

УДК 811.111.004.02

Oleksandr Lyuty¹, Yuliya Bykova²

¹ student of group CS-814 NU “Zaporizhzhia Polytechnic”

² senior teacher NU “Zaporizhzhia Polytechnic”

AI AS A PROTECTION AND THREAT

Artificial intelligence (AI) is one of the modern tools nowadays.

Although it is a recent technology, it brings further improvement in the way cybersecurity is developing to detect threats and respond to them. It

provides faster, more effective security solutions by using machine learning algorithms that analyze huge datasets, detect different anomalies, and automate security measures. With constant improvements being done to AI-based security systems such as Microsoft Defender and Darktrace, prevention of cyberattacks will require just a bit of human intervention. Additionally, attack prevention is possible because of help of AI through spotting unusual behavior and all sorts of possible threats in banking and financial transactions.

On the other hand, AI may cause harm to users if it will be used by hackers. They use AI-powered attacks, including phishing scams, deepfake spoofs, and AI-based malware that can bypass traditional security detections. With generative AI, attackers create fake content that looks like real, making cyber threats enormously difficult and more challenging to catch. These challenges show the need for reliable AI management and ethical standards to prevent exploit.

The future of AI in cybersecurity at the same time is promising and difficult. As it constantly improves, AI will play an important role in real-time threat responses, generate new ways to close security holes, and create new encryption methods. To prevent AI-related risks, it is critical to maintain ethical standards for AI and ensure human supervision. It is also essential for permanently enhancing international cybersecurity frameworks and investing in AI-based protection methods to ensure the safety of digital areas against newly emerging threats.