UDC 004.89
JEL L32
DOI 10.32782/2786-765X/2024-7-10

Kostiantyn Zavrazhnyi
PhD in Economics, Junior Researcher of the Department of Economics,
Entrepreneurship and Business Administration,
Sumy State University
ORCID: https://orcid.org/0000-0002-0408-0269
Anzhelika Kulyk
PhD student,
Sumy State University
ORCID: https://orcid.org/0009-0009-0743-8973

METHODOLOGICAL PRINCIPLES OF ASSESSING THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE INFORMATION SECURITY OF MANAGEMENT SYSTEMS OF ENTERPRISES[1]

The study focuses on the urgent problem of ensuring cybersecurity of modern enterprises in the context of the widespread implementation of artificial intelligence (AI) technologies. Given the growing number and complexity of cyberthreats, the authors analyze in detail how AI can be an effective tool for detecting and countering cyber threats, as well as the challenges associated with its use. The article discusses adversarial attacks, data poisoning attacks, and the use of deepfake technologies as tools for manipulation in cyberspace. The authors propose a modern approach to assessing cyber risks based on a modification of the GRS method, which allows classifying information assets of enterprises by level of vulnerability and developing effective protection strategies based on identification of cybersecurity priorities. The practical application of the proposed approach is demonstrated in a case study using the Google Drive platform as a example. The research uses generative artificial intelligence model Gemini, which allows identifying weaknesses in security systems, analyzing potencial risks and providing recommendations for eliminating vulnerabilities. Along with the benefits of AI implementation, such as automation of monitoring processes, analyzing big amounts of data in real time and predicting potencial threats, the study identified a number of challenges. In particular, the complexity of configuring and maintaining systems, the need for specialized knowledge to support them, the problem of algorithm transparency, and the risks of manipulation and attacks by intruders. The authors emphasize the importance of staff training for work with AI systems, including both technical knowledge and understanding of cyberspace risks. The need to develop clear policies for the use of these technologies is particularly emphasized. The study findings confirm that artificial intelligence can significantly improve the cybersecurity of multidisciplinary enterprises, but it requires a comprehensive approach. For effective use of the technology, the authors recommend improving attack detection algorithms, integrating ethical principles into the operation of systems, and developing strategies for the long-term development of enterprise cyber resilience.

Keywords: cybersecurity, enterprises, artificial intelligence, cyber resilience, cyber threats.

Problem statement. The implementation of artificial intelligence by multidisciplinary enterprises contributes to increasing the efficiency of management information systems. The technology provides automation of processes, accelerates data processing and anomaly detection, and facilitates decision-making based on predictive analytics. At the same time, the integration of AI into activity management systems requires changes in approaches to ensuring information security, as the number of cyber threats that also use artificial intelligence is increasing.

According to recent research, 97% of security professionals are concerned that their organizations could be victims of cyber incidents caused by AI technologies, 75% of professionals have been forced to change cybersecurity strategies due to new AI threats, and 73 % of security teams say they want to focus on preventive measures to reduce the likelihood of future incidents [1].

Machine learning systems are capable of not only analyzing large amounts of data in real time but also of detecting patterns that are impossible to detect using traditional tools. However, they are subject to attacks aimed at compromising algorithms by affecting their training and data processing. For example, data poisoning attacks can reduce the accuracy of AI predictions, while algorithmic attacks (adversarial attacks) manipulate data to create false classifications and conclusions.

The complexity of information security management in multi-profile enterprises is increasing along with the implementation of new systems,

[1] The paper is prepared within the scientific research project «Fulfillment of tasks of the perspective plan of development of a scientific direction "Social sciences" Sumy State University» (№ 0121U112685).

including supporting tools for business process management (CRM, project management systems, etc.), which provide critical support for the core functions of companies. Thus, a comprehensive assessment of the impact of AI on information security in management information systems is a necessary step for developing a strategy for protection against modern, rapidly changing cyber threats.

