Research on systems for analysis and prediction of cyber incidents in corporate networks based on artificial intelligence*

Yevheniia Ivanchenko[1,†], Tetiana Berestiana[1,*,†], Yevhen Kykhtenko[1,†], and Artem Rozhenko[1,†]

[1] State University of Information and Communication Technologies, 7 Solomianska str., 03110 Kyiv, Ukraine

Abstract

The article presents a comprehensive study of modern technologies for the analysis, detection, and prediction of cyber incidents in corporate networks under conditions of increasing complexity and intensity of cyber threats. Particular attention is paid to the application of artificial intelligence methods as a key tool for enhancing the cybersecurity level of information systems. Existing approaches to cyber threat classification and the detection of anomalous behavior in network traffic – including signature-based, heuristic, and behavioral methods – are analyzed, and their main limitations in the context of adaptive and targeted attacks are identified. The feasibility of using machine learning and deep learning methods for automated analysis of large data volumes, improving detection accuracy for complex and previously unknown threats, and predicting potential cyber incidents at early stages is substantiated. The paper explores possibilities of integrating intelligent algorithms into security monitoring and incident response systems to enable a transition from a reactive to a proactive cybersecurity model. The obtained results confirm the effectiveness of applying artificial intelligence technologies in corporate networks and outline promising directions for further research aimed at developing adaptive and self-learning cyber incident prevention systems.

Keywords

cyber incidents, cybersecurity, artificial intelligence, machine learning, corporate networks, cyberattack, anomaly detection, cyber threats, deep learning, information security, intrusion detection systems, proactive cyber defense.

1. Introduction

In the context of ongoing digital transformation of corporate infrastructures, ensuring cybersecurity has become critically important [1, 2]. The rapid digitalization of business processes, along with the expansion of corporate network perimeters driven by cloud environments, mobile devices, and the Internet of Things (IoT), significantly increases the attack surface and complicates the task of maintaining information security. According to leading analytical agencies, the number of cyber incidents in the corporate sector is growing annually, while the financial and reputational damage caused by successful attacks is reaching critical levels [1].

The evolution of cyber threats is characterized by increasing complexity, stealth, and variability, which significantly complicates the application of traditional approaches to their detection and mitigation [3]. Modern adversaries actively employ social engineering techniques, exploitation of zero-day vulnerabilities, polymorphic malware, and methods of stealthy long-term intrusion, known as Advanced Persistent Threats (APT). Such attacks may remain undetected for weeks or even months, gradually compromising critical assets of corporate infrastructures.

Classical monitoring and response systems — signature-based intrusion detection systems, basic SIEM solutions, and passive network traffic analysis — are increasingly demonstrating limited effectiveness in the face of growing data volumes, high attack dynamics, and the emergence of

* CSDP'2026: Cyber Security and Data Protection, May 7, 2026, Lviv, Ukraine

* Corresponding author.

† These authors contributed equally.

evivancenko@gmail.com (Y. Ivanchenko); t.berestiana@duikt.edu.ua (T. Berestiana); firementer@gmail.com (Y. Kykhtenko); a.rozhenko@stud.duikt.edu.ua (A. Rozhenko)

0000-0003-3017-5752 (Y. Ivanchenko); 0009-0007-1455-234X (T. Berestiana); 0009-0008-1696-1048 (Y. Kykhtenko); 0009-0000-2900-349X (A. Rozhenko)

new, previously unknown patterns of malicious activity [4, 5]. These systems are primarily designed to detect known threats based on predefined rules and signatures; therefore, they are inherently incapable of adapting to fundamentally new attack vectors without regular manual updates. Moreover, the continuous growth in the volume of telemetry data in large-scale corporate networks leads to analyst overload and a decrease in the speed of response to actual incidents [5].

