AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 9.918 IMPACT FACTOR
Volume-3| Issue-5| 2025 Published: |30-05-2025|

"LEGAL AND INSTITUTIONAL FOUNDATIONS FOR COMBATING CYBERCRIME IN THE CONTEXT OF NEW UZBEKISTAN"

https://doi.org/10.5281/zenodo.15448649

Atkhamjonov Abboskhan
(Atxamjonov Abbosxon Atxamjon o'g'li)
Master's student (1st year),
Department of International Relations and Contemporary Political Processes,
Faculty of International Relations and Economics,
Diplomat University.

Abstract

This article analyzes the legal and institutional foundations for combating cybercrime in the context of New Uzbekistan. It explores the reforms implemented by the Republic of Uzbekistan in recent years, the adopted normative legal documents, the formation of new organizations, and the mechanisms of international cooperation that collectively contribute to the establishment of a national cybersecurity system.

Keywords

Cybercrime, cybersecurity, digitalization, legal framework, Uzbekistan, institutional mechanism.

(YANGI O'ZBEKISTON SHAROITIDA KIBERJINOYATLARGA QARSHI KURASHNING HUQUQIY VA INSTITUTSIONAL ASOSLARI.)

Annotatsiya

Mazkur maqolada Yangi O'zbekiston sharoitida kiberjinoyatlarga qarshi kurashishning huquqiy va institutsional asoslari tahlil qilinadi. So'nggi yillarda raqamlashtirish jarayonlarining jadallashuvi bilan birga kiberjinoyatlar sonining ortishi kuzatilmoqda. Maqolada O'zbekiston Respublikasining kiberxavfsizlik sohasidagi asosiy qonunlari, institutlari va xalqaro hamkorlikdagi ishtiroki ko'rib chiqiladi.

Xususan, Mamlakatda raqamlashtirish jarayonining jadallashuvi bilan bog'liq holda yuzaga kelayotgan kibertahdidlar va ularga qarshi ko'rilayotgan chora-tadbirlar yoritiladi.

Shuningdek, mavjud muammolar va ularni bartaraf etish bo'yicha takliflar keltiriladi.

Kalit so'zlar

Yangi O'zbekiston, tashqi siyosat, kiberjinoyatlar, xavfsizlik, xalqaro hamkorlik, axborot-kommunikatsiya.

Аннотация

В данной статье анализируются правовые и институциональные основы противодействия киберпреступности в условиях Нового Узбекистана. В последние годы наблюдается рост количества киберпреступлений, происходящий параллельно с ускоренными процессами цифровизации. В статье рассматриваются ключевые законы Республики Узбекистан в сфере кибербезопасности, действующие институты, а также участие страны в международном сотрудничестве.

Особое внимание уделяется возникающим киберугрозам, связанным с цифровой трансформацией страны, и мерам, предпринимаемым для их нейтрализации. Кроме того, в статье представлены актуальные проблемы и предложения по их устранению.

Ключевые слова

Новый Узбекистан, внешняя политика, киберпреступления, безопасность, международное сотрудничество, информационно-коммуникационные технологии.

Introduction.

The rapid development of globalization and digital technologies is profoundly impacting all spheres of human life. Information and communication technologies (ICT) are driving significant transformations across various sectors, including everyday life, the economy, education, healthcare, public administration, and many others. At the same time, the emergence of new risks in the digital environment–particularly the growing scale of cybercrimes–has become a pressing issue for modern society.

Cybercrime refers to criminal activities committed using computer systems, networks, or digital devices. These crimes include phishing, fraud, identity theft, malware (such as viruses and Trojans), cyberattacks on government institutions, and illegal use of artificial intelligence, among other forms. Such crimes not only cause economic damage but also erode public trust, create fear, and give rise to complex legal challenges. Preventing these threats is a strategic priority, especially for states striving for deeper global integration.

In recent years, the digitalization policy has become one of the key priorities of the state policy in the Republic of Uzbekistan. Initiatives such as "E–Government," the "Digital Uzbekistan – 2030" Strategy, the implementation of electronic public

services, and distance learning systems have significantly expanded the country's digital infrastructure. However, these advancements have also created new opportunities for cybercriminals. The sharp increase in cybercrime incidents in Uzbekistan from 2020 to 2023 underscores the urgent need to strengthen legal and institutional measures in this area.

