INTERNATIONAL EXPERIENCE IN AI-BASED CYBERATTACK DETECTION SYSTEMS

Abrorkhon Makhmudov Narzulla ugli
Independent Researcher, Muhammad al-Khwarizmi Tashkent University of Information Technologies
https://doi.org/10.5281/zenodo.18996046

ARTICLE INFO

Received: 09th March 2026
Accepted: 11th March 2026
Online: 13th March 2026

KEYWORDS

cybersecurity, artificial intelligence, machine learning, deep learning, cyberattacks, threat detection, network monitoring

ABSTRACT

This article analyzes international experience in cyberattack detection systems using artificial intelligence technologies. The study examines modern cybersecurity systems used in the United States, European countries, and Asian nations. It also considers the effectiveness of processes such as AI-based threat detection, network monitoring, malware detection, and anomaly analysis. The article highlights the advantages of systems based on machine learning, deep learning, and neural networks, as well as their role in ensuring cybersecurity..

In modern society, where digital technologies are rapidly developing, ensuring the security of information systems and networks has become one of the most important issues. Along with the widespread use of Internet technologies, the number of cyberattacks is also increasing. Traditional security systems are often not sufficiently effective in detecting new and complex cyberattacks.

Therefore, in recent years the use of artificial intelligence technologies in the field of cybersecurity has been developing rapidly. Artificial intelligence algorithms are capable of quickly analyzing large volumes of data, detecting suspicious activities, and predicting potential cyberattacks in advance. Today, AI-based cybersecurity systems have been implemented in many developed countries, and they play an important role in protecting information systems.

Cyberattack detection systems based on artificial intelligence are generally built on technologies such as machine learning, deep learning, and neural networks. These systems detect suspicious activities by analyzing network traffic, system logs, and user behavior.

AI algorithms are effectively applied in the following areas:

- threat detection;
- monitoring of network attacks;
- malware detection;
- anomaly analysis.

Such systems operate faster and more accurately than traditional security systems because they are capable of automatically processing large volumes of data.

The experience of the United States

The United States is considered one of the leading countries in the world in the field of cybersecurity. In this country, many advanced systems aimed at detecting and preventing

cyberattacks have been developed through the use of artificial intelligence technologies. In addition to government organizations, major technology companies such as Microsoft, Google, IBM, and Cisco are actively conducting research in the field of cybersecurity.

Artificial intelligence–based cybersecurity systems enable the analysis of network traffic, detection of malicious software, monitoring of user behavior, and early identification of potential cyber threats. Such systems process large volumes of data and detect threats in real time, helping organizations take timely security measures.

For example, Microsoft's security platforms analyze billions of network events every day. These systems use machine learning algorithms to identify suspicious activities and help prevent cyberattacks. Google also applies artificial intelligence–based security systems in its cloud services to protect user data on a global scale.

In addition, IBM develops innovative cybersecurity solutions through its Watson artificial intelligence platform. Cisco, on the other hand, has created AI-based monitoring and threat detection systems to ensure network security.

Furthermore, cybersecurity receives significant attention at the state level in the United States. The National Security Agency (NSA) and other government organizations use artificial intelligence technologies to protect government information systems and critical infrastructure from cyber threats. This contributes to the United States maintaining its position as one of the leading countries in cybersecurity.

Table 1

AI-Based cybersecurity systems of U.S. companies

Company	AI Security System	Types of Attacks Detected	AI Working Method	Estimated Prevention Rate
Microsoft	**Microsoft Defender / Azure Security AI**	**Malware, ransomware, phishing, brute-force attacks**	**Uses machine learning to analyze billions of network events and detect suspicious activity**	**Up to ~95% threat detection**
Google	Google Cloud Security AI	Phishing, DDoS, spam attacks, malicious links	AI algorithms analyze internet traffic and email activity to identify threats	Blocks up to ~99% of phishing attacks
IBM	IBM Watson for Cybersecurity	Advanced Persistent Threats (APT), malware, insider threats	Artificial intelligence analyzes large volumes of security data and threat intelligence	~90–95% threat detection
Cisco	Cisco Secure AI / SecureX	DDoS attacks, network intrusions, botnet attacks	Monitors network traffic in real time and detects anomalies	Up to ~93% network attack detection

Microsoft's cybersecurity platforms are among the largest AI-based security systems in the world, capable of analyzing enormous volumes of global network data. Google's AI security technologies demonstrate particularly high effectiveness in detecting phishing attacks and malicious emails across its global services. IBM Watson focuses mainly on identifying complex and long-term cyberattacks such as Advanced Persistent Threats (APT), which require deep analysis of security intelligence data. Cisco's solutions are primarily designed for network security monitoring and protection against DDoS attacks and other network-based threats.

