UDC: 343.9.004.056

LEGAL MECHANISMS FOR COMBATING CYBERCRIME

Azizbek Khamdamov
Student, Tashkent State University of Law
azizbekkhamdamov908@gmail.com
https://orcid.org/0009-0003-6038-3103

Abstract: This article examines legal mechanisms for combating cybercrime in the context of digital transformation. The study analyzes the national legislation of Uzbekistan, international legal standards, and foreign practices. Statistical data demonstrate the rapid growth of cybercrime, highlighting the need to improve legal regulation. The research proposes preventive legal measures, development of cybersecurity infrastructure, and strengthening international cooperation.

Keywords: cybercrime, information security, digital law, cybersecurity, electronic crimes, legal regulation.

Introduction

In the twenty-first century, the rapid development of digital technologies has led to the transformation of economic systems, public administration, and social relations. The widespread implementation of information and communication technologies has resulted in a significant shift of public services, banking and financial operations, electronic commerce, and civil legal relations into the virtual environment. At the same time, the process of digitalization has contributed to the emergence and rapid spread of new forms of unlawful activities, particularly cybercrime.

In the Republic of Uzbekistan, the development of the digital economy has been identified as one of the priority directions of state policy. In particular, the “Digital Uzbekistan – 2030” Strategy, approved by Presidential Decree No. PF–6079 dated October 5, 2020, предусматривает large-scale digital transformation of public administration, the economy, and the social sector. Within the framework of this strategy, the expansion of e-government systems, digital services, and online financial transactions has elevated the issue of information security to the level of national security priorities.

In order to legally regulate the risks emerging within the digital environment, the Law of the Republic of Uzbekistan “On Cybersecurity” was adopted, establishing legal provisions for the protection of information infrastructure, the prevention of cyberattacks, and the determination of the powers and responsibilities of state authorities in this field. This law serves as

the fundamental legal framework for the formation and development of the national cybersecurity system.

Furthermore, the Law “On Informatization” establishes the general principles for ensuring security in the use of information resources and information systems, as well as defining the rights and obligations of information owners. This regulatory act plays a significant role in shaping legal liability mechanisms within digital relations.

The criminal law foundations for combating cybercrime are enshrined in the Criminal Code of the Republic of Uzbekistan, which provides for liability measures for the unlawful use of information technologies, unauthorized access to computer information, and electronic fraud. In recent years, the growing number of fraud cases committed through electronic payment systems has demonstrated the necessity of further improving these legal provisions.

Alongside the widespread introduction of digital technologies in public administration, strengthening information security has been identified as a key priority in the Development Strategy of New Uzbekistan, approved by Presidential Decree No. PF–60 dated January 28, 2022, this document also identifies these issues as a distinct priority task, emphasizing that ensuring cybersecurity and protecting the information space constitute important directions of state policy.

According to statistical data, alongside the growth in the number of Internet users in the country, the proportion of cybercrimes has also been steadily increasing. According to information provided by internal affairs authorities, a significant share of fraud-related offenses committed in recent years has been carried out through information technologies. This trend demonstrates the necessity of improving existing legal mechanisms in accordance with modern technological threats.

These circumstances indicate that strengthening criminal liability alone is insufficient in combating cybercrime; rather, it requires the development of preventive legal mechanisms, enhanced institutional cooperation, and the improvement of the regulatory framework in line with international standards. Therefore, conducting a comprehensive scientific analysis of legal mechanisms for combating cybercrime represents one of the pressing tasks facing contemporary legal science.

The rapid development of the digital economy is transforming all spheres of social life. Along with the sharp increase in the number of Internet users, cybercrime has emerged as a global security challenge. According to the International Telecommunication Union (ITU), the number of Internet users worldwide reached 5.4 billion in 2024, accounting for approximately 67 percent of the global population.

According to INTERPOL reports, cybercrime has become the fastest-growing category of crime over the past five years, with global economic losses reaching approximately USD 8 trillion in 2023. According to forecasts, this figure may reach USD 13 trillion by 2027.

In Uzbekistan, the issue of cybersecurity has also gained particular relevance as a result of the digitalization of public services, the banking sector, and commercial platforms. According to data from internal affairs authorities, approximately 32 percent of fraud-related crimes recorded in the country in 2023 were committed via the Internet.

The purpose of this study is to provide a scientific analysis of the legal mechanisms for combating cybercrime and to develop proposals for their improvement.

Literature Review

The problem of cybercrime has been extensively studied by numerous foreign scholars. American researcher J.Wall characterizes cybercrime as a new criminal phenomenon of a transnational nature and emphasizes that traditional criminal law mechanisms are insufficient to effectively address it.

Russian scholar V.B.Naumov examines the legal regulation of information security, highlighting the decisive role of state legal policy in ensuring cybersecurity and countering cyber threats.

