. On August 28, 2023, the “Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023-2027” was approved. On November 29, 2024, the Cabinet of Ministers of Azerbaijan approved the “List of Critical Information Infrastructure Facilities.”

By the Decree of the President of the Republic of Azerbaijan dated January 16, 2025, the "Concept of Digital Development in the Republic of Azerbaijan" was approved.

Detection of modern cyberattacks is critical for the sustainable operation of the cyber-physical system. Traditional defense mechanisms are becoming increasingly ineffective due to the methods used by attackers. Cyber-attack risks arise from the integration of the cyber and physical domains, in other words, the integration of the IT and OT domains. In this context, the development of adaptive, more effective methods for detecting cyberattacks is an urgent need to protect IT and OT infrastructures from such threats.

Critical situations are ideal for cybercriminals because they can exploit the weakest link – the human factor. Cybercriminals exploit the human factor to gain unauthorized access, steal credentials, and infect systems with malicious software (malware).

It is important to develop detection algorithms and countermeasures for all known cyberattacks in advance to reduce their impact and minimize damage to the system. However, research shows that a more in-depth analysis of CPS systems’ cybersecurity is required, particularly regarding the applicability of artificial intelligence-based approaches.

The top five research universities working on this issue include the University of California, Berkeley (USA), Beijing University of Science and Technology (China), KTH Royal Institute of Technology (Sweden), Politecnico di Milano (Italy), and Hamburg University of Technology (Germany).

As we move towards Industry 4.0, CPS is becoming increasingly complex, distributed, and data-driven, which gradually turns intrusion and anomaly detection into a big data problem. The challenge is to

analyse large amounts of data, heterogeneous in nature, with minimal computational effort.

Using sensors, actuators, and other devices to collect data from CPS provides useful information for their subsequent analysis. However, today the volume of stored data is becoming too large to be processed by traditional algorithms. Researchers have to ulilize various approaches, such as data partitioning and the utilization of a priori knowledge. Thus, working with big data necessitates formalizing new methods used by researchers and creating new algorithms that use the capabilities of machine learning methods to work with large-volume and high-dimensional data. However, existing algorithms are not always effective due to their high computational complexity.

Machine learning methods are widely used to analyse the CPS data for cyberattacks. In theory, machine learning algorithms can achieve high performance, i.e., minimize the false alarm rate and maximize detection accuracy [10]. However, an infinite number of training samples is usually required. In practice, this condition is impossible due to the limited computing power and the requirement for a real-time response [10]. In this regard, attackers often look for and target the weakest link - the most vulnerable functional component in CPS. The most vulnerable devices can be a good starting point for an effective study of security vulnerabilities. Existing methods cannot comprehensively analyse common multi-stage cyber attacks in the CPS environment [30].

Solving the considered problems is an important task; therefore, various methods and algorithms have been developed and applied in practice. Most of them consider either cybersecurity only in the IT environment or security in the operational technology environment. Ensuring protection against cyber-physical attacks is a serious problem that requires cyber resilience assessment methods that can study close interactions and interdependencies between cyber and physical components in the cyber-physical systems. However, existing methods do not take this specificity into account.

In light of the above, it can be concluded that, at present, there is no unified approach to designing safe and cybersecure CPS. This

dissertation research is aimed at developing methods and algorithms to ensure the cybersecurity of IT components and the safety of the operational technology components.

The object and subject of the research. The **object** of the research is IT cybersecurity and OT safety of the CPS systems; the **subject** of the research is models and methods for control processes to ensure the cyber resilience of the CPS systems.

The purpose and objectives of the work. The aim of the dissertation is to develop methods and algorithms for ensuring the cyber resilience and information security of cyber-physical systems based on intelligent analysis of big data on cyberattacks and system failures.

The following **objectives** are solved in the work to achieve this goal**:**

- Analysis and study of existing methods and algorithms for cyber resilience of the CPS systems;
- Development of a conceptual model for CPS cyber-resilience;
- Development of methods and algorithms for intelligent processing of big data to ensure the cyber resilience of CPS;
- Development of methods and algorithms for cybersecurity of CPS information technologies;
- Development of methods for the safety of CPS operational technologies;
- Development of a method for determining the criticality of functional CPS components' vulnerabilities;
- Development of a method for assessing the CPS risks.

The **research methods** are based on the application of information security theory, machine learning, probability theory, fuzzy number theory, pattern recognition theory, risk analysis, and decision making.

The main provisions for the defense

- Conceptual model for cyber resilience of CPS;
- An algorithm for detecting outliers in big data based on the k-means method to reduce the risk of blocking CPS;

- An algorithm for analysing big data of the CPS based on weighted clustering;
- A method for parallel processing of big data to reduce the risk of CPS failure;
- A method for clustering big data of the CPS based on a consensus ensemble;
- A method for classifying cyberattacks on CPS using extreme machine learning;
- A method for detecting DoS cyberattacks on CPS using an ensemble of classifiers;
- An algorithm for detecting malware in CPS based on images;
- A method for detecting anomalies in operational technologies of CPS based on hierarchical hidden Markov models for a water treatment system;
- A method for detecting anomalies in acoustic signals of CPS using transfer learning;
- A method for detecting cyberattacks on the CPS devices using a deep hybrid model for a water treatment system;
- A method for classifying CPS failures based on images;
- A method for determining the criticality of functional CPS components vulnerabilities based on the Bayesian attack graph for natural gas pipeline transportation;
- Method for assessing the CPS risks using the fuzzy Sugeno integral for wind energy generation.

The **scientific novelty** of the work is as follows:

- a three-level conceptual model has been developed to solve a number of problems related to cyber-resilience of CPS;
- an algorithm for detecting outliers in big data based on the k-means method has been developed to reduce the risk of CPS blocking;
- an algorithm for analysing CPS big data based on weighted clustering has been developed;

- a method for parallel processing of big data has been developed to reduce the risk of CPS failure;
- a method for cluster analysis of CPS big data based on a consensus ensemble has been developed;
- a method for classifying cyberattacks on CPS using extreme machine learning has been developed;
- a method for detecting DoS attacks on CPS using an ensemble of classifiers has been developed;
- an algorithm for detecting malware in CPS based on images has been developed;
- a method for detecting anomalies in CPS operational technologies based on hierarchical hidden Markov models has been developed for a water treatment system;
- a method for detecting anomalies in the CPS acoustic signals using transfer learning has been developed;
- a method for detecting cyberattacks on CPS devices using a deep hybrid model has been developed for a water treatment system;
- a method for classifying CPS failures based on images has been developed;
- a method for determining the criticality of functional CPS components vulnerabilities based on the Bayesian attack graph for natural gas pipeline transportation has been developed;
- a method for assessing CPS risks using the Sugeno fuzzy integral for wind energy generation has been developed.

The theoretical and practical significance of the work. The scientific and practical value of the problems considered in the dissertation is that the developed methods and algorithms can be used to ensure the cyber resilience of CPS systems in order to improve OT safety and IT cybersecurity. The developed methods and algorithms have been published in scientific journals and presented in the form of a thesis at international scientific conferences and are publicly available for use. The scientific validity and reliability of the obtained results are con-

firmed by the use of modern research methods, as well as by comparison with the results of previously proposed methods and algorithms in the studied area in order to confirm their effectiveness.

The results obtained in the dissertation thesis have practical significance and can be used in the following areas:

- development of proposals for strategies and programs to ensure the cyber resilience of CPS;
- cyberattack detection systems to ensure the reliability, cybersecurity, cyber resilience, and efficiency of CPS;
- usage by experts in the analysis of the CPS cyber resilience to improve the safety of OT and IT cybersecurity.

Approbation and application of the results. The main scientific, theoretical and practical results of the dissertation were presented and discussed at: seminars of the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan, as well as at the following Republican and international scientific conferences: III Republican Scientific and Practical Conference on "Applied mathematics issues and new information technologies" (Sumgait, December 15-16, 2016); I Republican Conference on "Current scientific and practical problems of software engineering" (Baku, May 17, 2017); I Republican Scientific and Practical Conference on "Big data: opportunities, multidisciplinary problems and prospects" (Baku, February 25, 2016); XIII International Scientific and Technical Conference "Recognition-2017" (Kursk, Russia, May 16-19, 2017); IV Republican Conference on "Current multidisciplinary scientific and practical problems of information security" (Baku, December 14, 2018); X International Conference on "Application of Information and Communication Technologies" (AICT-2016) (Baku, October 12-14, 2016); III Republican Scientific and Practical Conference on "Current problems of information security" (Baku, December 8, 2017); XV International Scientific and Technical Conference "Recognition-2019" (Kursk, Russia, May 14-17, 2019); XIII International Youth Scientific Conference on "Technical Sciences. Industrial Management" (Borovets, Bulgaria, March 11-14, 2020); "Global Cyber Security Forum 2019" (Kharkiv, Ukraine, November 14-16, 2019); XIV International

Scientific and Technical Conference "Recognition-2018" (Kursk, Russia, September 25-28, 2018); XIII International Conference on "Application of Information and Communication Technologies" (AICT-2019) (Baku, October 23-25, 2019); V Republican Conference on "Current multidisciplinary scientific and practical problems of information security" (Baku, November 29, 2019); International Conference on "Information Security: Problems and Prospects" (Baku, October 29, 2021); NATO ARW International Scientific Seminar on "Cybersecurity of Industrial Control Systems (ICS)" (Baku, October 27-29, 2021); XI "National Supercomputer Forum (NSCF-21)" (Pereslavl-Zalessky, Russia, November 30 - December 3, 2021); XVI International Conference on "Application of Information and Communication Technologies" (AICT-2022) (Washington, USA, October 12-14, 2022); XVII International Scientific and Technical Conference "Recognition-2023" (Kursk, Russia, September 12-15, 2023).

The applicant took part in grant competitions held by the Science Development Foundation under the President of the Republic of Azerbaijan (No. EİF-11-1(3)-82/08/1, EİF-RİTN-MQM-2/İKT-2-2013-7(13)-29/18/1, EİF-KETPL-2-2015-1(25)-56/05/1, AEF-MCG-2023-1(43)-13/04/1-M-04), the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) and the Azerbaijan National Academy of Sciences.

Name of the organization where the dissertation thesis was performed. The dissertation was completed at the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

Scientific publications. On the topic of the dissertation, 33 scientific papers have been published, of which 17 articles have been published in foreign journals, including 2 articles in peer-reviewed journals recommended by the Higher Attestation Commission under the President of the Republic of Azerbaijan, 4 articles are included in the International Scopus database, and 11 works are included in the Web of Science database. 16 papers have been published in the materials of the International and Republican conferences.

Structure and scope of the work. The dissertation consists of an introduction, five chapters, a conclusion, and a list of references (409 titles, including 11 works in Azerbaijani, 13 works in Russian, and 385 works in English). The main content of the work is presented on 318 pages, including 54 figures and 80 tables.

MAIN CONTENT OF THE WORK

The **introduction** substantiates the relevance of the topic of the dissertation, formulates the goal and objectives, presents the scientific novelty, theoretical and practical value of the work, and outlines the main provisions submitted for defense, as well as the structure and content of the work.

The **first chapter** is devoted to the analysis and study of existing methods and algorithms for ensuring cyber resilience and information security of CPS. The creation of CPS systems has set new challenges for people. Ensuring the information security of CPS is one of the most complex problems in a wide range of protection technologies against cyberattacks. This chapter describes the operating principle of cyber-physical systems. The main types of cyberattacks and threats to CPS are considered. An analysis of existing research papers on the intelligent processing of big data of CPS, ensuring cybersecurity of information technology, detecting anomalies in operational technology, and assessing the cyber resilience of CPS is performed. The chapter consists of six sections.

The first section analyses the features of the creation and development of CPS. The general structure of CPS is described, and the main standards that can serve as a useful guide for assessing the cyber resilience of CPS are presented. To analyse the latest research in the field of CPS cybersecurity, four categories of research were identified: assessing the consequences of cyberattacks, modeling attacks on CPS, detecting cyberattacks on cyber-physical systems, and developing a security architecture.

The second section analyses the methods and algorithms for intelligent processing of CPS big data. The use of sensors, actuators, and other devices for collecting CPS data provides valuable information for their subsequent analysis. Working with big data necessitates the formalization of new methods used by researchers and the creation of new algorithms that use the capabilities of machine learning methods. Researchers must employ various approaches, such as data partitioning and the use of a priori knowledge, to mitigate risk, prevent DoS

cyberattacks, and block the functioning of CPS IT. However, existing algorithms are not always effective due to high computational complexity.

The third section is devoted to the analysis and study of methods for ensuring IT cybersecurity and OT safety of CPS. Some modern solutions in the field of risk analysis, intrusion detection, cyber resilience, and CPS incident response are described. Traditional defense mechanisms are becoming less effective due to their frequent use by intruders. In this regard, the development of more effective methods for detecting cyberattacks is the most important task of protecting the IT and OT of CPS from cyber threats. Based on the analysis of existing research in the field of security, an "attack tree" and threats based on the functional model of CPS are proposed. The branches of the "tree" include the following types of cyberattacks: a) attacks on sensor devices; b) attacks on actuators; c) attacks on computing components; d) attacks on communications; d) attacks on feedback. Detecting anomalies in an industrial scenario is important because undetected failures can result in severe critical damage.

