ANALYSIS OF THE MAIN THREATS IN THE SPHERE OF CYBERSECURITY

CZU: 004.056:005.342
DOI: https://doi.org/10.53486/tids2026.28

OLGA PUGACHEVA
Francysk Skaryna Gomel State University
e-mail: OPugacheva@gsu.by
ORCID ID: 0000-0003-4554-0038

Abstract. This article analyzes the main threats in cybersecurity. To this end, it examines the key reasons for the relevance of this study for organizations and individuals seeking to ensure their security in the digital world. This study of the main threats in cybersecurity includes an analysis of quantitative data such as the increasing number of cyberattacks, the diversity of cyberattack methods and threat channels, the main areas of cyberattacks, the consequences of cyberattacks, and the types of stolen data, as well as technological changes associated with the use of artificial intelligence (AI).

As AI is becoming an important resource in the arsenal of cybercriminals, this article analyzes the main risks of using AI, the ways in which AI is used in the development and evolution of malware, and important aspects of using AI in social engineering. This allows us to draw conclusions about the need for organizations to develop strategies to minimize risks and ensure the safe use of AI technologies in information security, and for their specialists to constantly update their defense methods and respond to new threats.

The results demonstrate the novelty of the analysis, which encompasses a comprehensive analysis of current and future threats, taking into account the role of AI, including its use for malicious purposes and social engineering; identifying the dual role of AI – both as a defense tool and a means of complicating attacks; and examining current technological development trends and their impact on cybersecurity.

The practical significance of the study lies in its ability to help organizations and professionals understand and prepare for current threats; substantiate the need to develop AI-informed defense strategies; and help professionals develop skills for continually updating defense methods in a dynamically changing environment.

Keywords: analysis, cybersecurity, cyberattacks, threats, artificial intelligence

JEL Classification: A12, C8, O33, C45, Y10

INTRODUCTION

Analyzing the main cybersecurity threats is a crucial part of an information security strategy and an asset for any organization seeking to ensure its security in the digital world.

It is essential for the following key reasons (Pugacheva Olga, 2025):

– increased cyberattacks. Each year, we see an increase in the number and complexity of cyberattacks. Hackers are using increasingly sophisticated methods, making continuous threat monitoring and analysis essential;

– diversity of threats. Threats can range from simple viruses and malware to complex attacks such as phishing, DDoS attacks, supply chain attacks, and more. Understanding these threats allows organizations to better prepare and protect themselves;

– economic impact. Cyberattacks can have serious financial consequences for organizations, including data loss, reputational damage, and fines. Threat analysis helps minimize risks and losses;

– regulatory compliance. Many industries are subject to strict cybersecurity regulations. Threat analysis helps organizations meet these requirements and avoid legal consequences;

- technological change. The rapid advancement of technologies such as cloud computing, IoT (Internet of Things), and artificial intelligence (AI) is creating new vulnerabilities. Threat analysis enables the timely identification and remediation of these vulnerabilities;

- increased awareness. Threat analysis helps increase employee and management awareness of cybersecurity risks, leading to a more responsible security culture within the organization;

- forecasting and preventative measures. Understanding current and potential threats allows organizations not only to respond to incidents but also to take proactive measures to prevent them.

The purpose of this study is to analyze the main cybersecurity threats facing organizations so that they can build a robust defense system, which is impossible without up-to-date knowledge of current cyberattack trends.

RESEARCH OF THE MAJOR CYBERSECURITY THREATS

1. Analysis of the Number of Cyberattacks

Every year, experts note that the number of successful cyberattacks is rapidly growing, and their complexity and aggressiveness continue to increase. This trend is illustrated by the data presented in Figure 1.