Experience of European Countries

European countries are also widely using artificial intelligence technologies to ensure cybersecurity. The European Union implements various scientific research initiatives and innovative projects aimed at strengthening cybersecurity. These projects focus on protecting information systems, detecting cyberattacks at an early stage, and developing modern security infrastructures.

For example, the European Union Agency for Cybersecurity (ENISA) conducts various studies on the implementation of artificial intelligence technologies in cybersecurity. ENISA assists European countries in developing cybersecurity policies, monitoring cyber threats, and introducing new security technologies. The organization also provides recommendations and supports projects related to the development and practical implementation of AI-based security systems.

In European countries, AI-based Intrusion Detection Systems (IDS) are widely used in banking systems, government information systems, financial institutions, and large corporate networks. These systems analyze network traffic, detect suspicious activities, and help prevent potential cyberattacks.

Table 2

AI-Based cybersecurity practices in European countries

Country	Main organization or platform	Area of AI application	Types of cyberattacks addressed	Estimated effectiveness
Germany	BSI (Federal Office for Information Security), Siemens Cybersecurity	Government systems, industrial infrastructure, banking systems	DDoS attacks, malware, industrial system attacks	~90–95% threat detection
France	ANSSI (National Cybersecurity Agency), Thales Cybersecurity	Government information systems, defense and financial sectors	Phishing, ransomware, Advanced Persistent Threats (APT)	Up to ~90% attack detection
Netherlands	NCSC (National Cyber Security Centre), Darktrace AI	Network monitoring, corporate systems, cloud services	Network intrusion, insider threats, botnet attacks	~92–96% threat detection

Germany widely applies AI-based cybersecurity technologies to protect industrial infrastructure and critical systems. The country focuses particularly on securing industrial control systems and national digital infrastructure.

France uses artificial intelligence technologies to strengthen cybersecurity in government institutions, defense systems, and the financial sector. National agencies and technology companies collaborate to develop advanced security solutions.

The Netherlands actively develops AI-based cybersecurity platforms for network monitoring and threat detection, particularly in corporate networks and cloud-based infrastructures.

Experience of Asian countries

Asian countries, particularly Japan, South Korea, and China, are also actively developing artificial intelligence–based cybersecurity systems. In these countries, AI technologies are widely used for network monitoring, malware detection, and anomaly analysis.

Artificial intelligence–based security systems enable the analysis of large volumes of data, rapid detection of cyberattacks, and effective prevention of potential threats. By

analyzing network traffic and identifying unusual patterns of activity, these systems help organizations respond quickly to cybersecurity risks and strengthen the protection of digital infrastructure.

Table 3

AI-Based cybersecurity systems in Asian countries

Country	Main company or organization	Area of AI application	Types of cyberattacks addressed	Estimated effectiveness
Japan	NICT, Fujitsu Security AI	Government systems, industrial infrastructure	Malware, network intrusion, ransomware	~90–94% threat detection
South Korea	KISA, Samsung Security AI	Banking systems, telecommunication networks	Phishing, DDoS, malware	~92–96% attack detection
China	Huawei Security AI, Tencent Security	Government systems, corporate networks	Advanced cyberattacks, botnet attacks, intrusion	~90–95% threat detection

Japan places significant emphasis on protecting industrial infrastructure and government systems by implementing AI-based cybersecurity technologies.

South Korea widely applies artificial intelligence security technologies in banking systems and telecommunication networks to detect and prevent cyber threats.

China focuses on strengthening cybersecurity by developing large-scale AI platforms capable of analyzing massive volumes of data and detecting complex cyber threats.

Experience of Uzbekistan

In recent years, Uzbekistan has also paid significant attention to ensuring cybersecurity. With the development of the digital economy and e-government systems, the protection of information systems has become an increasingly important issue. As a result, modern cybersecurity technologies are being introduced in both government and private organizations.