In the fourth section, the methods and algorithms for assessing the cyber resilience of CPS are analysed and investigated. Currently, many approaches have been proposed to analyse the cyber resilience of CPS, but little attention is paid to the correlation between devices and vulnerabilities. The existing methods cannot comprehensively analyse common multi-stage cyberattacks in the cyber-physical environment. Most current works are mainly focused on theoretical studies and contain only a brief assessment of the cyber resilience of CPS based on machine learning methods. The vulnerability graph is a promising method that lists all possible paths of cyberattacks using a series of exploits. Therefore, researchers and practitioners are interested in analyzing the cyber resilience of CPS based on graph theory. The goal of cyber resilience is to comprehensively protect the entire cyber-physical system by covering all available cyber resources.

The fifth section outlines the scientific problem of the research. The main concepts and definitions used in the dissertation are given. The main focus is on describing the concept of cyber resilience in CPS.

The main types of cyberattacks and cyber threats to CPS are considered.

The sixth section is devoted to developing a conceptual model for ensuring the cyber resilience of CPS. The proposed conceptual model is a hierarchical architecture that consists of three main levels: the edge computing level, the fog computing level, and the cloud computing level (Fig. 1).

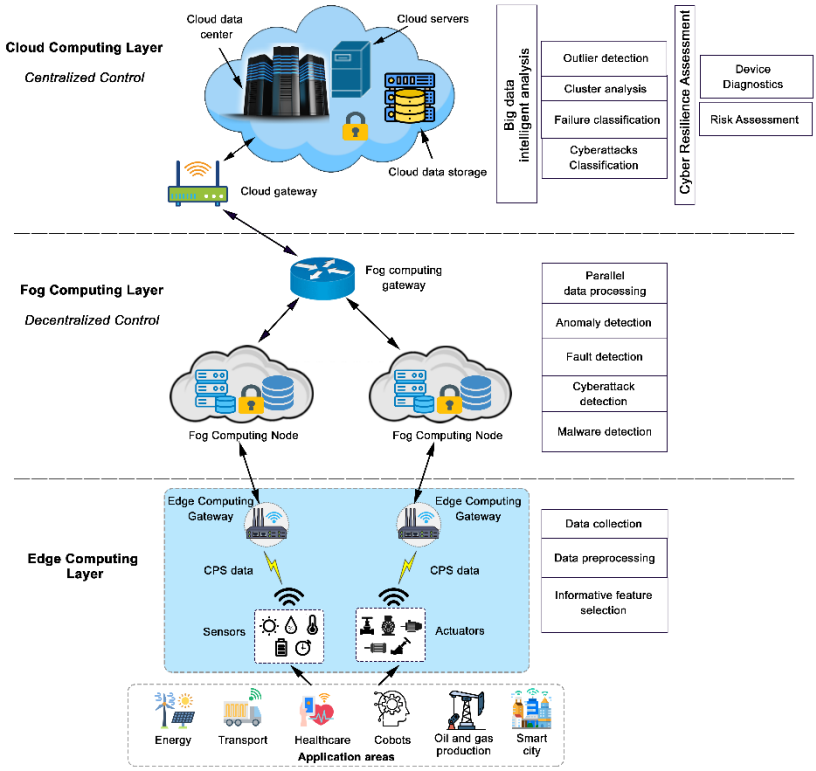


Fig. 1. The conceptual model for CPS cyber resilience

The edge computing level includes intelligent devices such as sensors and actuators that are used to collect data and pre-process it in real time. This level temporarily stores data and can generate initial decisions on detecting an abnormal state. The edge computing level also

performs protocol-based cybersecurity authentication. Although this layer pre-processes sensor and actuator data in real time, additional processing is required to refine the results obtained and make subsequent decisions. For this purpose, the obtained data is transferred to the fog computing layer.

The fog computing layer includes a large number of distributed nodes, containing gateways, fog computing services, routers, access points, base stations, and switches. Fog computing provides a decentralized platform aimed at detecting abnormal operation of the cyber-physical systems, system failures caused by cyberattacks, and malware detection, and extends cloud services to network edge processing and analysis. The fog computing layer is located at the network edge, where fog computing nodes are placed on end devices and cloud layers. This reduces computational complexity and energy consumption, ensures the use of fewer resources, and provides high effective power. In this case, the calculations can be both static and dynamic (mobile).

The cloud computing layer consists of multiple servers, a data warehouse, a cloud data center, and gateways. This layer enables high-performance computing and provides services for various areas, including energy, transportation, healthcare, cobots, oil and gas production, smart cities, etc. The cloud computing layer performs centralized management, ensures permanent storage of large volumes of data, and carries out its intelligent analysis, including assessment of the cyber resilience of the CPS. Intelligent analysis of big data provides the possibility of streaming and batch processing. This leads to a minimum of human action in the production process, and expert data assessment (parallel processing, outlier detection, cluster analysis, failure, and cyberattack classification) can be carried out in real-time by a small group of experts or using machine learning technologies. Cloud computing devices are connected to fog computing nodes using wired connections and wireless media (Bluetooth, 5G, ZigBee, WiFi, and wireless LAN). The cloud computing layer trains large, complex models based on deep neural networks, which can be transferred to edge and fog computing nodes on demand. This reduces the consumption of computing resources at the fog and edge computing layers.

The proposed architecture can provide the necessary guidance to researchers, industrialists, and specialists in analysing each layer of the CPS architecture in terms of system modeling, management, monitoring, data collection, and analysis to achieve the required reliability, cybersecurity, cyber resilience, and efficiency. Analysis of existing methods for managing processes to ensure the cyber resilience of CPS shows that the following issues are relevant: development of methods and algorithms for intelligent processing of big data to ensure the cyber resilience of CPS; development of methods and algorithms for ensuring the cybersecurity of IT in CPS and the safety of OT in CPS; development of a method for determining the criticality of the CPS functional components vulnerabilities and a method for assessing the CPS risks.

So, the features of the formation and development of CPS were studied. The analysis of methods and algorithms for the intelligent processing of CPS big data, ensuring IT cybersecurity and OT safety of CPS, as well as assessing the cyber resilience of CPS, was conducted.

The **second chapter** is devoted to the development of methods and algorithms for the intelligent processing of big data ensuring the cyber resilience of CPS. When analysing data, the quality of information is of paramount importance. This task is complicated by the growth of large volumes of collected information. Working with big data requires large computing resources. In this regard, researchers pay special attention to the development of effective methods and algorithms for intelligent analysis of big data. The high degree of importance of the tasks to be solved has led to the emergence of a whole "galaxy" of different methods in this area. The methods differ from one another in ease of implementation, suitability for data processing, and the basic principles underlying them. The chapter consists of four sections.

The first paragraph introduces an outlier detection algorithm for big data, based on the k-means method, to reduce the risk of CPS blocking. Big data analytics requires large computational and memory resources. Since these resources are not always available and require high costs, proposing new big data analytics algorithms is considered

to be one of the most cost-effective approaches. The k-means algorithm has a fast convergence speed and does not require a lot of computational resources. Therefore, it is popular in clustering small datasets, but requires large computational costs when the size of the datasets increases.

Let $x_i \in R^n$ $(i = \overline{1,n})$ be a point from the dataset, where n is the total number of points in the input dataset, $x_i \in c_p \in R^k$ $(p = \overline{1,k})$ is the cluster number, where k is the number of clusters, S_W is the compactness of the clusters, S_{BW} is the separability of the clusters from each other, and S_B is a distance measure of the each cluster center (O_p) from the center of all points (O) in the input dataset.

$$S_W = \sum_{p=1}^{k} \sum_{i=1}^{n} (x_i - O_p)(x_i - O_p)^T, \quad (1)$$

$$S_{BW} = \sum_{p=1}^{k-1} \sum_{q=p+1}^{k} (O_p - O_q)(O_p - O_q)^T, \quad (2)$$

$$S_B = \sum_{p=1}^{k} (O_p - O)(O - O_p)^T, \quad (3)$$

$$O = \frac{1}{n} \sum_{i=1}^{n} x_i, \quad O_p = \frac{1}{n_p} \sum_{x_i \in C_p} x_i, \quad n_p = |C_p|, \quad p = 1,2,\dots,k. \quad (4)$$

Three algorithms are proposed for detecting outliers in CPS big data using clustering. For the first proposed algorithm, the task is to maximize the following function:

$$F_1(x) = \frac{S_B + S_{BW}}{S_W} \longrightarrow \max. \quad (5)$$

For the second algorithm, the task is to maximize the following function:

$$F_2(x) = \frac{S_B * S_{BW}}{S_W} \longrightarrow \max. \quad (6)$$

In the third algorithm, the problem is to maximize the objective function with respect to the regularization parameter (α), which is determined experimentally:

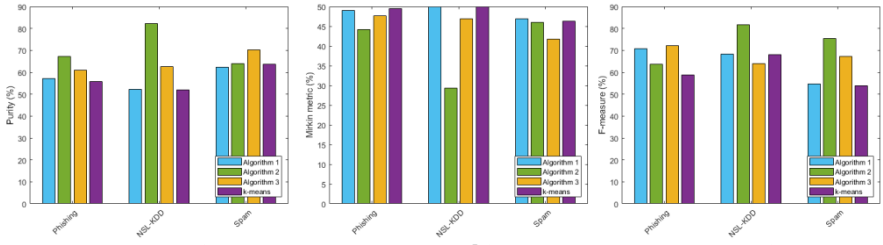
$$F_3(x) = \frac{1}{S_W} (\alpha S_B + (1 - \alpha) S_{BW}) \longrightarrow \max. \quad (7)$$

The algorithms minimize the compactness of clusters and maximize the separation of clusters from each other by the distances between their centroids, and remove cluster centers from a selected common center of points in the dataset.

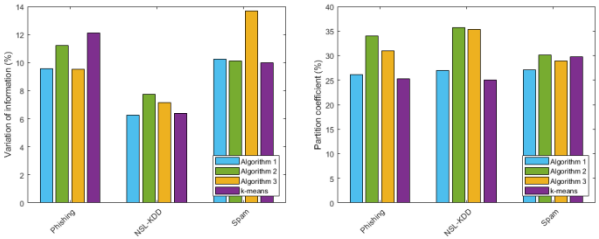
Numerical experiments are conducted on small, medium, and large

real datasets and demonstrate the effectiveness of the proposed algorithms. Three datasets are considered, including the Phishing and Spam datasets from the UCI repository and the NSL-KDD dataset. The NSL-KDD cyberattack signature dataset is created on the KDD-99 database. It contains a training set (125,973 samples) and a test dataset (22,544 samples). Labels are assigned to each instance as either "anomaly" or "normal." All samples (148,517) are considered in this study. The Spam dataset contains spam and non-spam emails. It includes features that indicate how often a particular word or character occurs in an email and measures the length of capital letter sequences. The considered dataset contains two classes: spam ("anomaly") or "normal". The Phishing dataset contains 11,055 samples containing information about phishing websites. It includes thirty features (IP address, URL and anomalous URL lengths, website redirects and others). The datasets were divided into two classes. During preprocessing, the values in the datasets were standardized.

The influence of the regularization parameter α on the efficiency of the third proposed algorithm was considered for various datasets. To evaluate the efficiency of the proposed algorithms, the clustering metrics based on the distance between pairs of data points were considered, namely, purity, Mirkin metric, partition coefficient (PC), variation of information (VI), F-measure, and V-measure. The obtained results for the first, second, third proposed algorithms, and the k-means algorithm are more clearly illustrated in Fig. 2.



a) b) c)



d) e)

Fig. 2. Comparison of the proposed algorithms with the k-means algorithm based on evaluation metrics

Comparison with the k-means algorithm proved the superiority of the proposed approach [5]. Based on the experimental results, it can be concluded that the three proposed algorithms outperform the k-means algorithm in terms of purity, F-measure, and PC metrics for the Phishing dataset. For the NSL-KDD dataset, the best results were obtained when applying the first and second proposed algorithms according to the three metrics given above. In all metrics, the second algorithm showed the best result for the Phishing dataset. At the same time, the purity, Mirkin, F-measure, and PC metrics showed good results for the NSL-KDD dataset when applying the second algorithm. The third proposed algorithm showed the best results for the NSL-KDD dataset and Spam dataset, and the lowest values were observed for the Phishing dataset. It can be concluded that the third algorithm works well on small and large experimental datasets, while the second algorithm showed the best results on medium-sized datasets.

So, numerical experiments were conducted on data sets of different dimensions and demonstrated the effectiveness of the proposed algorithms. Comparison with the k-means algorithm proved the superiority of the proposed algorithms.

The second section introduces the algorithm of CPS big data analysis based on weighted clustering. This study aims to develop a clustering approach for detecting anomalies in big data. The weights obtained by summing the weights of each point in the dataset were assigned to clusters. The weighting is used to improve the clustering solution.