Analysis of the recent research and publications. An analysis of the scientific works of leading experts in the field of information security shows that the use of artificial intelligence in cybersecurity systems, especially for monitoring and analyzing large amounts of data in real time, plays a crucial role in increasing the effectiveness of threat response and detecting anomalies.

Scientists [2] are researching methods for solving complex cybersecurity problems, including using neural networks, expert systems, intelligent agents, and data processing. Researchers [3] note that AI algorithms in the field of cybersecurity have reached a significant level of maturity, allowing them to effectively overcome numerous problems that previously required human intervention.

Dvorskyy V. [4], Ponomarenko M. [4], Verkhusha O. [4] emphasize the importance of implementing modern cyber defense systems, conducting regular audits, and training personnel to minimize vulnerabilities and increase the competitiveness of enterprises.

Scientists [5] believe that proactively addressing cybersecurity issues using AI is essential for multi-discipline enterprises that use smart factories, autonomous systems, cyber-physical systems (CPS), the Internet of Things (IoT), cloud computing, and big data. Artificial intelligence has the potential to automatically generate cybersecurity data, making it a powerful tool for supporting enterprise cybersecurity and information sharing.

Researchers [6] identify three main approaches to ensuring cybersecurity of industrial systems: network isolation, multi-layered perimeter protection, and access control. However, given the constant evolution of cyber threats, they emphasize that modern systems require more dynamic solutions. The study [7] highlights the importance of applying artificial intelligence to detect threats, as machine learning mechanisms can increase the accuracy and speed of cyberattack detection, providing more reliable protection for enterprise management systems.

The purpose of the article. Previous studies have demonstrated the effectiveness of neural networks and machine learning algorithms in detecting anomalies in network traffic and user behavior in multi-sector enterprises, particularly in the financial and industrial sectors. However, existing solutions often suffer from a lack of transparency and interpretability of AI models, which makes it difficult to assess their reliability and identify potential biases. Undetected cyberattacks can lead to significant financial losses, reputational damage, and even production shutdowns. The goal of this study is to develop a methodological framework for assessing the impact of AI on information security, in particular by creating practical solutions for detecting and preventing such common attacks as phishing, DDoS attacks, and malware. The research aims to analyze the capabilities and limitations of modern AI methods in detecting and countering cyber threats, as well as to identify ways to increase the transparency and interpretability of artificial intelligence models.

Summary of the main research material. At the same time, as artificial intelligence systems continue to develop, new forms of attacks aimed at deceiving these methods are also emerging in cyberspace. Cyberattacks on modern enterprises are multi-vector and often combine several methods. Attackers can use both known software vulnerabilities and social engineering. The lack of centralized control over software development and updates creates significant risks, as fraudsters can easily discover and exploit previously unknown vulnerabilities. AI technologies that can detect patterns of normal and abnormal activity can help mitigate and localize attacks. However, as AI systems evolve, cybercriminals are also improving their methods, developing increasingly sophisticated attacks designed to deceive AI systems. In particular, attacks using hostile samples that are deliberately designed to mislead machine learning systems are becoming increasingly common.

Deepfake technology, based on artificial intelligence, creates new challenges for information security. The ability to create highly realistic fake images and videos opens up opportunities for manipulation and deception.The incident in Hong Kong in February 2024, when a finance department employee was attacked using deepfake, demonstrates the high level of threat posed by such technologies. By creating a deepfake video of the participants in the negotiation process, the attackers were able to deceive the employee and commit a financial fraud worth 25 million US dollars [8].

Cyberattacks target common vulnerabilities in software, such as improper access control, outdated security systems, or inadequate software updates, and open-source components used in AI systems. «Algorithm attacks» or «AI adversarial

attacks» and «data poisoning attacks» are two types of threats aimed at disrupting the operation of artificial intelligence. Algorithm attacks (adversarial attacks) involve adding invisible «noise» to input data, causing AI algorithms to make false predictions or classifications. This can be used to mislead image recognition models, fraud detection systems, etc. Data poisoning attacks involve introducing specially crafted or modified data into training sets. This can cause the model to learn incorrectly, leading to errors in predictions or analysis when used. Such attacks can significantly reduce the efficiency and reliability of AI-based systems [9].

