# OPPORTUNITIES FOR ARTIFICIAL INTELLIGENCE IN CYBERSECURITY ISSUES

*Aysaev Iskandar Muzaffarovich*
*Head of the Advanced Training Department, "Cybersecurity Center" State Institution*
*i.aysaev@csec.uz*

**Abstract:** *This article examines the role and capabilities of artificial intelligence in ensuring cybersecurity. It is noted that the multiplicity and complexity of threats in cyberspace complicate the fight against traditional protection measures. The article provides an analysis of some problems in the field of cybersecurity, the possibilities of artificial intelligence, practical solutions and suggestions, as well as conclusions.*

**Keywords:** *cybersecurity, artificial intelligence, cyberattacks, anomaly detection, security technologies.*

**Аннотация:** *Мазкур мақолада сунъий интеллектнинг киберхавфсизликни таъминлаш масалаларидаги роли ва имкониятлари ўрганилади. Кибермакондаги таҳдидларнинг кўплиги ва мураккаблиги анъанавий ҳимоя чоралари билан курашишни мураккаблаштираётгани таъкидланади. Мақолада кибрхавфсизлик соҳасидаги баъзи муаммолар таҳлили, сунъий интеллект имкониятлари, амалий ечимлар ва таклифлар ҳамда хулосалар келтирилган.*

**Калит сўзлар:** *киберхавфсизлик, сунъий интеллект, киберҳужумлар, аномалия аниқлаш, хавфсизлик технологиялари.*

**Аннотация:** *В данной статье рассматриваются роль и возможности искусственного интеллекта в вопросах обеспечения кибербезопасности. Отмечается, что многочисленность и сложность угроз в киберпространстве усложняют борьбу с традиционными мерами защиты. В статье представлен анализ некоторых проблем в области кибербезопасности, возможности искусственного интеллекта, практические решения, предложения и выводы.*

**Ключевые слова:** *кибербезопасность, искусственный интеллект, кибератаки, обнаружение аномалий, технологии безопасности.*

Geopolitical events occurring in the world, namely the escalation of contradictions between the main "centers of power," are also causing significant changes to the platform for ensuring international information security. These circumstances emerge as a global factor influencing the adoption of organizational and technical decisions appropriate for ensuring the cybersecurity of the information infrastructure of the Republic of Uzbekistan.

Various threats and cyberattacks occurring in cyberspace limit traditional security tools in a sense, because they require the continuous processing of a massive volume of data. Judging from the report on the activities of the "Cybersecurity Center" State Institution for the past year 2025, malicious network requests directed at information systems and resources, as well as data stored and processed at critical

information infrastructure facilities in our republic, have increased significantly. Identified vulnerabilities, including "DDoS" and "Bruteforce" attacks on websites, modification of resource content, data theft, and the use of sites for "phishing" purposes, acquisition of data in databases via SQL injection, unauthorized access to files containing personal data, passwords, and plastic card data, downloading them, and performing unauthorized actions on the data can lead to serious consequences.

Due to the increase in the number of threats and their varying degrees of complexity, traditional protective measures are increasingly becoming insufficient. The expansion of digital infrastructure and transformation issues, along with the widespread implementation of cloud technologies and IoT (Internet of Things) devices, also widens the vector of cyber threats and attacks.

Priority directions are defined in the Cybersecurity Strategy of the Republic of Uzbekistan and the normative-legal document aimed at improving the system of preventing cybercrime, approved by Decree No. PF-38 of the President of the Republic of Uzbekistan dated March 10, 2026. These include strengthening national cyber stability, protecting critical information and state digital infrastructure, systematically reducing cyber risks, increasing the level of digital security for citizens, the private sector, and the state, actively combating cybercrime, developing digital innovations and artificial intelligence technologies, and strengthening technological independence in the field of cybersecurity. This indicates that strengthening cybersecurity in the country is a strategic necessity; at the same time, it requires the improvement of existing technologies and the introduction of new innovative methods. We can directly see from the document that, along with the development of artificial intelligence technologies, it is necessary to increase their role and importance in ensuring cybersecurity.

**Artificial intelligence (AI)** is a set of programs designed to reproduce human skills. Artificial intelligence is the ability to help perform tasks such as finding solutions to existing problems, planning, acquiring knowledge, and working on oneself in a timely and complete manner. In general, AI is a set of models and methods capable of drawing specific conclusions based on received data.

