ISSN: 2224-6878 | Pakistan Volume 6, No. 6.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

METHODS FOR DETECTION OF CYBER ATTACKS BASED ON ARTIFICIAL INTELLIGENCE

Aslonov Kodir Ziyodullayevich
Asia International University

Abstract.
This article analyzes methods for detecting cyberattacks using artificial intelligence technologies. As a result of the rapid development of modern information and communication technologies, cybersecurity issues are gaining relevance. Traditional security tools cannot always provide sufficient efficiency in detecting increasingly complex cyberattacks. Therefore, the use of artificial intelligence technologies based on machine learning and deep learning algorithms has become one of the important directions. The study covers the principles of operation, advantages and practical application of artificial intelligence-based cyberattack detection systems.

Keywords: artificial intelligence, cybersecurity, cyberattack, machine learning, deep learning, neural networks, network security, IDS systems.

Introduction. As a result of the development of the digital economy and the widespread introduction of information systems into all sectors, the issue of ensuring cybersecurity is gaining strategic importance. Today, the widespread use of information systems in the activities of state organizations, commercial enterprises and educational institutions makes them vulnerable to various cyber threats. The use of malicious programs, denial-of-service attacks, phishing and other methods aimed at illegally obtaining information by cybercriminals is increasing. Timely detection and prevention of these threats are one of the important tasks of information security.

In recent years, artificial intelligence technologies have been effectively used in various fields. In particular, the use of artificial intelligence in cybersecurity systems allows for the analysis of large volumes of data, the identification of hidden patterns, and the automatic detection of cyberattacks. In this regard, the study of approaches based on artificial intelligence is of scientific and practical importance.

Literature review on the topic . The use of artificial intelligence in detecting cyberattacks has been studied by many foreign and domestic scientists. The scientific literature has widely covered the effectiveness of machine learning algorithms in analyzing network traffic and detecting anomalous activity. According to the results of the research, algorithms such as Random Forest, Support Vector Machine, Decision Tree and K-Nearest Neighbors show high accuracy in classifying cyberattacks.

With the development of deep learning technologies, neural network-based models have also begun to be actively used in the field of cybersecurity. In particular, the use of Convolutional Neural Network and Long Short-Term Memory models allows you to identify connections in complex network traffic. Scientific studies have shown that these approaches are more effective than traditional methods in detecting new and previously unknown threats.

Research methodology. With the development of digital technologies, the number of threats to information systems and computer networks is also increasing. Therefore, the development and implementation of effective methods for protecting information resources has become an urgent issue. Cybersecurity methods are aimed at ensuring the confidentiality, integrity and availability of information. These methods include technical, software and organizational measures. The main goal of cybersecurity is to protect information systems from various threats and attacks.

ISSN: 2224-6878 | Pakistan Volume 6, No. 6.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

One of the most common ways to ensure cybersecurity is the use of authentication mechanisms. Authentication refers to the process of verifying the authenticity of a user. Today, along with simple passwords, two-factor authentication and biometric identification methods are also used. These approaches significantly reduce the likelihood of unauthorized access to systems. The use of strong authentication mechanisms helps prevent cybercriminals from hacking into accounts. Therefore, improving authentication tools in modern information systems is of great importance.

Data encryption is one of the most important methods of cybersecurity protection. During the encryption process, data is transformed using special algorithms and made into a form that can only be read by authorized users. This method ensures the confidentiality of data during transmission or storage. Modern cryptographic algorithms reduce the risk of illegal acquisition and use of information. Encryption technologies are widely used in e-commerce, banking systems, and government information resources. As a result, it is possible to ensure a high level of data security.

Firewalls or firewall technologies are also one of the important tools of cybersecurity. A firewall monitors incoming and outgoing network traffic and blocks dangerous connections. This technology plays an important role in protecting the internal network from external threats. Firewalls work based on predefined security rules. They are able to detect and filter malicious traffic. Thus, the level of protection of systems from illegal access is increased.

Intrusion detection systems are of particular importance in ensuring cybersecurity. Such systems constantly monitor network activity and identify suspicious situations. Intrusion detection systems use signature-based and anomaly-based methods. Signature-based systems are designed to detect known threats. Anomaly-based systems analyze deviations from normal activity. This allows them to detect new and unknown attacks.

The use of artificial intelligence technologies is one of the modern methods of cybersecurity. Machine learning algorithms allow you to identify threats by analyzing large amounts of data. Artificial intelligence systems are highly effective in identifying hidden patterns in network traffic. They are distinguished by their real-time operation and rapid detection of attacks. These technologies are creating new opportunities in the field of cybersecurity. At the same time, they also increase the effectiveness of traditional protection tools.

Regularly updating software is also an important cybersecurity measure. Vulnerabilities in software are often exploited by cybercriminals to launch attacks. Updates released by developers help to address these vulnerabilities. Timely updates to operating systems and applications significantly increase system security. Updates also provide additional protection against new threats. Therefore, it is essential to maintain a regular update policy in information systems.