Consequently, in the era of New Uzbekistan, combating cybercrime has become a matter of national policy. The adoption of the Law "On Cybersecurity" in 2022, the inclusion of specific provisions related to cybercrime in the new edition of the Criminal Code, and the establishment of relevant state institutions represent major steps forward in this direction.

This article provides a systematic analysis of the legal and institutional foundations for combating cybercrime in the context of New Uzbekistan. Specifically, the paper:

1. Highlights the relevance and challenges of the topic;
2. Reviews current legal norms (including the Criminal Code and special laws);
3. Analyzes the functions of state bodies and newly established institutions;
4. Examines international cooperation and the adoption of best foreign practices;
5. Proposes concrete solutions and policy recommendations.

The methodological basis of this research includes legal analysis, statistical data interpretation, document review, and comparative legal methods. This article may be of practical and theoretical value to legal scholars, policymakers, law enforcement professionals, and IT specialists.

1. The Concept, Risks, and Legal Definition of Cybercrime.

According to Article 3 of the Law of the Republic of Uzbekistan "On Cybersecurity" No. ORQ–764 dated April 15, 2022, cybercrime is defined as a set of offenses committed in cyberspace using software and technical means with the intent to obtain, alter, destroy information, or disable information systems and resources.

Cybercrimes are offenses committed through computer networks, software, and information systems. They can manifest in various forms, including:

1. Unauthorized acquisition of information;
2. Illegal access to systems;
3. Forgery using deepfake technologies;
4. Banking fraud and phishing attacks;
5. Illegal cryptocurrency mining and circulation of crypto assets.

Such crimes pose a threat not only to individual interests but also to the information infrastructure of the state. They undermine trust, compromise data integrity, and can disrupt the operation of critical systems.

2. Legal Foundations for Combating Cybercrime.

The Republic of Uzbekistan has established a comprehensive legal framework to address the growing threat of cybercrime. The following are the key normative legal documents that form the basis of this framework:

1.**The Criminal Code of the Republic of Uzbekistan**: Initially enacted in 1994 and adopted in a new version in 2023, the updated Criminal Code specifically addresses cybercrime. Article 278–1 criminalizes unauthorized access to computer information, while Article 278–2 deals with crimes committed using computer technologies.

2.**Law "On Informatization" (2020)**: This law defines the legal principles of information security and regulates the operation of information systems, ensuring their integrity and resilience.

3.**Law "On Cybersecurity" (2022)**: Signed by the President of Uzbekistan on April 15, 2022, this law provides a legal basis for combating cybercrime. It focuses on safeguarding government information systems and critical information infrastructure from cyber threats.

4.**Law "On Personal Data" (2019)**: This legislation aims to protect personal data and ensure its confidentiality in digital environments.

Furthermore, the 2023 revision of the Criminal Code reinforced the legal framework by clearly defining offenses such as unauthorized access to digital data and crimes using computer equipment. In October 2023, the Senate of Uzbekistan deliberated amendments to increase penalties for crimes involving deepfakes, phishing, and other forms of cybercrime. These legislative developments signify a decisive step toward strengthening the legal instruments necessary for effective cybersecurity governance.

3. Institutional Foundations.

In the Republic of Uzbekistan, several key institutions are actively engaged in the prevention and investigation of cybercrime. These institutional mechanisms form the backbone of the country's cybersecurity system.

3.1. Cybersecurity Center under the State Security Service

Established in 2018, this center is responsible for protecting the information systems of government institutions. It operates based on international best practices and focuses on detecting and preventing cyber threats within national infrastructure.

3.2. Department for Combating Cybercrime under the Ministry of Internal Affairs

This department is tasked with the investigation and prosecution of cybercrime cases. It plays a critical role in identifying cybercrimes and gathering digital evidence. Over the past three years, the number of cybercrimes has increased 8.3 times, highlighting the growing importance of its work.