Figure 1 demonstrates the main attack vectors that can affect the information systems of multi-profile enterprises and lead to negative consequences, from service denial to confidential data leakage.

Artificial intelligence can significantly improve threat detection and prediction through capabilities such as real-time big data analytics, where AI can process vast amounts of data quickly and efficiently, allowing systems to detect anomalies and suspicious activity almost instantly. AI systems can learn from historical data to understand what is «normal» for a particular network or environment, and detect deviations that may indicate potential threats. In anticipating potential attack vectors, AI can use predictive analytics to model possible attack scenarios based on historical data and current trends, allowing organizations to take proactive measures to protect their systems.

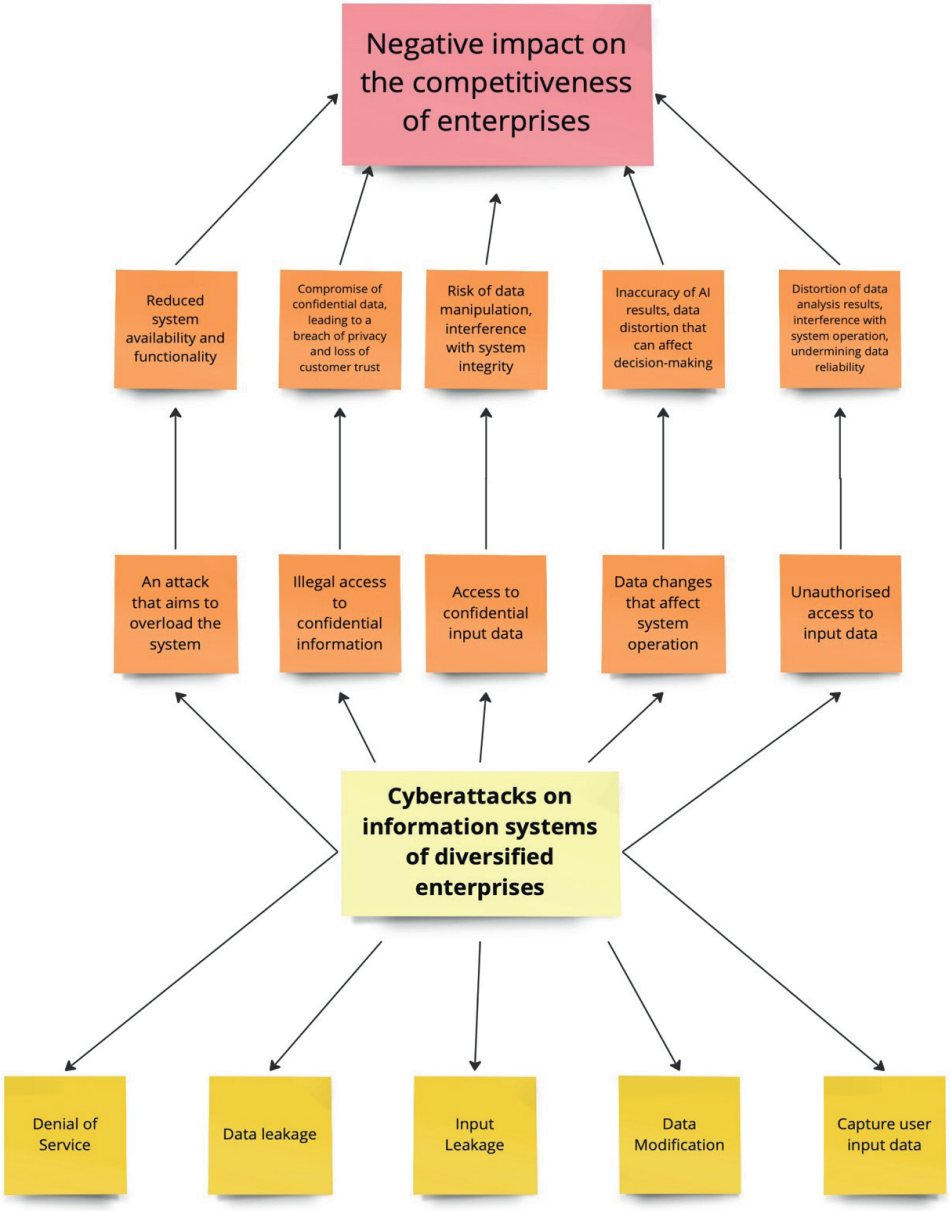

Figure 1. Cyberattacks on information systems of diversified enterprises.