In response to these challenges, both the research community and the cybersecurity industry are increasingly focusing on the application of artificial intelligence algorithms capable of performing multidimensional analysis of data streams and adaptively responding to changes in the behavioral characteristics of users and corporate network subsystems [6, 7]. Intelligent systems are able to learn from large datasets of past incidents, detect subtle anomalies in network behavior, and build predictive models to identify threats before their full manifestation. Machine learning and deep learning methods, including neural networks of various architectures, are increasingly considered key tools for improving anomaly detection accuracy, identifying hidden correlations between events, and developing predictive models for the early detection of cyber incidents [8–10].

Despite significant advances in the intellectualization of cybersecurity tools, the practical implementation of such systems within corporate ecosystems is accompanied by a number of methodological and technological challenges [11]. In particular, issues related to ensuring data quality and representativeness for model training, handling imbalanced datasets, minimizing false positives, and guaranteeing the scalability of computational processes under real corporate workloads remain highly relevant [12, 13]. Special attention must also be given to mechanisms for adapting trained models to new types of attacks, ensuring their robustness against adversarial attacks, and addressing the interpretability of decisions (explainability) to support auditing processes and compliance with regulatory requirements [14].

In contrast to existing approaches, which predominantly consider individual components of cybersecurity systems in isolation (such as SIEM, IDS/IPS, UEBA, or SOAR), this paper proposes a generalized approach to the design of an integrated system for cyber incident detection and prediction, based on the combination of XDR platforms with machine learning algorithms. The proposed approach involves the integration of heterogeneous telemetry sources (network, host, behavioral, and cloud-based) into a unified analytical environment, followed by data processing using intelligent models for anomaly detection, event correlation, and threat prediction.

A distinctive feature of the proposed approach is its focus on detecting complex and coordinated (multi-stage) cyber incidents through the analysis of event sequences across temporal and spatial dimensions, implemented using deep learning techniques (in particular, recurrent neural networks and autoencoders). This enables improved detection accuracy of stealthy attacks, reduction of false positives, and a transition from a reactive to a proactive cybersecurity model. The proposed approach also considers the possibility of further integration with SOAR platforms to automate response processes, thereby forming a foundation for the development of adaptive and self-learning cybersecurity systems for corporate networks.

The aim of the study is to conduct a comprehensive analysis of systems for cyber incident analysis and prediction in corporate networks based on artificial intelligence technologies, in order to determine their capabilities and limitations for effective application under real-world conditions of information infrastructure operation. To achieve this goal, the study involves the formalization of the problem domain through a unified classification of cyber incidents; analysis of the functional capabilities of modern detection and response systems; and comparative evaluation of approaches based on key performance criteria.

2. Problem Statement

A key element in the development of effective systems for cyber incident detection and prediction is a unified classification of cyber incidents, which enables the structuring of security events,

identification of their characteristic features, and ensures correct interpretation of data within monitoring, correlation, and response processes. Without a clear taxonomy, it is impossible to develop adequate algorithmic approaches to threat analysis, as different categories of incidents exhibit fundamentally different indicators of compromise (IoCs), behavioral patterns, and requirements for detection methods. The level of threat posed by a cyber incident directly depends on its category, which determines the requirements for the functional capabilities of cybersecurity systems [15].

Currently, a significant number of cyber incident taxonomies exist, taking into account various aspects of digital threats, including the type of attack, impact on the CIA triad (confidentiality, integrity, availability), target orientation, and techniques employed by adversaries [15]. In particular, the State Service of Special Communications and Information Protection of Ukraine applies a set of categories developed based on the recommendations of the European Union Agency for Cybersecurity (ENISA, Reference Incident Classification Taxonomy) and the joint document by ENISA and the Europol European Cybercrime Centre (Common Taxonomy for Law Enforcement and the National Network of CSIRTs) [16].

