Ideal Journal of Multidisciplinary Research
ISSN (E): 3054-3339
Volume 01, Issue 05, May, 2026
Website: https://researchiapress.com

CYBERSECURITY AND INFORMATION PROTECTION ISSUES IN THE DIGITAL SOCIETY

Alimova Komila Dekanovna
Teacher at Tashkent State Medical University
E-mail: komiladekanovna13@gmail.com
Phone: +998 99-081-59-26

Abdumajidova Mushtariy Shuxrat qizi
Student at Tashkent State Medical University
Phone: +998 95 094 54 51
E-mail: abdumajidovamushtariy056@gmail.com

Abstract
This article analyzes the role of cybersecurity in modern society, the threats associated with the rapid development of digital technologies, and the issues of ensuring information security. The paper also examines the main forms of cybercrime and their negative impact on governments, organizations, and personal data. During the research process, international experience, legal and regulatory documents, and modern cyber protection mechanisms were studied. The findings justify the necessity of a comprehensive approach and the improvement of digital literacy in ensuring information security.

Keywords: Cybersecurity, information security, cybercrime, digital technologies, data protection, internet, cyberattack.

Introduction

In the 21st century, the rapid development of digital technologies has deeply penetrated all spheres of human life. Today, public administration, banking and finance, healthcare, education, and business processes cannot be imagined without modern information and communication technologies. The expansion of the Internet, the development of artificial intelligence, and cloud technologies

Ideal Journal of Multidisciplinary Research
ISSN (E): 3054-3339
Volume 01, Issue 05, May, 2026
Website: https://researchiapress.com

have significantly facilitated human activities; however, they have also created new risks and threats. One of the most pressing issues among them is cybersecurity.

Cybersecurity refers to the protection of information systems, computer networks, and electronic data from unauthorized access, theft, destruction, or manipulation. In recent years, the sharp increase in cybercrime has forced governments and international organizations to pay serious attention to this issue. In particular, cyberattacks on banking systems, theft of personal data, the spread of malicious software, and internet fraud pose serious threats to global security.

Alongside the development of digital technologies, the human factor also plays an important role in cybersecurity. Many cyberattacks occur due to users' negligence, weak passwords, or access to suspicious links. Therefore, improving digital literacy and developing a culture of safe internet usage have become urgent tasks of modern society.

Today, the Republic of Uzbekistan is also implementing a number of reforms aimed at ensuring cybersecurity. Legal and regulatory frameworks are being improved to protect information systems, secure state electronic databases, and safeguard citizens' personal data.

The main purpose of this article is to analyze the importance of cybersecurity in the development of society and the state, study existing threats, and highlight effective mechanisms for ensuring information security.

Research Methodology

In the course of this research, modern scientific methods of analysis were widely used. The theoretical and methodological basis of the study consisted of scientific literature related to cybersecurity, information security, and digital technologies, as well as recommendations of international organizations and legal-regulatory documents. In order to comprehensively examine the topic, systematic, comparative, statistical, and legal analysis methods were applied.

First, scientific works, monographs, articles, and practical research studies of local and foreign scholars were examined to determine the role and significance of cybersecurity in modern society. In particular, theoretical views related to information security, cybercrime, data protection, and internet security were

Ideal Journal of Multidisciplinary Research
ISSN (E): 3054-3339
Volume 01, Issue 05, May, 2026
Website: https://researchiapress.com

analyzed. This made it possible to identify the scientific foundations of the topic and existing problems.

Comparative legal analysis was also effectively used during the research. In particular, the laws of the Republic of Uzbekistan related to information security and cybersecurity, presidential decrees, government resolutions, and other legal documents were studied. At the same time, international experience was analyzed through the study of cybersecurity standards and recommendations developed by the United Nations, the International Telecommunication Union (ITU), the European Union, and other international organizations. Based on these documents, similarities and differences between national and international approaches were identified.

In addition, statistical analysis methods were used to study cyberattacks, data theft, internet fraud, and other cybercrimes that have occurred in recent years both worldwide and in Uzbekistan. Statistical data helped identify the main factors threatening cybersecurity and their impact on society.

During the research process, a systematic approach was applied to examine cybersecurity issues in connection with technological, legal, social, and moral aspects. The role of government institutions, educational organizations, the private sector, and civil society institutions in ensuring information security was also analyzed separately.

These methodological approaches made it possible to comprehensively study the research topic, identify existing problems, and develop scientific and practical recommendations for ensuring cybersecurity.

Research Results

The analysis shows that cybercrime has become one of the most dangerous problems of modern society. In particular, phishing attacks, malware, ransomware, and illegal data theft cases are rapidly increasing. As a result of such attacks, government agencies, banking systems, and large companies suffer significant economic losses.

Furthermore, the leakage of personal data negatively affects citizens' privacy and rights. In particular, the uncontrolled sharing of personal information on social networks increases the risk of cyber fraud. The growing number of online fraud

Ideal Journal of Multidisciplinary Research
ISSN (E): 3054-3339
Volume 01, Issue 05, May, 2026
Website: https://researchiapress.com

cases in recent years demonstrates the need to strengthen information security awareness among the population.