Source: compiled by the authors

Along with the benefits of implementing artificial intelligence in cybersecurity systems, enterprises face challenges. Table 1 shows the main problems associated with the use of artificial intelligence in cybersecurity systems, discusses the causes of these problems, possible consequences and appropriate solutions.

In order to assess the effectiveness of using artificial intelligence in cybersecurity of multi-profile enterprises, a SWOT analysis was conducted (Figure 2). The analysis provides a comprehensive view of the potential and risks associated with the use of AI in cybersecurity and can contribute to the development of effective strategies for protecting information systems.

One of the main stages of ensuring information security of an enterprise is conducting a thorough risk assessment. To increase the effectiveness of information protection systems, a study was conducted to develop a methodology for assessing

Table 1

Problems of using artificial intelligence in the cybersecurity of multi-profile enterprises and their solutions

Problem	Cause	Consequences	Solution
Insufficient contextual awareness	Limited range of analyzed data, lack of deep understanding of the threat context.	False positives, missed threats.	Expanding the spectrum of analyzed data, integrating additional contextual data.
The complexity of setting up and maintaining AI systems	High complexity of algorithms, need for special knowledge.	Setup errors, low efficiency.	Simplifying interfaces, training staff, engaging experts.
AI vulnerability to manipulation	The ability to deceive algorithms with specially prepared data.	Wrong decisions, wrong conclusions.	Protection through advanced anomaly detection methods, robust training protocols.
The “black box” problem	The complexity of interpreting and evaluating decisions made.	Lack of trust in the system, difficulty in auditing.	Ensuring transparency, using tools to explain processes.
Ethical issues	The possibility of using AI for illicit purposes.	Violation of privacy, discrimination.	Establishing ethical principles, regular audits.
Attacks on AI algorithms	Specially designed methods to mislead algorithms.	False results, reduced system efficiency.	Protecting models from adversarial attacks, data poisoning.

Source: compiled by the authors

Figure 2. SWOT analysis

Source: compiled by the authors

and reducing cyber risks, which includes the following key stages: inventory of information assets, risk assessment using the modified GRS (Gross Risk Score) method, and development of a risk mitigation plan.

When assessing risks for each information asset, three parameters are analyzed: confidentiality (C), integrity (I) and availability (A), each of which is rated on a three-point scale:

• 3 – the highest level of criticality of the consequences of cyber risks,

• 1 – the lowest level of criticality.

Next, the probability of risk realization is determined for each parameter, also on a scale from 1 to 3, where 3 means the highest probability and 1 – the lowest.

The overall risk assessment for each asset is calculated using the GRS formula:

$$GRS = (C \times ProbabilityC) + (I \times ProbabilityI) + (A \times ProbabilityA)$$

$$GRS = (C \times ProbabilityC) + (I \times ProbabilityI) + (A \times ProbabilityA)$$

The proposed method allows to determine the overall risk level for each asset, which helps prioritize protective measures and ensure maximum cybersecurity effectiveness at the enterprise. Table 2 presents the stages of the asset inventory process, key actions, tools and methods, as well as performance indicators that help assess the quality of the measures taken.

