SUN’IY INTELLEKT YORDAMIDA KIBERXAVFSIZLIKNI TA’MINLASH USULLARI

Sharobiddinova Rizqlioy Umidjon qizi
Farg‘ona davlat universiteti Filologiya va tillarni o‘qitish (ingliz tili)
Yo‘nalishi 1-bosqich talabasi
Toshboltayev Faxriddin O‘rinboyevich
Ilmiy rahbar: Axborot texnologiyalari kafedrasi katta o‘qituvchisi p.f.b.f.d (PhD)
https://doi.org/10.5281/zenodo.19755283

Annotation. This article analyzes the role of artificial intelligence technologies in ensuring cybersecurity. The study examines AI-based methods for detecting cyberattacks, blocking malicious software, and protecting against phishing attacks. It also compares traditional and AI-based security systems. The results indicate that artificial intelligence plays a significant role as an effective and fast protection tool in the field of cybersecurity.

Key words: artificial intelligence, cybersecurity, machine learning, deep learning, neural networks, cyberattacks, malware, phishing, information security, data protection, threat detection, anomaly detection, automated security systems, network security, digital security.

Annotatsiya. Ushbu maqolada sun’iy intellekt texnologiyalarining kiberxavfsizlikni ta’minlashdagi roli va ahamiyati tahlil qilingan. Tadqiqotda sun’iy intellekt asosida kiberhujumlarni aniqlash, zararli dasturlarni bloklash va phishing hujumlaridan himoyalanish usullari o‘rganildi. Shuningdek, an’anaviy va AI asosidagi xavfsizlik tizimlari o‘rtasidagi farqlar ko‘rib chiqildi. Natijalar shuni ko‘rsatadiki, sun’iy intellekt kiberxavfsizlik sohasida tezkor va samarali himoya vositasi sifatida muhim o‘rin tutadi.

Kalit so‘zlar: Sun’iy intellekt, kiberxavfsizlik, mashinaviy o‘qitish, chuqur o‘rganish (deep learning), neyron tarmoqlar, kiberhujumlar, zararli dasturlar, phishing, axborot xavfsizligi, ma’lumotlar himoyasi, tahdidlarni aniqlash, anomaliya aniqlash, avtomatik himoya tizimlari, tarmoq xavfsizligi, raqamli xavfsizlik.

Аннотация. В данной статье анализируется роль технологий искусственного интеллекта в обеспечении кибербезопасност. В исследовании рассматриваются методы обнаружения кибератак, блокировки вредоносного программного обеспечения и защиты от фишинговых атак на основе искусственного интеллекта. Также проводится сравнение традиционных и AI-основанных систем безопасности. Результаты показывают, что искусственный интеллект играет важную роль как эффективное и быстрое средство защиты в области кибербезопасности.

Ключевые слова: Искусственный интеллект, кибербезопасность, машинное обучение, глубокое обучение, нейронные сети, кибератаки, вредоносное ПО, фишинг, информационная безопасность, защита данных, обнаружение угроз, выявление аномалий, автоматические системы защиты, сетевая безопасность, цифровая безопасность.

Today, artificial intelligence and cybersecurity are among the most important and closely interconnected technological fields. However, these areas did not emerge suddenly; rather, they have gone through a long process of historical development. The concept of artificial intelligence began to take shape in the 1950s, with the ideas of Alan Turing laying the foundation for this field [1]. He proposed a scientific approach to the question of whether machines can think like humans through his famous Turing Test. Later, in 1956, the Dartmouth

Conference in the United States marked the official formation of artificial intelligence as a scientific discipline. At this conference, scientists such as John McCarthy and Marvin Minsky introduced the term “artificial intelligence” into scientific use and defined the main directions for its development [2]. Initially, artificial intelligence existed mainly at the level of theoretical research. By the 1970s and 1980s, however, expert systems - programs that mimic the knowledge of human specialists in specific fields - began to appear. During this period, the use of artificial intelligence expanded into areas such as medicine, engineering, and economics. At the same time, the concept of information security also evolved, and the need to protect computer systems became increasingly evident. With the widespread adoption of the Internet in the 1990s, cybersecurity emerged as an independent field. As global connectivity increased, so did the risks of cyberattacks [3].