Let $X = (x_1, x_2, \dots, x_n)$ be the points in the dataset, where n is the total number of points in the dataset, $x_i = (x_{i1}, x_{i2}, \dots, x_{im}) \in R^m$ is the point in the considered dataset, where m is the dimension of the data points, $C = (C_1, C_2, \dots, C_k)$ are the clusters, where C_p $(p = \overline{1,k})$ is the p^{th} cluster and k is the number of clusters. The task is to minimize the function for detecting anomalies in the dataset as follows:

$$f(x) = \sum_{p=1}^{k} \sum_{x_i \in C_p} \left|C_p\right|_W * \left\|x_i - O_p\right\|^2 \longrightarrow \min, \qquad (8)$$

where $\left|C_p\right|_W$ is the weight of the p^{th} cluster.

In this case, the cluster weight is defined as the sum of the weights of all points in the cluster:

$$\left|C_p\right|_W = \sum_{x_i \in C_p} w(x_i),\ p = 1,2, \dots, k, \qquad (9)$$

where the weights of the points are calculated based on their distance from the center of all points in the dataset

$$w(x_i) = \|x_i - O\|,\ O = \frac{1}{n}\sum_{i=1}^{n} x_i, \qquad (10)$$

and the center of the p^{th} cluster (O_p) is defined as

$$O_p = \frac{1}{n_p}\sum_{x_i \in C_p} x_i\ ,\ n_p = \left|C_p\right|,\ p = 1,2, \dots, k. \qquad (11)$$

In the algorithm, each cluster is represented by its center, and the goal is to find a solution that minimizes the distance between each point and the center of the cluster to which it is assigned.

The experimental results demonstrated the effectiveness of the proposed approach in simultaneously achieving both clustering and anomaly detection for the considered experimental datasets. Comparison with the k-means algorithm showed that the proposed algorithm detects anomalies in CPS more accurately (Table 1). To evaluate the performance of the proposed approach, the relative improvement was used:

$$\frac{\text{proposed\_method} - \text{k-means}}{\text{k-means}} \times 100\%.$$

Based on the experimental results, it can be concluded that the proposed approach outperforms the k-means algorithm according to four metrics (purity, Mirkin, F-measure, and PC metric) on the NSL-KDD dataset.

Table 1

Performance comparison of the proposed algorithm and the k-means algorithm

Metrics / Dataset	Purity (%)	Mirkin (%)	F-measure (%)	VI (%)	PC (%)
NSL-KDD	3.78 (+)	0.44 (+)	0.66 (+)	13.03 (-)	10.55 (+)
Phishing	5.58 (+)	2.18 (+)	1.21 (-)	17.72 (+)	8.88 (+)

Purity, Mirkin, PC, and VI showed good results on the Phishing dataset. The F-measure metric values were quite close for both approaches on the NSL-KDD and Phishing datasets. The proposed approach becomes more effective with the increase in the analysed dataset size.

So, the experimental results demonstrated the effectiveness of the proposed approach in simultaneously achieving both clustering and anomaly detection. The experimental results showed that "weighting" improves the clustering solution, and the proposed algorithm detects anomalies in cyber-physical system more accurately than the k-means algorithm.

The third section presents a method for parallel processing of big data to reduce the risk of CPS failure. Analysis of large datasets requires substantial computing power, which is not always feasible. This study aims to solve the problem of accelerating the clustering process. It was achieved by combining parallelization and dividing the dataset into small packages (batches) using k-means clustering.

Let $X = \{x_1, x_2, \dots, x_n\}$ be a finite number of data points in n-dimensional space, q be the batch size, the maximum value $q (q < n)$ of which is determined by the PC parameters and is also processed in a reasonable time, $C = \{C_1, C_2, \dots, C_k\}$ be a set of clusters, where $C_p^q (p = 1,2, \dots, k)$ is the p^{th} cluster of the q^{th} batch, and k is the number of clusters, O_p^q is the centroid of the p^{th} cluster in the q^{th} batch.

The objective function is defined as follows:

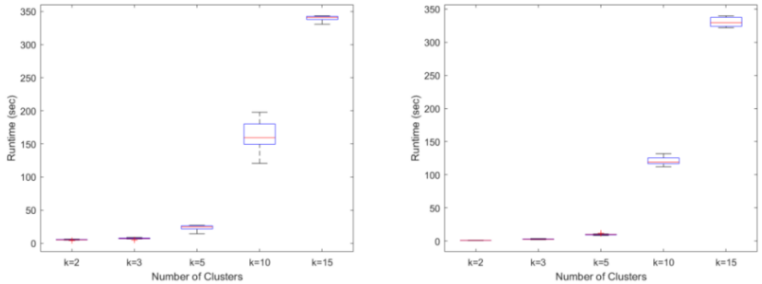
$$f(x) = \sum_{p=1}^{k} \sum_{x_i \in C_p} \left\| x_i - O_p^q \right\|^2 \rightarrow \min, \qquad (12)$$

$$O_p^q = \frac{\Sigma_{x_i \in C_p^q} x_i}{\left|C_p^q\right|}, \; p = 1,2, \dots, k, \qquad (13)$$

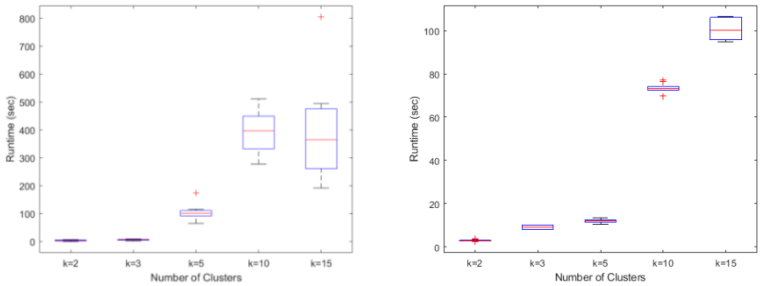
where $\|.\|$ is the Euclidean norm in $\Re^m$, $\left|C_p^q\right|$ is the number of data points in cluster C_p^q.

The resulting centroid obtained after applying the k-means algorithm to the set of centroids of all batches is denoted as O_p^* $(p = 1,2, \dots, k)$. In this case, the dataset is divided into several equal batches. The resulting clusters are created in parallel without full memory loading, which significantly speeds up clustering. The method works in parallel and iteratively. The relevance of the study is that the use of small-dimensional batches reduces computational cost and increases the convergence rate of the clustering algorithm.

The experiments were conducted on two datasets: Phone Accelerometer dataset and Individual Household Electric Power Consumption dataset. The Phone Accelerometer dataset contains 1,048,575 samples and 4 features. And for the second dataset, the number of samples was 2,075,259, and nine features. In the experiments, these datasets are divided into equal fragments (batches). Each batch has the same size (5000, 10000, 15000, and 20000 samples). k samples are randomly selected in the batch to initialize the centroids. In the study, the proposed approach was compared with the k-means algorithm with the number of clusters equal to two, three, five, ten, and fifteen to prove its effectiveness in parallel clustering of big data. The comparison of the execution time of the proposed approach and k-means for two real datasets is shown in Fig. 3.



a) b)



c) d)

Fig. 3. Performance comparison of the proposed method and the k-means algorithm on the Phone Accelerometer (a, b) and Individual Household Electric Power Consumption (c, d) datasets

For additional evaluation of the proposed method, an analysis was performed with different numbers of batches using the Individual Household Electric Power Consumption dataset as an example (Fig. 4). For k=2 and k=3, the proposed method is relatively dependent on the change in the number of batches for the experimental datasets. The proposed approach provides a more noticeable improvement with an increase in the number of clusters and batches.

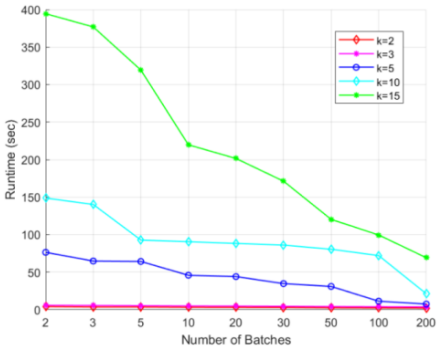


Fig. 4. Performance of the proposed method with different numbers of batches for the Individual Household Electric Power Consumption dataset

Thus, it is possible to increase the number of batches (more than 200), which was done earlier.

Based on the experimental results, the computational efficiency of the method was proven in comparison with the k-means algorithm. Analysing the effect of the batch size on the average value of the function and the average execution time of the method, it can be concluded that efficiency is achieved even with a small batch size. Despite the increase in the number of clusters, the speed of the proposed approach is significantly higher compared to the k-means algorithm. The method is capable of clustering large cyber-physical system data in a short time and can be used to analyse large data to reduce the risk of system failure.

However, splitting the data into small batches increased the convergence rate and lowered the computational costs of the clustering algorithm. The method was compared with the k-means algorithm to prove its effectiveness in parallel clustering of CPS big data.

The fourth section presents a method for clustering big data CPS based on a consensus ensemble. The consensus approach is to find a consistent solution due to the possibility of joint use of cluster analysis methods. The most suitable clustering scheme for a specific area can be constructed by applying a consensus approach to different sets of algorithms according to their advantages and distinctive features. When developing a final solution, different points of view are considered, which not only do not contradict, but, on the contrary, compensate for the shortcomings of each method. Consensus clustering helps to create "robust" partitions, handle noise, and outliers. It serves as a promising solution for clustering big data from cyber-physical systems. In this case, the problem is the development of a utility function and its effective optimization.

The goal of the study is to find a consensus partition π by solving the following optimization problem:

$$\pi^* = \underset{\pi}{\operatorname{argmax}}(w_i U(\pi, \pi_i)), \tag{14}$$

where π^* is a consensus function, U represents a utility function that measures the similarity between π and any π_i, and the partition π_i is a basic partition ($1 \le i \le r$) and $w_i \in [0,1]$, $\sum_{i=1}^{r} w_i = 1$.
Weights are assigned to individual clustering methods using a purity-based utility function:

$$f = (1-\lambda) \cdot \sum_{i=1}^{r} w_i U(\pi, \pi_i) + \lambda \cdot \|w\|^2 \longrightarrow \max \quad (15)$$

subject to

$$\sum_{i=1}^{r} w_i = 1, w_i \ge 0, \forall i. \quad (16)$$

where $0 \le \lambda \le 1$ is a regularization parameter that indicates the trade-off between maximizing the weighted utility function and the smoothness provided by w [22].

A statistical analysis of big data clustering demonstrates the feasibility of applying weighted consensus clustering to the analysis of label-free CPS big data. For this purpose, the purity-based utility function was replaced by a function based on the Davies-Bouldin and Calinski-Harabasz indices. The Davies-Bouldin (DB) index is based on the ratio of intra-cluster and inter-cluster distances. DB is calculated as follows:

$$DB = \frac{1}{k} \sum_{i=1}^{k} R_i \quad (17)$$

$$R_i = \max_{i \ne j} \left(\frac{\delta(C_i) + \delta(C_j)}{dist(C_i, C_j)} \right), \quad (18)$$

where k is the number of clusters, δ is intra-cluster variance, and *dist* is the distance between i and j clusters. The target value is the minimum of the index.

The Calinski-Harabasz (CH) index is characterized by the following function:

$$CH = \frac{B(k)/(k-1)}{W(k)/(n-k)}, \quad (19)$$

where

$$B(k) = \sum_{i=1}^{k} n_i \, dist^2(O_i, O), \quad (20)$$

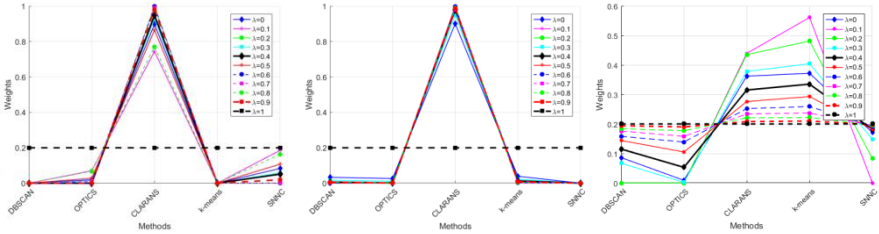
$$W(k) = \sum_{i=1}^{k} \sum_{x \in C_i} dist^2(x, O_i), \quad (21)$$

k is the number of clusters, n is the number of objects in the considered

dataset D, C_i is the i^{th} cluster, n_i is the number of objects in C_i, O is the center of the data set D, O_i is the center of C_i in the dataset, $W(k)$ is the sum of the intra-cluster variances for all clusters, and $B(k)$ is the weighted sum of the squared distances between C_i and the data set D [22]. The most probable number of clusters is the value of k at which the CH index reaches its maximum value.

Experimental results on datasets of varying dimensions, using different distance metrics, demonstrated that the proposed method is highly effective and outperforms modern methods in terms of data clustering quality. Fig. 5 shows the effect of the λ parameter on the weights of five clustering methods for the considered datasets (NSL-KDD dataset, Phishing dataset, and Phone Accelerometer dataset). The experimental results proved the effectiveness of the proposed method for data clustering compared with DBSCAN (Density-Based Spatial Clustering of Applications with Noise), OPTICS (Ordering Points to Identification the Clustering Structure), CLARANS (Clustering Large Applications with Randomized Search), k-means, and SNNC (Shared Nearest Neighbor Clustering) methods. For the Phishing dataset, the proposed consensus approach using squared Euclidean distance gave the best results, according to the purity metric (0.7166), Mirkin metric (0.4062), F-measure metric (0.7283), and PC (0.3053) metric. The results of the main partitions exceeded the VI indicator and amounted to 0.0948. The proposed method using squared Euclidean distance showed the best result for all five metrics and coincided with the result of the CLARANS method for the NSL-KDD dataset.

