UDC 004.8–004.056.53

THE ROLE OF AI IN PROTECTING AGAINST CYBERATTACKS AND IN DEVELOPING NEW METHODS OF INFORMATION SECURITY

Dolmatovich A.A., Buzanovskaya S.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Goncharova I.V. – Lecturer at the Department of Foreign Languages

Annotation. The article examines the role of artificial intelligence (AI) in the field of cybersecurity, analyzes its capabilities in detecting and preventing cyberattacks, and discusses the key problems and limitations associated with its use. The main types of cyber threats, including viruses, phishing, DDoS attacks, spoofing and ransomware, are considered and their consequences for organizations are analyzed. Special attention is paid to the advantages of AI, such as accelerated threat detection, improved data analysis accuracy, and adaptability to new types of attacks.

Key words: phishing, AI, spoofing, ransomware attacks, machine learning, cyberattacks.

Introduction. In recent years, cyberattacks have grown increasingly complex and varied, presenting new challenges for organizations in information security. As reliance on digital technologies deepens and data volumes rise, safeguarding information has become critically important. Artificial Intelligence (AI) provides innovative solutions to bolster defenses against cyberattacks, automate threat detection, and develop proactive security measures.

Main part. Understanding the landscape of cyberattacks is crucial for effective AI application in cybersecurity. Common threats include viruses and worms, which propagate across networks and devices, often disrupting user operations. *Phishing* attacks employ deceptive websites, emails, or messages to steal sensitive login credentials. *DDoS* attacks aim to overwhelm servers, causing service outages. *Spoofing* involves falsifying IP addresses or other data to mask the origin of malicious traffic. Lastly, ransomware attacks are particularly damaging, as they encrypt systems or data, demanding payment for their release. Recognizing these diverse attack vectors allows for the development of targeted AI-powered defense mechanisms [1].

Understanding the diverse characteristics and significant consequences of cyberattacks – ranging from economic losses to national security threats – is crucial for assessing risks and developing effective defense strategies. Artificial Intelligence (AI) is revolutionizing cybersecurity against complex threats by enhancing security measures through continuous learning and adaptation in tools like firewalls and antivirus software, excelling at phishing detection via content analysis, and assisting in comprehensive risk assessment to strengthen defenses. Utilizing techniques like machine learning for large-scale data processing and neural networks for behavioral anomaly detection, AI fundamentally changes information security approaches, making its integration vital for organizations to protect assets and data against evolving threats and build more resilient frameworks [2, 3].

Using AI in incident warning and response systems allows you to automate the collection and analysis of logs. This allows you to speed up and increase the accuracy of the response to possible threats. Thus, the introduction of AI methods and technologies not only enhances information security, but also changes the security management process, making it more predictable and effective.

The effectiveness of AI in cybersecurity can be judged by its *speed of threat detection,* as AI's real-time data analysis allows for quicker identification than conventional approaches, vital for rapid incident response. Furthermore, the *accuracy of detection* is enhanced through machine learning algorithms trained on historical data, minimizing false positives and improving overall protection. Finally, AI demonstrates superior *adaptability to new threats* by rapidly learning from current data and updating its models, offering greater flexibility compared to traditional systems needing manual updates. The analysis indicates that AI technologies can significantly bolster organizational security by providing faster, more precise, and adaptive protection. However, it is essential to recognize that AI is not a cure-all and should complement other security measures for maximum effectiveness. The capabilities and successes of neural networks are amazing, but there are a number of tasks that even AI cannot solve without problems. One of them is slow data processing and training. It would seem that AI is used precisely for fast data processing, but it is still too slow, especially when it comes to training [5, 6]. AI is also unable to integrate skills into a new context. Neural networks receive and apply knowledge in isolation, within the framework of specific tasks. They cannot flexibly integrate skills and reuse them to solve new problems in a different context [7]. Despite the potential of AI, its problems and limitations must also be taken into account to achieve more efficient work.

The future of AI in cybersecurity is poised for significant evolution, driven by several key trends. Advanced machine learning algorithms will become increasingly adept at threat detection and prevention, rapidly adapting to novel attacks. A greater emphasis will be placed on proactive defense, enabling systems to anticipate and neutralize threats before they materialize through insightful data analysis. The widespread adoption of AI will necessitate careful consideration of ethical and legal considerations, including privacy, accountability, and regulatory compliance. This expansion will also fuel a demand for specialized skills, requiring adaptations in training and development of specialists. Finally, enhanced collaboration and data sharing among organizations will provide AI systems with broader datasets for continuous learning and model refinement, ultimately bolstering collective cybersecurity defenses. The trajectory of AI in cybersecurity will be influenced by technological advancements, evolving defense strategies, and the need to address ethical and legal questions. The integration of AI will be a crucial element in combating cyber threats, providing stronger and more adaptive protection for organizations.

Conclusion. During the conducted research on the role of artificial intelligence in cybersecurity, it is clear that AI is fundamentally changing approaches to information protection, opening up new ways to detect and prevent cyberattacks. Its use allows cybersecurity systems to process enormous amounts of data at high speed. Also, AI-based systems allow identifying anomalies and potential threats that often go unnoticed. However, the introduction of artificial intelligence into cybersecurity is also not without its pitfalls. To ensure the reliability and efficiency of AI-based systems, it is extremely important to develop a comprehensive approach that will take into account all potential risks and benefits. Only under such conditions it will be possible to successfully integrate AI into cybersecurity systems.

References

1. Cyber-attack - what is it [Electronic resource]. Mode of access: https://skyeng.ru/magazine/wiki/it-industriya/chto-takoe-kiberataka/. Date of access: 12.03.2025.

2. Pacheco J. A Security Framework for Internet of Things End Nodes with Neural Networks / J. Pacheco, V.H. Benitez, J. Pan. – International Journal of Machine Learning and Computing. – 2019. – Vol. 9. – P. 381-386.

3. Whitehead D.E. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies in 2017 / D.E. Whitehead, K. Owens, D. Gammel, J. Smith // 70th Annual Conference of Protective Relay Engineers (CPRE). – Moscow: MPEI, 2017. – P. 1-8.

4. Liu H. Secure Internet of Things (IoT) Based on Smart World Critical Infrastructures: Research, Study, and Feasibility Analysis / H. Liu, Qian S. Qian, G.W. Hatcher, H. Xu, W. Liao // IEEE Standard Access. – 2019. – Vol. 7, – P. 79523-79544.

5. Tarik N. Ensuring the Security of Critical Infrastructures Based on SCADA: Challenges and Open Problems / N. Tarik, M. Asim, F.A. Khan // Procedía Computer Science. – 2019. – Vol. 55. – P. 612-617.

6. Imperfect Technology: Problems and Limitations of Neural Networks [Electronic resource]. Mode of access: https://awwwake.ru/journal/problemy-i-ogranichenija-nejrosetej. Date of access: 09.03.2025.

7. Cyberattacks: Growing threats, awareness strategies and effective defense measures. [Electronic resource]. Mode of access: https://apni.ru/article/11342-kiberataki-rastushie-ugrozy-strategii-povysheniya-osvedomlyonnosti-i-effektivnye-mery-zashity. Date of access: 15.03.2025.