UDC 004.8:004.056

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ETHICAL HACKING

Sorokin K.D.

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

Malikova I.G. – Senior Lecturer at the Department of Foreign Languages

Annotation. The growth of cyber threats requires more effective cybersecurity approaches. Ethical hacking (penetration testing), is used to identify vulnerabilities in information systems before they are exploited by attackers. Artificial intelligence technologies are increasingly applied in cybersecurity practices. This article analyzes the role of AI in ethical hacking, its application in penetration testing, and the advantages and limitations of its use.

Keywords: Artificial intelligence, ethical hacking, cybersecurity, penetration testing, machine learning.

***Introduction*.** The proliferation of digital services and online infrastructures creates new challenges for information security. Organizations are increasingly dependent on complex networks, distributed applications, and cloud platforms, which often pose additional security risks. As a result, identifying weaknesses in these environments has become an important task for cybersecurity professionals.

Penetration testing plays an important role in protecting information systems. During this process, security experts simulate the methods used by attackers to identify weaknesses before they can be exploited [2, 3]. However, manual testing is often time-consuming and requires extensive knowledge. Thanks to the latest technological advances, intelligent analytical tools have emerged that can process large amounts of security-related data. These tools help specialists identify suspicious patterns, analyze network behavior, and predict potential vulnerabilities. Consequently, modern cybersecurity strategies increasingly include automated analytical methods to improve the effectiveness of security testing [1].

Modern organizations must constantly assess their security level, due to new vulnerabilities appearing as technology develops and the interconnection of systems increases. The integration of intelligent technologies into cybersecurity processes has also increased the ability of organizations to respond faster and more effectively to emerging threats [1]. Automated security platforms are capable of processing logs, network packets, and system events in real time, which significantly improves threat detection efficiency and allows security teams to focus on analyzing the most important issues. Large corporate infrastructures, cloud environments, and Internet of Things systems generate huge amounts of security data, making manual analysis impractical and emphasizing the need for intelligent data-driven approaches. In practice, these technologies are used to automatically scan vulnerabilities, analyze network traffic in real time, and detect anomalies in mission-critical systems. They can also help in compliance monitoring by ensuring that the organization's security practices comply with regulatory requirements and internal policies [1].

Main part. Advanced computing techniques support various stages of security assessment. One key stage is information gathering, where analysts collect data about the environment. Automated algorithms process publicly available information, network metadata, and system configurations to identify potential entry points [3].

Another important application is identifying vulnerabilities. Data-driven models, trained on historical incidents, recognize patterns related to known vulnerabilities. These models help detect configuration errors, outdated software components, or suspicious network behavior.

Intelligent technologies also contribute to modeling attack scenarios. By analyzing system architecture and data paths, automated tools simulate intrusion strategies [4]. Automation reduces repetitive work, such as system scanning, log processing, and traffic analysis, letting experts focus on decision-making. The overall structure of the penetration testing process, including the stages where such simulations may occur, is shown in Figure 1.The penetration testing process typically includes several sequential stages from information gathering and vulnerability analysis to attack simulation.

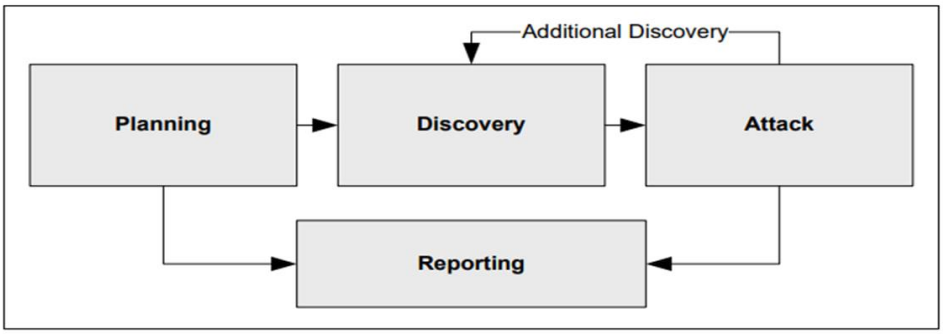

Figure 1 – Penetration testing process scheme

The integration of analytical technologies offers several advantages.

Firstly, automated systems speed up the assessment process by analyzing large amounts of data quickly [1].

Secondly, data-driven models improve risk prioritization. Instead of analyzing each problem, these systems assess the likelihood and potential impact, allowing professionals to focus on the most important vulnerabilities [5].

Scalability is another advantage, as automated analysis is more efficient than manual approaches, especially in environments with thousands of interconnected devices and services.

Finally, intelligent technologies enable continuous monitoring, increasing the ability to detect new threats [5].

Despite the advantages of automated tools, there are limitations.

One issue is the potential misuse of these technologies. The same capabilities that help professionals can also be used by attackers to automate cyber attacks [5].

Another concern is accuracy and reliability. Analytical systems depend on training data, which may be incomplete, leading to false alarms or missed vulnerabilities. Cybersecurity also requires context and creative problem-solving, which automated tools can't fully replicate. Therefore, intelligent technologies should be considered as supplemental tools, not replacements for specialists.

Conclusion. Modern cybersecurity environments require more advanced and adaptive methods for identifying system vulnerabilities. The integration of artificial intelligence technologies significantly enhances the effectiveness of ethical hacking by automating data analysis, supporting vulnerability detection, and enabling the simulation of potential attack scenarios. AI-based tools allow cybersecurity professionals to process large volumes of security data more efficiently and improve the prioritization of detected risks. At the same time, the use of artificial intelligence in cybersecurity introduces new challenges related to reliability, transparency of analytical models, and the potential misuse of these technologies by malicious actors. Therefore, artificial intelligence should be considered as a complementary tool that supports the work of cybersecurity specialists rather than replacing human expertise.

References

1. International Business Machines Corporation. AI in Cybersecurity Report [Electronic resource]. Mode of access: https://www.ibm.com/think/topics/ai-security. Date of access: 20.02.2026.

2. Engebretson P. The Basics of Hacking and Penetration Testing. Amsterdam: Syngress, 2013 [Electronic resource]. Mode of access: https://share.google/7J2aSY3gyuBm2s2rJ. Date of access: 21.02.2026.

3. National Institute of Standards and Technology. Guide to Penetration Testing // NIST Special Publication 800-115 [Electronic resource]. Mode of access: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. Date of access: 01.03.2026.

4. Artificial Intelligence–Based Ethical Hacking for Health Information Systems: Simulation Study [Electronic resource]. Mode of access: https://www.jmir.org/2023/1/e41748/. Date of access: 21.02.2026.

5. Zaheer F. Ethical Hacking with AI: Predicting and Preventing Cyber Attacks in Real-Time [Electronic resource]. Mode of access: https://www.researchgate.net/profile/Faisal-Zaheer/publication/389647956_Ethical_Hacking_with_AI_Predicting_and_Preventing_Cyber_Attacks_in_Real-Time/links/67cb0681cc055043ce6f28df/Ethical-Hacking-with-AI-Predicting-and-Preventing-Cyber-Attacks-in-Real-Time.pdf. Date of access: 21.02.2026.