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

CYBERSECURITY: THE RELEVANCE OF INFORMATION PROTECTION IN A DIGITALIZED SOCIETY

Rustamjonova Mokhinur Jo‘rabek qizi

Kokand University, Andijan Branch

Faculty of Social-Humanitarian Sciences and Pedagogy

Student of Correspondence Group 24-02, Computer Engineering

Annotation: This article explores the concept of cybersecurity, its significance and role in modern society, the types of cyber threats, and the measures to prevent them. The technical, organizational, and legal aspects of cybersecurity are analyzed in detail, along with a comprehensive overview of necessary steps to ensure information security for users. Furthermore, the article highlights the importance of fostering cybersecurity awareness within the education system and emphasizes the need to promote a culture of digital safety. The content holds practical relevance for general users, specialists, and professionals in the field of education.

Keywords: Cybersecurity, information security, cyber threats, phishing, malware, information technologies, data protection, digital security, cybersecurity in education, cyber culture.

The rapid advancement of information technologies has significantly increased the integration of digital environments into human life. Sectors such as e-government, online education, digital payments, and social networks are increasingly reliant on the internet and digital tools. While these conveniences offer numerous benefits, they also introduce serious threats, with cybersecurity being one of the most critical issues in the digital era. This article provides a comprehensive overview of the essence of cybersecurity, its main types, emerging cyber threats, and methods to prevent and mitigate them. It also explores the relevance of cybersecurity within society and the education system, emphasizing both technical and legal measures needed to ensure data and system safety.

- **The Essence of Cybersecurity**

Cybersecurity encompasses the set of tools, policies, security concepts, safeguards, guidelines, risk management approaches, and technologies used to protect digital devices, networks, software, and data from digital threats[1]. It is considered an essential part of overall information security, ensuring the confidentiality, integrity, and availability of data[2]. Cybersecurity is important not only for institutions and government bodies but also for every individual user. Anyone connected to the internet is exposed to varying degrees of cyber risks.

- **Common Types of Cyber Threats**

Understanding and classifying cyber threats is a crucial first step toward achieving security. The most widespread types include:

➢ Phishing – Emails and messages that appear to be from trusted sources but are designed to trick users into disclosing personal information, such as passwords or bank details[3].

➢ Malware – Viruses, Trojans, worms, and ransomware are used to disrupt systems, steal data, or lock files and demand ransom for their release[4].

➢ Hacking – Unauthorized access to databases, website defacement, and attempts to disable government or corporate systems are common actions carried out by hackers[5].

- **Measures to Ensure Cybersecurity**

A comprehensive cybersecurity strategy involves technical, organizational, and legal measures:

- o Installing and regularly updating antivirus and anti-spyware software.
- o Using strong, regularly changed passwords on devices and platforms.
- o Updating systems and software in a timely manner.
- o Encrypting sensitive data and creating backup copies.

Awareness-raising efforts play a crucial role. Users must be informed about potential cyber threats and trained in basic information security practices. In particular, schools and universities should include cybersecurity education as part of the curriculum[6].

- **Legal and Institutional Frameworks**

Effective cybersecurity also depends on the implementation of national and international legal frameworks. In Uzbekistan, laws such as “On Informatization” and “On Personal Data” provide the legal foundation for data protection. International standards like ISO/IEC 27001:2022 outline best practices for information security management systems[7].

- **The Importance of Cybersecurity Education**

As new generations grow up immersed in digital technologies, it becomes essential to equip them with the knowledge and skills to navigate the internet safely. Teaching children the rules of safe internet use is a shared responsibility of both educational institutions and parents. Promoting digital safety culture is key to preparing a secure digital future.

Conclusion

In conclusion, cybersecurity is not solely a concern for IT professionals but a pressing issue for every internet user. Ensuring data security, protecting personal information, and acting responsibly in the digital environment are fundamental skills in today’s society. Governments, educators, and communities must work together to enhance the cybersecurity framework and culture.

References:

[1]: Ahmedov, S. (2021). Foundations of Cybersecurity and Information Protection. Tashkent: Fan Publishing. (in Uzbek)

[2]: Muhammadjonov, J. (2020). Digital Technologies and Information Security. Tashkent: TUIT Press. (in Uzbek)

[3]: Qodirov, N. (2022). "State Policy in Ensuring Information Security", Scientific Research in Uzbekistan, No.4, pp. 45–51.

[4]: Hasanova, D. (2021). "Cybersecurity: Global Threats and National Measures", Journal of World Economy and International Relations, No.3, pp. 33–39.

[5]: ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization, 2022.

[6]: National Curriculum on Cyber Hygiene in Schools. Ministry of Public Education, Uzbekistan. (internal resource)