According to these documents, cyber incidents are classified into the following main categories: Abusive Content (including spam, dissemination of child sexual abuse material, and other forms of content misuse); Malicious Code (covering viruses, worms, trojans, ransomware, and other types of malware); Information Gathering (including network scanning, social engineering, and phishing); Intrusion Attempts (exploitation of vulnerabilities, brute-force attacks, authentication attacks); Intrusion (successful breaches and unauthorized access to systems); Availability (DoS/DDoS attacks and sabotage); Information Content Security (unauthorized data modification and data breaches); Fraud (unauthorized use of resources and financial manipulation); Vulnerable (systems with unpatched critical vulnerabilities); and Other (incidents that do not fall into the aforementioned categories) [18]. Each category is assigned a unique code, type, and description, enabling unambiguous identification of threats and prioritization of response actions.

3. Literature Review

It is important to note that modern complex attacks, particularly APT campaigns, often span multiple categories within the aforementioned taxonomy simultaneously. For example, a typical attack may begin with information gathering (phishing), proceed to the intrusion phase (vulnerability exploitation), include the deployment of malicious code (installation of a backdoor), and ultimately result in a breach of confidentiality (data exfiltration). Such multi-stage behavior complicates event correlation and requires detection systems to be capable of tracking extended sequences of actions across both temporal and spatial dimensions [15–17].

These taxonomies not only define the spectrum of threats but also establish the requirements for the functional capabilities of detection and response systems. The practical implementation of these requirements necessitates standardized approaches to organizing monitoring, analysis, and incident response processes, as defined by international cybersecurity standards. In this context, cyber incident classification serves as a methodological foundation for selecting appropriate analytical approaches and technological solutions for cybersecurity in corporate networks [18–20].

The practical implementation of classification approaches requires formalized cyber incident management processes based on widely recognized international standards. A leading role in this context is played by the guidelines of the U.S. National Institute of Standards and Technology (NIST), which provide a unified methodological framework for the development of cybersecurity systems. The NIST SP 800-94 standard defines architectural and functional principles for intrusion detection and prevention systems (IDS/IPS), as well as the general stages of the incident response lifecycle [22]. This document establishes requirements for preparation, detection, analysis,

containment, eradication, and recovery from cyber incidents, thereby ensuring a systematic approach to security management in corporate networks.

4. Research Methodology

Based on NIST recommendations and related industry practices of ENISA, three main classes of solutions — SIEM, IDS/IPS, and SOAR — have become widely adopted in modern corporate environments, each addressing specific stages of the cyber incident management lifecycle [23]. At the same time, the effectiveness of these systems largely depends on their ability to process large volumes of heterogeneous data and identify complex correlations between events, which necessitates their intellectualization through the application of artificial intelligence methods [23].

5. Research Results

SIEM systems (Security Information and Event Management) provide centralized collection, normalization, correlation, and analysis of security events from various components of corporate infrastructure, including firewalls, routers, servers, cloud services, and endpoints. Through correlation mechanisms that aggregate disparate events into logical chains, SIEM systems are capable of detecting multi-stage attacks that may not appear suspicious when considered in isolation. An additional advantage of SIEM lies in its support for long-term log storage, which is critical for auditing, regulatory compliance (e.g., GDPR, PCI DSS, ISO 27001), and digital forensics during incident investigations [23].

However, the practical use of SIEM systems is associated with several significant limitations. First, traditional SIEM solutions rely on predefined correlation rules, requiring continuous manual maintenance and updates, especially in response to emerging attack types. Second, large corporate networks generate millions of events per day, which inevitably leads to analyst overload due to a high volume of false-positive alerts. Third, the deployment and maintenance of SIEM solutions require substantial financial resources and highly skilled personnel. These limitations drive the development of next-generation SIEM systems with integrated machine learning capabilities for automated anomaly detection [23].

Intrusion Detection and Prevention Systems (IDS/IPS) operate at the network or host monitoring level and perform analysis of traffic or the behavior of individual components of an information system. IDS (Intrusion Detection Systems) are primarily focused on passive detection of anomalies and suspicious activities, generating alerts for analysts, whereas IPS (Intrusion Prevention Systems) extend this approach by actively blocking malicious activities in real time [23]. Among the most widely used open-source implementations are Snort and Suricata, which support both signature-based and behavioral analysis.

