INTERNATIONAL JOURNAL OF POLITICAL SCIENCES AND ECONOMICS
Impact Factor (research bib) - 9,78
https://ijmri.de/index.php/ijpse , German international journals company
ISSN 2751-9708

THE ROLE OF ARTIFICIAL INTELLIGENCE AND CYBERSECURITY IN MODERN INFORMATICS

Abdullayeva Nafisa Nazirovna

Andijan State Medical Institute Academic Lyceum, Informatics Teacher

Annotation: This article analyzes the interconnection between artificial intelligence (AI) and cybersecurity in the modern development of informatics. It highlights how AI enhances the efficiency of processing large volumes of data, conducting analysis, and supporting decision-making processes. At the same time, modern cybersecurity systems built on AI are shown to outperform traditional approaches. The study employed literature review, case analysis, and examination of recent security systems. The results indicate that while AI plays a crucial role in detecting and preventing cyber threats, it also introduces new vulnerabilities that can be exploited. The authors emphasize that ethical responsibility, transparency, and strengthened human oversight are essential conditions for the sustainable development of informatics in the future.

Keywords: Informatics, artificial intelligence, cybersecurity, machine learning, threat detection, ethical responsibility.

Introduction

Informatics, as a field of study, has undergone a profound transformation with the rapid development of artificial intelligence (AI) and the increasing importance of cybersecurity. AI provides the ability to process vast amounts of data, extract meaningful patterns, and support decision-making in diverse domains, ranging from healthcare and education to finance and national security. Simultaneously, the rise of cyber threats, such as data breaches, ransomware attacks, and phishing schemes, highlights the critical need for advanced cybersecurity systems. The integration of AI into informatics brings both opportunities and challenges: while AI enhances efficiency and accuracy, it also generates new vulnerabilities that cybercriminals can exploit. Therefore, this article aims to analyze the intersection of artificial intelligence and cybersecurity within informatics, exploring their methodologies, applications, and the implications for the digital future.

Methods

This study employed a qualitative review methodology by synthesizing relevant scientific literature, case studies, and reports published between 2018 and 2024. Key themes were identified through content analysis, focusing on three areas: (1) the application of AI techniques such as machine learning, deep learning, and natural language processing within informatics; (2) the role of AI in strengthening cybersecurity measures, including anomaly detection and

intrusion prevention; and (3) the risks and ethical issues associated with deploying AI in security-sensitive environments. The analysis further compared real-world examples, such as AI-based fraud detection systems in the financial sector and cybersecurity frameworks in critical infrastructure.

Results

The findings indicate that AI has become indispensable in managing and interpreting large-scale data within informatics. Machine learning algorithms demonstrate high efficiency in predictive modeling, improving diagnostic accuracy in healthcare and optimizing logistics in business systems. In cybersecurity, AI has enabled the development of advanced threat detection systems that surpass traditional rule-based mechanisms by identifying previously unseen attack vectors. For instance, AI-powered tools can detect unusual network behaviors, thus reducing response times to potential intrusions. However, the research also revealed significant challenges. AI systems are themselves vulnerable to adversarial attacks, data poisoning, and algorithmic biases. Moreover, overreliance on automated systems without adequate human oversight may lead to ethical dilemmas and security risks.

Discussion

The integration of AI into informatics creates a dynamic environment where efficiency, accuracy, and automation are maximized. In cybersecurity, AI enhances proactive defense mechanisms, shifting the paradigm from reactive to predictive security models. However, this technological advancement requires strong ethical frameworks, transparent algorithms, and international cooperation to mitigate risks. Educational institutions should also update curricula in informatics to emphasize both AI and cybersecurity competencies, preparing future specialists to navigate the complexities of the digital age. The results suggest that while AI-driven solutions are powerful, they should complement rather than replace human expertise in cybersecurity.

Conclusion

Artificial intelligence and cybersecurity represent two fundamental pillars of modern informatics. Their interaction is both synergistic and complex: AI enhances data management and threat detection, yet it also introduces new vulnerabilities that necessitate robust security measures. To ensure sustainable progress, stakeholders must adopt a balanced approach, integrating technical innovation with ethical responsibility and continuous monitoring. The future of informatics will depend on the ability to harness AI's potential while maintaining resilient cybersecurity systems, ultimately contributing to a safer and more intelligent digital society.

References:

1. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach. Pearson.
2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
3. Symantec Cybersecurity Report (2023). Trends in Global Cybersecurity. Symantec Corporation.
4. IBM Security (2022). The Role of Artificial Intelligence in Cyber Defense. IBM Research.

5. Brundage, M., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. ArXiv preprint arXiv:1802.07228.