3.3. Inspectorate for Supervision in the Field of Informatization and Telecommunications ("Uzkomnazorat")

This regulatory body monitors illegal activities on the internet, ensuring compliance with information and telecommunication regulations.

3.4. Newly Established Institutions UzSOC Cybersecurity Monitoring Center (established in 2023): Its primary function is to detect cyber threats within the infrastructure of state bodies.

Cybersecurity Center under the Central Bank: Specializes in protecting the financial system from cyber threats.

Group–IB Center for Combating Digital Crime (Tashkent): Operates as part of international cybersecurity cooperation, focusing on advanced cyber investigations.

4. International Cooperation.

The Republic of Uzbekistan actively engages in international cooperation in the field of cybersecurity through multilateral agreements and partnerships with international organizations, foreign countries, and their competent agencies. In 2022, Uzbekistan announced its initiative to accede to the Budapest Convention on Cybercrime, signaling its commitment to harmonizing national cybercrime legislation with international standards. Additionally, the country is collaborating under the framework of the United Nations Cybercrime Program, which aims to enhance global cyber resilience and promote best practices in combating cyber threats.

5. Cybercrime Statistics and Emerging Threats

In the summer of 2022, the head of the Cybersecurity Center under the Ministry of Internal Affairs reported that the number of cybercrimes in Uzbekistan had increased 8.3 times over the past three years.

In particular, there was a sharp rise in fraudulent schemes in Tashkent involving the unauthorized appropriation of funds from citizens' bank cards. As a result of such cybercrimes in 2022 alone, residents of Tashkent suffered financial losses amounting to at least 45.2 billion UZS. However, only approximately 9.2 billion UZS of that amount was successfully recovered.

Furthermore, in the 2023 Global Cybersecurity Index, Uzbekistan ranked 93rd out of 176 countries—slipping from its 88th position in 2022.

These figures highlight the urgent need to enhance institutional capacities, improve digital literacy, and implement more robust technical and legal frameworks to address the growing cyber threat landscape.

6. Education and Workforce Development

Starting from 2025, the Academy of the Ministry of Internal Affairs will launch a master's program in "Legal Support of Cybersecurity." This initiative is aimed at preparing specialists to combat cybercrime.

Additionally, from the 2025/2026 academic year, the Academy of the Ministry of Internal Affairs will begin offering a bachelor's degree program in "Criminal Justice in the Field of Digital Technologies" under the "Jurisprudence" department. The program will span four years.

At Tashkent State University of Law, a new joint master's program in "Cyber Law and Cybercrime Investigation" will be introduced in the upcoming academic year.

7. Practical Issues and Ways to Address Them

In recent years–particularly in 2022–cases of fraud involving the unauthorized use of bank cards have sharply increased in Tashkent. This trend has become a pressing issue posing a threat to the financial security of the country. Such fraudulent activities not only cause significant financial losses for bank customers but also undermine public trust in the entire banking system.

This problem is multifaceted and can be analyzed from several key perspectives:

1. Technological infrastructure vulnerabilities – Some banks' information systems do not fully comply with modern cybersecurity standards. This creates opportunities for cyberattacks and fraud schemes such as phishing, skimming, and other technical methods used by criminals.

2.Insufficient human resource capacity – There is a shortage of qualified specialists in the field of information security within financial institutions. Moreover, the technical capacity and experience of law enforcement agencies in combating cybercrime are, in some cases, inadequate.

3. Low levels of digital literacy among the population– Many individuals lack sufficient knowledge and skills to protect their personal information, particularly sensitive data related to bank cards. This makes it easier for fraudsters to manipulate users into disclosing confidential details.

Strategies for Mitigation.

To prevent fraud and minimize existing risks, it is essential to implement the following measures:

Implementation of modern cybersecurity technologies within banking systems: Encryption of sensitive data, two–factor authentication, real–time transaction monitoring, and automatic blocking of suspicious activities should be widely adopted.

Strengthening the technical and professional capacity of law enforcement agencies: Specialized units for cybercrime should be established, and professionals trained using international best practices. Additionally, agencies must be equipped with advanced software tools and hardware technologies.

