

УДК 004.056

Polina Kharina¹, Nataliia Zhukova²

¹ student of group CST-224 NU “Zaporizhzhia Polytechnic”

² PhD (Philology), Associate Professor NU “Zaporizhzhia Polytechnic”

INTEGRATION OF GENERATIVE AI INTO EDUCATION CYBERSECURITY

Artificial intelligence (AI) is key in educational cybersecurity, helping protect data, prevent cyberattacks, and educate students on advanced defense techniques. AI for educational institutions can automate threat analysis, identify anomalies in network traffic, and simulate real-world cyberattacks to train students.

Microsoft emphasizes the importance of security and AI management and suggests implementing the Zero Trust model and Microsoft Defender solutions to protect data. Organizations should consider the risks associated with data breaches and automated attacks and introduce strict rules for using AI [1].

There is also the threat of AI-generated cyberattacks, such as phishing campaigns and deepfakes, which require strict regulatory measures and monitoring. Access control systems, automated defense mechanisms, and rapid incident response strategies must be implemented in the educational environment.

In addition, a focus on cybersecurity in distance and hybrid learning is important [2]. AI solutions can detect fraudulent activity, prevent unauthorized access, and protect learning platforms from attack. Implementing AI can reduce staff workloads, increase threat detection rates, and strengthen the protection of educational ecosystems.

Furthermore, AI-driven predictive analytics can help educational institutions proactively identify network vulnerabilities before exploiting them. AI-powered security tools can analyze user behavior, detect anomalies, and alert administrators in real time, minimizing security risks [3]. Institutions like the University of South Florida have begun investing in AI and cybersecurity education to train future professionals in advanced digital defense strategies [4]. Additionally, AI can personalize cybersecurity training, enabling students to engage with simulated attacks tailored to their learning levels.

Another emerging application of AI in educational cybersecurity is using AI-powered chatbots and virtual assistants to support security awareness and response [5]. These tools can provide students and faculty instant guidance on

cybersecurity best practices, detect phishing attempts in emails, and assist in reporting suspicious activities. Some universities are also exploring AI-driven automated penetration testing [6], where AI continuously scans institutional networks for vulnerabilities, simulating hacker behavior to improve defenses. By integrating these technologies, educational institutions can create a more resilient security infrastructure while fostering a culture of cybersecurity awareness.

However, integrating AI into education cybersecurity requires a responsible approach. Educational institutions must develop clear policies on the use of AI, conduct training for staff and students, and combine automated technology with expert analysis. Only an integrated approach will ensure strong data protection and effective training for cybersecurity professionals.

REFERENCES

1. Get ready for AI: How education institutions can secure and govern AI [Electronic resource]. – Access mode: <https://www.microsoft.com/en-us/education/blog/2025/01/get-ready-for-ai-how-education-institutions-can-secure-and-govern-ai/> (accessed: 2025.03.04). – Title from the monitor.
2. Masson K. Safeguarding the Virtual Classroom: AI-Enhanced Cybersecurity in Remote and Hybrid Education [Electronic resource] / K. Masson. – Access mode: <https://elearningindustry.com/safeguarding-the-virtual-classroom-ai-enhanced-cybersecurity-in-remote-and-hybrid-education/> (accessed: 2025.03.04). – Title from the monitor.
3. Cybersecurity Recommendations for Experimenting with AI Tools in Higher Education [Electronic resource]. – Access mode: <https://collegiseducation.com/insights/technology-management/cybersecurity-and-ai-tools-in-higher-education/> (accessed: 2025.03.04). – Title from the monitor.
4. University of South Florida Gets Investment in AI and Cybersecurity Education [Electronic resource]. – Access mode: https://www.wsj.com/articles/university-of-south-florida-gets-40-million-to-start-cyber-and-ai-college-2a257e9a?utm_source/ (accessed: 2025.03.04). – Title from the monitor.
5. AI-Powered Chatbots [Electronic resource]. – Access mode: https://files.eric.ed.gov/fulltext/EJ1338316.pdf?utm_source/ (accessed: 2025.03.04). – Title from the monitor.
6. Automated Penetration Testing [Electronic resource]. – Access mode: https://imagine.jhu.edu/classes/leveraging-ai-for-penetration-testing/?utm_source/ (accessed: 2025.03.04). – Title from the monitor.