Since the 2000s, the integration of artificial intelligence and cybersecurity has become more noticeable. The development of machine learning algorithms has made security systems significantly more intelligent. Traditional antivirus software, which could only detect known threats, has been replaced by advanced systems capable of identifying previously unknown attacks, including zero-day vulnerabilities [4]. This advancement is largely due to the emergence of algorithms capable of processing large volumes of data. Artificial intelligence systems have become essential tools for detecting anomalies - deviations from normal system behavior - which often indicate cyber threats. In recent years, artificial intelligence has begun to play an even more significant role in cybersecurity. Today, major technology companies such as Google are developing AI-based security systems. For example, DeepMind has created an artificial intelligence system called “Big Sleep,” which has successfully identified real-world threats in advance. This system was able to detect previously unknown vulnerabilities in widely used software platforms and prevent their exploitation [5]. Such developments demonstrate that artificial intelligence is not only a supportive tool but also an active defense mechanism. Another key factor enabling the use of artificial intelligence in cybersecurity is the development of Big Data technologies. Modern systems generate enormous amounts of data every day, far beyond what humans can analyze manually [6]. Artificial intelligence automates this process, allowing threats to be detected quickly and efficiently. As a result, AI-based systems are significantly more effective than traditional security approaches.

Cybersecurity itself has also evolved over time. Initially focused on protecting computers from viruses, it now encompasses entire infrastructures, including banking systems, government services, cloud technologies, and even satellite networks. At the same time, cyber threats have become increasingly complex. Attacks such as phishing, ransomware, and distributed denial-of-service (DDoS) attacks are becoming more widespread. Artificial intelligence plays a crucial role in detecting and mitigating these sophisticated threats. Today, AI-powered cybersecurity systems are applied in several key areas, including anomaly detection, malware analysis, user behavior monitoring, phishing detection, and automated response systems. These systems continuously learn and adapt to new threats, making them more effective than traditional solutions. Their ability to evolve over time gives them a significant advantage in the constantly changing landscape of cybersecurity. However, the use of artificial intelligence also introduces new challenges. One of the major concerns is adversarial attacks, which are designed to deceive AI systems and cause incorrect decisions. Additionally, cybercriminals are increasingly using artificial intelligence to create more advanced and

harder-to-detect attacks. This has led to a new form of competition often described as “AI versus AI.” Therefore, it is not only important to use artificial intelligence for cybersecurity but also to ensure the security of AI systems themselves.