In the field of cybersecurity, AI allows for the automatic analysis of large volumes of data. It can find masked patterns in traffic and system behavior, detecting potential threats or vulnerabilities faster than human capabilities. For example, AI-based systems can distinguish unannounced threats (anomalies) with high accuracy through comparing incoming data in real-time and using machine learning methods. This helps to significantly reduce the number of false positives (incorrect alerts) and false negatives (situations where serious threats are missed).

Thanks to continuous learning (machine learning) capabilities, AI can learn from newly emerging threats and adapt to attack methods. AI solutions in the field of cybersecurity allow for early detection of threats, rapid response, overall improvement of the system's security status, and proactive measures to be taken. In this way, AI creates the opportunity to expand modern cybersecurity defense and attack approaches, as well as protection across network and system resources.

Another main advantage of using AI is the automation of repetitive tasks in cybersecurity. With the help of AI, security systems begin to achieve a level of self-

management, meaning if a threat is detected, the system can execute the necessary response without employee intervention. As a result, more attention is paid to analyzing complex threats and developing innovative solutions.

The following practical systems and technologies can be shown as examples of the real application of AI in cybersecurity:

***Next-Generation Firewalls (NGFW)*** *– Firewalls that control traffic flows collect information about threats using AI instead of simple rules and detect new cyber threats. They can automatically detect suspicious patterns in traffic and take appropriate blocking or warning measures.*

***Endpoint security solutions*** *– Programs that protect devices such as computers, smartphones, and IoT also use AI. They analyze programs and operating systems running on devices, identifying outdated and vulnerable elements as well as embedded malicious code. When an attack is detected, AI immediately isolates or removes the source of the threat.*

***Intrusion Detection and Prevention Systems (IDS/IPS)*** *– These tools monitor network traffic and aim to proactively detect unacceptable actions. AI increases their sensitivity, analyzes large volumes of logs, blocks unauthorized access attempts, and eliminates the attack before it can continue. Cloud infrastructure security – AI analysis power is necessary in numerous cloud services and data centers. AI collects data coming from all sources in the cloud, analyzes it, identifies vulnerabilities and potential cyberattacks, and forms a global picture of security.*

***IoT (Internet of Things) security*** *– Many industrial and household IoT devices are used in enterprises. With the help of AI, the state of each IoT device is analyzed: if a deviation from normal traffic or behavior is detected, it is compared with similar patterns in others. For example, if one device is compromised, it quickly issues an advance warning against attacks on other devices.*

***XDR and SIEM platforms – Extended Detection and Response (XDR)*** *and Security Information and Event Management (SIEM) systems collect data from various products and sources (logs, threat message databases, etc.). AI consolidates and analyzes this information, generating comprehensive analyses that take external threat factors into account, and provides a broad understanding of the enterprise or organization's security posture.*

The technologies mentioned above significantly increase the quality of the security infrastructure in enterprises and government agencies. Using them automates frequently occurring tasks in protecting systems and allows employees to focus their attention on cyber-threatening situations.

Thus, AI provides important capabilities in the fight against cyber risks. AI significantly speeds up data analysis and threat detection, which helps implement effective measures against threats that cannot be achieved using traditional methods. Practical solutions (NGFW, EDR, IDS/IPS, cloud and IoT protection, XDR/SIEM, etc.). At the same time, it is required to create defense mechanisms for AI systems themselves using reliable and data-driven approaches.

**References:**

1. A.B. Menisov. Cyber Shield. Artificial Intelligence and Cybersecurity. EDP Hub. – 2024. – 162 p.

2. S.I. Samygin, A.V. Kuznetsova. Artificial Intelligence and Information Security of Society. Monograph. – M., - 2025. – 118 p.

3. A.B. Menisov. Cyber Shield. Artificial Intelligence and Cybersecurity. – M., - 2024 – 189 p.

4. Russell, S., & Norvig, P. Artificial Intelligence: A Modern Approach. Pearson, 2021.

5. Goodfellow, I., Bengio, Y., & Courville, A. Deep Learning. MIT Press, 2016.

6. Kshetri, N. Cybersecurity and Artificial Intelligence: The Next Frontier. Springer, 2022.