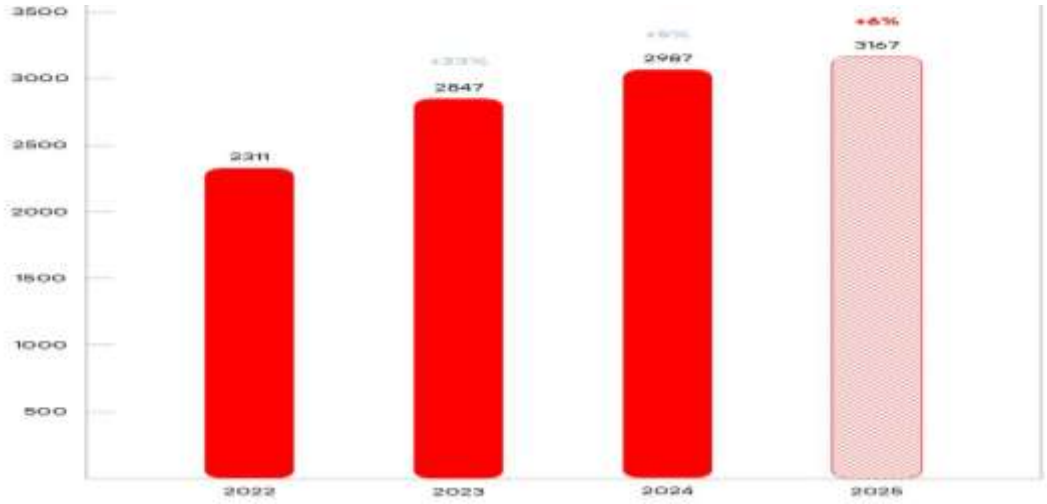


Figure 1. Number of successful attacks on organizations worldwide in 2022-2025.
Source: *Attack trends in 2026.*

The data shows that the total number of successful attacks on organizations globally was 6% higher in 2025 than in 2024, 11% higher in 2024 than in 2023, and 37% higher in 2023 than in 2022. Experts also note that because most cyberattacks are not made public due to reputational risks, it is impossible to calculate the exact number of threats.

2. Diversity of Cyberattack Methods and Threat Channels

As Figure 2 shows, the primary methods of cyberattacks on organizations worldwide in 2025 were malware (71%) and social engineering (51%). The share of successful malware-based attacks on organizations increased by 5 percentage points compared to last year, while the number of social engineering attacks remained unchanged.

The number of attacks using legitimate software doubled compared to 2024 and quadrupled compared to 2023, reaching 8% of total incidents.

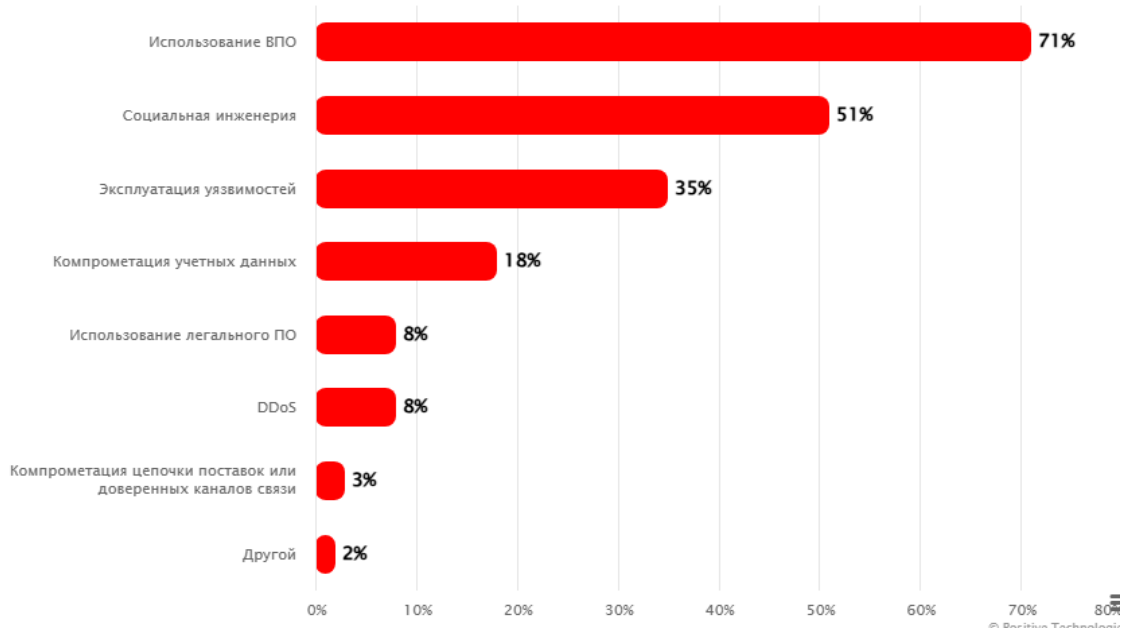


Figure 2. Attack methods on organizations (percentage of successful attacks) in 2025.
Source: *Attack trends in 2026.*

The social engineering channels used in attacks on organizations worldwide in 2025 are shown in Figure 3. The primary social engineering channel is email (86%). This is because attackers most often use phishing emails to infect victims with malware and further develop the attack. These are followed by organizational websites (23%), social media and instant messaging (6%), phone calls (3%), and other channels (2%).