Uzbek legal scholars consider cybersecurity to be an integral component of national security and emphasize the necessity of modernizing legal regulatory mechanisms in parallel with the development of the digital economy.

Analytical findings indicate that the majority of existing studies primarily focus on technical aspects, while have not yet been sufficiently systematized comprehensive legal mechanisms.

Methodology

During the research, the following scientific methods were employed: comparative legal analysis, statistical analysis, analysis of normative legal documents, a systematic approach, and a comparative study of international experience.

Results And Discussion

Cybersecurity Ventures According to research findings, one organization worldwide falls victim to a ransomware attack every 11 seconds.

Cybercrimes mainly manifest in the following forms: phishing and online fraud, theft of bank card data, the distribution of malicious software (malware), and the illegal dissemination of personal data.

The fight against cybercrime is carried out on the basis of the following regulatory legal acts:

Table 1.
The Significance of Regulatory Legal Acts in Combating Cybercrime

№	Regulatory Legal Acts on Combating Cybercrime	Purpose	Content
1	Criminal Code of the Republic of Uzbekistan	Protection of information systems, digital resources, and the property and personal rights of users; prevention of cybercrime; and ensuring the criminal liability of offenders.	The Criminal Code of the Republic of Uzbekistan establishes the primary criminal law mechanism for combating cybercrime.
2	Law of the Republic of Uzbekistan "On Informatization"	Legal regulation of the information space, protect-tion of the rights of information resource ow-ners, ensuring information security, and safeguarding the interests of the state and society.	The Law "On In-formatization" estab-lishes the general legal framework governing the use of information resources, information systems, and informa-tion technologies wi-thin the country.
3	Law of the Republic of Uzbekistan "On Cybersecurity"	Formation of the national cybersecurity system, pre-vention and detection of cyberattacks, ensuring the stable functioning of in-formation infrastructure, and strengthening cyber-security cooperation among the state, business sector, and society.	It establishes provi-sions for the protection of state information systems and critical infrastructure facilities against cyberattacks, as well as defining the functions of authorized bodies and the res-ponsibilities of cy-bersecurity stake-holders.

4	Presidential Decrees on the Development of the Digital Economy	Digitalization of public administration, expansion of the e-government system, development of IT infrastructure, increasing the share of digital services, and strengthening information security.	The documents adop-ted within the frame-work of the "Digital Uzbekistan – 2030" Strategy and the De-velopment Strategy aim at advancing the digital economy and expanding electronic public services in the country.

The Law "On Cybersecurity," adopted in 2022, established the institutional foundations for the protection of state information systems.

Examining advanced foreign practices, the primary legal instrument for combating cybercrime in the European Union is the Budapest Convention on Cybercrime. This convention establishes mechanisms for the recognition of electronic evidence, cross-border investigations, and interstate cooperation. In the United States, integration between the public and private sectors has been implemented through the Cybersecurity and Infrastructure Security Agency.