Table 2

Stages of asset inventory and cybersecurity performance indicators

Stage	Action	Details	Tools and methods	Performance indicators
Asset inventory	Definition of protection objects.	Compilation of a complete list of information assets (hardware, software, data).	User surveys, documentation analysis, network scanning.	Completeness of the asset list, accuracy of data.
	Asset classification	Asset allocation by category (servers, workstations, network equipment, etc.).	Classification matrices.	Completeness of the list of assets, accuracy of data.
Risk assessment	Threat identification.	Identification of potential threats (internal, external).	Threat analysis, expert assessments, vulnerability scanning.	List of detected threats.
	Vulnerability analysis.	Identifying weaknesses in the security system.	Vulnerability scanning.	Number of vulnerabilities discovered.
	Probability analysis.	Determining the probability and consequences of threats.	Risk matrices, expert assessments.	GRS value for each asset.
Risk reduction.	Prioritization.	Ranking assets by risk level.	Priority matrix.	Time required to fix critical vulnerabilities.
	Developing an action plan.	Creating a detailed risk mitigation plan.	Project planner.	Completeness of the plan, responsible persons identified.
	Implementing measures.	Implementation of planned activities (software installation, firewall rules configuration, staff training).	Administration tools, training systems.	Percentage of completed activities.
Monitoring and evaluation of effectiveness	Security system monitoring.	Constant monitoring of the security system status (intrusion detection systems, log analysis).	SIEM systems, log analyzers.	Number of detected incidents, incident response time.
	Assessment of the effectiveness of measures.	Comparison of the level of risk before and after the implementation of measures.	Comparative analysis, user surveys.	Risk level change, user satisfaction.

Source: compiled by the authors

We suggest that multi-profile enterprises start projects for implementing artificial intelligence to improve cybersecurity by defining critical activities and identifying key business processes that are crucial for the company's operation. The next stage involves identifying supporting systems and tools that support critical activities and key processes. The next step is to identify risks to critical business processes and supporting systems and use AI to analyze and identify potential threats and vulnerabilities that could affect the security and sustainability of the company's core business.

Critical business processes directly affect the profitability and stable functioning of enterprises. Interruption of these activities can cause significant financial losses and negatively affect the company's reputation. Supporting systems and tools are hardware and software that support critical business processes. They ensure the smooth operation of the company's core functions, promote effective communication and collaboration between employees, form the necessary infrastructure for data storage and processing, and provide tools for rapid response to potential cyber threats. Integrating AI into supporting systems significantly increases their efficiency, ensuring accurate detection of potential threats and automated countermeasures. For example, effective communication systems contribute to the rapid exchange of information about security incidents, and a reliable server infrastructure guarantees data integrity.

We propose a modern approach to cyber risk detection using large language models. In particular, we investigate the ability of the Gemini model, trained on a large text data set, to detect atypical attacks and vulnerabilities in data storage systems. To conduct the study, define a critical business activity – processing VIP customer orders. This process requires a high level of accuracy and timeliness, as the satisfaction of key customers and the company's reputation depend on it. To process VIP customer orders, multi-profile enterprises use CRM systems (for example, Salesforce), email, messengers for communication, and payment systems for financial transactions. We formulate a request: «Assess possible security risks when processing VIP customer orders in the Salesforce system. Identify potential threats, including data leaks, phishing attacks on customers, and risks of system compromise». Table 3 describes the process of using AI recommendations aimed at identifying and eliminating vulnerabilities in the enterprise's information systems.

The case study is Google Drive, which is a popular file storage and sharing tool widely used by multi-enterprises. The research demonstrates that the use of generative artificial intelligence, such as the Gemini model, can increase the level of cybersecurity in the process of handling confidential customer data in Google Drive. Thanks to AI's ability to effectively identify security vulnerabilities, analyze potential risks, and offer specific recommendations for their elimination, companies can significantly reduce their vulnerability to cyberthreats. Table 4 shows the stages of using AI to identify risks in critical activities and support systems of multi-enterprises, as well as solutions that help improve their security.