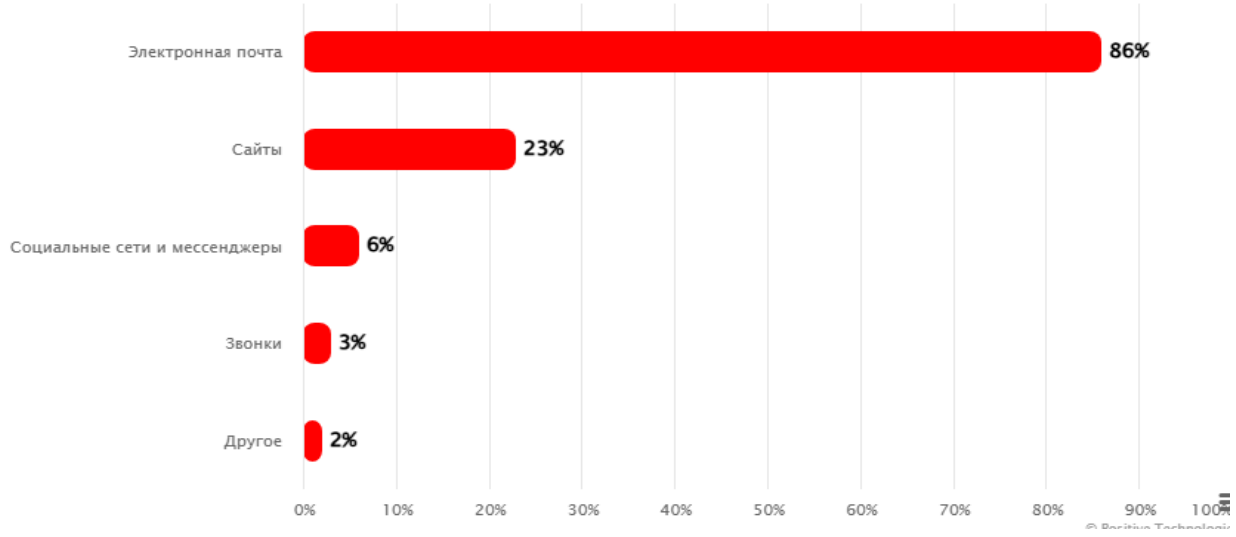


Figure 3. Social engineering channels in attacks on organizations around the world in 2025
Source: *Attack trends in 2026.*

3. Main Areas of Cyberattack

Victims of cyberattacks include a wide range of organizations, from small businesses to large corporations. Figure 4 shows the most vulnerable industries worldwide in 2025.

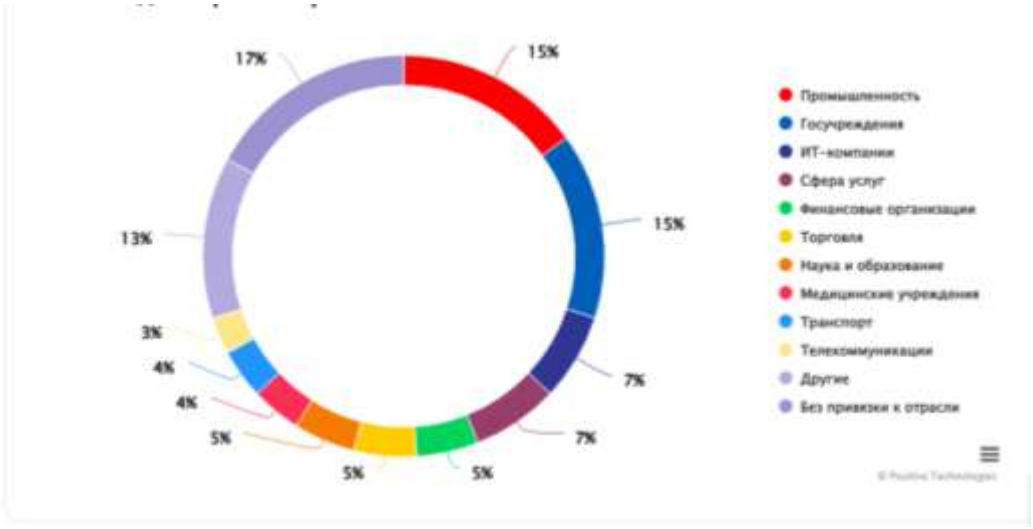


Figure 4. The areas of activity of organizations around the world subject to cyberattacks in 2025