And for the considered Phone Accelerometer dataset, the proposed approach outperformed clustering methods such as DBSCAN and OPTICS in terms of purity metric, Mirkin metric, F-measure metric, and PC metric, but was slightly inferior according to VI.
The best result is shown by the proposed approach using the squared Euclidean metric.



a) NSL KDD b) Phishing c) Phone Accelerometer

Fig. 5. Dependence of clustering methods weights on the parameter λ

Experimental results on the considered three datasets of different dimensions, using different distance metrics, have demonstrated that the method is highly effective and outperforms modern approaches in terms of the quality of CPS data clustering. A comparison with DBSCAN, OPTICS, CLARANS, k-means, and SNNC methods was made. The proposed method, which uses the squared Euclidean metric, showed the best result.

The **third chapter** is devoted to the development of methods and algorithms for ensuring the cybersecurity of cyber-physical system information technologies. Cyberattacks are one of the causes of abnormal phenomena observed in the operation of the CPS information technology, as well as when transmitting traffic over the network. Network traffic anomalies can lead to the incorrect operation of a separate channel or entire network segments, resulting in denial of service on this network equipment. Network attacks are constantly changing, since attackers use individual approaches. This is also affected by changes in software and hardware. The chapter consists of three sections.

The first paragraph presents a method for classifying cyberattacks on CPS using the extreme learning machine (ELM). To select the most informative features, a genetic algorithm of the firefly behavior was used to improve the accuracy and increase the speed of the classification algorithm. The extreme learning machine method has a high computational speed and does not require iterative parameter tuning during training.

The experiments were conducted on the NSL-KDD dataset. All cyberattacks in the NSL-KDD dataset are divided into four groups: DoS (Denial of Service) attack, Users to Root (U2R) attack, Remote to Local (R2L) attack, and Probe attacks. Each record has 41 features. The method is evaluated with different activation functions: radial basis activation function (RBF), triangular basis activation function (TriBas), and Gaussian activation function (Table 2). The Gaussian activation function was used for different values of the variance (σ) and mean (μ) parameters. The best detection accuracy for DoS, U2R, and R2L attacks was achieved for the Gaussian activation function with σ=0.1 and μ=4 (DoS – 86.89%, U2R – 99.99% and R2L – 99.94%). In the case of Probe attacks, high accuracy (99.06%) was obtained for the Gaussian activation function with variance σ=0.2 and mean value equal to zero (μ=0).

The proposed method demonstrated high results in both speed and classification accuracy when using the Gaussian activation function for the NSL-KDD dataset.

Table 2

Comparison of intrusion detection accuracy using different activation functions

Activation function	DoS	Probe	U2R	R2L
RBF	80.01%	91.79%	99.88%	**99.94%**
TriBas	81.60%	95.62%	99.65%	99.57%
Gaussian (σ =0.2, μ =0)	84.26%	**99.06%**	99.95%	99.70%
Gaussian (σ =0.1, μ =4)	**86.89%**	90.01%	**99.99%**	**99.94%**

The considered classifier, based on the ELM method, provides an acceptable quality of cyberattack classification and high performance, making it an attractive solution for real-time intrusion detection systems in CPS IT.

The proposed method was compared with support vector machines (SVM), random forest (RF), artificial neural network, and deep neural network (DNN) algorithms, and demonstrated the highest accuracy

when using the Gaussian activation function (99.78%) (Table 3).

Table 3

Performance evaluation of the proposed approach on the NSL-KDD dataset

Method	Bayes Net	Logit Boost	IBk	SVM	RF	DNN	MLP	ELM (Gauss)
Accuracy (%)	69.9	78.8	99.6	93.8	97.93	91.5	81.43	**99.78**

So, the proposed method for classifying cyberattacks on CPS allowed an increase in the speed of the classification algorithm. The method was evaluated using various activation functions and compared with support vector machine, random forest, artificial neural network, and deep neural network algorithms, demonstrating the highest performance when the Gaussian activation function was employed.

The second section presents a method for detecting DoS cyberattacks on cyber-physical system using an ensemble of classifiers. As a result, DoS attacks on the server or data network limit services, which in turn can lead to cyber-physical system failure.

The proposed method, which indicates the probability of belonging to certain classes, returns a vector of classification estimates for each data point. The peculiarity of the proposed approach is that for each point from the data set, the obtained class label corresponds to the maximum value among all estimates obtained by the classification methods for this point.

Decision tree (DT), the k-nearest neighbors algorithm (KNN), support vector machines (SVM) with different kernel functions, and a naive Bayes classifier (NB) were considered as classifiers. The most accurate result was shown by an ensemble of five classifiers (Table 4). Despite the fact that NB shows the lowest result (80.45%), when adding it to the ensemble of classifiers, the accuracy of the proposed approach increased and amounted to 92.33% for five classifiers.

Table 4

Comparison of the proposed method with other classifiers using the accuracy metric [10, 12]

Class / Method	DoS	"Normal" state	Other attacks
DT	86.32% [7]	77.19% [7]	64.25% [8]
KNN	88.21% [3]	79.67% [3]	65.80% [6]
SVM(Linear)	87.21% [5]	77.96% [6]	66.22% [5]
SVM(Polynom)	86.64% [6]	79.50% [4]	68.31% [3]
SVM(RBF)	87.25% [4]	78.84% [5]	65.38% [7]
NB	80.45% [8]	71.25% [8]	66.50% [4]
DT+KNN+ SVM(Polynom)	90.74% [2]	84.77% [2]	74.53% [2]
DT+KNN+ SVM(Poly-nom)+NB+SVM (Linear)	**92.33% [1]**	**88.58% [1]**	**83.35% [1]**

Based on the obtained ranks for the purity, Mirkin, F-measure, VI, and PC metrics, the resulting rank was calculated for all clustering methods:

$$rank(method) = \sum_{s=1}^{M} \frac{(M-s+1)\cdot r_s}{M}, \qquad (22)$$

where M is the number of methods, and r_s is the number of times the method appears in rank s.

The ensemble DT+KNN+SVM(Polynom)+NB+SVM(Linear) showed the best rank according to all four metrics: accuracy, precision, recall, and F-measure for the DoS class [10].

So, a method for detecting DoS cyberattacks on CPS systems where decision trees, the k-nearest neighbors algorithm, support vector machines with different kernel functions, and a naive Bayes classifier were considered as classifiers. An ensemble of five classifiers was the most effective and showed an accurate result [10, 12].

In the third section, an algorithm for detecting malware in CPS based on images is presented. Existing technologies can reduce the risk of malware infection using various tools. However, there is no

perfect defense against increasingly sophisticated types of malware. A transfer learning-based algorithm is developed that combines malware visualization and the Radon transform. In this study, images were obtained based on binary malware samples. The Radon transform is a reversible image transformation. Therefore, it can be considered a method for representing image texture and is applied to the obtained grayscale malware images. Unlike most methods, the Radon transform does not require the development of new features and is based on visual analysis of malware samples.

The experimental results showed that combining features from two deep neural networks (AlexNet and MobileNet) can effectively classify malware in CPS even with small image changes. The detection loss curves and classification accuracy curves of images from the Microsoft malware BIG, IoT_Malware, and MaLNet-Image datasets are shown in Fig. 6.

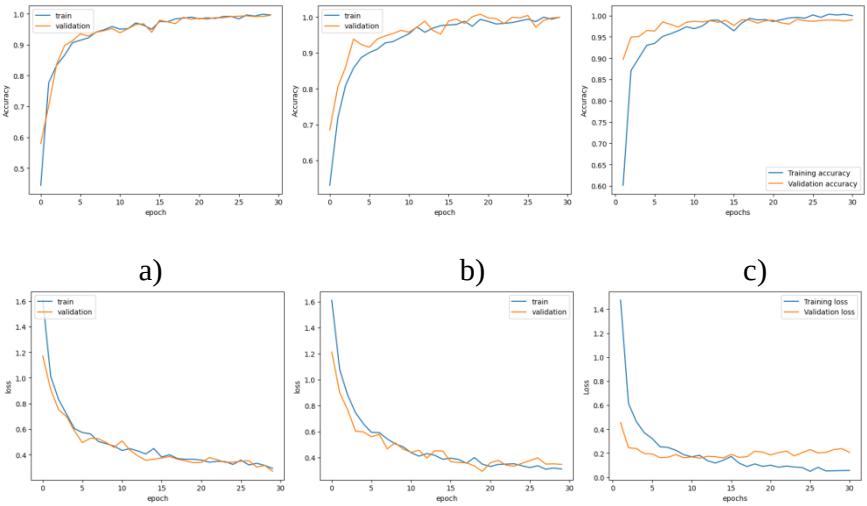


Fig. 6. Malware detection accuracy and loss curves for the Microsoft malware BIG (a, d), IoT_Malware dataset (b, e), and MaLNet-Image (c, f) malware datasets

According to the F-measure metric for the Microsoft malware BIG dataset, the malware classes Lollipop, Vundo, Keli-hos_ver3, Keli-hos_ver1, and Obfuscator.ACY showed results >90%. However, the malware families Ramnit, Tracur, and Gatak were less accurately recognized by the precision metric and amounted to 76%, 82%, and 90%, respectively. For the MaLNeT+Images dataset, according to the precision, recall, and F-measure metrics, the malware classes Addisplay and SPR (security and privacy risk) were recognized with 100% accuracy. At the same time, the proposed approach also showed quite high accuracy for other considered malware classes. For four classes of the IoT_Malware dataset, the following results were obtained by the precision metric: Benign (99.50%), Gafgyt (97.99%), Tsunami (96.09%), and Mirai (97.88%). The class of the Mirai malware family aimed at infecting CPS was identified most accurately using the recall metric. At the same time, the precision and F-measure metrics identified the Benign class with almost 100% accuracy.

Comparison with Xception, Inception, EfficientNet, CNN, VGG16, LeNet, and other methods proved the superiority of the proposed algorithm (Table 5).

Table 5

Performance evaluation of the proposed approach using deep learning-based methods

Method	Dataset	Accuracy (%)
VGG16	Microsoft malware dataset	98.94
MobileNet		99.25
Xception		99.17
LeNet, AlexNet, InceptionV3		99.70
CNN		98.64
InceptionV3		99.60
Proposed approach		**99.89**
Adversarial learning	IoT_Malware dataset	97.67
CNN		95.00
Proposed approach		**99.95**
Vision Transformer	MalNet-Image dataset	97.00
EfficientNetB0+SVM+RF		92.90
Proposed approach		**99.20**

The study demonstrated stable performance with an accuracy of 99.89%, 99.95%, and 99.20% for the Microsoft malware BIG, IoT_Malware, and MalNeT-Images malware datasets, respectively.

So, the proposed algorithm does not require the development of new features and is based on the analysis of malware images. Experimental results demonstrated that the combination of features from two deep neural networks (AlexNet and MobileNet) can effectively classify malware in CPS even with small changes in images. Comparison with various deep neural models proved the superiority of the proposed algorithm.

The **fourth chapter** is devoted to the development of methods for the cybersecurity of CPS OT. The abnormal state of CPS can be caused by faulty components, temporary failures, improper configuration, cyberattacks, or a combination of these factors. An attacker interferes with CPS to manipulate the readings of sensors or actuators, resulting in abnormal system operation. Anomaly detection in an industrial scenario is important because undetected failures can lead to critical damage. Early detection of anomalies can improve the reliability of failure-prone industrial equipment and reduce operation and maintenance costs. The chapter consists of four sections.

The first section presents a method for detecting anomalies in CPS operational technology based on hierarchical hidden Markov models (HHMM). In this case, the observed events are modeled using hidden Markov model. The hierarchical hidden Markov model is suitable for problems with a complex hierarchical structure and those that are time-dependent. Normal and abnormal states obtained from the hierarchical hidden Markov model can be used as input data for identifying cyberattacks on the cyber-physical systems (Fig. 7).

The first step in detecting cyber-physical system's anomalies using hierarchical hidden Markov model is to collect sensor data. Then, the most informative features are selected from among them. Using vector quantization methods (e.g., the k-means algorithm) generates meaningful observations for the model. The Baum-Welch algorithm performs correction of the model parameters during the training phase. A probable sequence of the first-level hidden Markov model states

leads to the generation of a feature vector. Applying vector quantization to these features creates a sequence of observations from the second-level hidden Markov model, etc. Then, during the testing phase, a sequence of states is determined using the Viterbi algorithm, which uses the parameters of the training phase.

If no “unusual” behavior is detected in the cyber-physical system components, the model moves to the next hierarchical level and checks for a cyberattack on the system.