A key advantage of IDS/IPS lies in their ability to detect intrusions at an early stage at the network traffic level, before an attack reaches critical assets. Support for signature-based methods ensures effective protection against known attack types with minimal latency. At the same time, IDS/IPS systems are highly dependent on the актуальність signature databases and are unable to detect zero-day threats without the use of additional behavioral techniques. Behavioral analysis, in turn, may generate a significant number of false positives, especially in dynamic corporate environments. The scalability of such systems in networks with throughput exceeding 10 Gbps also remains a technological challenge [23].

SOAR platforms (Security Orchestration, Automation and Response) represent a relatively new class of solutions that have emerged in response to analyst overload in Security Operations Centers (SOC) and the fragmentation of security tools [24]. SOAR platforms automate routine incident response operations through formalized workflows (playbooks), orchestrate interactions among various security tools (SIEM, EDR, TIP, vulnerability scanners), and standardize operational

procedures within monitoring centers. The use of SOAR enables a reduction in the mean time to respond (MTTR) from several hours to tens of minutes and significantly decreases the workload of analysts through automated handling of typical scenarios [24].

At the same time, the effectiveness of SOAR solutions largely depends on the quality of playbook formalization and the maturity level of SOC processes. Automation without sufficient oversight may lead to inefficient or even harmful decisions in non-standard situations. In addition, SOAR platforms do not perform deep threat analysis independently — their effectiveness is determined by the quality of analytical signals received from adjacent detection systems. Therefore, SOAR is primarily considered an orchestration platform rather than a standalone cyber threat detection solution [24].

Thus, each of the considered classes of technological solutions addresses specific aspects of cyber incident management; however, none of them provides comprehensive protection against modern complex threats when operating in isolation. This necessitates the intellectualization and integration of different approaches based on artificial intelligence methods.

Based on the classification of cyber incidents and the analysis of the functional capabilities of modern security systems, it becomes evident that most contemporary threats are complex, multi-stage, and coordinated in nature [1–4, 7, 15, 24–26]. Such incidents combine elements of network attacks, account compromise, privilege abuse, and stealthy lateral movement within corporate infrastructures, which significantly complicates their timely detection using traditional security tools. In this regard, a comparative analysis of existing solutions is justified, taking into account the specifics of detecting complex and coordinated threats.

Traditional SIEM systems and signature-based IDS/IPS are effective for detecting individual incidents and known attack patterns. Their reliance on static rules and signatures ensures a low level of false positives for known threats and has proven effective in relatively stable threat landscapes. However, in the context of modern dynamic threats, the reactive nature of analysis and dependence on the timeliness of rules result in low resilience to zero-day attacks and a lack of capabilities for early-stage incident prediction [4–6, 34].

UEBA (User and Entity Behavior Analytics) systems, based on behavioral analysis, partially overcome these limitations. They detect deviations from baseline normal behavior using statistical methods and machine learning algorithms, making them effective for identifying insider threats, compromised accounts, and lateral movement scenarios-cases where traditional signature-based systems often fail. However, without deep integration with network and host telemetry sources, UEBA systems lack the full contextual awareness required to detect coordinated external attacks [7, 8, 34].

A significant qualitative improvement in detecting complex threats is provided by systems based on artificial intelligence and deep learning. AI-based IDS employ classical machine learning algorithms — such as Random Forest, Support Vector Machines, and XGBoost — that are capable of learning from large volumes of network events and detecting anomalies with significantly higher accuracy than rule-based approaches [9, 10]. DL-based IDS take this approach further: recurrent neural networks (RNN, LSTM) effectively model temporal dependencies in event sequences, which is critical for detecting slow or distributed attacks; convolutional neural networks (CNN) are successfully applied to network traffic classification; and autoencoders provide powerful mechanisms for anomaly detection in high-dimensional feature spaces. These approaches demonstrate increased resilience to zero-day threats and lower false-positive rates compared to rule-based systems, although they require substantial computational resources and careful preparation of training datasets [11, 12, 22–23, 34].