Source: *Attack trends in 2026.*

The data shows that government agencies (15%), industrial enterprises (15%), and IT companies (7%) were the most frequently targeted sectors. New to the global attack landscape in 2025 is the service sector – hotels, cafes and restaurants, travel agencies, etc. – which has supplanted healthcare organizations, which have been a priority target for attackers in recent years. In 2025, it accounted for 7%. In 2024, healthcare was among the top five most attacked sectors (6%), and in 2023, it ranked second in terms of the number of cyberattacks.

4. Consequences of Cyberattacks and the main types of stolen data

Figure 5 shows the main consequences of cyberattacks in 2025. They show that nearly two-thirds (64%) of successful attacks on organizations resulted in confidential information leaks, while disruptions to the organization's core business accounted for 47%.

Comparing these figures to 2024, there is an increase in attacks associated with data leaks from 53% to 64%, and an increase in the proportion of successful attacks that resulted in business disruption from 31% to 47%.

Compared to 2024, the proportion of successful attacks that resulted in business disruption increased from 31% to 47%, and the percentage of attacks associated with data leaks increased from 53% to 64%.

Other consequences (use of organizational resources, damage to state interests, direct financial losses to the organization, etc.) together accounted for 27%.

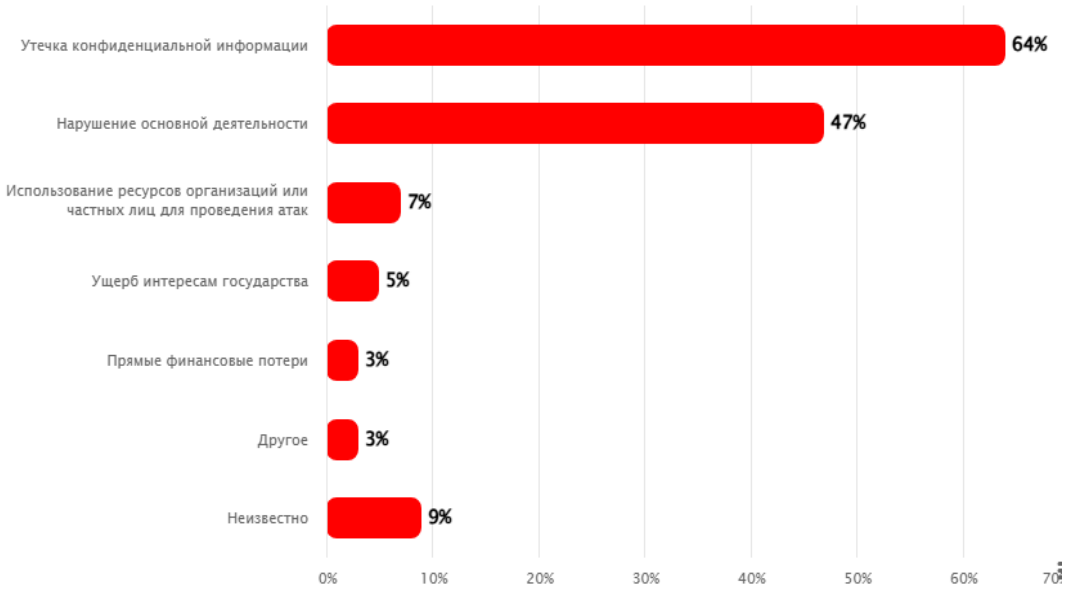


Figure 5. Main consequences of cyberattacks (percentage of successful attacks) in 2025.
Source: *Attack trends in 2026.*

The main types of stolen data in successful attacks on organizations are shown in Figure 6.

