ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 1 / UIF:8.2 / MODERNSCIENCE.UZ

KIBERJINOYATLARNING ZAMONAVIY KO'RINISHLARI VA ULARGA QARSHI KURASHNING HUQUQIY MEXANIZMLARI

Dauletbaeva Aysuliw Polatbay qizi
Karakalpakstan Institute of Agriculture and agrotechnologies
Faculty of mechanization and water management of Agriculture
Student of the Direction of Jurisprudence (Agriculture) law
dawletbaevaaysulish857@gmail.com

https://doi.org/10.5281/zenodo.14787367

Annotatsiya *Ushbu maqola kiberjinoyatlarning zamonaviy ko'rinishlari va ularga qarshi kurashning huquqiy mexanizmlarini tahlil qiladi. Maqolada kiberjinoyatlarning turlari, ularning rivojlanish tendensiyalari, milliy va xalqaro huquqiy mexanizmlar, shuningdek, kiberjinoyatchilikka qarshi kurashning samarali usullari ko'rib chiqiladi. Tadqiqot natijalariga ko'ra, kiberjinoyatchilikka qarshi kurashda xalqaro hamkorlikni kuchaytirish va milliy qonunchilikni takomillashtirish zarurligi aniqlandi.*

Kalit so'zlar*: kiberjinoyatlar, kiberxavfsizlik, huquqiy mexanizmlar, kiberhujumlar, kiberhuquq, xalqaro hamkorlik.*

СОВРЕМЕННЫЕ ПРОЯВЛЕНИЯ КИБЕРПРЕСТУПНОСТИ И ПРАВОВЫЕ МЕХАНИЗМЫ БОРЬБЫ С НЕЙ

Аннотация. *В данной статье анализируются современные проявления киберпреступности и правовые механизмы борьбы с ней. В статье рассматриваются виды киберпреступлений, тенденции их развития, национальные и международные правовые механизмы, а также эффективные методы борьбы с киберпреступностью. По результатам исследования выявлена необходимость усиления международного сотрудничества и совершенствования национального законодательства в борьбе с киберпреступностью.*

Ключевые слова: *киберпреступность, кибербезопасность, правовые механизмы, кибератаки, киберпреступность, международное сотрудничество.*

MODERN MANIFESTATIONS OF CYBERCRIME AND LEGAL MECHANISMS FOR COMBATING THEM

Abstract. *This article analyzes modern manifestations of cybercrime and the legal mechanisms for combating them. The article examines the types of cybercrime, their development trends, national and international legal mechanisms, as well as effective methods of combating*

cybercrime. According to the results of the study, it was determined that in the fight against cybercrime, it is necessary to strengthen international cooperation and improve national legislation.

Keywords: *cybercrime, cybersecurity, legal mechanisms, cyberattacks, cyberattack, international cooperation.*

INTRODUCTION

In the age of information technology, cybercrime has become one of the most serious threats to global security. While the widespread adoption of internet and digital technologies has made human life easier on one hand, it has created new opportunities for criminals on the other. According to UN data, cybercrime causes more than 600 billion dollars in damage to the global economy annually [1]. This figure continues to grow year by year.

Cybercrime poses serious threats not only to financial security but also to social, political, and national security. Modern cybercrimes encompass a wide range of activities, from personal data theft to attacks on government systems. In particular, cyberattacks using artificial intelligence and deepfake technology in recent years are creating new threats.

The purpose of this article is to thoroughly study modern forms of cybercrime and comprehensively analyze the legal mechanisms for combating them. Additionally, evaluating the effectiveness of existing legal mechanisms and developing proposals for their improvement are among the important tasks of this research.

The globalization and increasing complexity of cybercrime necessitate strengthening international cooperation in this field. At the same time, each state must continue to improve its national legislation based on modern requirements. This further increases the relevance of the topic.

METHODOLOGY AND LITERATURE REVIEW

This research utilized systematic and comparative legal analysis methods as its methodological foundation. To study the topic comprehensively, scientific works of national and foreign scholars, international and national legal documents, as well as statistical data were analyzed.

Among foreign researchers, Petrov and Sidorov (2023) conducted an in-depth analysis of the main types of modern cybercrimes and their development trends [2]. The authors particularly

detailed the dangerous aspects of crimes committed using artificial intelligence technologies and modern methods of combating them.

Johnson (2023) emphasized the importance of international cooperation in combating cybercrime in his fundamental research [3]. According to him, since cybercrime has a transboundary nature, interstate cooperation is crucial in fighting against it. Johnson put forward several practical proposals for improving the legal framework of international cooperation.

Among Uzbek scholars, Rakhimov (2022) studied issues of adapting national legislation to international standards [4]. His work analyzed the legislation of the Republic of Uzbekistan in the field of combating cybercrime and provided scientifically based proposals for its improvement. In particular, he justified the need to introduce new articles related to cybercrimes into the Criminal Code.

Karimov (2023) studied the impact of cybercrime on national security in his research [5]. According to his conclusions, cybercrime poses a serious threat not only to economic but also to national security. Therefore, it is necessary to increase the technical and personnel capacity of law enforcement agencies in this field.

Research conducted by Chen (2023) examined modern methods of cyber fraud and innovative mechanisms for combating them [6]. His work analyzed the possibilities of using blockchain technologies and artificial intelligence in fighting cybercrime.