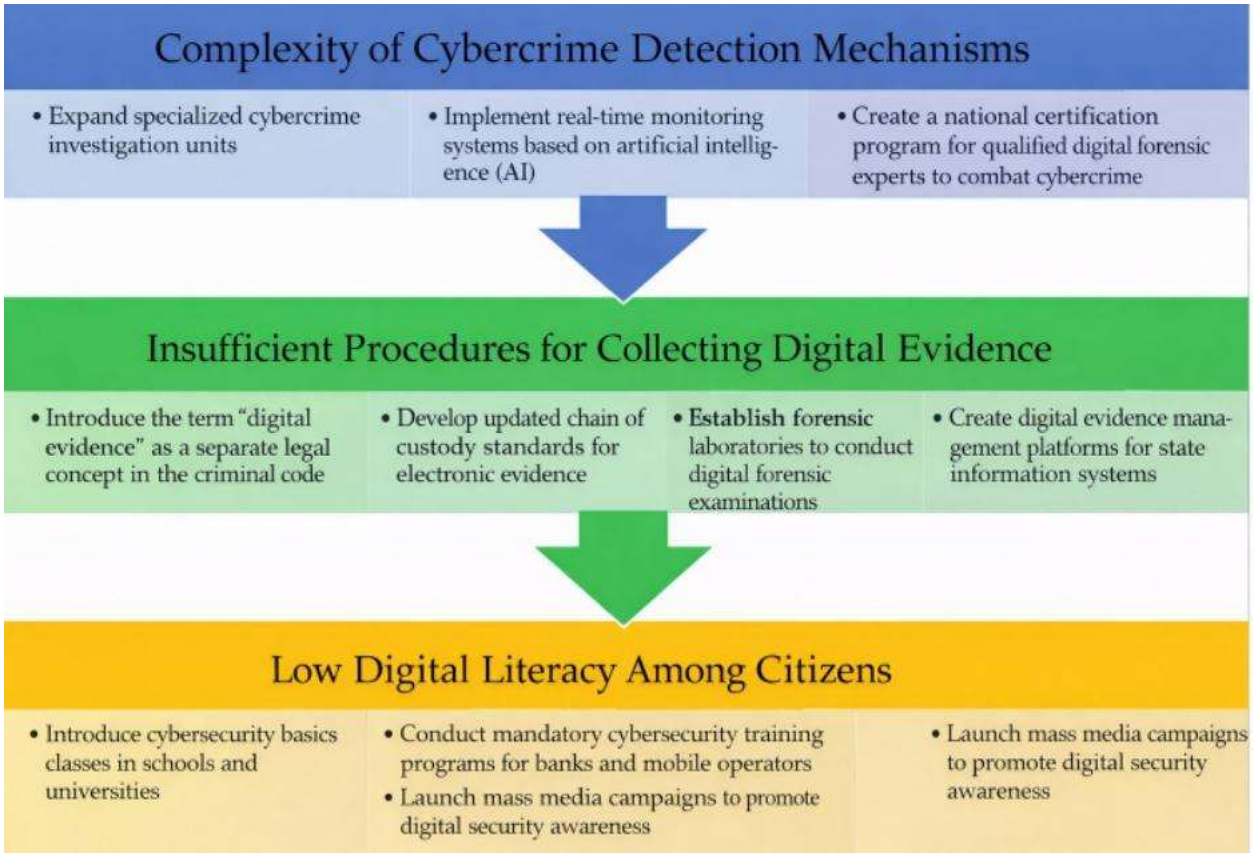

Complexity of Cybercrime Detection Mechanisms
• Expand specialized cybercrime investigation units
• Implement real-time monitoring systems based on artificial intelligence (AI)
• Create a national certification program for qualified digital forensic experts to combat cybercrime
Insufficient Procedures for Collecting Digital Evidence
• Introduce the term "digital evidence" as a separate legal concept in the criminal code
• Develop updated chain of custody standards for electronic evidence
• Establish forensic laboratories to conduct digital forensic examinations
• Create digital evidence management platforms for state information systems
Low Digital Literacy Among Citizens
• Introduce cybersecurity basics classes in schools and universities
• Conduct mandatory cybersecurity training programs for banks and mobile operators
• Launch mass media campaigns to promote digital security awareness
• Launch mass media campaigns to promote digital security awareness

Figure 1. Cybercrime Challenges and Evidence-Based Solutions

As a result of the conducted research and analysis, several key challenges were identified, including the complexity of cybercrime detection mechanisms, insufficient procedures for collecting digital evidence, issues related to international jurisdiction, and the low level of digital literacy among citizens.

Conclusion

The findings of the study demonstrate that the rapid development of digital technologies, while creating new opportunities across all spheres of society and the economy, has also led to a significant increase in cybercrime risks. The digitalization of Internet services, electronic commerce, remote banking operations, and public services has transformed the information space into an active environment for new forms of criminal activity. Therefore, combating cybercrime should be viewed not only as a function of law enforcement agencies but also as an essential component of national security, economic stability, and the protection of citizens' rights.

In our view, the modernization of legal mechanisms, the development of the digital evidence institution, the improvement of the regulatory framework in accordance with international standards, and the strengthening of preventive approaches constitute key prerequisites for establishing a stable and secure digital environment in Uzbekistan. Systematic reforms implemented in these areas will not only reduce the level of cybercrime but will also contribute to the country's innovative development by strengthening trust in the digital economy.

LIST OF LITERATURES

1. President of the Republic of Uzbekistan. Decree No. PF–6079 dated October 5, 2020 "On the Approval of the Digital Uzbekistan – 2030 Strategy" —https://lex.uz/docs/5030957
2. Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, 15.04.2022-y., O'RQ–764. https://lex.uz/docs/5960609
3. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni. https://lex.uz/docs/56032
4. O'zbekiston Respublikasi Jinoyat kodeksi. https://lex.uz/docs/111453
5. O'zbekiston Respublikasi Prezidentining 28.01.2022-yildagi PF–60-son Farmoni — 2022–2026-yillarga mo'ljallangan Taraqqiyot strategiyasi. https://lex.uz/docs/5841063
6. International Telecommunication Union. Measuring Digital Development Report, 2024. https://www.itu.int
7. INTERPOL Global Crime Trend Report, 2023. https://www.interpol.int
8. O'zbekiston Respublikasi IIV statistik ma'lumotlari, 2023. https://iiv.uz

9. Wall D. Cybercrime: The Transformation of Crime in the Information Age. — Polity Press, 2020
10. Наумов В.Б. Информационное право. — Москва: Норма, 2021
11. Cybersecurity Ventures Report, 2023. https://cybersecurityventures.com