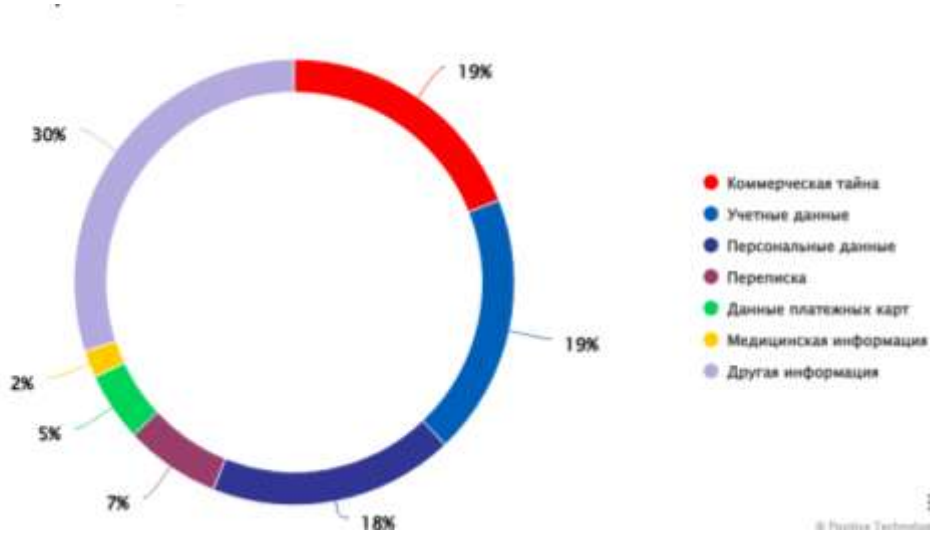


Figure 6 Types of stolen data in successful attacks on organizations
Source: *Attack trends in 2026.*

The most frequently stolen items from organizations were trade secrets (19%), credentials (19%), and personal data (18%).

Since 2024, there has been an increase in the theft of credentials from organizations and a decline in interest in personal information. This trend continued in 2025: credentials were stolen in 19% of attacks (an increase of 8 percentage points compared to 2023 and a decrease of 6 percentage points compared to 2022), while personal data was stolen in 18% (a decrease of 27 percentage points compared to 2023 and an increase of 18 percentage points compared to 2022). The share of trade secret leaks remains virtually unchanged year-over-year at 19%. Experts attribute the increased interest in credential theft to the fact that such data can be used by cybercriminals to carry out further attacks and/or sell on the shadow market.

5. Technological Changes Associated with the Use of AI Tools

Artificial intelligence is not only a tool for business and science, but also a new resource in the cybercriminal arsenal. The main risks of using AI, the ways in which AI is used in the development and evolution of malware, and important aspects of using AI in social engineering are presented in Table 1.

Table 1. Threats associated with the use of AI technologies

Threats associated with the use of AI technologies		
Risks of using AI and their characteristics	**Directions for the use of AI in the development and evolution of malware**	**Key aspects of using AI in social engineering**
1. Attack automation. AI can be used to automate cyberattacks such as phishing, password cracking, or distributed denial-of-service (DDoS) attacks. Algorithms can analyze vulnerabilities and find ways to exploit them faster and more efficiently than humans could.	1. Adaptive attacks. AI can be used to create malware that can adapt to different conditions and systems. For example, such programs can analyze the defense mechanisms on the target system and modify their attack methods to bypass these defenses.	1. Personalization of attacks. AI allows attackers to collect and analyze data about their victims, such as their interests, behavior, and social connections. This allows them to create personalized messages that are more convincing and believable, increasing the likelihood of an attack's success.
2. Advanced data analysis. AI can process and analyze large volumes of data, which can be used by attackers to identify vulnerabilities in security systems or to create targeted attacks based on collected user information.	2. Phishing automation. AI can be used to automate phishing attacks. Algorithms can analyze social media and other information sources to create convincing fake messages that are targeted to specific users based on their interests and behavior.	2. Phishing automation. AI can automate the creation of phishing emails and messages. Algorithms can generate multiple message variations tailored to specific audiences, making them more effective.
3. Creating fake content. Technologies such as generative neural networks can be used to create fake images, videos, or text, which can lead to disinformation and manipulation.	3. Malicious code generation. Using generative neural network technologies, it is possible to create new malicious code that is unique and less detectable by antivirus programs. This can significantly increase the effectiveness of malware.	3. Behavior analysis. AI can be used to analyze user behavior online, identifying patterns and anomalies. This helps attackers understand when and how best to attack, as well as predict how victims will react to certain actions.
4. Bypassing security systems. AI can be used to develop methods to bypass intrusion detection systems and other defense mechanisms, rendering them less effective.	4. Bypassing security systems. AI can analyze the behavior of security systems and find ways to evade their detection. For example, algorithms can study antivirus software patterns and adapt their actions to avoid detection.	4. Content generation. AI-based text generation technologies, such as GPT, can create plausible and well-formed messages. This allows attackers to generate fake messages from trusted sources, such as colleagues or well-known companies.
5. Vulnerabilities in AI systems themselves.	5. Targeted research.	5. Social media analysis.