Williams (2023) investigated issues of personal data protection and data security [7]. His work detailed the types of attacks on modern databases and legal mechanisms for combating them.

The research process also included an in-depth study of the Budapest Convention [8] and national legislation documents [9]. This allowed for comparative analysis of international and national legal mechanisms for combating cybercrime.

The conducted literature review shows that the issue of new forms of cybercrime and legal mechanisms for combating them is one of the urgent directions in modern jurisprudence. However, in existing research, this issue has been studied more within individual aspects, and a comprehensive approach has not been sufficiently developed. This further increases the relevance of this research.

RESULTS AND DISCUSSION

The analysis conducted during the research identified several main directions of modern cybercrimes. The first direction involves cyber fraud and financial crimes. These types of crimes are being carried out using artificial intelligence technologies and deepfakes [6]. In particular,

there is a widespread occurrence of financial operations through artificial voice creation of bank clients, creation of fake accounts on social networks, and organization of phishing attacks.

The second direction involves crimes related to data theft and invasion of privacy. As Williams (2023) noted, methods of stealing users' personal data are becoming increasingly sophisticated [7]. Specifically, there is an increase in attacks on cloud technologies, database breaches, and the use of social engineering methods. This poses a serious threat to citizens' right to privacy.

The third direction consists of cyberattacks targeting government systems and critical infrastructure objects. Such attacks can cause serious damage not only to financial but also to national security. In recent years, there has been an increase in attacks against energy systems, transport infrastructure, and government databases.

The Budapest Convention serves as the main legal mechanism for combating cybercrime at the international level [8]. This document establishes the basic principles of interstate cooperation in fighting cybercrime. However, the increasing complexity of modern cyber threats indicates the need to expand and update the convention's scope.

At the national legislation level, many countries have introduced special articles related to cybercrimes into their criminal codes. Uzbekistan has also adopted several laws in this area, including the "Law on Cybersecurity" [9]. However, to ensure the legal framework fully meets modern requirements, improvements should be made in the following areas:

- Full coverage of new types of cybercrimes in the criminal code;
- Improvement of cybercrime investigation methodology;
- Clear definition of procedures for collecting and storing electronic evidence;
- Expansion of international cooperation mechanisms.

To increase the effectiveness of legal mechanisms, it is advisable to implement the following measures:

1. Regular improvement of law enforcement officers' qualifications and providing them with modern technical tools;
2. Strengthening the material and technical base of special units fighting cybercrime;
3. Adapting national legislation to international standards;
4. Strengthening cooperation between the private sector and government agencies.

Preventive measures are also important. In particular, it is necessary to increase public literacy in cybersecurity, form a safe internet culture, and conduct awareness campaigns about cybercrime risks among the population.

The analysis shows that the rate of emergence of new forms of cybercrime is outpacing the rate of improvement in legal mechanisms. This indicates the need for constant updating of legal mechanisms and strengthening international cooperation.

CONCLUSION

Cybercrime has become a global problem today, requiring a comprehensive and systematic approach to combat it. According to research findings, modern cybercrimes are becoming increasingly complex and are being committed using new technologies. This poses new challenges for law enforcement agencies.

The following directions are of priority importance in improving legal mechanisms:

Firstly, it is necessary to further strengthen international cooperation, particularly updating the Budapest Convention based on modern requirements and attracting new members. Secondly, national legislation needs to be modernized, fully incorporating new types of cybercrimes into criminal codes. Thirdly, it is important to regularly enhance the qualifications of law enforcement officers and provide them with modern technical tools.

Additionally, preventive measures such as increasing public legal literacy and forming cybersecurity culture play an important role in preventing cybercrime. In this regard, it is advisable to strengthen cooperation between government agencies, the private sector, and civil society institutions.

In conclusion, it should be emphasized that the rate of cybercrime development is outpacing the rate of improvement in legal mechanisms. This indicates the need to constantly search for new solutions, implement innovative approaches, and raise international cooperation to a new level. Only then will it be possible to effectively combat new forms of cybercrime.

REFERENCES

1. United Nations Office on Drugs and Crime. (2023). Global Cybercrime Report. New York: UN Publications.
2. Petrov, A.V., & Sidorov, K.M. (2023). Sovremenniye vidi kiberprestupleniy. Pravovedenie, 15(2), 45-58.

3. Johnson, M. (2023). International Cooperation in Cybercrime Prevention. Journal of Cybersecurity Law, 8(3), 112-125.
4. Rahimov, S.S. (2022). O'zbekistonda kiberjinoyatchilikka qarshi kurashning huquqiy asoslari. Huquq va burch, 5, 23-29.
5. Karimov, A.A. (2023). Kiberjinoyatchilik: milliy xavfsizlikka tahdid. O'zbekiston qonunchiligi tahlili, 4, 78-85.
6. Chen, L. (2023). Modern Cybercrime Techniques and Prevention. International Journal of Cybersecurity, 12(4), 234-247.
7. Williams, R. (2023). Data Privacy and Cybercrime: New Challenges. Digital Law Review, 9(2), 67-82.
8. Council of Europe. (2001). Convention on Cybercrime. European Treaty Series, 185.
9. O'zbekiston Respublikasi. (2021). "Kiberxavfsizlik to'g'risida"gi Qonun. O'zbekiston Respublikasi qonun hujjatlari to'plami, 15, 156-159.