In ensuring cybersecurity, the knowledge and skills of users in information security are also of great importance. Many cyberattacks occur as a result of errors related to the human factor. Phishing emails, malicious links and social engineering methods take advantage of the carelessness of users. Therefore, organizations should regularly organize information security training. Improving the security culture of users is an important component of cybersecurity. As a result, the overall level of protection of information systems increases significantly.

Using artificial intelligence technologies to detect cyberattacks is a complex process that involves data collection, processing, feature extraction, and model training. First, data on network traffic, system logs, and security events is collected. In the next step, the data is cleaned and prepared for analysis. After that, important features are extracted and fed into a machine learning model.

Artificial intelligence algorithms classify cyberattacks by identifying differences between normal and anomalous activity. Once the model is trained, it is able to identify threats based on new data. This process is significant because it can be done in real time.

ISSN: 2224-6878 | Pakistan Volume 6, No. 6.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

Results and Discussion . Research shows that artificial intelligence-based systems are more effective than traditional signature-based security tools. Such systems can process large amounts of data in a short time and detect anomalies in network activity. Using machine learning algorithms, the accuracy of detecting malicious activity is significantly increased and the number of false positives is reduced.

Another important advantage of artificial intelligence technologies is the ability to detect previously unseen attacks. Traditional systems rely mainly on known attack signatures, while artificial intelligence can also detect new threats based on behavioral analysis. At the same time, the implementation of such systems requires a large amount of training data and high computing resources. These factors are considered some of the limitations of artificial intelligence technologies.

Conclusion. The introduction of artificial intelligence technologies into the field of cybersecurity is increasing the effectiveness of detecting and combating cyberattacks. Machine learning and deep learning algorithms are creating the opportunity to deeply analyze network activity, identify anomalous situations, and predict new types of threats. The results of the study showed that artificial intelligence-based systems are an important tool in protecting modern information systems. In the future, the creation of self-learning and adaptive security systems will remain one of the priority tasks of scientific research in this area.

References

1. Stallings W. Network Security Essentials: Applications and Standards. - Pearson Education, 2020.
2. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016.
3. Bishop CM Pattern Recognition and Machine Learning. – Springer, 2018.
4. Sarker IH Machine Learning: Algorithms, Real-World Applications and Research Directions // SN Computer Science. - 2021. - Vol. 2. – No. 3.
5. Sommer R., Paxson W. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. - 2010.
6. Ahmed M., Mahmood AN, Hu J. A Survey of Network Anomaly Detection Techniques // Journal of Network and Computer Applications. - 2016. - Vol. 60. – P. 19–31.
7. Shone N., Ngoc TN, Phai VD, Shi Q. A Deep Learning Approach to Network Intrusion Detection // IEEE Transactions on Emerging Topics in Computational Intelligence. - 2018. - Vol. 2. – No. 1.
8. Jalolov, T. S. (2024). ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ С ИСПОЛЬЗОВАНИЕМ ФАЛЬШИВЫЙ ИНФОРМАЦИЯ ОПРЕДЕЛИТЬ МЕТОДЫ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 53-59.
9. Sadriddinovich, J. T. (2024). BASICS OF PSYCHOLOGICAL SERVICE. PSIXOLOGIYA VA SOTSIOLOGIYA ILMIY JURNALI, 2(4), 61-67.
10. Jalolov, T. S. (2024). PYTHONNING MATEMATIK KUTUBXONALARINI O'RGANISH: KENG QAMROVLI QO'LLANMA. BIOLOGIYA VA KIMYO FANLARI ILMIY JURNALI, 2(5), 71-77.
11. Jalolov, T. S. (2024). РАЗВИТИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В САМОДВИЖАЩИХСЯ РОБОТАХ. Methods of applying innovative and digital technologies in the educational system, 1(2), 1-7.
12. Jalolov, T. S. (2024). ЭКОЛОГИЧЕСКИЙ СИСТЕМЫ ИСКУССТВЕННЫЙ В МОНИТОРИНГЕ ИНТЕЛЛЕКТ ТЕХНОЛОГИЙ ПРИЛОЖЕНИЕ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 86-92.

ISSN: 2224-6878 | Pakistan Volume 6, No. 6.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

13. Jalolov, T. S. (2024). MATNNI QAYTA ISHLASH ORQALI TIL O ‘RGATISH ILOVALARINI RIVOJLANTIRISH. Modern digital technologies in education: problems and prospects, 1(2), 103-108.
14. Jalolov, T. S. (2024). ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭКОНОМИЧЕСКОМ МОДЕЛИРОВАНИИ. Methods of applying innovative and digital technologies in the educational system, 1(2), 27-32.
15. Jalolov, T. S. (2024). AVTONOM ROBOTLARDA SUN'IY INTELLEKT TEXNOLOGIYALARINI RIVOJLANTIRISH. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 56-61.
16. Jalolov, T. S. (2024). СОЗДАНИЕ ДИАГНОСТИЧЕСКИХ СИСТЕМ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМЕ ЗДРАВООХРАНЕНИЯ. Methods of applying innovative and digital technologies in the educational system, 1(2), 14-20.
17. Jalolov, T. S. (2024). KIBERMUHOFAZANING TA'LIM JARAYONIDAGI O'RNI. PEDAGOGIK TADQIQOTLAR JURNALI, 2(1), 189-192.