The research findings indicate that, in addition to using modern protective technologies, increasing users' information culture is also crucial for ensuring cybersecurity. Many cyberattacks are connected to human factors, such as negligence or insufficient knowledge of security measures.

Moreover, the study revealed the necessity of strengthening cooperation between the state and the private sector, introducing modern security technologies, and regularly monitoring information systems. Protecting strategically important information resources is one of the key factors in ensuring national security.

Discussion

Ensuring cybersecurity is one of the most important conditions for the development of modern society. In today's digital era, public administration, banking and finance, education, healthcare, and many other sectors depend heavily on information technologies, which further increases the relevance of cybersecurity issues. Therefore, strengthening cooperation among government agencies, educational institutions, the private sector, and civil society is of great importance in ensuring information security.

First of all, developing a culture of information security within the education system is one of the key priorities. For this reason, it is necessary to organize special courses, seminars, and practical training sessions on cybersecurity in schools, academic lyceums, colleges, and higher educational institutions. Such activities help young people learn safe internet usage, personal data protection, and methods for identifying malicious links and fraud schemes.

In addition, improving the digital literacy of the population is an effective tool in preventing cybercrime. Therefore, it is necessary to regularly conduct awareness campaigns on information security among internet users.

The introduction of modern protection technologies in organizations and enterprises is also an essential condition for ensuring cybersecurity. In particular, the use of strong authentication systems, multi-level security mechanisms, antivirus software, and data encryption technologies significantly increases the security of information systems. Moreover, regular monitoring of information

Ideal Journal of Multidisciplinary Research
ISSN (E): 3054-3339
Volume 01, Issue 05, May, 2026
Website: https://researchiapress.com

systems, conducting security audits, and timely identification of technical vulnerabilities are important for preventing cyberattacks.

The human factor also plays an important role in cybersecurity. Therefore, regular professional development courses and practical training sessions should be organized for employees working in organizations. Furthermore, the expansion of artificial intelligence, cloud technologies, and smart systems creates not only new opportunities but also new risks and threats. Consequently, the protection of information systems requires the use of innovative technologies and modern software solutions.

The development of international cooperation is another important factor in ensuring cybersecurity. Since cybercrimes are transnational in nature, effective cooperation among states is essential in combating them.

Overall, a comprehensive and systematic approach is important in ensuring cybersecurity. By combining technical protection tools, legal mechanisms, educational systems, and public cooperation, it is possible to ensure security in the digital environment and effectively combat cybercrime.

Conclusion

In conclusion, cybersecurity is an integral part of modern digital society. Although the development of information technologies facilitates human life, it also creates new risks and threats. Therefore, protecting information systems, ensuring the security of personal data, and combating cybercrime have become urgent tasks of today.

The research findings demonstrated that ensuring cybersecurity cannot be limited only to technical measures. Improving digital literacy, developing a culture of safe internet usage, and educating young people about information security rules are of great importance. In particular, introducing special educational programs on information security and increasing users' security awareness can help prevent cyber threats.

Furthermore, it is necessary to strengthen cooperation among government agencies, educational institutions, the private sector, and civil society organizations. The introduction of modern security technologies, regular monitoring of information systems, and conducting security audits contribute to ensuring stability and security in the digital environment.

Ideal Journal of Multidisciplinary Research
ISSN (E): 3054-3339
Volume 01, Issue 05, May, 2026
Website: https://researchiapress.com

International experience shows that cooperation among states is also important in combating cybercrime. Since cyberattacks have a global nature, effective measures require the exchange of international experience and the implementation of modern standards.

Overall, a comprehensive and systematic approach is essential in ensuring cybersecurity. By integrating legal, technological, moral, and organizational measures, it is possible to strengthen information security, protect society from cyber threats, and ensure sustainable digital development.

References

1. Republic of Uzbekistan. Law "On Cybersecurity". Tashkent, 2022.
2. Stallings W. Cybersecurity Essentials. Pearson Education, 2019.
3. Whitman M., Mattord H. Principles of Information Security. Cengage Learning, 2021.
4. National Institute of Standards and Technology (NIST). Cybersecurity Framework. Washington, 2020.
5. Kaspersky Lab. Cyberthreat Report 2023. Moscow, 2023.
6. Cisco Systems. Annual Cybersecurity Report. California, 2022.
7. Karimov Sh. "Legal Foundations of Information Security". Law and Society Journal, 2021, No. 5, pp. 44–51.
8. Ahmedov Q. "Digital Technologies and Cybersecurity Issues". Journal of Modern Information Technologies, 2023, No. 2, pp. 18–25.
9. Alimova, K.D. "The Path Leading to Darkness: Socio-Psychological Analysis of Drug Addiction Problems Among Youth and Preventive Strategies." Modern Education and Development, Vol. 47, No. 3, pp. 51–60, 2026.