The proposed methods prove the effectiveness of using AI, in particular generative models, in detecting and eliminating cyberthreats. At the

Table 3

Stages of implementing AI recommendations to improve cybersecurity

Stage	Action
Analysis of the received recommendations	Conducting a detailed analysis of risks and vulnerabilities posed by AI in critical business activities (processing VIP customer orders) and supporting systems (CRM, servers, messengers). Identifying the most critical issues that could impact business security.
Infrastructure improvements	If AI identifies security vulnerabilities, such as data leaks or outdated systems, contact the IT department to quickly fix the problems. For example: implement encryption of sensitive data, update systems, automate processes to reduce the risk of human error and increase efficiency.
Continuing dialogue with AI	Formulating additional requests to AI, for example: «What changes in the CRM system can minimize the risk of data leakage?», «How to improve the process of real-time threat detection?», «What can be implemented to optimize automated incident response?». Developing a step-by-step plan based on the received recommendations.
Continual improvement	Regularly update security measures and monitor new threats using AI. Periodic checks to monitor vulnerabilities and ensure that implemented measures are up to date. AI helps not only identify problems, but also update them and develop effective solutions.

Source: compiled by the authors

Table 4

AI implementation model to improve cybersecurity

Stage	Solution	Performance ID
Identifying critical business activities and supporting systems	Processing of confidential customer data for reporting purposes. Google Drive Software.	Report.
Generating a query to identify risks	«Analyze possible threats associated with the transfer and storage of confidential customer data in the Google Drive system. Identify risks of data leakage, unauthorized access, possible threats of phishing attacks, and vulnerabilities in user authentication mechanisms.»	Report on identified risks.
Staff training	Cyber hygiene trainings.	Test results.
Security policy updates	Using multi-level authentication and data encryption.	Approved security policies.
Technical measures	Automate user activity monitoring in Google Drive and integrate AI systems to detect anomalous activity in real time.	Reducing the number of security incidents.

Source: compiled by the authors

same time, there is a need for further research to improve the resilience of AI systems to new attacks and ensure the security of management information systems of multidisciplinary enterprises.

Conclusions. The study findings show that using artificial intelligence to automate cybersecurity tasks such as threat detection, incident response, and vulnerability management increases the resilience of information systems in multidisciplinary enterprises. These technologies allow for effective real-time analysis of big amounts of data in real time, detection of anomalies, and prediction of potential cyberattacks. It is important that AI not only identifies threats, but also offers specific solutions to eliminate them, which helps optimize security processes.

The authors' approach to cyber risk assessment using a modified Gross Risk Score method allows prioritizing security measures by classifying assets by risk level, which ensures efficient resource allocation. The case study on the Google Drive platform demonstrates the practical applicability of the method and the capabilities of the Gemini model, which not only identifies security vulnerabilities but also offers tools for automating response and preventing attacks.

Along with the advantages, the study identified disadvantages associated with the implementation of AI, in particular, the complexity of configuring and maintaining systems, vulnerability to adversarial attacks, and problems with algorithm transparency. These challenges highlight the importance of addressing issues related to algorithm transparency, protection against manipulation, and staff training.

The results obtained have practical value for increasing the cyber resilience of multidisciplinary enterprises. Companies can use the proposed approaches to improve their cybersecurity systems, determine priorities in protecting assets, and ensure the sustainable functioning of critical business processes. Prospects for further research include improving algorithms for detecting and countering threats, developing a methodology for integrating ethical principles into AI systems, and improving methods for training staff to work with these technologies.

References

1. GenAI in Cybersecurity: Friend or Foe? Report Voice of SecOps 2024. Deep Instinct. Available at: https://info.deepinstinct.com/voice-of-secops-v5-2024?_ga=2.90597402.180254519.1732114564-1531014459.1732114564
2. Shankarapani M., Ramamoorthy S., Movva R. et al. (2011) Malware detection using assembly and API call sequences. *J Comput Virol,* vol. 7. DOI: https://doi.org/10.1007/s11416-010-0141-5
3. Das R. & Sanndhane R. (2021) Artificial intelligence in cyber security. *Journal of physics: conference series,* vol. 1964. DOI: https://doi.org/10.1088/1742-6596/1964/4/042072
4. Dvorskyi V., Ponomarenko M. & Verkhusha O. (2024) Innovative strategies for increase competitiveness of companies in the digital era: from market analysis to implementation of technologies. *Economic Synerge»*, vol. 3. DOI: https://doi.org/10.53920/ES-2024-3-7
5. Nakrekanti M. & Polisetti R. (2024) Exploring artificial intelligence in cybersecurity within the Industry 4.0 framework: a comprehensive survey. *Journal of Engineering Sciences,* vol. 15 (04). DOI: https://doi.org/10.15433.JES.2024.V1514.43P.232

