SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

ADVANTAGES AND RISKS OF ARTIFICIAL INTELLIGENCE-BASED CYBERSECURITY SYSTEMS

Курбонова Фируза Зариповна

Doctor of Philosophy (PhD) in Technical Sciences, Associate Professor,

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan,

Tashkent, Uzbekistan

https://doi.org/10.5281/zenodo.20959898

Abstract. This article analyzes the advantages and risks of artificial intelligence (AI)-based cybersecurity systems in the modern digital environment. The rapid development of information technologies, cloud computing, and Internet of Things (IoT) devices has significantly increased the number and complexity of cyber threats. Traditional security mechanisms based mainly on predefined rules and signatures are often insufficient to detect advanced attacks. AI technologies, including machine learning, deep learning, and behavioral analysis, provide new opportunities for real-time threat detection, automated response, vulnerability assessment, and prediction of cyber incidents.

At the same time, the implementation of AI in cybersecurity introduces several challenges, including dependence on high-quality data, false positive and false negative results, high computational requirements, privacy issues, and adversarial attacks against AI models. The article discusses the benefits and limitations of AI-based cybersecurity solutions and highlights the importance of combining artificial intelligence with human expertise to build secure digital infrastructures.

Keywords: artificial intelligence, cybersecurity, machine learning, deep learning, cyber threats, intrusion detection, information security.

Annotatsiya. Ushbu maqolada zamonaviy raqamli muhitda sun’iy intellekt (AI) asosidagi kiberxavfsizlik tizimlarining afzalliklari va xavflari tahlil qilinadi. Axborot texnologiyalari, bulutli xizmatlar va IoT qurilmalarining rivojlanishi natijasida kiberhujumlar soni va murakkabligi oshib bormoqda. An’anaviy himoya vositalari ko‘plab yangi tahdidlarni aniqlashda yetarli bo‘lmay qolmoqda.

Sun’iy intellekt, mashinali o‘qitish va chuqur o‘rganish texnologiyalari yordamida tahdidlarni real vaqt rejimida aniqlash, hujumlarga avtomatik javob berish va kiberxavflarni oldindan baholash imkoniyati paydo bo‘lmoqda.

Shu bilan birga, AI tizimlarining ma’lumotlarga bog‘liqligi, noto‘g‘ri aniqlash holatlari, yuqori hisoblash resurslariga ehtiyoj va AI modellariga qarshi hujumlar kabi muammolar mavjud.

Kalit so‘zlar: sun’iy intellekt, kiberxavfsizlik, mashinali o‘qitish, axborot xavfsizligi, kiberhujum.

Аннотация. В данной статье рассматриваются преимущества и риски систем кибербезопасности на основе искусственного интеллекта. Развитие цифровых технологий приводит к увеличению количества сложных киберугроз, что требует применения интеллектуальных методов защиты.

Анализируются возможности искусственного интеллекта в области обнаружения угроз, автоматизации процессов защиты, анализа поведения пользователей и прогнозирования атак.

Также рассматриваются основные проблемы использования AI, включая зависимость от качества данных, ошибки классификации, высокие вычислительные требования и уязвимость моделей перед adversarial-атаками.

Ключевые слова: искусственный интеллект, кибербезопасность, машинное обучение, кибератаки, защита информации.

Introduction

In the modern digital era, cybersecurity has become one of the most important areas of information technology. The rapid growth of the Internet, cloud computing, mobile technologies, and Internet of Things (IoT) devices has created new opportunities but also increased the number of cyber threats.

Cybercriminals use advanced techniques such as malware, phishing, ransomware, botnets, and advanced persistent threats (APT) to compromise information systems.

Traditional cybersecurity methods based on predefined rules and signatures are often unable to detect new and rapidly changing attacks. Therefore, artificial intelligence has become an important technology for improving modern cybersecurity.

AI-based systems can analyze large amounts of information, detect abnormal activities, and automatically respond to potential threats.

1. The Role of Artificial Intelligence in Cybersecurity

Artificial intelligence refers to computer systems that can perform tasks requiring human intelligence, such as learning, decision-making, and pattern recognition. In cybersecurity, AI is used in:

- network monitoring;
- malware detection;
- intrusion detection;
- user behavior analysis;
- vulnerability assessment;
- automated incident response.

Machine learning algorithms allow security systems to learn from previous attacks and recognize new threat patterns.

Deep learning methods help analyze complex data and detect hidden cyber risks.

2. Advantages of AI-Based Cybersecurity Systems

2.1 Real-Time Threat Detection and Monitoring

One of the main advantages of AI-based cybersecurity is the ability to detect threats in real time. Modern systems generate huge volumes of:

- network traffic;
- security logs;
- user activity data;
- application events.

AI algorithms analyze this information continuously and identify suspicious behavior. AI can detect:

- unusual login attempts;
- abnormal network communication;
- unauthorized access;
- suspicious file activities.

