

CYBERSECURITY AND PERSONAL DATA PROTECTION

Ikromiddinova Marhabo To'liqinjon qizi

Gulistan State Pedagogical Institute.

e-mail: marhaboikromiddinova@gmail.com

<https://doi.org/10.5281/zenodo.19798984>

Annotasiya. Ushbu maqolada raqamli muhitda shaxsiy ma'lumotlarni himoya qilishning ahamiyati zamonaviy texnologiyalar jadal rivojlanishi va internetdan foydalanishning ortib borishi sharoitida tahlil qilinadi. Unda kiberjinoyatlarning asosiy turlari, ularning kelib chiqish sabablari hamda shaxs va jamiyat uchun salbiy oqibatlarini yoritib berilgan. Xususan, ma'lumotlar sizib chiqishi, shaxsni o'g'irlash va onlayn firibgarlik kabi zamonaviy tahdidlarga alohida e'tibor qaratilgan. Shuningdek, O'zbekiston va xalqaro qonunchilik tajribasi asosida kiberxavfsizlikni ta'minlashga qaratilgan samarali huquqiy va tashkiliy choralar tahlil qilinadi. Maqolada aholi o'rtasida raqamli savodxonlikni oshirish, internetdan xavfsiz foydalanish madaniyatini shakllantirish hamda kiberxatarlarning oldini olish bo'yicha profilaktik choralarni kuchaytirish zarurligi ta'kidlangan.

CYBERSECURITY AND PERSONAL DATA PROTECTION

Abstract. This article examines the importance of protecting personal data in the digital environment in the context of rapid technological development and increasing internet usage. It analyzes the main types of cybercrimes, their causes, and their negative consequences for individuals and society. Special attention is given to modern threats such as data breaches, identity theft, and online fraud. Drawing on the experience of Uzbekistan and international legislation, the article highlights effective legal and organizational measures aimed at ensuring cybersecurity. Furthermore, it emphasizes the importance of improving digital literacy among the population, raising awareness about safe internet practices, and developing preventive strategies to minimize cyber risks.

Key words: Cybersecurity, personal data protection, digital environment, cybercrime, data breach, identity theft, online fraud, digital literacy, information security, internet safety.

КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В данной статье рассматривается важность защиты персональных данных в цифровой среде в условиях стремительного развития технологий и роста использования интернета. Анализируются основные виды киберпреступлений, их причины и негативные последствия для личности и общества. Особое внимание уделяется современным угрозам, таким как утечка данных, кража личности и онлайн-мошенничество. На основе опыта Узбекистана и международного законодательства выделяются эффективные правовые и организационные меры по обеспечению кибербезопасности. Кроме того, подчеркивается необходимость повышения цифровой грамотности населения, формирования культуры безопасного поведения в интернете и разработки профилактических мер для снижения киберрисков.

In recent years, cybersecurity and personal data protection have assumed paramount importance not only within the sphere of technology but also across broader social and economic domains. As digital technologies and internet-based services continue to expand at an unprecedented pace, ensuring their security has become a critical priority.

This article explores the significance of cybersecurity, examines key issues related to personal data protection, and highlights major developments in this field.

The early 2000s witnessed the rapid proliferation of the internet, which gave rise to a global technological revolution. However, this progress was accompanied by the emergence of new and complex threats. In 2013, classified documents disclosed by Edward Snowden revealed that the United States National Security Agency (NSA) had been engaged in extensive surveillance activities. This revelation significantly undermined public trust and intensified concerns regarding the security and privacy of personal data worldwide.

By 2017, the global spread of the WannaCry ransomware attack had compromised hundreds of thousands of computer systems and resulted in billions of dollars in economic losses.

The attack primarily targeted national healthcare systems, governmental institutions, and large corporations. This incident served as a wake-up call, prompting governments and organizations to reassess and strengthen their cybersecurity frameworks and policies.

Personal Data Protection as the Cornerstone of Security

In the contemporary digital landscape, vast amounts of personal data are continuously transmitted and processed online. On a daily basis, individuals provide sensitive information to numerous applications and websites, often without fully understanding the associated risks. The introduction of the European Union's General Data Protection Regulation (GDPR) in 2018 marked a milestone in the advancement of data protection standards. Its impact extended far beyond Europe, reshaping global approaches to data privacy and accountability. Notably, organizations are now required to ensure transparency regarding how user data is collected, stored, and processed.

In 2021, major technology companies, including Facebook, faced substantial financial penalties due to violations of data privacy regulations. These cases underscored the critical importance of robust data protection mechanisms, not only for safeguarding users but also for maintaining corporate integrity and public trust.

Advancement of Cybersecurity in Uzbekistan

Uzbekistan has likewise undertaken significant measures to enhance its cybersecurity infrastructure. In 2019, the President of the Republic of Uzbekistan approved a resolution aimed at strengthening the national information security system. Furthermore, in 2020, the Ministry for the Development of Information Technologies and Communications introduced a comprehensive national cybersecurity strategy.

At present, various digital solutions are being implemented to ensure the protection of personal data, including the "e-imzo" system and advanced technologies designed to secure electronic services. These initiatives are playing a vital role in establishing a solid foundation for the country's transition towards a digital economy.

Conclusion

In conclusion, cybersecurity and personal data protection have become pressing concerns for individuals, organizations, and governments alike. The increasing frequency and sophistication of cyberattacks necessitate stricter global regulations and more proactive security measures. Uzbekistan is actively contributing to these efforts by developing and implementing national cybersecurity strategies. At the individual level, users must adopt modern tools and practices to safeguard their personal information. Ultimately, ensuring data security is not only essential for personal protection but also a fundamental component of national and global cybersecurity.

References

1. European Union. (2018). General Data Protection Regulation (GDPR). Official Journal of the European Union.
2. Greenwald, G. (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan Books.
3. Kaspersky Lab. (2017). WannaCry Ransomware: Technical Analysis and Impact Report.
4. Symantec Corporation. (2017). WannaCry Ransomware Attack Analysis Report.
5. United Nations. (2020). Cybersecurity and Cybercrime: Global Trends and Challenges.
6. Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan. (2020). National Cybersecurity Strategy of Uzbekistan.
7. President of the Republic of Uzbekistan. (2019). On Measures to Ensure Information Security in the Republic of Uzbekistan.
8. Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Pearson Education.