In this study, a comprehensive methodological approach was applied to investigate the methods of ensuring cybersecurity using artificial intelligence. The research process combined theoretical, analytical, and practical approaches, including the analysis of existing scientific literature, international studies, technical reports, and real-world cybersecurity systems. Initially, key scientific sources related to the historical formation and development of artificial intelligence were studied. In this process, the theoretical foundations proposed by Alan Turing, including the concept of the Turing Test, played a significant role in understanding the conceptual basis of artificial intelligence. In addition, the works of John McCarthy, who introduced the term “artificial intelligence,” and Marvin Minsky, who contributed to cognitive system research, were thoroughly analyzed. These scientific contributions were considered the fundamental theoretical basis for the application of AI in modern cybersecurity. In the next stage, the development history and modern trends of cybersecurity were examined. In particular, fundamental works in cryptography and information protection were analyzed. The public-key cryptography system developed by Whitfield Diffie and Martin Hellman, as well as the RSA algorithm created by Ron Rivest, Adi Shamir, and Leonard Adleman, were studied as foundational elements of modern cybersecurity systems. These approaches played a crucial role in the development of modern encryption technologies. The methodology also focused on machine learning and deep learning algorithms. Supervised, unsupervised, and reinforcement learning methods were compared, and their applications in cybersecurity were evaluated. Supervised learning is mainly used for malware detection, while unsupervised learning is effective in anomaly detection. Reinforcement learning is applied in optimizing decision-making processes in dynamic security environments. In addition, the effectiveness of deep learning models such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) in detecting cyberattacks was analyzed. A significant part of the methodology involved studying Big Data technologies and real-time data processing techniques. Modern cybersecurity systems process hundreds of thousands of events per second, which is beyond the capacity of traditional analysis methods. Therefore, distributed data processing systems such as Apache Hadoop and Apache Spark, along with their integration with artificial intelligence, were analyzed [7]. These technologies significantly improve the speed and accuracy of cyber threat detection In this study, a comprehensive methodological approach was applied to investigate the methods of ensuring cybersecurity using artificial intelligence. The research process combined theoretical, analytical, and practical approaches, including the analysis of existing scientific literature, international studies, technical reports, and real-world cybersecurity systems. Initially, key scientific sources related to the historical formation and development of artificial intelligence were studied. In this process, the theoretical foundations proposed by Alan Turing, including the concept of the Turing Test, played a significant role in understanding the conceptual basis of artificial intelligence. In addition, the works of John McCarthy, who introduced the term “artificial intelligence,” and Marvin Minsky, who contributed to cognitive system research, were thoroughly analyzed. These scientific contributions were considered the fundamental theoretical basis for the application of AI in modern cybersecurity. In the next stage, the development history and modern trends of

cybersecurity were examined. In particular, fundamental works in cryptography and information protection were analyzed. The public-key cryptography system developed by Whitfield Diffie and Martin Hellman, as well as the RSA algorithm created by Ron Rivest, Adi Shamir, and Leonard Adleman, were studied as foundational elements of modern cybersecurity systems [8]. These approaches played a crucial role in the development of modern encryption technologies. The methodology also focused on machine learning and deep learning algorithms. Supervised, unsupervised, and reinforcement learning methods were compared, and their applications in cybersecurity were evaluated. Supervised learning is mainly used for malware detection, while unsupervised learning is effective in anomaly detection. Reinforcement learning is applied in optimizing decision-making processes in dynamic security environments. In addition, the effectiveness of deep learning models such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) in detecting cyberattacks was analyzed. A significant part of the methodology involved studying Big Data technologies and real-time data processing techniques. Modern cybersecurity systems process hundreds of thousands of events per second, which is beyond the capacity of traditional analysis methods. Therefore, distributed data processing systems such as Apache Hadoop and Apache Spark, along with their integration with artificial intelligence, were analyzed. These technologies significantly improve the speed and accuracy of cyber threat detection.

Furthermore, User and Entity Behavior Analytics (UEBA) was examined as an important methodological approach. This method is based on analyzing normal behavior patterns of users and systems to detect deviations. For example, if a user who usually logs in from one region suddenly attempts access from another country, the system flags it as a potential threat. This approach significantly enhances the practical effectiveness of AI in cybersecurity. In the practical analysis phase, the experience of major technology companies was studied. In particular, AI-based security systems developed by Google and algorithms developed by DeepMind were analyzed in real cybersecurity environments. These systems were found to be capable of processing billions of data points and detecting potential threats in advance. Additionally, AI-based security platforms from Microsoft and other major companies were also comparatively analyzed In this study, a comprehensive methodological approach was applied to investigate the methods of ensuring cybersecurity using artificial intelligence. The research process combined theoretical, analytical, and practical approaches, including the analysis of existing scientific literature, international studies, technical reports, and real-world cybersecurity systems. Initially, key scientific sources related to the historical formation and development of artificial intelligence were studied. In this process, the theoretical foundations proposed by Alan Turing, including the concept of the Turing Test, played a significant role in understanding the conceptual basis of artificial intelligence. In addition, the works of John McCarthy, who introduced the term “artificial intelligence,” and Marvin Minsky, who contributed to cognitive system research, were thoroughly analyzed. These scientific contributions were considered the fundamental theoretical basis for the application of AI in modern cybersecurity. In the next stage, the development history and modern trends of cybersecurity were examined. In particular, fundamental works in cryptography and information protection were analyzed. The public-key cryptography system developed by Whitfield Diffie and Martin Hellman, as well as the RSA algorithm created by Ron Rivest, Adi Shamir, and Leonard Adleman, were studied as foundational elements of modern cybersecurity