Threats associated with the use of AI technologies		
Risks of using AI and their characteristics	**Directions for the use of AI in the development and evolution of malware**	**Key aspects of using AI in social engineering**
AI algorithms may contain vulnerabilities that can be exploited by attackers to manipulate results or gain access to sensitive information.	AI can be used to gather information about targets by analyzing data from open sources such as social media, websites, and databases. This allows attackers to better understand their victims and plan more effective attacks.	AI can analyze social media data to identify connections between people and their interests. Attackers can use this information to create more targeted attacks based on what interests the victim.
6. Ethical and legal issues. The use of AI in security may raise questions about privacy, human rights, and the legitimacy of such technologies.	6. Improved encryption. AI-based malware can use more sophisticated encryption methods to protect its components from analysis and detection, making it more resistant to attempts to neutralize it.	6. 6. Scenario Modelin. AI can help model various social engineering scenarios, allowing attackers to test different approaches and strategies to determine the most effective manipulation methods.
7. Errors and bias. AI algorithms can be error-prone or biased, which can lead to incorrect conclusions and actions regarding security.	7. Attack Scalability: With AI, attackers can quickly scale their attacks by using automated systems to launch multiple attacks simultaneously on different targets.	7. Vulnerability detection. AI can be used to analyze security systems and identify human vulnerabilities. For example, it can determine which employees are most susceptible to manipulation or how internal security policies can be circumvented.
8. Technology Dependency. Organizations' increasing reliance on AI systems may lead to risks associated with their failure or compromise.	8. Data-driven learning. Malware can learn from data from previous attacks to improve its methods and increase its effectiveness in the future. This allows it to evolve and adapt to new threats and defenses.	8. Big Data Processing. AI is capable of processing massive amounts of data from various sources, allowing attackers to quickly identify vulnerabilities and attack opportunities.

Source: *Pugacheva, O. V., 2024*

An analysis of the table's information allows us to draw the following conclusions:

- given the identified risks, it is important to develop strategies to minimize them and ensure the safe use of AI technologies in information security;

- AI significantly enhances the capabilities of malware, making it more complex, adaptive, and difficult to detect, creating significant challenges for cybersecurity professionals, who must constantly update their defenses and respond to new threats;

- AI significantly enhances the capabilities of social engineering, making attacks more targeted and effective. This creates significant challenges for organizations and individuals, who must be more aware of potential threats and develop critical thinking skills to protect against manipulation.

CONCLUSIONS

Research shows that recent years have seen a significant increase in the number, diversity, and distribution channels of cyberattacks, reinforcing the need for continuous improvement of security systems.

One of the current trends is the use of artificial intelligence by cybercriminals, enabling them to automate and sophisticate attacks, create new types of malware, and employ social engineering techniques. Despite the potential of AI to enhance security, its use for cybercriminal purposes requires special attention and the development of countermeasures.

To counter new types of threats and minimize risks, organizations must develop and implement comprehensive strategies that include constantly updating their defense and response methods, as well as training specialists.

The study's novelty lies in:

- a comprehensive analysis of current and future threats, taking into account the role of AI, including its use for malicious purposes and social engineering;
- identifying the dual role of AI – both as a defense tool and a means of complicating attacks;
- examining current technological development trends and their impact on cybersecurity.

The study's practical significance lies in its ability to help organizations and professionals understand and prepare for current threats; substantiate the need to develop AI-inclusive defense strategies; and help professionals develop skills to continually update their defense methods in a dynamically changing environment.

REFERENCES

Attack trends in 2026, 2026. Available at: https://ptsecurity.com/research/analytics/trendy-atak-v-2026-godu/#id8 [Accessed 10.03.2026].

Pugacheva, Olga, 2025. Innovative technologies in educational activities and ensuring digital security «Technological innovations in digital security», international conference (1; 2025; Chişinău). Proceedings of the First Edition of the International Conference «Technological innovations in digital security», May 15-16, 2025, Chişinău / scientific committee: Stratan Alexandru. – Chişinău: SEP ASEM, 2025. – 256 p. (pp. 168-175).

Pugacheva, O. V., 2024. Use of artificial intelligence in the economy and society: directions, problems and regulation. *Proceedings of the F. Skorina Gomel State University*, No. 5 (146). pp. 136-141.