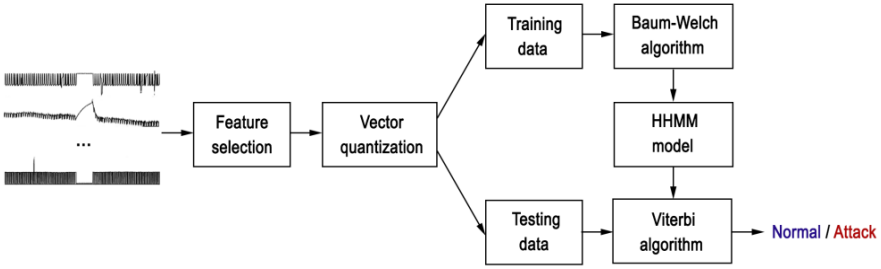


Fig. 7. General flowchart of the proposed method

The comparison was made with various models such as deep neural network, support vector machines, TABOR (Time Automata and Bayesian netwORk), one-dimensional convolutional neural network, LSTM-CUSUM model, and MAD-GAN model (Table 6). The evaluation of the proposed method using the F-measure metric gives higher performance. This proves the success of detecting anomalies in CPS using the hierarchical hidden Markov model.

The advantage that can be expected from using hierarchical hidden Markov model over a large single-layer hidden Markov model is that the hierarchical hidden Markov model is less likely to suffer from overfitting, since individual subcomponents are trained independently on smaller amounts of data. As a consequence, the hierarchical hidden Markov model requires significantly less training data to achieve performance comparable to HMM model.

Table 6

Evaluation of the proposed approach

Method	Metrics		
	Precision	Recall	F-measure
DNN	0.9830	0.6785	0.8028
SVM	0.9250	0.6990	0.7963
TABOR	0.8617	0.7880	0.8232
1D CNN	1.0000	0.8530	0.9200
LSTM-CUSUM	0.9070	0.6770	0.7750
MAD-GAN	0.9610	0.9420	0.9510
Proposed method	**0.9998**	**0.9164**	**0.9563**

So, the proposed method enabled us to distinguish between normal and abnormal states of CPS. It requires significantly less training data to achieve high performance. A comparison was made with known machine learning methods. Experiments have demonstrated the effectiveness of detecting cyberattacks on the cyber-physical system using the developed method.

In the second section, a method for detecting anomalies in CPS acoustic signals using transfer learning is presented. A deep learning architecture is used to analyse the acoustic signals, which are preprocessed to obtain spectrograms and scalograms. The SPOCU (scaled polynomial constant unit) activation function is considered to improve the accuracy of the proposed method. The extreme gradient boosting (XGBoost) algorithm is used because it has high performance and requires less computational resources during the training stage [26].

The dataset containing acoustic signals of four different cyber-physical systems device types was used for the experiments: valves, pumps, fans, and sliders. For each device type, various real-life anomaly scenarios were considered: contamination, leakage, rotational imbalance, rail damage, etc. The following pre-trained deep neural networks are considered for feature extraction from spectrogram and scalogram images: Xception, MobileNet, DenseNet, and Inception. Comparison with different deep neural models showed that Densenet+XGBoost outperforms other considered models in detecting

anomalies from equipment signals according to the F-measure metric (Table 7). The proposed model achieved a significant improvement in anomaly detection from sensor data by an area under the ROC-curve of 95.45% compared to previously proposed models.

Table 7

Evaluation of the proposed method effectiveness [26]

Model	Metrics	Device			
		Fun	Pump	Slider	Valve
Inception+ XGBoost	Recall	87.0	95.0	98.0	100
	Precision	89.1	87.9	100	94.3
	F-measure	92.3	90.6	98.1	96.3
Xception+ XGBoost	Recall	100	88.0	98.0	100
	Precision	84.2	100	100	92.6
	F-measure	96.8	92.8	98.1	95.3
Mobilenet +XGBoost	Recall	96.0	88.0	94.0	100
	Precision	78.7	95.7	100	96.2
	F-measure	92.0	90.9	96.1	97.2
Densenet+ XGBoost	Recall	99.9	96.0	98.0	100
	Precision	87.0	100	100	97.1
	F-measure	98.2	97.1	98.1	97.7

Therefore, transfer learning was employed to work with acoustic signals that had been pre-processed to obtain spectrograms and scalograms. The extreme gradient boosting method was used because it has high performance and does not require significant computational resources at the training stage. To evaluate the performance of the method, it was compared with deep neural models for various types of devices.

In the third section, a method for detecting cyberattacks on CPS devices using a deep hybrid model is presented. The proposed method combines the advantages of a one-dimensional convolutional neural network (CNN), a gated recurrent unit (GRU) neural network, and a long short-term memory (LSTM) neural network. The outputs of the GRU, CNN, and LSTM models are combined to improve the accuracy

of cyberattack detection on CPS and fed to two fully connected layers consisting of 150 neurons. They are followed by a softmax layer. To improve the accuracy of the method, the SPOCU activation function is considered. The AdamW+Amsgrad optimizer is applied to reduce the training error of the deep neural model and increase the training speed. The experiments were conducted on two datasets: SWaT (secure water treatment) dataset and GHL (gasoil heating loop) dataset, which contain information about the "normal" state of CPS and failures caused by cyberattacks (Fig. 8).

The method was evaluated using different optimizers: stochastic gradient descent (SGD), SGD with weight decay (SGDW), Adam, Adam with weight decay (AdamW), and AdamW+Amsgrad. The proposed method with the AdamW+Amsgrad optimizer showed the best results (Fig. 8).

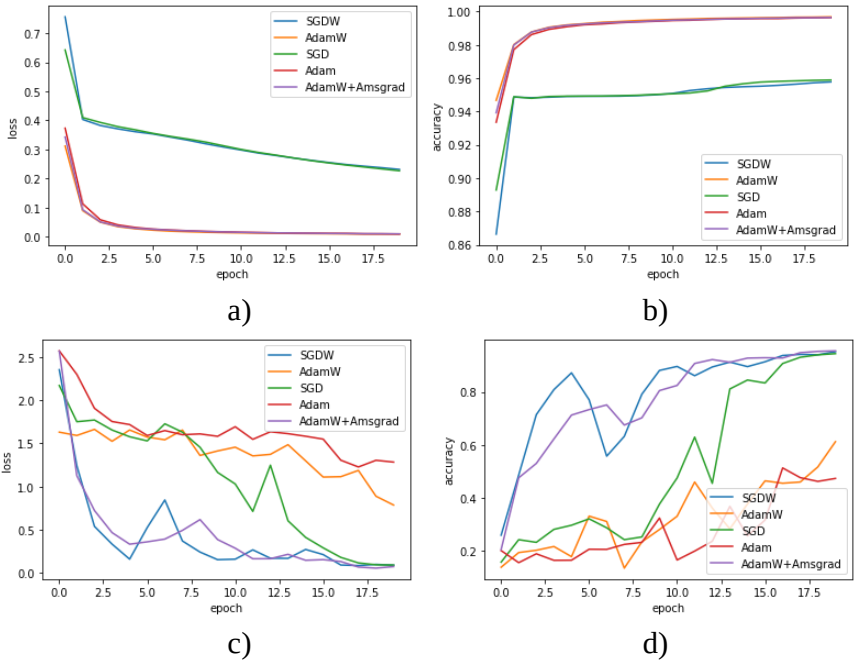


Fig. 8. The loss and accuracy curves of cyberattack detection for the proposed method on SWaT (a, b) and GHL (c, d) datasets

The proposed method provides high accuracy in detecting cyberattacks on CPS compared to known machine learning methods, such as a simple deep neural network, support vector machines (Table 8).

Therefore, the proposed method combines the advantages of deep neural networks, such as CNN, GRU, and LSTM. To improve the accuracy of the method, the SPOCU activation function was considered. The experiments were conducted on two datasets: SWaT and GHL, which contain information about the "normal" state of the considered cyber-physical system and failures caused by cyberattacks. The method demonstrated high accuracy in detecting cyberattacks on CPS, outperforming well-known machine learning methods, including simple deep neural networks and support vector machines.

In the fourth section, an image-based classification method for the CPS failures is presented. The performance evaluation and timely detection of CPS faults can reduce the operating and maintenance costs. The developed method combines the advantages of the deep neural network (DNN) and CNN. The frequency and time features, as well as the images of the vibration signal, are considered as the input data for the deep hybrid model.

Table 8

Evaluation of the proposed method on various datasets

Dataset	Metrics		
	Precision (%)	Recall (%)	F-measure (%)
Secure Water Treatment dataset	99.76	99.75	99.74
Gasoil Heating Loop dataset	97.06	95.66	96.04

The images of the short-time Fourier transform spectrogram and the continuous wavelet transform scalogram obtained from the CPS sensor signals are considered as the input data for the proposed method.

As an example, the problem of detecting faults of an oil electric submersible pump (ESP) was considered. The vibration signal carries

the most important information about the state of mechanical devices, including oil equipment. The features characterizing the faults of the CPS components are extracted for intelligent analysis of raw signals and improving the accuracy of diagnosis.

Analysis of the graphical representation of the ROC curve allows us to evaluate the quality of the proposed deep hybrid model. The experimental results show that this is the best model for ESP fault detection, based on the considered features obtained from vibration signals (the area under the ROC curve (AUC) was 100%) (Fig. 9).

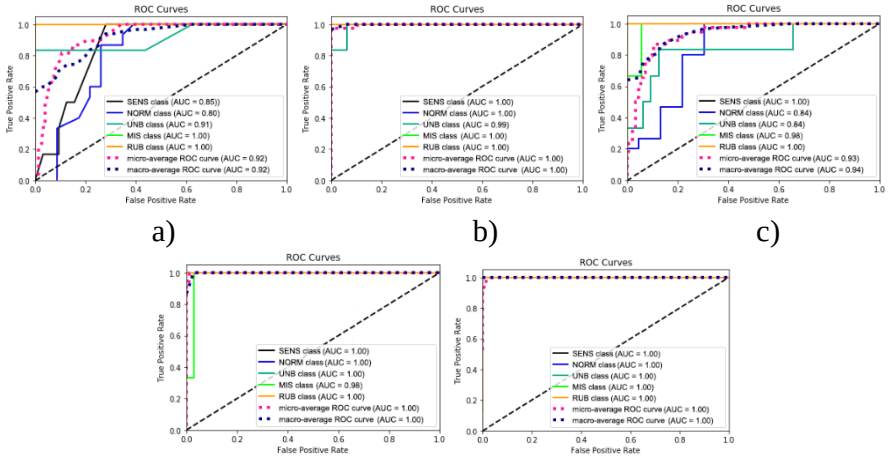


Fig. 9. ROC curves for assessing the classification accuracy of the considered methods for five classes: faulty sensor (SENS), normal operational condition (NORM), unbalance (UNB), misalignment (MIS), and rubbing (RUB) [20]

Experimental evaluation shows that the proposed deep hybrid model outperforms previously proposed deep learning-based methods, including k-nearest neighbors (KNN) (Table 9).

The propoed method for image-based classification of the cyber-physical system failures was developed. The method combines the advantages of DNN and CNN.

Table 9

Performance comparison of the proposed approach with other methods using recall metrics [20]

Method	Classes				
	NORM (%)	UNB (%)	MIS (%)	RUB (%)	SENS (%)
Ensemble approach	97.82	97.51	76.00	48.29	95.65
KNN	97.50	89.50	60.00	33.50	87.00
KNN+	97.50	89.50	68.00	38.00	89.00
KNN+FS	97.50	90.50	71.00	35.50	89.50
KNN+EFS	98.00	93.00	81.00	34.50	91.00
Proposed method	**100**	**100**	**99.93**	**100**	**100**

Frequency, time, and spectral information of vibration signals obtained from sensors were considered as input data for the proposed method. The problem of detecting faults in an oil submersible pump was considered, and the experimental evaluation showed that the proposed method outperformed known machine learning methods [20].

The results of this study show that the proposed deep hybrid model can automatically and simultaneously extract the characteristics of sensor signals that are sensitive to faults in the time, frequency, and time-frequency domains. Therefore, the proposed hybrid model, utilizing deep neural networks, can be applied to the fault diagnosis of CPS equipment.

The **fifth chapter** is devoted to the development of methods for assessing the cyber resilience of CPS. The most important task is to maintain the ability of the CPS to function correctly even under destructive information impacts, since successful cyberattacks on such systems can lead to negative financial consequences and environmental disasters, as well as loss of life. Since attackers often look for and target the weakest link – the most vulnerable functional component in CPS – the most vulnerable devices can be a good starting point for an effective study of the cyber resilience of the system. Existing methods

cannot comprehensively analyze common multi-stage cyberattacks in the CPS environment. The chapter consists of two sections.

The first section presents a method for determining the criticality of functional CPS components' vulnerabilities based on the Bayesian attack graph. The integration of intelligent devices and technologies in various industries has significantly changed the entire technological infrastructure. The CPS recognizes the environment using sensors, makes decisions according to its purpose, and provides corrective actions using actuators. The connection between IT and OT networks is important when modeling the CPS systems. The convergence of IT and OT is growing, allowing for more efficient management and operation of CPS. The severity of the CPS component failure affects the system, depending on the number of components and their diversity. This proves the need to measure the criticality of system components' vulnerabilities. Timely detection of critical security flaws in CPS enables the identification of risks and potential threats. To solve this problem, threat models are created to better understand the potential vulnerabilities that must be considered to ensure the system's reliability. Selecting the optimal solution for assessing the criticality of functional vulnerabilities of CPS components is a complex process, since all vulnerabilities must be identified, classified, and quantified in accordance with a unified approach within the cyber resilience process. Statistics over the past few years show an increase in the number of cyberattacks on CPS, with the majority of cases aimed at gaining control over the control subsystem.