The most comprehensive approach to detecting modern cyber threats is implemented in XDR (Extended Detection and Response) solutions. XDR has emerged as an industry response to the limitations of isolated security systems, integrating the capabilities of SIEM, EDR (Endpoint

Detection and Response), NDR (Network Detection and Response), and UEBA into a unified platform with centralized telemetry [13, 14]. Cross-domain event correlation across network, host, cloud, and application layers, combined with machine learning algorithms, enables XDR to effectively identify coordinated multi-stage attacks, reduce false-positive rates, and support proactive defense mechanisms in corporate networks [24–26]. Additionally, through a unified interface, XDR simplifies the work of analysts by providing a comprehensive view of incidents within a single pane of glass, eliminating the need to switch between multiple isolated systems.

6. Comparative Analysis

To systematize the obtained results, a comparative analysis of the described solutions was conducted based on functional, analytical, and qualitative criteria. Particular attention was given to indicators such as resilience to zero-day threats, false-positive rates, computational complexity of algorithms, and the suitability of systems for detecting coordinated and group-based attacks. The results of the comparison are summarized in Table 1.

Table 1.
Comparative Analysis of Modern Systems for Detecting Coordinated Cyber Incidents

№	System Name	Confi-dentia-lity	Availa-bility	Inte-grity	Analysis Methods	Type of Analy sis	Level of Auto-matio n	Predic-tive Capabi-lity	Integrati on with Corpo-rate Net-works	Resilien-ce to Zero-Day Attacks	Compu-tational Comple-xity	Suitabi-lity for Coor-dinated Attacks
1	SIEM (Traditi onal)	High	Medium	High	Correlation Rules, Signatures	Reacti ve	Partial	No	High	Low	Medium	No
2	IDS/IPS (Snort, Suricata)	Mediu m	High	High	Signature-Based Analysis, Rule-Based, Pattern Matching	Reacti ve	Low	No	Medium	Low	Low	No
3	UEBA	High	Medium	High	Behavioral Analysis, Statistical Methods, ML Models	Proact ive	High	Partial	Medium -High	High	High	Yes
4		High	Medium	High	Machine Learning, Classification, Anomaly Detection	Proact ive	High	Yes	Medium	High	High	Yes
5	DL-based IDS	High	Medium	High	Deep Learning (CNN, RNN, LSTM, Autoencoders)	Proact ive		Yes	Medium	Very High	Very High	Yes
6	SOAR Platfor ms	High	High	High	Orchestration, Playbooks, Response Automation	Reacti ve-Proact ive	Very High	Limited	High	Medium	Medium	Partial
7	XDR	High	High	High	Cross-Domain Correlation, Machine Learning, Telemetry	Proact ive	Very High	Yes	Very High	High	High	Yes

The analysis of Table 1 allows for the identification of clear differences between reactive and proactive approaches to cybersecurity. Traditional SIEM and IDS/IPS systems demonstrate a satisfactory level of integration with corporate networks and provide reliable detection of known

threats; however, their reliance on static rules limits their effectiveness in detecting zero-day and coordinated attacks. Behavioral systems such as UEBA and hybrid AI/DL-based IDS significantly improve the accuracy of detecting complex scenarios, but require substantial computational resources and high-quality training datasets. XDR solutions demonstrate the highest overall level of effectiveness across a range of criteria, combining the advantages of cross-domain correlation, machine learning, and centralized telemetry [15, 21, 26–29].

The results of the comparative analysis confirm that the optimal cybersecurity strategy for modern enterprises is not limited to selecting a single solution, but rather involves the development of a multi-layered architecture in which different classes of systems complement each other. At the same time, there is a clear trend toward the consolidation of security tools around XDR and SOAR platforms with integrated artificial intelligence capabilities, as the most promising direction for the development of corporate cybersecurity.