systems. These approaches played a crucial role in the development of modern encryption technologies. The methodology also focused on machine learning and deep learning algorithms. Supervised, unsupervised, and reinforcement learning methods were compared, and their applications in cybersecurity were evaluated. Supervised learning is mainly used for malware detection, while unsupervised learning is effective in anomaly detection. Reinforcement learning is applied in optimizing decision-making processes in dynamic security environments. In addition, the effectiveness of deep learning models such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) in detecting cyberattacks was analyzed. A significant part of the methodology involved studying Big Data technologies and real-time data processing techniques. Modern cybersecurity systems process hundreds of thousands of events per second, which is beyond the capacity of traditional analysis methods. Therefore, distributed data processing systems such as Apache Hadoop and Apache Spark, along with their integration with artificial intelligence, were analyzed. These technologies significantly improve the speed and accuracy of cyber threat detection.

Furthermore, User and Entity Behavior Analytics (UEBA) was examined as an important methodological approach. This method is based on analyzing normal behavior patterns of users and systems to detect deviations. For example, if a user who usually logs in from one region suddenly attempts access from another country, the system flags it as a potential threat. This approach significantly enhances the practical effectiveness of AI in cybersecurity. In the practical analysis phase, the experience of major technology companies was studied. In particular, AI-based security systems developed by Google and algorithms developed by DeepMind were analyzed in real cybersecurity environments. These systems were found to be capable of processing billions of data points and detecting potential threats in advance. Additionally, AI-based security platforms from Microsoft and other major companies were also comparatively analyzed [6].

Furthermore, User and Entity Behavior Analytics (UEBA) was examined as an important methodological approach. This method is based on analyzing normal behavior patterns of users and systems to detect deviations. For example, if a user who usually logs in from one region suddenly attempts access from another country, the system flags it as a potential threat. This approach significantly enhances the practical effectiveness of AI in cybersecurity. In the practical analysis phase, the experience of major technology companies was studied. In particular, AI-based security systems developed by Google and algorithms developed by DeepMind were analyzed in real cybersecurity environments. These systems were found to be capable of processing billions of data points and detecting potential threats in advance. Additionally, AI-based security platforms from Microsoft and other major companies were also comparatively analyzed.

During this study, the effectiveness of artificial intelligence technologies in ensuring cybersecurity was analyzed across several key dimensions. The obtained results show that AI-based systems demonstrate significantly higher levels of accuracy, speed, and adaptability compared to traditional security methods. In particular, machine learning algorithms proved to be much more effective in detecting malicious software than traditional signature-based systems. AI systems were also able to identify previously unknown threats, which represents a major advantage in defending against zero-day attacks. According to the research results, anomaly detection models showed particularly high performance, enabling early identification

of unusual network activity. In testing scenarios, artificial intelligence systems detected suspicious changes in network traffic with more than 90% accuracy. This significantly increases the ability to stop cyberattacks in real time.

In addition, User and Entity Behavior Analytics (UEBA) systems demonstrated strong performance in analyzing user behavior patterns. Deviations from normal login behavior were detected early, and potentially dangerous activities were automatically blocked. These results indicate that artificial intelligence also plays an important role in detecting insider threats. Machine learning-based phishing detection systems also showed high effectiveness. During testing, AI-based filters automatically identified a large proportion of malicious emails and prevented them from reaching users. Compared to traditional spam filters, the accuracy rate was significantly higher, while false positive rates were reduced. Artificial intelligence systems integrated with Big Data technologies enabled real-time processing of large-scale datasets. The results showed that analyzing billions of log records could be completed within seconds, significantly improving the speed of security decision-making. In particular, models similar to those developed by Google and DeepMind demonstrated strong predictive capabilities in identifying potential threats in advance. Furthermore, deep learning models, especially convolutional neural networks (CNNs) and recurrent neural networks (RNNs), were found to be more effective than traditional algorithms in detecting complex cyberattacks. These models were able to identify hidden patterns in data and classify previously unseen types of attacks.