However, this problem can be solved using the Bayesian Attack Graph (BAG), which allows for assessing the criticality of CPS components' vulnerabilities. It provides information on the relationships between vulnerabilities, which is an important factor. BAG depends on operating systems and network protocols, CPS access control rules, software identification, and vulnerability information.

Multi-criteria decision-making methods can be used as a suitable approach to solving the problem of ranking the criticality of CPS component vulnerabilities. They help decision makers select optimal alter-

natives based on specified criteria. There are such well-known methods of decision-making as Promethee I, Promethee II, Promethee III, among others. To determine the criticality of CPS component vulnerabilities, it is proposed to utilize the multi-criteria decision-making method known as Promethee II. It is considered relatively simple among multi-criteria analysis methods and is increasingly used by decision-makers. The method gives fairly stable results and is based on a pairwise comparison of alternatives corresponding to each criterion. Promethee II allows you to organize and identify the most critical vulnerabilities of the system under consideration. The vulnerability is quantified using the Common Vulnerability Scoring System (CVSS) and the National Vulnerability Database (NVD).

To illustrate potential cyber-attack scenarios that exploit vulnerabilities in the cyber-physical system components, we can consider the example of natural gas transportation as one of the critical infrastructure sectors (Fig. 10). Natural gas is transported through pipelines by compressor stations. They consist of several gas compressors that move gas through the pipeline. After filtration separation, natural gas is fed to the compressor unit. Lubrication and cooling systems of the compressor engine serve to protect and maintain the gas flow rate. OT of the considered CPS are programmable logic controllers (PLC) and remote terminal units (RTU) connected to sensors and actuators. Sensors transmit signals to controllers, which send control signals to actuators. Process operators interact with the control system through the human-machine interface (HMI). The data archive stores the values of the process parameters. The data server receives information from the controller and transmits it to other controllers or HMI. The control network transmits instructions and data between control and measurement units and SCADA devices. Engineering workstations can be connected to the corporate network or the Internet. Here, software development tools are installed, allowing a technician to make changes and additions to the system configuration centrally. Compressor stations in natural gas transportation are usually controlled by a distributed control system, possibly coupled with a separate security system. The stations are controlled remotely via remote terminal units connected to

a central SCADA (Supervisory Control and Data Acquisition system) WAN (Wide Area Network) system.

It is assumed that the attacker's goal may be to compromise the Engineering Workstation (EWS) data archive or workstation, which are usually the primary targets due to their interconnected nature. Three scenarios of cyberattacks on the natural gas transportation system are investigated (Fig. 10):

• Control manipulation

Depending on the system configuration, an attacker with the ability to interact with WAN SCADA could exploit CVE-2020-13500 vulnerability or CVE-2022-29966 vulnerability to manipulate system settings, files, or critical values associated with compressor stations. They could exploit CVE-2022-33139 vulnerability to bypass authentication and then manipulate monitoring values associated with compressor stations to overwhelm operators with false alarms or change flow setpoints to disrupt natural gas transportation, thereby expanding their manipulation capabilities.

• Denial of Control

An attacker with the ability to interact with the remote terminal units could exploit CVE-2022-29961 vulnerability or CVE-2022-29955 vulnerability to bypass authentication at the remote terminal units and issue commands that halt operation, and by exploiting CVE-2022-30262 vulnerability, could prevent operators from monitoring and controlling the PLC1 and PLC2 compressor stations. Alternatively, an attacker with the ability to interact with the Network Switch (NS) could exploit an unauthenticated connection (CVE-2021-30276 vulnerability or CVE-2021-31886 vulnerability) and issue specific commands to the remote terminal unit RTU that could halt operation or disrupt communication between the SCADA WAN network and the remote terminal unit RTU, preventing operators from monitoring and controlling the compressor stations.

• Loss of control

To do this, the attacker hacks the control system of the compressor station itself using CVE-2022-30262, CVE-2022-26657, CVE-30315, CVE-2022-30260, or CVE-2022-31801 vulnerabilities. This allows

code execution on the RTU and unrestricted communication via various network interfaces. Using CVE-2022-30313 and CVE-2022-30315 vulnerabilities provides penetration into the security network. Thus, the attacker makes manipulative settings or even achieves code execution on the programmable logic controller PLC2 to disable emergency shutdown systems and fire and gas safety systems.

Once the CPS system's devices in operational technology are compromised, attackers can use various CVSS to launch cyberattacks on control processes that affect physical operations. Information about vulnerabilities is taken from NVD descriptions. The attacker uses the connection of the CPS IT network to the Internet to execute malicious code.

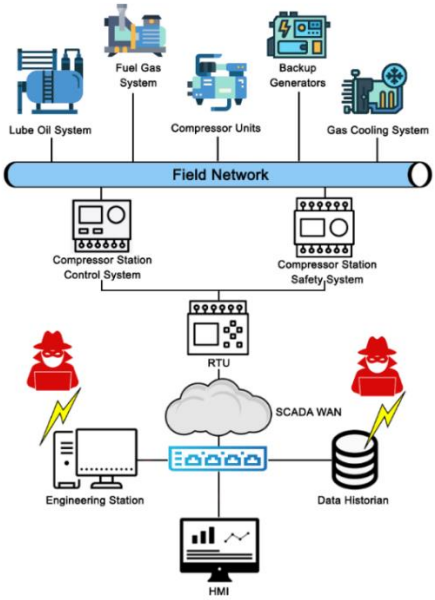


Fig. 10. Example of the CPS configuration

To conduct the experiments, information about various vulnerabilities of the CPS components was considered, including the base score,

the impact score γ, the sub-score of the exploitability ε, the attack vector, user interaction, the required privileges, and the exploit complexity score.

The proposed method was compared with well-known multi-criteria decision-making methods, such as TOPSIS (Technique for Order Preference by Similarity to Ideal Solution), VIKOR (VIseKriterijumska Optimizacija I Kompromisno Resenje), and ELECTRE (Elimination and Choice Translating Reality) (Table 10). The results of risk ranking using the Promethee II and TOPSIS methods are similar. Moreover, two different solution options for the VIKOR and ELECTRE methods were placed in the third and fourth positions.

Table 10
Comparison of the proposed method with well-known methods

CPS component	TOPSIS	VIKOR	ELECTRE	Proposed method
PLC_1	4	4	3	4
PLC_2	3	3	4	3
RTU	3	4	3	3
SW	1	1	1	1
DH	2	2	2	2
NS	1	1	1	1
HMI	1	1	1	1
EWS	1	1	1	1

To determine the criticality of the considered cyber-physical system components' vulnerabilities, the multi-criteria decision-making method Promethee II was used. It enabled the organization and identification of the most critical vulnerabilities in the components of the considered CPS. Vulnerabilities were quantitatively assessed using CVSS and the National Vulnerability Database. Three scenarios of cyberattacks on the natural gas transportation system were studied.

Comparison with well-known multi-criteria decision-making methods, such as TOPSIS, VIKOR, and ELECTRE, proved the effectiveness of the proposed method.

In conclusion, a quantitative method for assessing the criticality of vulnerabilities in CPS components is proposed [33]. It is based on the Promethee II multi-criteria decision-making method. The method allows ranking and identifying the most vulnerable components of the system. BAG was created on the basis of the considered CPS structure, taking into account the known vulnerabilities of its components. As a result, it was possible to identify the most critical vulnerabilities of the functional components of CPS using Promethee II.

The second section presents a method for assessing the risks of CPS using the Sugeno fuzzy integral. Protecting the CPS from cyberattacks is a significant challenge that requires effective cybersecurity risk assessment methods. Currently, the methods of analysing and assessing the risks of CPS can be divided into qualitative and quantitative methods. The former is based on expert assessment to determine the probability and potential impact of risks, and also reveal the nature of the risks. At the same time, quantitative risk analysis uses mathematical and statistical methods to calculate the probability and potential impact of risks. However, researchers prefer quantitative methods of risk analysis and assessment, as they allow for more accurate optimization of security resources.

The proposed risk assessment methodology comprises system modeling, defining and ranking the criticality of system components, and risk assessment. The modeled graph of cyberattacks aimed at the CPS devices allows obtaining various measurements for cyber risk assessment. Various measurements from the cyber and physical environments are combined into a single quantitative assessment, which is used to diagnose the system state. The vulnerability values of components in the cyber and physical layers of CPS are used to calculate the system risk based on the Sugeno fuzzy integral. Based on the obtained values, the most critical nodes of CPS are selected, and possible cyberattack paths are predicted.

To ensure the CPS cyber resilience based on the cyberattack graph, it is necessary to determine the criticality of its nodes. Risk assessment indices allow for measuring how vulnerable the system is to cyberattacks and determining the location of the CPS components relative to one another. The indices under consideration cover the following two main areas: (1) OT and (2) IT. The environments under consideration are (1) physical and (2) cyber components. The IT and OT indicators predict the state of CPS when an undesirable event occurs. For example, to analyse the state of a wind power system for failures, the operator must first know such parameters as the turn-on speed, nominal speed, turn-off speed, and nominal power at each node of the system. Failure of individual CPS components can cause uncontrolled deviations of various parameters due to cyberattacks by intruders, which can ultimately lead to the destruction of the system.

The cyberattack graph enables the connection of different vulnerabilities. It defines potential threats to the nodes of CPS based on the vulnerability information to represent the cyberattack paths in the system. In fact, CVSS evaluates the complexity of implementing a cyberattack, taking into account the vulnerabilities of each device that exists in a specific node of CPS.

CPS systems have a diverse topological structure. Let's consider some indices for assessing the criticality of the nodes of the cyberattack graph. These indices provide detailed information about the entire network. Let $G = (\mathcal{N}, \mathcal{E})$ be a graph, where $\mathcal{N} = \{1, \dots, \mathrm{n}\}$ is a set of nodes (vertices), and $\mathcal{E}$ is a set of edges, $\mathcal{E} = \{(i,j) | i,j \in \mathcal{N}\}$. n represents the total number of nodes in the network.

a) *Closeness centrality.* Closeness centrality of a node measures how close a node (i.e., i) is to all other nodes by calculating the shortest path length from one node to other nodes in the network. Nodes with a high closeness centrality score have more influence on other nodes in the network.

Definition (closeness centrality). Closeness centrality C_i^c for node i is calculated as follows:

$$C_i^c = \frac{n-1}{\sum_{\substack{j=1 \\ i \neq j}}^{n} d_{ij}}, \; i = 1, \dots, n, \tag{23}$$

where d_{ij} is the shortest distance from node i to node j. There may be several paths in the graph connecting i with j, among which d_{ij} is the shortest path.

b) *Eigenvector centrality* shows the connection between the most "influential" node of the graph and its neighboring nodes.

Definition (eigenvector centrality). Eigenvector centrality E_i^c for node i is defined as follows:

$$E_i^c = \frac{1}{\delta_{max}} \sum_{j=1}^{n} a_{ij} E_j^c, \; i = 1, \dots, n, \tag{24}$$

where δ_{max} denotes the largest eigenvalue of the adjacency matrix. The adjacency matrix is a square matrix of size $n \times n$, $\mathbb{A} = \left\| a_{ij} \right\|_{i,j=1}^{n}$, whose elements are defined as: $a_{ij} = 1$ when node i is connected to node j, and $a_{ij} = 0$ otherwise.

c) *Betweenness centrality* measures the number of shortest paths through a particular node in a graph. This graph-theoretic metric measures how often a node acts as a “bridge” on shortest paths between two other nodes. When translating a network into a graph-theoretic model, the edge betweenness centrality (B_i^c) of a node indicates the likelihood of the cyberattack passing through that node.

Definition (*betweenness centrality*). The betweenness centrality B_i^c of node i is defined as follows:

$$B_i^c = \sum_{\substack{k,j=1 \\ k \neq j \neq i}}^{n} \frac{\sigma_{kj,i}}{\sigma_{kj}}, \; i = 1, \dots, n, \tag{25}$$

where σ_{kj} is the total number of shortest paths from source node k to destination node j, and $\sigma_{kj,i}$ is the number of paths from k to j that pass through i.

Shortest paths refer to all the shortest paths between each pair of nodes in the graph. If one node is part of the shortest paths, then it has high betweenness centrality.

d) *Katz centrality* is a graph theory parameter that assigns importance to a node based on the network structure and the node's position within the network. It determines the number of nodes connected through this path, and the contribution of distant nodes is “penalized.”

Definition (Katz centrality). The Katz centrality K_i^c of node i is defined as:

$$K_i^c = \sum_{q=1}^{\infty} \sum_{j=1}^{n} \beta^q (\mathbb{A}^q)_{ji}, i = 1, \dots, n, \quad (26)$$

where $\beta \in (0,1)$ β∈(0,1) is the attenuation coefficient, i.e., the share of remote nodes' participation, and $(\mathbb{A}^q)_{ji}$ is the total number of connections of degree q between nodes i and j.