7. Discussion

This paper presents a comprehensive study of modern systems for the analysis, detection, and prediction of cyber incidents in corporate networks, taking into account the evolution of cyber threats and the increasing requirements for cyber resilience of information infrastructures. It is shown that modern cyber incidents are increasingly characterized by multi-stage, coordinated, and stealthy behavior — particularly in the form of APT attacks, which combine elements of different threat categories and may remain undetected for extended periods. This significantly limits the effectiveness of traditional reactive cybersecurity tools based on signature-based or rule-based analysis.

Approaches to the classification of cyber incidents based on ENISA and CERT-UA recommendations have been analyzed, enabling the development of a unified methodological framework for the identification and categorization of threats in corporate networks. It is demonstrated that the use of standardized taxonomies is a necessary prerequisite for the development of effective detection and response systems, as it provides a common language for describing security events, structuring indicators of compromise, and prioritizing response actions. At the same time, taxonomy alone does not ensure adequate protection without integration with technological mechanisms for incident analysis.

The role of NIST standards in shaping processes for incident detection, analysis, and response has been examined. It has been established that the NIST SP 800-94 standard provides a formalization of the architectural and functional principles of intrusion detection systems and the general incident response lifecycle; however, it does not define specific algorithmic approaches for detecting complex and previously unknown attacks. This creates opportunities for further research in the direction of enhancing cybersecurity tools through intelligent methods.

8. Conclusions

A comparative analysis of the functional capabilities and limitations of SIEM, IDS/IPS, and SOAR systems, behavioral UEBA systems, as well as intelligent AI-based and DL-based IDS solutions and XDR platforms has been conducted. It has been established that traditional systems are effective in detecting known attack patterns and provide reliable event collection and correlation; however, their reactive nature results in low resilience to zero-day threats and limited capability to detect coordinated attacks. Intelligent approaches based on neural networks, autoencoders, and recurrent models enable the identification of complex nonlinear correlations between events, improve resilience to emerging threats, and reduce false-positive rates. At the same time, the implementation of such systems requires substantial computational resources, high-quality

training data, and well-designed mechanisms for adapting models to the dynamically evolving threat landscape.

The results of the comparative analysis indicate that hybrid and integrated approaches are the most promising for countering coordinated and group-based attacks, particularly XDR solutions with cross-domain correlation and machine learning capabilities. The integration of centralized telemetry from multiple layers of corporate infrastructure, automated response through SOAR platforms, and proactive threat detection based on artificial intelligence forms the architectural foundation for the next generation of cybersecurity systems.

Overall, the results of the study confirm that effective cybersecurity of corporate networks in the context of modern threats requires a transition from isolated reactive solutions to integrated intelligent systems for cyber incident analysis and prediction. The application of artificial intelligence methods in combination with standardized taxonomies and process models provides a scientific and methodological foundation for the development of proactive, adaptive, and scalable cybersecurity systems capable of ensuring the stable operation of corporate information infrastructures in the long term.

Promising directions for future research include the development of hybrid threat detection architectures with support for explainable artificial intelligence (XAI), the investigation of methods for protecting models against adversarial attacks, and the design of self-learning systems capable of automatically adapting to new types of cyber threats.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] ENISA, Threat Landscape Report, Eur. Union Agency Cybersecur., 2023.

[2] R. von Solms, J. van Niekerk, From information security to cybersecurity, Comput. Secur., 2013.

[3] Symantec, Internet Security Threat Report, 2022.

[4] K. Scarfone, P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST SP 800-94, National Institute of Standards and Technology, 2007.

[5] K. Behl, Cyberwar: The Next Threat to National Security, Oxford University Press, 2017.

[6] L. Buczak, E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surv. Tutor., 2016.

[7] S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021.

[8] Goodfellow, Y. Bengio, A. Courville, Deep Learning, MIT Press, 2016.

[9] G. Kim, S. Lee, S. Kim, A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, Expert Syst. Appl., 2014.

[10] V. Chandola, A. Banerjee, V. Kumar, Anomaly detection: A survey, ACM Comput. Surv., 2009.

[11] R. Sommer, V. Paxson, Outside the closed world: On using machine learning for network intrusion detection, IEEE Symp. Secur. Priv., 2010.