Enhancing public digital literacy through mass media and awareness campaigns: Continuous educational efforts should be conducted by banks and government institutions. Public service announcements, social media campaigns, informational videos, and training sessions will play a key role in raising awareness.

Improvement of the regulatory and legal framework: Legislative reforms that introduce stricter penalties for cybercrime and ensure the effective enforcement of existing laws are necessary to support cybersecurity efforts.

In conclusion, fraud involving bank cards represents a complex and evolving challenge in today's information society. A comprehensive approach–integrating technical, organizational, legal, and educational measures–is crucial to effectively address this issue.

Conclusion and Recommendations

In the context of New Uzbekistan, the fight against cybercrime is becoming an integral component of national security. As digital technologies continue to advance rapidly, threats in the information space are also growing more complex. In response, the Republic of Uzbekistan has undertaken a number of legal, institutional, and organizational measures to ensure cybersecurity.

In particular, the recent amendments to the Criminal Code, the adoption of special laws, the establishment of new institutions, and the development of cooperation with international legal organizations reflect a consistent and systematic state policy in this area.

As a result of ongoing reforms, cybersecurity mechanisms aimed at protecting state infrastructure, the financial system, and citizens' personal data are being developed. However, despite these achievements, several pressing issues remain unresolved. These include a shortage of qualified specialists in the field, technical difficulties in investigating cybercrimes, and the generally low level of public awareness and digital literacy, all of which hinder effective counteraction against cyber threats.

Therefore, a comprehensive approach is essential to further enhance the cybersecurity system. Special attention should be given to the following areas: integrating international standards into national legislation; implementing modern investigation and monitoring tools; increasing public awareness and legal culture regarding cybersecurity; and strengthening the system for training highly qualified specialists in the field.

In conclusion, Uzbekistan has established a solid legal and institutional foundation for combating cybercrime. The reforms being implemented in this field contribute not only to ensuring the country's internal security but also to strengthening international cooperation.

Recommendations:

1. Regular publication of statistical data related to cybercrime;
2. Practical implementation of international standards;
3. Promoting a culture of information security among software developers and IT professionals;
4. Developing specialized judicial institutions focused on cybersecurity.

REFERENCES:

1. Criminal Code of the Republic of Uzbekistan (new edition). – Tashkent: Adolat Publishing House, 2023.
2. Law of the Republic of Uzbekistan "On Informatization". – Adopted on September 23, 2020. – Legal Information Portal: www.lex.uz.
3. Law of the Republic of Uzbekistan "On Cybersecurity". – Adopted on July 15, 2022. – www.lex.uz.
4. Proceedings of the October 2023 session of the Senate of the Oliy Majlis of the Republic of Uzbekistan. – www.senat.uz.
5. Official information on the activities of the Cybersecurity Center under the State Security Service. – Press Service of the State Security Service (SSS), 2023.
6. Data from the Department for Combating Cybercrime under the Ministry of Internal Affairs. – Official website of the MIA: www.iiv.uz, 2022–2024.
7. Annual Reports of the Inspectorate for Control in the Field of Informatization and Telecommunications ("Uzkomnazorat"), 2023.
8. Official information from the UzSOC Cybersecurity Monitoring Center – www.uzsoc.uz.
9. Group-IB Central Asia – Reports on digital crimes. – Tashkent, 2022–2023.

10. Budapest Convention – Council of Europe Convention on Cybercrime. – Strasbourg, 2001.

11. UN Program Documents on Cybersecurity – www.un.org, 2021–2023.

12. "Combating Cybercrime: Modern Threats and Legal Mechanisms" – Scholarly Article by A. Juraev. – *Bulletin of Legal Sciences*, 2023, No. 2.

13. Materials of the Cybersecurity Center under the Central Bank of the Republic of Uzbekistan. – www.cbu.uz, 2023.

14. Academy of Law Enforcement – Master's Program Presentation: "Legal Provision of Cybersecurity", 2024.

15. Academy of the Ministry of Internal Affairs – Program on "Combating Digital Crime". – Curriculum and methodological guidelines, 2023.