

ORGANIZATIONAL METHODS OF PROTECTING INFORMATION FROM ARTIFICIAL INTELLIGENCE

<https://doi.org/10.5281/zenodo.15129077>

Saidov Jasur Doniyor o'g'li

Gulistan State University, Department of Information Technologies, Doctor of Philosophy (PhD) in Pedagogical Sciences,

Asrorova Mavludaoy Umurzoq qizi

First year student of the Faculty of Information Technology and Physics and Mathematics, Gulistan State University

Abstract: *This article examines the impact of artificial intelligence technologies on information security and organizational methods for protecting information. The threats of unauthorized access to information, cybersecurity risks, and data manipulation using artificial intelligence tools are analyzed. At the same time, effective strategies for protecting information in organizations and measures to increase security are proposed.*

Keywords: *information security, artificial intelligence, cybersecurity, deepfake, phishing, Zero Trust, encryption, manipulation.*

With the development of artificial intelligence (AI) technologies, information security is facing new challenges. AI is expanding its capabilities, such as automating cyberattacks, creating fake information, and analyzing personal data, and is demanding new approaches to information protection.

Malware and automated attacks based on AI are threatening the information security of organizations. For example, attacks can be carried out by creating phishing messages that look more credible or analyzing confidential information.

Audio and video materials can be forged using deepfake technologies developed using AI. This poses a risk to organizations by spreading false information or manipulating documents.

AI makes social engineering attacks more effective by analyzing user behavior. As a result, the likelihood of obtaining confidential user information increases.

Organizations must have a strict information security policy. This policy defines who has access to information, when, and under what conditions. Organizations need to develop a clear information security policy and strictly adhere to it. It should include the following elements:

- Definition of user rights and obligations.
- Liability measures for information security violations.
- Regular training of employees on information security.
- Implementing AI-based security systems

- AI-based threat detection systems – using AI tools to detect cyberattacks in advance.
- Data encryption – using encryption algorithms to prevent unauthorized access to information.
- Network monitoring and AI tools – monitoring network traffic and identifying threats using AI.

Employee cybersecurity training

Organizational employees should be regularly trained in information security. This may include:

- Training on detecting phishing and social engineering attacks.
- Instructions on using strong passwords and authentication methods.
- Instructions on paying attention to suspicious messages and links.

AI protection measures

Zero Trust model – Any user or system should be approached based on the principle of minimal trust. Users and devices must be identified and authenticated.

- Encryption and anonymization – By encrypting data, it is possible to limit its use by third parties. In addition, anonymizing users' personal data prevents it from being analyzed by artificial intelligence.

- Monitoring and AI-based threat detection – Using artificial intelligence itself to monitor network traffic and identify threats in advance can be an effective measure.

State-level regulation – It is necessary to develop national regulatory documents and rules against the risks posed by artificial intelligence. Special information security centers should conduct constant monitoring to identify and combat attacks using artificial intelligence in advance.

Use of blockchain technologies – Decentralized and immutable blockchain technologies can play an important role in preventing information corruption. This technology can be used to verify the authenticity of data and reduce the likelihood of its manipulation.

Biometric authentication – Instead of simple passwords, it is necessary to use more reliable protection tools, such as biometric data such as eye scanners, voice or fingerprints.

Creating security systems based on artificial intelligence – It is necessary to use artificial intelligence tools to detect and eliminate artificial intelligence threats in advance. For example, it is important to create systems that predict cyberattacks and eliminate threats in real time.

- Compliance with regulations and legislation – It is necessary to implement security measures that comply with international and local legal requirements to protect information.

- Artificial intelligence against artificial intelligence – It is necessary to use artificial intelligence algorithms to strengthen protection systems. For example, security systems based on AI that predict malicious attacks in advance can be effective.

The development of artificial intelligence is creating new threats to information security. Organizations should implement security systems protected by artificial intelligence to protect information, regularly train employees, and form strong security policies. In this way, information resources can be effectively protected and modern cybersecurity threats can be countered.

REFERENCES:

1. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
2. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
3. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
4. Kissel, R. (2013). NIST Special Publication 800-88: Guidelines for Media Sanitization. National Institute of Standards and Technology.
5. Karimov I., Abduqodirov A. (2019). Axborot xavfsizligi va kriptografiya asoslari. Toshkent: Innovatsiya nashriyoti.
6. Saidov A., Ismoilov D. (2018). Kompyuter texnologiyalarida algoritmlarning qo'llanilishi. Toshkent: Universitet nashriyoti.
7. Xamidov O., Yo'ldoshev R. (2020). Axborot xavfsizligi tamoyillari. Toshkent: Fan va texnologiya.
8. Ergashev S. (2021). Sun'iy intellekt va kiberxavfsizlik. Toshkent: IT Park nashriyoti.
9. Usmonov M., Tursunov A. (2022). Sun'iy intellekt tahdidlari va ularga qarshi kurash choralari. Toshkent: Fan va innovatsiya.
10. Nematov S. (2023). Axborot xavfsizligi va sun'iy intellektga qarshi texnologiyalar. Toshkent: Ilmiy nashr.
11. O'G'Li, S. J. D., Qizi, M. M. Z., & Qizi, T. R. Z. O. (2024). AXBOROT TIZIMLARI VA ULARNING RIVOJLANISHI OMILLARI. Central Asian Journal of Multidisciplinary Research and Management Studies, 1(4), 66-69.
12. Saidov, J. D. (2021). Study of the process of database and creation in higher education. In International scientific and practice conference on "International experience in increasing the effectiveness of distance education: problems and solutions". Guliston.
13. Jasur Doniyor, O. G., Saidov, L., Allayorov, S. P., OMBORINI, S., & BAHOLASH, Y. M. Scientific progress. 2021. № 1. URL: <https://cyberleninka.ru/article/n/ma-lumotlar-omborini-yaratish-bo-yicha-kasbiy-kompetentligini-baholash-mezonlari> (дата обращения: 02.06. 2022).
14. Saidov, J., Ishchanova, I., Temirxolova, B., & Nurmuhammedova, Z. (2024). BILIMLAR BAZASINING ASOSIY XUSUSIYATLARI VA ULARGA OID LOYIHALASH. Theoretical aspects in the formation of pedagogical sciences, 3(7), 23-27.

15. Saidov, J., Nazarqulov, A., & Danaboyev, N. Z. (2024). ELEKTRON DIDAKTIK VOSITALAR YORDAMIDA BILIMLARNI SINASH MUAMMOLARI. Центральноазиатский журнал междисциплинарных исследований и исследований в области управления, 1(2), 143147.
16. Джуроев, М. Э. (2021). ЗНАЧЕНИЕ ГЕОХИМИЧЕСКИХ ПРОЦЕССОВ В ВЕРТИКАЛЬНОЙ И ГОРИЗОНТАЛЬНОЙ СВЕЗИ ПАРА
17. Sattarov, S. M., Khudaykulov, S. I., Djuraev, M. E., & Axunbabaev, M. M. (2018). DETERMINATION OF THE CONCENTRATION OF NON-CONSERVATIVE SUBSTANCES IN A MULTI-DENSITY FLOW. Bulletin of Gulistan State University, 2018(2), 7-12.
18. Djurayev, M., & Husenov, J. (2022). STUDIES IN GEOGRAPHY, CONFLICTS AND SOLUTIONS IN APPLIED GEOGRAPHY. Journal of Geography and Natural Resources, 2(01), 2428.