These indices provide detailed information about all CPS systems with a diverse topological structure.

The combination of the values of the CPS risk assessment criteria is performed using fuzzy integrals, which are defined with respect to fuzzy measures. It is assumed that the values of the fuzzy measure and all input parameters vary within a unit interval.

Definition (fuzzy measure). Let $N = \{1, \dots, n\}$ be a finite set and $\mu: 2^{\mathcal{N}} \to [0,1]$ be a function such that $\mu(\emptyset) = 0$ and $\mu(\mathcal{N}) = 1$. If for any A and B such that $A \subseteq B \subseteq \mathcal{N}$ the condition $\mu(A) \leq \mu(B)$ is satisfied, then the fuzzy set μ is called a fuzzy measure.

Definition (Sugeno λ-measure). Let $N = \{1, \dots, n\}$ be a finite set and $\lambda \in (-1, +\infty)$. The function $\mu: 2^{\mathcal{N}} \to [0,1]$ is a Sugeno λ-measure if the following conditions are satisfied:

$$\mu(\emptyset) = 0, \quad (27)$$

$$\mu(\mathcal{N}) = 1, \quad (28)$$

$$\mu(A) \leq \mu(B), \forall A, B \text{ such that } A \subseteq B \subseteq \mathcal{N}, \quad (29)$$

$$\mu(A \cup B) = \mu(A) + \mu(B) + \lambda\, \mu(A)\, \mu(B), \forall A, B \subseteq \mathcal{N}, A \cap B = \emptyset, \quad (30)$$

where $\emptyset$ is the empty set.

Equations (27) and (28) represent the measures of the empty set and the combination of all sets, respectively. Equation (29) represents the monotonicity property. Equation (30) represents the possible subsets and the union of subsets.

Applying equation (30) again, for each $A \subseteq \mathcal{N}$, the value of $\mu(A)$ can be calculated as follows:

$$\mu(A) = \left[\frac{\prod_{i \in A}(1 + \lambda \mu(\{i\}))}{\lambda}\right]. \quad (31)$$

Using the constraint $\mu(\mathcal{N}) = 1$ (28) and applying equation (31), the λ value can be calculated using equation (32):

$$\lambda + 1 = \prod_{i=1}^{n} (1 + \lambda \mu_i), \quad (32)$$

where $\mu_i = \mu(\{i\})$.

Definition (discrete Sugeno integral). Let μ be a fuzzy measure in $\mathcal{N}$. The discrete Sugeno integral of a function $x = (x_1, x_2, \dots, x_n)$: $[0,1]^n \to [0,1]$ with respect to μ is defined as:

$$SI_\mu(x) = \max_{1 \le i \le n}(min(x_{\pi(i)}, \mu(\{\pi(1), \pi(2), \dots, \pi(n)\}))) =$$
$$= \max_{1 \le i \le n}\{min\{x_{\pi(i)}, \mu(\{\pi(1)\})\}, \dots, min\{x_{\pi(n)}, \mu(\{\pi(1), \dots, \pi(n)\})\}\}, \quad (33)$$

where π – a permutation in $\mathcal{N}$ such that $x_{\pi(1)} \le \dots \le x_{\pi(n)}$.

The basic idea of the Sugeno integral is based on a weighted minimum and maximum, which allows us to estimate the importance of each model using fuzzy measures. The Sugeno fuzzy integral determines the highest level of similarity between the target and predicted values. The combination of the values of the risk assessment criteria of the cyber-physical system is performed using fuzzy integrals, which are defined relative to fuzzy measures. It is assumed that the values of the fuzzy measure and all input parameters vary within a unit interval.

In this study, a metric based on the Sugeno fuzzy integral is used to assess the risks of cyberattack paths. The risk of each node of the cyberattack graph is calculated as follows:

$$Risk_i = Probability_i \times ImpactSI_i, i = 1, \dots, n, \quad (34)$$

where $Probability_i$ is the probability of access to node i, which shows the number of cyberattack paths and is calculated as follows:

$$Probability_i = 1 - \prod_{j=1}^{n}(1 - P_j), \ i = 1, \dots, n, \quad (35)$$

where P_j is the probability of a cyberattack on node j.

Here, P_i is calculated as

$$P_i = AV_i \times AC_i \times UI_i \times PR_i, \ i = 1, \dots, n, \quad (36)$$

where AV_i is an attack vector, AC_i is an attack complexity, UI_i is the user interaction, PR_i is a privilege requirement.

The fuzzy Sugeno integral (SI) impact is calculated using B_i^c, C_i^c, E_i^c and K_i^c indices, as well as integrity (I_i), availability (A_i), and confidentiality (C_i) scores obtained from CVSS v3.1, as follows:

$$ImpactSI_i = SI(B_i^c, C_i^c, E_i^c, K_i^c, I_i, A_i, C_i), \ i = 1, \dots, n. \quad (37)$$

Nodes with high $ImpactSI$ values are considered more vulnerable to CPS cybersecurity threats. A metric based on multiple indices better characterizes each node of the system. Unlike a single index, it is more

informative. After calculating the required coefficients, they are combined using multi-criteria decision analysis. The Sugeno fuzzy integral is used to evaluate the risks associated with cyberattack paths, ensuring the cyber resilience of the considered cyber-physical system.

The variable R0 is introduced, i.e., the threshold value at which the CPS node with Risk above this threshold is considered "unstable." In practice, this value should be determined by experienced experts. If the node is "unstable," emergency measures are immediately taken to eliminate the risk. If the Risk is below R0, the node is considered "stable" and there is no risk. In this case, the next risk assessment can be performed after a certain interval. The final Risk decision makes the system more cyber-resistant from the perspective of cyber-physical security.

As an example, a wind power system was considered (Fig. 11). Wind power is one of the critical infrastructure sectors. Wind turbines are widely used in various facilities: enterprises, households, private homes, etc. Wind flows rotate the blades of a wind turbine, setting it in motion. The stronger the wind, the more energy is generated. This rotation starts the turbine, which also begins to rotate. Wind turbines are devices that convert wind energy into electrical energy. Energy is transmitted along the rotor shaft, which is connected to a gearbox that drives an electric generator. The turbine consists of a cooling system, a condition monitoring system, and a weather vane. They serve as input data for the controller, which determines the position of the blades and rotor. The battery management system monitors and controls multiple storage batteries, ensuring grid stabilization. The process parameter values obtained during monitoring are stored in the data archive. The human-machine interface HMI ensures interaction between process operators and the control system. Engineering workstations contain software development tools, with which a specialist can make changes and additions to the system configuration via a corporate network or the Internet. The remote terminal units RTU connection links the wind farm with the central SCADA system. Let's assume that an

intruder has exploited the vulnerabilities of the cyber-physical system's components and implemented the following cyberattack scenarios:

- *Manipulation and denial of control:* An attacker with the ability to interact with the SCADA server could exploit the CVE-2019-14925 vulnerability to manipulate system configurations, files, or critical values related to wind farm operations. The vulnerability could result in unauthorized access to sensitive data, including usernames, passwords, and other confidential information. An attacker could also abuse the fact that connections are not authenticated (CVE-2021-27395 vulnerability), allowing unauthorized manipulation of data and issuing RTU commands. It could stop logic tasks from running and disrupt communication between SCADA and remote terminal units RTU. This would prevent operators from controlling compressor stations.

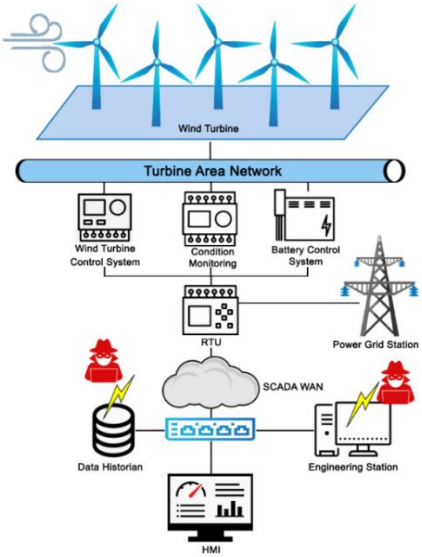


Fig. 11. Examples of cyberattack scenarios on CPS

- *Loss of control.* To compromise credentials and gain access to the wind farm network, the attacker exploits vulnerabilities CVE-

2019-9013, CVE-2022-1159, and CVE-2021-22797 to execute code on the remote terminal unit RTU (Table 11). This would allow control over individual turbines to be taken over.

Table 11
Information about vulnerabilities

Node	Vulnerability CVE-ID	*BS*	*IS*	*ζ*	*AV*	*C*	*I*	*A*	*UI*	*PR*	*AC*
1	CVE-2021-41773	7.5	3.6	3.9	0.85	0.56	0	0	0.85	0.85	0.77
2	CVE-2022-22720	9.8	5.9	3.9	0.85	0.56	0.56	0.56	0.85	0.85	0.77
3	CVE-2022-30522	7.5	3.6	3.9	0.85	0	0	0.56	0.85	0.85	0.77
4	CVE-2014-7844	7.8	5.9	1.8	0.55	0.56	0.56	0.56	0.85	0.85	0.77
5	CVE-2019-9557	6.1	2.7	2.8	0.85	0.22	0.22	0	0.62	0.85	0.77
6	CVE-2020-2512	5.9	3.6	2.2	0.85	0	0	0.56	0.85	0.85	0.44
7	CVE-2020-24673	9.8	5.9	3.9	0.85	0.56	0.56	0.56	0.85	0.85	0.77
8	CVE-2020-6992	6.7	5.9	0.8	0.55	0.56	0.56	0.56	0.85	0.27	0.77
9	CVE-2021-27395	8.1	5.2	2.8	0.85	0	0.56	0.56	0.85	0.62	0.77
10	CVE-2020-3960	8.4	5.8	2.0	0.55	0.56	0	0.56	0.85	0.62	0.77
11	CVE-2021-22797	7.8	5.9	1.8	0.55	0.56	0.56	0.56	0.62	0.85	0.77
12	CVE-2019-14925	6.5	3.6	2.8	0.85	0.56	0	0	0.85	0.62	0.77
13	CVE-2019-9013	8.8	5.9	2.8	0.62	0.56	0.56	0.56	0.85	0.85	0.77
14	CVE-2022-1159	7.2	5.9	1.2	0.85	0.56	0.56	0.56	0.85	0.27	0.77
15	CVE-2020-7566	7.3	5.2	2.1	0.62	0.56	0.56	0	0.62	0.85	0.77
16	CVE-2018-5452	7.5	3.6	3.9	0.85	0	0	0.56	0.85	0.85	0.77
17	CVE-2023-0286	7.4	5.2	2.2	0.85	0.56	0	0.56	0.85	0.85	0.44

An attacker could penetrate the internal network of the control system using vulnerability CVE-2018-5452 to manipulate the system configuration, operating parameters, and controller firmware.

This could disable the overspeed protection feature built into the remote terminal unit RTU and shed the load, resulting in a turbine shutdown. Using CVE-2020-7566 vulnerability, an attacker could compromise data and disable health monitoring systems that would provide early warning of a threat. Additionally, they can target programmable logic controllers PLCs and use CVE-2020-6992 vulnerability to compromise credentials and obtain execution code on the programmable logic controller PLC. With this, an attacker can compromise battery management functions, resulting in system downtime and potentially destabilizing cyber-physical system.

To conduct experiments, the values of the indices C_i^c, E_i^c, K_i^c, B_i^c, as well as integrity (I_i), availability (A_i), and confidentiality (C_i), obtained based on CVSS, were calculated for each node i of the system. This allowed us to identify critical nodes of the system. The indices were assigned "expert" weights. The higher the weight, the higher the "information content" of the index. Table 11 shows the index values for all nodes of the considered CPS. These values allow us to assess the criticality of the system devices based on the impact and probability values.

The proposed approach was chosen to determine the severity of the vulnerability according to the criteria:

$$\mathrm{R} = \begin{cases} \text{critical}, & \mathrm{v} \in [5, 10] \\ \text{high}, & \mathrm{v} \in [3, 5) \\ \text{medium}, & \mathrm{v} \in [2, 3) \\ \text{low}, & \mathrm{v} \in [0, 2) \end{cases}. \quad (38)$$

Various cyberattack paths aimed at possible graph nodes to change their states were considered.

This study aims to address a specific problem in the quantitative measurement of cyber-physical security in the considered cyber-physical system, taking into account factors that affect both its physical and cyber layers. The model combines the topology and vulnerabilities of

the cyber-physical network, ensuring the effectiveness of the proposed method in maintaining cyber resilience.

Therefore, the node risk assessment in the proposed method is based on the calculation of closeness centrality, eigenvector centrality, Katz centrality, edge betweenness centrality, integrity, and confidentiality scores. A wind power generation system was considered as an example. Unlike existing approaches, this study aimed to solve a specific problem: quantitatively measuring the cyber resilience of the considered CPS, taking into account factors that affect both its physical layer and cyber layer.

The **conclusion** reflects the most important results of the dissertation, and also formulates the main conclusions following from the proposed methods and algorithms, and the results obtained.