6. Mubarakova S., Amanzholova S. & Uskenbayeva R. (2022) Using machine learning methods in cybersecurity. *Eurasian Journal of Mathematical and Computer Applications*, vol. 10 (1). DOI: https://doi.org/10.32523/2306-6172-2022-10-1-69-78
7. Radanliev P., De Roure D., Walton R. et al. (2020) Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. *SN Applied Sciences,* vol. 2 (11). DOI: https://doi.org/10.1007/s42452-020-03559-4
8. Heather C. & Magramo K. (2024) Finance worker pays out $ 25 million after video call with deepfake 'chief financial officer'. *CNN World.* Available at: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
9. Zavrazhnyi K. & Kulyk A. (2024) Modern business cybersecurity challenges and the role of artificial intelligence in countering threats. *Economic bulletin of National technical university of Ukraine «Kyiv polytechnical institute»,* vol. 30. DOI: https://doi.org/10.20535/2307-5651.30.2024.313042

Стаття надійшла до редакції 21.10.2024

Завражний К.Ю.
кандидат економічних наук, молодший науковий співробітник
кафедри економіки, підприємництва та бізнес-адміністрування,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-0408-0269
Кулик А.К.
аспірантка,
Сумський державний університет
ORCID: https://orcid.org/0009-0009-0743-8973

МЕТОДОЛОГІЧНІ ЗАСАДИ ОЦІНЮВАННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ СИСТЕМ УПРАВЛІННЯ ДІЯЛЬНІСТЮ ПІДПРИЄМСТВ

Дослідження присвячене актуальній проблемі забезпечення кібербезпеки сучасних підприємств у контексті широкого впровадження технологій штучного інтелекту (ШІ). З огляду на зростання кількості та складності кіберзагроз, автори детально аналізують, як ШІ може бути ефективним інструментом для виявлення та протидії таким загрозам, а також виклики, пов'язані з його використанням. У статті розглядаються змагальні атаки, атаки з отруєнням даних та використання deepfake-технологій як інструменти маніпуляцій в кіберпросторі. Автори пропонують сучасний підхід до оцінки кіберризиків, заснований на модифікації методу GRS, що дозволяє класифікувати інформаційні активи підприємств за рівнем вразливості та розробляти ефективні стратегії захисту на основі визначення пріоритетів у сфері кібербезпеки. Практичне застосування запропонованого підходу продемонстровано у кейс-стаді на прикладі платформи Google Drive. У дослідженні використано генеративну модель штучного інтелекту Gemini, яка дозволяє виявляти слабкі місця у системах безпеки, аналізувати потенційні ризики та надавати рекомендації щодо усунення вразливостей. Разом із перевагами впровадження ШІ, такими як автоматизація процесів моніторингу, аналіз великих обсягів даних у реальному часі та прогнозування потенційних загроз, дослідження виявило ряд викликів. Зокрема, складність налаштування та обслуговування систем, необхідність спеціальних знань для їх підтримки, проблема прозорості алгоритмів та ризики маніпуляцій і атак з боку зловмисників. Автори підкреслюють важливість підвищення кваліфікації персоналу для роботи з ШІ-системами, що включає як технічні знання, так і розуміння ризиків кіберпростору. Окремо наголошено на необхідності розробки чітких політик використання цих технологій. Результати дослідження підтверджують, що штучний інтелект може суттєво підвищити рівень кібербезпеки багатопрофільних підприємств, однак вимагає комплексного підходу. Для ефективного використання технології автори рекомендують вдосконалити алгоритми виявлення атак, інтегрувати етичні принципи в роботу систем і розробку стратегій довготривалого розвитку кіберстійкості підприємств.

Ключові слова: кібербезпека, підприємства, штучний інтелект, кіберстійкість, кіберзагрози.