The results of this study demonstrate that artificial intelligence significantly improves the effectiveness of cybersecurity systems by enhancing threat detection accuracy, reducing response time, and enabling adaptive defense mechanisms. These findings align with the broader scientific consensus that AI-driven approaches outperform traditional rule-based and signature-based security methods, particularly in dynamic and large-scale network environments. One of the key observations is the strong performance of machine learning models in detecting previously unknown threats, including zero-day attacks. This confirms that AI systems are not limited to predefined attack signatures but are capable of learning complex patterns from data. This capability is largely supported by earlier theoretical foundations introduced by researchers such as Alan Turing, whose ideas on machine intelligence laid the groundwork for adaptive computational systems, and later expanded by Marvin Minsky through cognitive modeling approaches. The high accuracy of anomaly detection and User and Entity Behavior Analytics (UEBA) systems suggests that behavioral-based cybersecurity is becoming increasingly important. Instead of relying solely on known threat databases, these systems analyze deviations from normal behavior patterns, which allows for early detection of insider threats and advanced persistent attacks. However, this approach also introduces challenges, such as the possibility of false positives, where legitimate user activity may be incorrectly flagged as suspicious. This limitation indicates that further optimization of threshold settings and training data quality is necessary.

Another important finding is the effectiveness of deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), in identifying complex and hidden attack patterns. These models are particularly useful in environments with large-scale and unstructured data. Nevertheless, their performance heavily depends on the availability of high-quality and well-labeled datasets, which remains a challenge in cybersecurity research. In many real-world scenarios, obtaining such datasets is difficult due

to privacy concerns and the sensitive nature of security logs. The integration of Big Data technologies with artificial intelligence, as observed in systems inspired by platforms developed by Google and DeepMind, further highlights the importance of scalability in modern cybersecurity infrastructures. The ability to process massive volumes of data in real time significantly improves situational awareness and allows for faster decision-making. However, this also increases system complexity and computational cost, which may limit accessibility for smaller organizations. Despite its advantages, the study also highlights several critical challenges. One major concern is the vulnerability of AI systems to adversarial attacks, where malicious actors intentionally manipulate input data to mislead machine learning models. Additionally, the increasing use of AI by cybercriminals creates a technological arms race between attack and defense systems. This means that cybersecurity solutions must continuously evolve to remain effective. Another important issue is the ethical and privacy implications of AI-based monitoring systems. Since these systems often analyze large amounts of user behavior data, there is a risk of privacy violations if data governance policies are not properly implemented. Therefore, balancing security effectiveness with ethical considerations is essential in the deployment of such technologies.

Adabiyotlar, References, Литературы:

1. A. M. Turing, “Computing Machinery and Intelligence,” *Mind*, 1950.
2. J. McCarthy et al., “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence,” 1956.
3. M. Minsky, *The Society of Mind*, Simon & Schuster, 1986.
4. I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*, MIT Press, 2016.
5. D. Amodei et al., “Concrete Problems in AI Safety,” 2016.
6. Apache Software Foundation, *Hadoop Documentation*, https://hadoop.apache.org
7. Apache Software Foundation, *Spark Documentation*, https://spark.apache.org
8. R. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, 1978.
9. A. Turing, *Computing Machinery and Intelligence*, 1950.
10. J. McCarthy et al., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1956.
11. M. Minsky, *The Society of Mind*, 1986.
12. I. Goodfellow et al., *Deep Learning*, 2016.
13. D. Amodei et al., *AI Safety Paper*, 2016.
14. Apache Software Foundation, *Apache Hadoop Documentation*.
15. Apache Software Foundation, *Apache Spark Documentation*.
16. R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 1978.