RESULTS

The main scientific, theoretical, and practical results obtained in solving the problems within the dissertation work are as follows:

1. The analysis of existing methods showed that the following problems are relevant: development of methods and algorithms for intelligent processing of big data to ensure the cyber resilience of CPS systems; development of methods and algorithms for ensuring IT cybersecurity and protection from OT of CPS; development of a method for determining the criticality of vulnerabilities of the functional components of CPS system and a method for assessing the risks of CPS. The statement of the scientific problem of the study is presented. A three-level conceptual model was developed to address a number of issues related to CPS cyber-resilience.

2. Algorithms based on clustering, which take into account the compactness and separability of clusters, have been developed for detecting outliers in big data using the k-means method to reduce the risk of CPS blocking.

3. An algorithm for CPS big data analysis based on weighted clustering is proposed. The weights obtained by summing the weights of each point from the dataset were assigned to clusters.

4. A method for parallel processing of big data was developed to reduce the risk of CPS system failure. It reduced the clustering time compared to the k-means algorithm.

5. A method for cluster analysis of CPS system big data based on a consensus ensemble using the squared Euclidean metric is proposed.

6. A method for classifying cyberattacks on the CPS systems using extreme machine learning and a genetic algorithm of the "firefly" behavior was developed.

7. A method for detecting DoS cyberattacks on CPS systems using an ensemble of classifiers, where for each point from the data set, the obtained class label corresponds to the maximum value among all estimates obtained by classification methods for this point, has been developed [10, 12].

8. An algorithm for detecting malware in CPS systems based on images using deep neural networks is proposed.

9. A method for detecting anomalies in CPS OT based on hierarchical hidden Markov models for a water treatment system was developed.

10. A method for detecting anomalies in CPS acoustic signals using transfer learning and the extreme gradient boosting method has been developed [26].

11. A method for detecting cyberattacks on CPS devices for a water treatment system using a deep hybrid model is proposed.

12. A method for image-based classification of the CPS failures for the electrical submersible pump was developed [20].

13. A method for determining the criticality of CPS functional components vulnerabilities based on the Bayesian attack graph for transporting natural gas through a pipeline has been developed.

14. A method for assessing the CPS risks using the fuzzy Sugeno integral for a wind energy generation system has been developed.

The results obtained in the experimental studies showed the advantages of the developed methods and confirmed the potential of the selected approaches.

The main results of the dissertation were published in the following scientific papers:

1. Imamverdiyev, Y.N., Sukhostat, L.V. Anomaly detection in network traffic using extreme learning machine // IEEE International Conference on Application of Information and Communication Technologies (AICT'2016). Baku, Azerbaijan, – 2016, – p. 418-421. (**WoS, Scopus**)
2. Имамвердиев, Я.Н., Сухостат, Л.В. Вопросы безопасности киберфизических систем // "Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları" üzrə III respublika elmi-praktiki konfransı. Сумгаит, Азербайджан, – 2016, – с. 257-259.
3. Имамвердиев, Я.Н., Сухостат, Л.В. Вопросы применения методов машинного обучения для решения проблем информационной безопасности // "Big data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı. Баку, Азербайджан, – 2016, – с. 127-131.
4. Алгулиев, Р.М. Киберфизические системы: основные понятия и вопросы обеспечения безопасности / Р.М.Алгулиев, Я.Н.Имамвердиев, Л.В.Сухостат // Информационные технологии, – 2017, 7, – с. 517–528. (**РИНЦ**)
5. Alguliyev, R.M. Anomaly Detection in Big Data based on Clustering / R.Alguliyev, R.Aliguliyev, Y.Imamverdiyev [et al.] // Statistics, Optimization and Information Computing, – 2017, 5 (4), – p. 325-340. (**Scopus (Q3)**)
6. Имамвердиев, Я.Н. Обнаружение аномалий в сетевом трафике на основе информативных признаков / Я.Н.Имамвердиев, Л.В.Сухостат // Radio Electronics, Computer Science, Control, – 2017, 3, – с. 113-120. (**WoS (Q4)**)
7. Alguliyev, R. An anomaly detection based on optimization / R.Alguliyev, R.Aliguliyev, Y.Imamverdiyev [et al.] // International Journal of Intelligent Systems and Applications, – 2017, 9 (12), – p. 87-96. (**Scopus (Q4))**
8. Алыгулиев, Р.М., Имамвердиев, Я.Н., Сухостат, Л.В. Оптимизационный подход к обнаружению аномалий в Big data // XIII Международная научно-техническая конференция «Распознавание-2017». Курск, Россия, – 2017, – с. 38-40. (**РИНЦ**)
9. Алгулиев, Р.М., Имамвердиев, Я.Н., Сухостат, Л.В. Обеспечение информационной безопасности киберфизических систем // "Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika konfransı. Баку, Азербайджан, – 2017, – с. 40-45.
10. Алгулиев Р.М., Алыгулиев Р.М., Имамвердиев Я.Н., Сухостат Л.В. Обнаружение DoS атак с применением ансамбля классификаторов // "İnformasiya təhlükəsizliyinin multidissiplinar problemləri" III respublika elmi-praktiki konfransı. Баку, Азербайджан, – 2017, – с. 12-18.
11. Alguliyev, R. Cyber-physical systems and their security issues / R.Alguliyev, Y.Imamverdiyev, L.Sukhostat // Computers in Industry, – 2018, 100, – p. 212-223. (**WoS (IF=4.769, Q1), Scopus (Q1)**)

12. Alguliyev, R.M. An improved ensemble approach for DoS attacks detection / R.M.Alguliyev, R.M.Aliguliyev, Y.N.Imamverdiyev [et al.] // Radio Electronics, Computer Science, Control, – 2018, 2 (45), – p. 73-82. (**WoS (Q4)**)
13. Alguliyev, R. Weighted clustering for anomaly detection in big data / R.Alguliyev, R.Aliguliyev, Y.Imamverdiyev [et al.] // Statistics, Optimization & Information Computing, – 2018, 6 (2), – p. 178–188. (**Scopus (Q3)**)
14. Alguliyev, R.M., Aliguliyev, R.M., Sukhostat, L.V. Purity-based consensus clustering for anomaly detection in Big data // XIV International scientific conference "Recognition - 2018". Kursk, Russia, – 2018, – p. 17-20. (**РИНЦ**)
15. Сухостат, Л.В. Обнаружение атак на киберфизические системы на основе глубокого обучения // "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı. Баку, Азербайджан, – 2018, – с. 42-46.
16. Alguliyev, R.M., Aliguliyev, R.M., Sukhostat, L.V. Consensus clustering by weight optimization of input partitions // IEEE 13th International Conference "Application of Information and Communication Technologies (AICT'2019). Baku, Azerbaijan, – 2019, – p. 1-4. (**WoS, Scopus**)
17. Алгулиев, Р.М., Имамвердиев, Я.Н., Шыхалиев, Р.Г., Сухостат, Л.В. Об одном подходе по выявлению кибератак на киберфизические системы с применением глубокой гибридной модели // The First International Scientific and Practical Forum «GLOBAL CYBER SECURITY FORUM 2019». Харьков, Украина, – 2019, – с. 27-28.
18. Alguliyev, R.M., Imamverdiyev, Y.N., Sukhostat, L.V. Detection of cyber-attacks on cyber-physical systems using deep neural network. XV International scientific conference "Recognition - 2019". Kursk, Russia, – 2019, – p. 18-20. (**РИНЦ**)
19. Сухостат, Л.В. Вопросы защиты персональных данных в киберфизических системах // "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" V respublika konfransı. Баку, Азербайджан, – 2019, – с. 92-96.
20. Alguliyev, R.M. Intelligent diagnosis of petroleum equipment faults using a deep hybrid model / R.M.Alguliyev, Y.N.Imamverdiyev, L.V.Sukhostat // SN Applied Sciences, – 2020, 2 (5), – p. 1-16. (**WoS (Q2), Scopus (Q3)**)
21. Alguliyev, R.M. Efficient algorithm for big data clustering on single machine / R.M.Alguliyev, R.M.Aliguliyev, L.V.Sukhostat // CAAI Transactions on Intelligence Technology, – 2020, 5 (1), – p. 9-14. (**WoS (Q2), Scopus (Q1)**)
22. Alguliyev, R.M. Weighted Consensus Clustering and its Application to Big Data / R.M.Alguliyev, R.M.Aliguliyev, L.V.Sukhostat // Expert Systems with Applications, – 2020, 150, – p. 1-15. (**WoS (IF=6.954, Q1), Scopus (Q1)**)
23. Alguliyev, R.M., Imamverdiyev, Y.N., Sukhostat, L.V. Diagnostics of DoS attacks on cyber-physical systems based on hierarchical hidden Markov models // XIII International Conference for young researchers "TECHNICAL SCIENCES. INDUSTRIAL MANAGEMENT". Borovets, Bulgaria, – 2020, – p. 39-41.

24. Alguliyev, R.M. Parallel batch k-means for big data clustering / R.M.Alguliyev, R.M.Aliguliyev, L.V.Sukhostat // Computers and Industrial Engineering, – 2021, 152, – p. 1-11. (**WoS (IF=7.180, Q1), Scopus (Q1)**)
25. Alguliyev, R.M. Hybrid DeepGCL model for cyber-attacks detection on cyber-physical systems / R.M.Alguliyev, Y.N.Imamverdiyev, L.V.Sukhostat // Neural Computing and Applications, – 2021, 33 (16), – p. 10211-10226. (**WoS (IF=5.102, Q2, Scopus (Q1)**)
26. Sukhostat, L.V. An intelligent model based on deep transfer learning for detecting anomalies in cyber-physical systems / L.V.Sukhostat // Radio Electronics, Computer Science, Control, – 2021, 3, – p. 124-132. (**WoS (Q4)**)
27. Сухостат, Л.В. Об одном подходе по обнаружения аномалий в киберфизических системах на основе акустических сигналов // 1st International Conference on "Information security: problems and prospects". Баку, Азербайджан, – 2021, – с. 115-118.
28. Сухостат, Л.В. Обзор некоторых решений безопасности современных АСУ ТП / Л.В.Сухостат // Телекоммуникации, – 2022, 2, – с. 14-23. (**РИНЦ**)
29. Sukhostat, L.V. Anomaly detection in industrial control system based on the hierarchical hidden Markov model / Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series D: Information and Communication Security (IOS Press), – 2022, 62, – p. 48-55.
30. Алгулиев, Р.М., Алыгулиев, Р.М., Сухостат, Л.В. Оценка критичности киберфизических систем на основе графа атак // XVII International scientific conference "Recognition - 2023". Курск, Россия, – 2023, – с. 52-54. (**РИНЦ**)
31. Alguliyev, R. Radon transform based malware classification in cyber-physical system using deep learning / R.Alguliyev, R.Aliguliyev, L.Sukhostat // Results in Control and Optimization, – 2024, 14, – p. 1-14. (**WoS (IF=3.2, Q1), Scopus (Q1)**)
32. Alguliyev, R.M. Method for Quantitative Risk Assessment of Cyber-Physical Systems based on Vulnerability Analysis / R.M.Alguliyev, R.M.Aliguliyev, L.V.Sukhostat // Kybernetika, – 2024, 60 (6), – p. 779-796. (**WoS (IF=2.2, Q3), Scopus (Q3)**)
33. Alguliyev, R. An approach for assessing the functional vulnerabilities criticality of CPS components / R.Alguliyev, R.Aliguliyev, L.Sukhostat // Cyber Security and Applications, – 2025, 3, – p. 1-7. (**Scopus (Q1)**)

The role of the applicant in papers published with coauthors:

[2-4,9,11] An analysis of methods and algorithms for ensuring cyber resilience and information security of CPS was conducted.

[21,24] Development of methods for parallel big data processing to reduce the risk of CPS failure.

[13] An algorithm for analysing CPS big data based on weighted clustering was proposed.

[5,7,8] The algorithms for detecting outliers in big data based on the k-means method were proposed to reduce the risk of CPS blocking.

[14,16,22] A method for cluster analysis of CPS big data based on the consensus ensemble was proposed.

[1,6] A method for classifying cyberattacks on CPS using extreme learning machine was proposed.

[10,12] Development of a method for detecting DoS attacks on CPS using an ensemble of classifiers.

[31] An algorithm for detecting malware in the CPS based on images was proposed.

[23] A method for detecting anomalies in the OT CPS based on hierarchical hidden Markov models is proposed.

[17,18,25] Development of a method for detecting attacks on CPS devices using a deep hybrid model.

[20] A method for classifying CPS failures based on images was proposed.

[30,33] A method for determining the criticality of vulnerabilities in CPS functional components based on the Bayesian attack graph was proposed.

[32] A method for assessing the CPS risks using the fuzzy Sugeno integral was proposed.

The defense of the dissertation will be held on 31 October 2025 at 10^{00} at the meeting of the ED 1.35 Dissertation Council operating under the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

Address: Az 1141, Baku city, B.Vahabzadeh street, 9a.

The dissertation can be viewed in the library of the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

Electronic versions of the dissertation and abstract are posted on the official website of the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

The abstract was sent to the necessary addresses on 29 September 2025.

Printed: 27.09.2025

Paper format: 60x84 1/16

Volume: 76002 characters

Printing: 20 copies