ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 11,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

PROTECTION OF THE RIGHTS OF CYBERCRIME VICTIMS IN UZBEKISTAN LEGISLATION: NATIONAL AND FOREIGN EXPERIENCE

Assistant Lecturer, Department of Law, Tashkent State Agrarian University,

Atkhamjonov Abboskhon

Abstract: This article examines the mechanisms for protecting the rights of cybercrime victims under the legislation of Uzbekistan. It analyzes relevant provisions of the Criminal Code, the Law "On Personal Data," and the Law "On Cybersecurity." The study also compares national regulations with the Budapest Convention and the practices of the United States and European countries, proposing recommendations to strengthen victim protection in O'zbekistan.

Keywords: cybercrime, cybersecurity, victim rights, Uzbekistan legislation, personal data, Budapest Convention, international practice, legal protection.

O'ZBEKISTON QONUNCHILIGIDA KIBERJINOYAT QURBONLARINING HUQUQLARINI HIMOYA QILISH: MILLIY VA XORIJIY TAJRIBA

Toshkent davlat agrar universitetining "Huquqshunoslik" kafedrasi Assistant o'qituvchi

Atxamjonov Abbosxon Atxamjon o'g'li

Annotatsiya: O'zbekiston qonunchiligida kiberjinoyat qurbonlarining huquqlarini himoya qilish tartibi tahlil qilinadi. Jinoyat kodeksi, "Shaxsiy ma'lumotlar to'g'risida"gi Qonun va "Kiberxavfsizlik to'g'risida"gi Qonundagi normativ mexanizmlar baholanadi. Shuningdek, Budapesht Konvensiyasi hamda AQSh va Yevropa davlatlari tajribasi bilan qiyosiy tahlil berilib, O'zbekistonda kiberjinoyat qurbonlarini himoya qilishni takomillashtirish bo'yicha takliflar ishlab chiqiladi.

Kalit so'zlar: kiberjinoyat, kiberxavfsizlik, qurbon huquqlari, O'zbekiston qonunchiligi, shaxsiy ma'lumotlar, Budapesht Konvensiyasi, xalqaro tajriba, huquqiy himoya.

ЗАЩИТА ПРАВ ЖЕРТВ КИБЕРПРЕСТУПЛЕНИЙ В ЗАКОНОДАТЕЛЬСТВЕ УЗБЕКИСТАНА: НАЦИОНАЛЬНЫЙ И ЗАРУБЕЖНЫЙ ОПЫТ

Ассистент кафедры права Ташкентского государственного аграрного университета,

Атхамжонов Аббосхон Атхамжон ўғли

Аннотация: В статье анализируются механизмы защиты прав жертв киберпреступлений в законодательстве Узбекистана. Рассматриваются нормы Уголовного кодекса, Законов «О персональных данных» и «О кибербезопасности». Проведено сравнение с Будапештской конвенцией, а также опытом США и европейских государств. На основе анализа предлагаются рекомендации по совершенствованию защиты жертв киберпреступлений в Узбекистане.

Ключевые слова: киберпреступления, кибербезопасность, права жертв, законодательство Узбекистана, персональные данные, Будапештская конвенция, международный опыт, правовая защита.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 11,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

Introduction

Along with the rapid development of digital democracy in Uzbekistan, the number of cybercrimes is also increasing. Such offenses as online fraud, unauthorized collection and distribution of personal data, cyberbullying, digital extortion pose a direct threat to the privacy, property interests and information security of citizens. In such conditions, the issue of effective protection of the rights of victims of cybercrime has become one of the priorities of state policy.

In recent years, Uzbekistan has modernized the regulatory framework in the field of cybersecurity. The adoption of the Law "On Cybersecurity", the new edition of the Law "On Personal Data", the introduction of special articles on cybercrimes in the Criminal Code have made it possible to provide stronger protection for the rights of victims. At the same time, since digital threats are global in nature, international standards - including the principles of the Budapest Convention and the experience of advanced foreign countries - are gaining importance in further improving national legislation.

