UDC004.056

Daulietova H. A.
Chopliak V. V.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERATTACKS AND CYBER DEFENSE

Vinnytsia National Technical University

Анотація
У роботі розглянуто роль штучного інтелекту в сучасній кібербезпеці. Проаналізовано як можливості його використання для захисту інформаційних систем, так і ризики застосування зловмисниками. Визначено основні напрями розвитку технологій штучного інтелекту у сфері кіберзагроз.
Ключові слова: штучний інтелект, кібербезпека, кібератаки, машинне навчання, захист інформації.

Abstract
The paper examines the role of artificial intelligence in modern cybersecurity. It analyzes both the possibilities of its use to protect information systems and the risks of its use by attackers. It identifies the main directions of development of artificial intelligence technologies in the field of cyber threats.
Keywords: artificial intelligence, cybersecurity, cyberattacks, machine learning, information security

Introduction

The rapid evolution of digital technologies has significantly increased the complexity and frequency of cyber threats. Artificial intelligence (AI) has become a crucial tool in the field of cybersecurity, offering advanced capabilities for both defense mechanisms and offensive cyber operations [1, 3].

Research results

On the defensive side, AI technologies, particularly machine learning algorithms, are widely used to detect anomalies in network traffic and identify potential threats in real time [1]. These systems are capable of processing vast amounts of structured and unstructured data, recognizing hidden patterns, and adapting to new types of cyber threats. In addition, AI-based security solutions can automate incident response, reduce human error, and significantly increase the speed and accuracy of threat detection, thereby enhancing the overall resilience of information systems.

However, cybercriminals also leverage AI to improve the efficiency and sophistication of their attacks. For instance, AI can be used to generate highly convincing phishing emails that mimic legitimate communication, automate password-cracking processes through intelligent guessing techniques, and create deepfake content for identity fraud and social manipulation [3]. Moreover, attackers may use AI to bypass traditional security systems by continuously adapting their strategies in response to defensive measures.

The dual-use nature of artificial intelligence makes it both a powerful defensive tool and a significant potential threat. As AI technologies continue to evolve, it becomes increasingly important to develop robust cybersecurity strategies, implement ethical guidelines, and enhance regulatory frameworks in order to mitigate risks associated with their misuse and ensure a secure digital environment.

Conclusion

Artificial intelligence plays a transformative role in modern cybersecurity. While it significantly enhances the ability to detect and prevent cyber threats, it also introduces new challenges due to its potential misuse by attackers. Therefore, balancing innovation and security remains a key priority for future research.

REFERENCES

1. Djenna, A., & Erradi, M. (2023). *Artificial Intelligence for Cybersecurity: A Review of Applications and Challenges*. International Journal of Computer Science and Network Security. Vol. 23.

2. ENISA (European Union Agency for Cybersecurity). (2024). *Adversarial Machine Learning and Cybersecurity Threats*. Technical Report. URL https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

3. Brundage, M., et al. (2022). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute. URL: https://arxiv.org/pdf/1802.07228.

4. Sachaniuk-Kavets'ka, N. V., & Nykyporets, S. S. (2026). LLM-based automation for translating mathematical formulae and symbols: Challenges and perspectives for technical communication. *Scientific Innovations and Advanced Technologies. Series "Education/Pedagogy"*, 3(55), 660-677. https://doi.org/10.52058/2786-5274-2026-3(55)-660-677.

5. Kravchenko, K., Ketsyk-Zinchenko, U., Suduk, I., Nykyporets, S., & Cherednychenko, V. (2025). Effectiveness of online platforms in developing language skills of higher education students. *Revista Eduweb*, 19(3), 303-314. https://doi.org/10.46502/issn.1856-7576/2025.19.03.19.

Даулєтова Ганна Асланбєківна – студентка групи 1БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: anna123dauletova@gmail.com

Науковий керівник: ***Чопляк Вікторія Володимирівна*** – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: nikavnuchkova@gmail.com.

Daulietova Hanna Aslanbekivna – student, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: anna123dauletova@gmail.com.

Scientific Supervisor: ***Chopliak Victoriia Volodymyrivna*** – teacher of English, Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: nikavnuchkova@gmail.com.