[12] H. He, E. Garcia, Learning from imbalanced data, IEEE Trans. Knowl. Data Eng., 2009.

[13] R. Zuech, T. Khoshgoftaar, R. Wald, Intrusion detection and big heterogeneous data: A survey, J. Big Data, 2015.

[14] Biggio Roli., F. Roli, Wild patterns: Ten years after the rise of adversarial machine learning, Pattern Recognition, 2018.

[15] O. Kopytsia, D. Uzlov, Methods for determining the categories of cyber incidents and assessing information security risks, 2023.
[16] I. Opirskyy, O. Harasymchuk, O. Mykhaylova, Y. Sovyn, I. Tyshyk, Detection of network attacks based on the RedHunt virtual machine (2025) // Adv. Cybersecur. Next Gener. Syst. Appl., Boca Raton: CRC Press, 2025. pp. 310–330, doi:10.1201/9781003546153-14.
[17] D. Zhuravchak, M. Opanovych, A. Tolkachova, V. Dudykevych, A. Piskozub, Design of an integrated defense-in-depth system with an artificial intelligence assistant to counter malware, 2024, East. Eur. J. Enterp. Technol., 6 (2(132)), pp. 64–73, doi;10.15587/1729-4061.2024.318336.
[18] O. Deineka, O. Harasymchuk, A. Partyka, A. Obshta, Application of LLM for Assessing the Effectiveness and Potential Risks of the Information Classification System According to SOC 2 Type II // CEUR Workshop Proc., 2025, 3991, pp. 215–232.
[19] O. Vakhula, I. Opirskyy, AI-driven Security as Code for software development using multi-agent systems // CEUR Workshop Proc., 2025., vol. 4024: Joint proceedings of the workshops at the Fourth international conference on cyber hygiene & conflict management in global information networks (CH&CMiGIN 2025) Kyiv, Ukraine, 2025. p. 170-185.
[20] H. Hulak, L. Kriuchkova, P. Skladannyi, I. Opirskyy, Formation of requirements for the electronic record-book in guaranteed information systems of distance learning. Paper presented at the CEUR Workshop Proceedings, 2021, p. 137-142.
[21] CERT-UA, List of Cyber Incident Categories, 2021.
[22] NIST, Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), 2007.
[23] ENISA, Security Orchestration, Automation and Response (SOAR): State of Play and Roadmap, 2021.
[24] NIST, Special Publication 1270: Towards a Standard for Evaluating AI Systems in Cybersecurity, 2022.
[25] ENISA, Artificial Intelligence Cybersecurity Challenges, 2021.
[26] A Survey on Machine Learning for Cyber Security, In: IEEE Transactions on Dependable and Secure Computing, 2020.
[27] NLP-Driven Approaches for Cyber Threat Intelligence and Log Analysis, Communications of the ACM, 2021.
[28] N. Mohamed, Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms, Knowledge and Information Systems, 2025.
[29] ENISA, AI Threat Landscape: Artificial Intelligence in Cybersecurity, 2020.
[30] N. Kreps, Narkhede, J. Rao, Kafka: A distributed messaging system for log processing, Proceedings of the NetDB, 2011.
[31] Shackleford, SOAR Platforms: Security Orchestration, Automation and Response, SANS Institute, 2018.
[32] V. Shulha et al., Analysis of existing methods, models, systems, and tools for information security assessment in corporate environments considering specific threats, Mod. Inf. Prot., 2025. doi:10.31673/2409-7292.2025.041201.
[33] V. Shulha et al., Methods and models for countering group cyber threats based on artificial intelligence, Cybersecur. Educ. Sci. Tech., 2025. doi:10.28925/2663-4023.2025.30.998.
[34] O. Deineka, O. Harasymchuk, A. Partyka, Y. Dreis, Y. Khokhlachova, Y. Pepa, Detection confidential information by large language models. Inform. Autom., Pomiary W Gospodarce I Ochronie Środowiska, 15(3), 91-99, 2025. doi:10.35784/iapgos.6910.