The relevance of this study is that in the context of increasing cybercrime, it has become a requirement not only to strengthen the responsibility of offenders, but also to restore the rights of victims of cybercrime, protect them, and develop mechanisms for psychological and legal assistance. This article assesses the effectiveness of current legislation, identifies existing problems, and develops proposals based on international experience.

The results of the study showed that, along with the increase in the number of cybercrimes in Uzbekistan, the system for protecting victims needs to be further improved. Although the current legislation, including the Law "On Cybersecurity", the Law "On Personal Data" and the articles of the Criminal Code on cybercrimes, has increased responsibility for offenders, specific regulatory guarantees for victims and mechanisms for financial and psychological assistance are insufficient.

The issues of cross-border cybercrime, standards for collecting and storing electronic evidence, as well as the level of digital literacy of society remain urgent problems. Therefore, international experience, in particular the Budapest Convention and the experience of advanced countries, provide important guidance in forming a modern cybersecurity system in Uzbekistan.

Based on the research, the following main scientific and practical conclusions were drawn:

1. It is necessary to establish the concept of “cybercrime victim” as a separate legal institution in Uzbekistan.

2. Mechanisms for psychological, legal and financial assistance to victims should be introduced at the institutional level.

3. National standards for the collection, storage and use of electronic evidence should be developed, which will speed up the investigation process and increase its efficiency.

4. It is necessary to increase the digital literacy of the population, implement comprehensive preventive programs on phishing, deepfake and other modern cybersecurity threats.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 11,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

Thus, a comprehensive and systematic approach to protecting victims of cybercrime will serve to strengthen the digital security of Uzbekistan, reliably protect the personal data and digital rights of citizens. The results of this study will create a scientific basis for the development of cybersecurity policy in the country and effective control of cybercrime

Materials and methods

This study is based on an analysis of the current regulatory and legal framework of the Republic of Uzbekistan on cybersecurity and cybercrime. The main sources used were the Law "On Cybersecurity" (2022), the new edition of the Law "On Personal Data", articles of the Criminal Code of the Republic of Uzbekistan on cybercrime, as well as relevant resolutions of the Cabinet of Ministers and materials of the National Cybersecurity Concept. In studying international experience, official documents and scientific articles in open sources on the Budapest Convention, European Union norms, and the legislation of the USA, Great Britain and South Korea were analyzed. The research methodology used comparative legal analysis, regulatory legal monitoring, a systematic approach and logical-analytical analysis methods. Comparative legal analysis allowed us to compare the legislation of Uzbekistan with international standards, and regulatory legal monitoring served to assess the effectiveness of existing procedures. Using a systematic approach, the existing institutional mechanisms for protecting victims of cybercrime were considered in their interrelation. Logical-analytical analysis made it possible to draw scientifically based conclusions on identifying and improving existing problems.

The results of this study include a number of theoretical and practical conclusions based on the analysis and studies conducted to ensure digital democracy and privacy in Uzbekistan. During the study, the achievements made in Uzbekistan in the field of digital democracy and information security, existing problems and measures to be taken in the future were studied.

Tadqiqotning metodologik asosini O‘zbekistonning kiberxavfsizlik sohasidagi yangi normativ-huquqiy bazasi, xalqaro standartlar va zamonaviy ilmiy-uslubiy manbalar tashkil etdi. Asosiy materiallar sifatida quyidagilar tahlil qilindi:

1. Current regulatory legal acts of the Republic of Uzbekistan:

– Law "On Cybersecurity";

– New edition of the Law "On Personal Data";

– Amendments to the Criminal Code regarding cybercrimes;

– Law "On Electronic Government";

– National Cybersecurity Concept;

– Instructions and statistical reports approved by the Ministry of Digital Technologies, the Cybersecurity Center and the Ministry of Internal Affairs.

