UDC 004.8:004.056.53

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Kaplunova A. A. Lobatskaya E. S.

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

Perevyshko A. I. – Senior Lecturer at the Department of Foreign Languages

Annotation. This article provides a general overview of the use of artificial intelligence in cybersecurity. AI can have different applications in the field of security. In the future, new technologies created using artificial intelligence will be described, which are likely to have an impact on the development of cybersecurity systems.

Keywords. cybersecurity, artificial intelligence, machine learning, RNN, CNN, data protection, advantages.

***Introduction*.** Artificial intelligence is used in many areas of life. Thanks to the introduction of machine learning in AI, it can be configured to search for ideas offline, organize company data, and constantly check for threats and viruses in huge databases, thereby ensuring round-the-clock data protection. The development of AI has made it possible to develop voice assistants that recognize face and fingerprint scanners, as well as systems to prevent fraud on the Internet. Thanks to this, the development of cybersecurity and the design of new AI-based security systems are now coming to the fore in the world of modern technology.

Artificial intelligence in cybersecurity uses self-learning algorithms that aim to identify and analyze behavioral patterns to detect threats and respond to them in real time. AI can automate repetitive tasks by detecting viruses, malware, and spyware in large amounts of data, thereby making security systems even more active.

Main part. Many types of artificial intelligence are used in cybersecurity, but Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are considered the most common. Initially, CNN was created for image analysis, but later better applications were found in data analysis systems. CNNs use a method called convolution, which involves applying multiple filters to the input data to identify specific features or patterns. This process allows you to thoroughly examine the input data, recognizing signs of malicious data and file behavior. They are also good at detecting phishing pages, as a web page can be converted into an image, and CNN can quickly determine whether this page is real or not. The strength of these networks is the parallel processing of large amounts of data, which allows you to quickly transfer information and react to a detected threat.

Recurrent neural networks (RNNs) are designed to process sequential data where the order of the elements matters. RNNs have an “internal memory” that allows them to store the previous elements of the sequence when processing the current element, which allows them to work well with large texts and data series. They can identify similar behaviors and trends in databases, helping to detect anomalies and third-party intrusion. CNN's ability to process consistent data allows them to recognize long-term dependencies, contributing to early detection of cyber attacks and proactive threat removal [1].

The most common use of AI is to detect of network attacks, including DDoS (distributed denial of service). The systems check basic network characteristics such as the structure of IP addresses, packet numbers and counts, session duration, and frequency of access server failures. If the number of similar requests from different locations increases dramatically on the same server, the system mistakes this behavior for a DDoS attack and sends a warning. AI models don't just compare network performance; they study the past data about the network and users, the time and how long the work was performed with the data. This reduces the number of false alarms and makes threat detection more accurate.

The second key use of artificial intelligence in cybersecurity is the detection of malicious software. AI models analyze file structure, document loading and closing behavior, and network

activity. If the security system notices deviations in the program's behavior, such as changing system files, creating hidden directories and processes, or connecting to unverified sources, the model classifies it as viral and malicious. Similarly, AI detects phishing emails: the model analyzes the text of the message, verifies the authenticity of links and visual elements. If hidden links to a domain with an abnormal structure and characteristic fraudulent patterns are detected, the system automatically blocks such messages and emails [2].

The integration of artificial intelligence (AI) technologies into cybersecurity systems represents a significant advancement in the protection of digital infrastructures. Traditional cybersecurity approaches were primarily based on signature-based detection methods, where incoming data was compared with a database of previously identified threats. If a match was detected, the system generated an alert and initiated appropriate countermeasures. However, due to the rapid evolution of information technologies and the constant emergence of new types of cyber threats, this method has become less effective. The main advantages of using AI are:

1 One of the primary advantages of AI in cybersecurity is its proactive capability. Unlike conventional systems that react only to known threats, AI-based solutions can analyze patterns of behavior and detect anomalies that may indicate previously unknown attacks. Machine learning algorithms are capable of processing extremely large volumes of data within a short period of time, identifying hidden correlations and unusual activities, such as abnormal login attempts or deviations from typical user behavior.AI-Driven Virtual Production, AI is used to automate and improve game development, in areas such as animation, character management, visualisation and rendering.

2 Another important benefit is improved vulnerability management. AI systems can continuously monitor networks and analyze large datasets to detect irregularities that may signal potential weaknesses. This significantly reduces the time between the appearance of a threat and its detection, thereby minimizing the exposure window and lowering overall risk.

3 AI expands the scope of cybersecurity coverage. Advanced algorithms are capable of handling multiple processes simultaneously, which enhances network visibility and improves the identification of hidden threats. The use of machine learning and deep learning models increases the accuracy of threat detection compared to traditional rule-based systems [3].

The integration of artificial intelligence into cybersecurity represents a fundamental transformation in the approach to digital protection. AI not only enhances traditional security mechanisms but also introduces proactive, adaptive, and predictive capabilities that are essential in the modern threat landscape.

Conclusion. AI systems are able to detect new and previously unknown threats, analyze vast volumes of structured and unstructured data, and generate actionable threat intelligence in real time. The ability of AI to identify emerging malware, distinguish between legitimate and malicious automated traffic.

The automation of routine processes and large-scale data analysis increases efficiency, reduces response time to incidents, and lowers overall operational costs. The scalability of AI-powered solutions enables organizations of different sizes to expand their cybersecurity capabilities without proportional increases in human or technical resources

Artificial intelligence serves as a cornerstone of modern cybersecurity architecture, combining predictive analytics, automated defense mechanisms, advanced anomaly detection, and continuous learning to provide comprehensive and forward-looking protection against contemporary and future cyber threats.

References

1. Cybok: The Cyber Security Body Of Knowledge [Electronic resource]. – Mode of access: https://www.cybok.org/ataglance/. – Date of access: 21.03.2025.

2. Cybersecurity First Principles: A Reboot of Strategy and Tactics [Electronic resource]. – Mode of access: https://taek.edu.kg/wp-content/uploads/2025/02/Kiberbezopasnost_glavnue_princupu.pdf. – Date of access: 21.03.2025.

3. Security engineering: A Guide to Building Dependable Distributed Systems [Electronic resource]. – Mode of access: https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3.pdf. – Date of access: 21.03.2025.