Early detection helps organizations reduce damage caused by cyberattacks.

2.2 Detection of Unknown Cyber Threats

Traditional antivirus systems depend mainly on known signatures. However, attackers constantly create new malware variants.

AI uses behavioral analysis instead of only searching for known patterns.

AI can detect:

- zero-day attacks;
- unknown malware;
- polymorphic viruses;
- advanced persistent threats.

This allows cybersecurity systems to identify threats that have never been seen before.

2.3 Automated Incident Response

AI can automatically react to detected threats. Possible actions include:

- blocking malicious connections;
- isolating infected devices;
- stopping suspicious processes;
- updating security rules.

Automation improves response speed and reduces the workload of cybersecurity specialists.

2.4 User Behavior Analysis

AI can analyze normal user activity and detect unusual behavior.

Examples:

- suspicious login locations;
- abnormal file access;
- unusual data transfers.

This helps prevent:

- stolen account usage;
- insider attacks;
- unauthorized access.

2.5 Vulnerability Detection

AI helps organizations identify security weaknesses before attackers exploit them. AI-based systems can:

- scan networks;
- detect vulnerabilities;
- evaluate risks;
- recommend security improvements.

This creates a proactive cybersecurity approach.

3. AI Techniques Used in Cybersecurity

3.1 Machine Learning

Machine Learning allows systems to learn from data. Main approaches:

Supervised Learning

Uses labeled data to classify activities.

Applications:

- malware detection;
- spam filtering;
- phishing detection.

Unsupervised Learning

Finds hidden patterns without predefined labels.

Used for:

- anomaly detection;
- unknown attack identification.

Reinforcement Learning

Allows systems to improve through experience.

Used for:

- adaptive defense;
- automated security decisions.

3.2 Deep Learning

Deep Learning uses artificial neural networks.

CNN (Convolutional Neural Networks)

Used for:

- malware classification;
- pattern recognition.

RNN and LSTM

Used for:

- network traffic analysis;
- time-based behavior detection.

Autoencoders

Used for:

- anomaly detection;
- intrusion detection.

Deep learning improves the ability to identify complex cyber threats.

4. Risks and Challenges of AI-Based Cybersecurity

4.1 Dependence on Data Quality

AI models require large and reliable datasets.

Poor data quality can cause:

- incorrect decisions;
- missed attacks;
- reduced accuracy.

Creating high-quality cybersecurity datasets remains a major challenge.

4.2 False Positive and False Negative Results

AI systems may produce incorrect results.

False Positive occurs when safe activity is identified as dangerous.
False Negative occurs when a real attack is not detected.
Both situations reduce security effectiveness.

4.3 High Computational Requirements

Advanced AI models require:

- powerful processors;
- large storage;
- specialized infrastructure.

This can increase implementation costs.

4.4 Adversarial Attacks Against AI

Attackers can manipulate AI systems by creating specially designed inputs.
Examples:

- modifying malware;
- changing traffic patterns;
- misleading AI models.

Therefore, AI systems themselves must be protected.

4.5 Privacy and Ethical Issues

AI cybersecurity systems analyze large amounts of data.
This creates risks related to:

- privacy;
- personal information protection;
- unauthorized monitoring.

Organizations must use AI responsibly.

4.6 AI Usage by Cybercriminals

AI can also be used for attacks.
Attackers may use AI to:

- create phishing messages;
- automate attacks;
- develop intelligent malware.

Therefore, cybersecurity must continuously evolve.

Conclusion

Artificial intelligence has become an important technology for modern cybersecurity. AI-based systems provide many advantages, including real-time monitoring, unknown threat detection, automated response, and improved vulnerability management.

However, AI also creates new challenges, such as dependence on data quality, false results, computational costs, and adversarial attacks.

The future of cybersecurity depends on the effective combination of artificial intelligence, strong security standards, and professional human expertise. AI will become an essential tool for protecting digital infrastructure against increasingly complex cyber threats.

REFERENCES

1. Russell S., Norvig P. **Artificial Intelligence: A Modern Approach.** Pearson, 2021.
2. Goodfellow I., Bengio Y., Courville A. **Deep Learning.** MIT Press, 2016.
3. National Institute of Standards and Technology (NIST). **Artificial Intelligence Risk Management Framework (AI RMF 1.0).** https://www.nist.gov/itl/ai-risk-management-framework
4. IEEE Access. **Machine Learning and Deep Learning Approaches for Cybersecurity: A Survey.** IEEE, 2022.
5. Computers & Security. **A Survey on Machine Learning Techniques for Cyber Security.** Elsevier, 2021.
6. European Union Agency for Cybersecurity (ENISA). **Artificial Intelligence and Cybersecurity.** https://www.enisa.europa.eu/