2. International regulatory frameworks and recommendations:

– Budapest Convention (Cybercrime Convention);

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 11,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

– Council of Europe standards on electronic evidence;

– Personal data protection mechanisms established by the European Union GDPR requirements;

– UN resolutions on cybersecurity;

– National cybersecurity strategies of the USA (NIST), Great Britain (NCSC), South Korea and Singapore.

3. Practical materials:

– statistical data from official bodies of Uzbekistan on the dynamics of cybercrime;

– analytical data on online fraud, phishing, personal data leakage, financial cyberattacks committed in recent years;

– current practice on victims' appeals (information from the prosecutor's office, the Ministry of Internal Affairs, cybersecurity centers).

The following modern scientific and analytical methods were used in the study:

1. Comparative legal analysis method - Uzbek legislation was compared with international standards (Budapest Convention, GDPR, NIST, etc.). This method made it possible to determine the level of legal protection for victims of cybercrime.

2. Regulatory and legal monitoring - was used to assess the practical effectiveness of new laws and amendments adopted in recent years. Through this, the real statistics of cybercrimes, the level of registration and consideration of victims' appeals were studied.

3. Statistical analysis - was carried out on the basis of official statistical data on the number of cybercrimes, their types, the social portrait of victims, and the scale of damage caused. This helped to identify the growth trends of cybercrimes.

4. Systematic approach - a comprehensive consideration of technical, legal, social and psychological factors that can lead to cybercrimes. In particular, the mechanisms of psychological, legal, and financial assistance provided to victims were analyzed in interaction.

5. Logical-analytical analysis - was used to identify gaps in legislation, problems in practice, and develop scientifically based proposals to eliminate them.

6. Case-study method - current cybercrime cases, such as phishing, bank card withdrawals, extortion through messengers, and fraud through deepfake, which have become widespread in recent years, were analyzed as specific examples.

Analysis of research results

The results of the study showed that the system of protection of victims of cybercrime is being formed in Uzbekistan, but it is not yet fully institutionalized. Although the current Law “On Cybersecurity”, the new edition of the Law “On Personal Data” and amendments to the Criminal Code have increased liability for cybercrimes, separate regulatory mechanisms for victims are not sufficiently strong.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 11,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

1. Existing problems in protecting victims of cybercrime.

1.1. Legal gaps

– A separate "victim status" for victims of cybercrime is not clearly defined in Uzbekistan.

– A compensation mechanism for citizens whose personal data has been disclosed or who have suffered financial losses as a result of a crime is not fully formed.

– Procedural norms for collecting and storing electronic evidence are not interpreted uniformly in practice.

1.2. Practical problems

– Victims often do not report cybercrime in a timely manner, because there is a perception that "it is useless".

– There is a lack of qualified specialists in technical expertise, digital trace recovery, and cross-border inquiries in cybercrime investigations.

– The fact that a large part of cybercrime is committed through international platforms, foreign servers, or anonymous networks complicates the investigation.

– Rapid cooperation with banks on financial fraud (phishing, smishing, social engineering) has not yet been sufficiently established.

1.3. Low digital literacy of the population

– More than 60% of cybercrime occurs due to non-compliance with security rules by users themselves.

– The population is low-aware of new threats such as deepfake, artificial intelligence-generated false content, and calls from bank employees.

2. Assessment based on international standards

– prompt reporting of cybercrimes,

– immediate freezing of electronic evidence,

– acceleration of cross-border cooperation,

– state assistance to victims (legal aid, psychological support).

The analysis shows that although these principles exist in Uzbekistan, they do not fully function in practice or procedural mechanisms are not sufficiently developed.

3. Theoretical innovations and scientific conclusions

The following theoretical innovations were put forward based on the study:

3.1. It is necessary to form the concept of "victim of cybercrime" as an independent legal institution.

ORIGINAL ARTICLE
INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE
ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 11,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

This institution will allow for a clear definition of the rights of victims, types of assistance and state guarantees.

3.2. Introduction of the category of "digital harm" into the legislation in compensation for damages related to cybercrimes

For example: moral damage due to leakage of personal data, damage to reputation, online blackmail.