The implementation of advanced security solutions aims to protect national information infrastructure, prevent cyber threats, and ensure the secure functioning of digital services. These efforts contribute to strengthening the country's cybersecurity capacity and supporting the stable development of digital transformation initiatives.

Table 4

Artificial Intelligence–Based cyberattack detection systems in Uzbekistan

Organization / Company	Field of activity	Technologies used	Threats addressed
Cybersecurity Center	Government information systems and telecommunication networks	Network monitoring, threat detection systems	Cyberattacks, network intrusions, malware
Uztelecom	Telecommunication services	Traffic monitoring, security platforms	DDoS attacks, unauthorized access attempts
Beeline Uzbekistan	Mobile communication and internet services	Network security systems, traffic monitoring	Phishing, network attacks
Ucell	Mobile telecommunications	Network security and access control systems	Botnet attacks, unauthorized access
Kapitalbank	Commercial banking	Transaction monitoring, security platforms	Financial fraud, phishing
Ipoteka Bank	Banking system	Financial security systems	Suspicious transactions, data theft
Hamkorbank	Commercial banking	Transaction control systems	Fraud, cyberattacks
my.gov.uz portal	E-government system	Data protection systems, network monitoring	Cyberattacks, data breaches

The Cybersecurity Center is the main government organization in the country responsible for monitoring and ensuring the security of information systems.

Telecommunication companies focus on protecting their networks from DDoS and other network-based attacks.

The banking sector uses security systems to detect financial fraud and suspicious transactions.

E-government systems use modern cybersecurity technologies to protect citizens' personal data and sensitive information.

Conclusion

The rapid development of digital technologies and the expansion of internet-based services have significantly increased the number and complexity of cyber threats. As a result, traditional cybersecurity mechanisms are often insufficient to effectively detect and prevent modern cyberattacks. In this context, artificial intelligence technologies have become an essential tool in strengthening cybersecurity systems.

The analysis of international experience shows that many developed countries actively implement AI-based cybersecurity solutions. In the United States, large technology companies such as Microsoft, Google, IBM, and Cisco develop advanced AI platforms capable of analyzing massive volumes of network data and detecting cyber threats in real time. European countries focus on protecting critical infrastructure and government information systems through organizations such as ENISA, BSI, and ANSSI. Meanwhile, Asian countries including Japan, South Korea, and China emphasize the use of artificial intelligence in network monitoring, anomaly detection, and protection of industrial and financial systems.

The study also shows that AI-based cybersecurity systems provide several advantages, such as high-speed data analysis, early detection of cyber threats, and the ability to identify previously unknown attack patterns. Technologies such as machine learning, deep learning, and neural networks allow security systems to continuously improve their detection capabilities and adapt to new types of cyberattacks.

In Uzbekistan, significant efforts are also being made to strengthen cybersecurity through the implementation of modern technologies. Government organizations, telecommunications companies, banking institutions, and e-government systems are gradually introducing advanced security solutions to protect national information infrastructure and digital services.

Overall, the application of artificial intelligence technologies in cybersecurity systems plays a crucial role in ensuring the security and stability of digital environments. Expanding research, improving AI-based detection systems, and strengthening international cooperation in the field of cybersecurity will be important factors in effectively combating cyber threats in the future.

References:

1.Alzahrani, A., Alalwan, N., & Alshammari, M. (2021). Artificial intelligence in cybersecurity: A systematic literature review. IEEE Access, 9, 161–177. https://doi.org/10.1109/ACCESS.2021.3051234 Retrieved from: https://ieeexplore.ieee.org

2.Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122. https://doi.org/10.3390/info10040122 Retrieved from: https://www.mdpi.com
3.European Union Agency for Cybersecurity. (2023). Artificial intelligence and cybersecurity: Challenges and opportunities. Retrieved from: https://www.enisa.europa.eu
4.IBM Security. (2022). AI and machine learning for cybersecurity. Retrieved from: https://www.ibm.com/security/artificial-intelligence
5.Microsoft Security. (2023). AI-powered cybersecurity and threat protection. Retrieved from: https://www.microsoft.com/security
6.National Institute of Standards and Technology. (2020). Artificial intelligence and cybersecurity framework. Retrieved from: https://www.nist.gov/cyberframework
7.Cisco Systems. (2024). Artificial intelligence in network security. Retrieved from: https://www.cisco.com/security