3.3. Inclusion of psychological support in the list of mandatory public services

Cases such as cyberbullying, blackmail, threats with intimate materials have a serious impact on mental health.

3.4. It is necessary to develop a single national standard for the storage and use of electronic evidence.

This will ensure the authenticity, integrity and legal force of evidence in investigative processes.

Offers

1. Establish a "Cybercrime Victims Protection Center" in Uzbekistan. This center can provide legal advice, psychological assistance, and rapid technical support.

2. Introduce a real-time information exchange system between banks, law enforcement agencies, and cybersecurity centers, which will help in the early detection of financial cybercrimes.

3. Introduce mandatory digital literacy training programs for the general population.

4. Develop separate legal norms against fraud based on artificial intelligence and deepfake.

5. Accelerate the process of full accession to the Budapest Convention (if the process is ongoing).

Conclusion

Although Uzbekistan's regulatory and legal framework in the field of cybersecurity has improved significantly in recent years, the increase in the number of cybercrimes requires stronger protection of the rights of victims. The study showed that, although the current Law "On Cybersecurity", the Law "On Personal Data" and new norms introduced into the Criminal Code have strengthened the mechanisms for bringing cybercrimes to justice, specific legal guarantees for victims of cybercrimes have not yet been fully formed.

Also, the complete absence of standards for working with electronic evidence, the insufficient development of the technical examination system, the low level of digital literacy, as well as the often cross-border nature of cybercrimes create serious problems in practice. This indicates the need for international cooperation, including the widespread use of the principles of the Budapest Convention.

Analysis of foreign experience confirms that the system of protection of victims of cybercrime will be effective not only by strengthening punitive measures, but also by establishing the institutional level of psychological, legal and technical assistance by the state. Therefore, the

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 11,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

urgent task of the day is to introduce a separate legal institution for victims of cybercrime in Uzbekistan, introduce the category of "digital damage" into the legislation, strengthen cooperation between banks and law enforcement agencies for the early detection of cybercrime, and increase the digital literacy of society. This indicates the need to form a new model of protection of victims of cybercrime in Uzbekistan, which is comprehensive, systematic and based on international experience. The proposed approaches will serve to strengthen the stability of national cybersecurity, reliably protect the personal data and digital rights of citizens.

REFERENCES

1. Constitution of the Republic of Uzbekistan. - 2023 edition.

2. Criminal Code of the Republic of Uzbekistan. - September 22, 1994.

3. Law "On Informatization". - December 11, 2003.

4. Decree of the President of the Republic of Uzbekistan "On Measures to Ensure Cybersecurity", April 15, 2022.

5. UN Universal Declaration of Human Rights, 1948.

6. Sh. Kholmurodov. Cybercrimes and Problems of Their Prevention. - Tashkent, 2021.

7. M. Tokhtayev. Information Security and Criminal Law. - Tashkent, 2022.

8. Laws of the Republic of Uzbekistan on Information Technologies and Information Security (2020). Resolutions and decrees of the President of the Republic of Uzbekistan. Tashkent: "Uzbekistan" publishing house.

9. European Union General Data Protection Regulation (GDPR). (2018). Regulation of the European Parliament and the Council of the European Union. Published in Belgium.

10. Singh, S., & Soni, P. (2021). "Digital Democracy and Privacy Concerns: A Global Overview." International Journal of Technology and Politics, 17(4), 234-245.

11. Barrett, M., & McDonald, H. (2018). "Cybersecurity and Privacy in the Digital Age: A Global Perspective." International Journal of Information Security, 17(1), 53-67.

12. Shamsiev, A. (2021). "Digital Democracy and Participation in Society: The Case of Uzbekistan." Journal of Youth and Society, 7(5), 45-55.

13. OECD Digital Government Policy Framework (2020). OECD Digital Government Review: Uzbekistan. OECD Publishing.

14. Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company.

15. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Strasbourg, France.

16. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. U.S. Department of Commerce.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 11,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

17. European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape Report 2024. European Union, Brussels.

18. Wall, D.S. (2020). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.