

Date: 19th June-2026

ISSUES OF LEGAL REGULATION OF CYBERCRIME IN CRIMINAL
LEGISLATION

Dauletbaeva Aynur Baxramovna

3rd year student of the Faculty of Law of
Karakalpak State University named after Berdakh

E-mail: dawletbaevaaynur0@gmail.com

Annotation: The article provides information on the concept of cybercrime, its various forms, and the existing regulatory mechanisms in Uzbekistan's current criminal legislation. The social, financial, and psychological consequences of cybercrimes, as well as the need to protect them, are demonstrated on a scientific basis. The article presents proposals for improving the Criminal Code, proposing the introduction of a new article for "Cybercrime," the differentiated application of sanctions, and their alignment with international standards.

Keywords: Cybercrime, Criminal Code, protection of personal data, sanctions, international experience, legal improvement

ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ КИБЕРПРЕСТУПНОСТИ В
УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ

Даулетбаева Айнур Бахрамовна

Каракалпакский государственный университет имени Бердаха
студент 3-го курса юридического факультета

dawletbaevaaynur0@gmail.com

Аннотация: В статье представлена информация о понятии киберпреступности, ее различных проявлениях и существующих механизмах регулирования в действующем уголовном законодательстве Узбекистана. Социальные, финансовые и психологические последствия киберпреступлений, а также необходимость их защиты, научно обоснованы. В статье представлены предложения по совершенствованию Уголовного кодекса, предлагается ввести новую статью, посвященную "Киберпреступлению," дифференцированно применять санкции и привести их в соответствие с международными стандартами.

Ключевые слова: Киберпреступность, Уголовный кодекс, защита персональных данных, санкции, международный опыт, правовое совершенствование.

JINOYAT QONUNCHILIGIDA KIBERJINOYATCHILIKNI HUQUQIY
TARTIBGA SOLISH MASALALARI

Dauletbaeva Aynur Baxramovna

Date: 19th June-2026

Berdaq nomidagi Qoraqalpoq davlat universiteti

yuridika fakulteti 3-bosqich talabasi

E-mail: dawletbaevaaynur0@gmail.com

Annotatsiya: Maqolada kiberjinoyat tushunchasi, ularning turli ko‘rinishlari va amaldagi O‘zbekiston jinoyat qonunchiligida mavjud tartibga solish mexanizmlari haqida ma’lumotlar keltirilgan. Kiberjinoyatlarning ijtimoiy, moliyaviy va psixologik oqibatlari, shuningdek, ularni himoya qilish zarurati ilmiy asosda ko‘rsatiladi. Maqolada Jinoyat kodeksini takomillashtirish bo‘yicha takliflar keltirilib, yangi "Kiberjinoyat" uchun mo‘ljallangan modda kiritish, sanksiyalarni differensial qo‘llash va xalqaro standartlarga moslashtirish taklif etilgan.

Kalit so‘zlar: Kiberjinoyat, Jinoyat kodeksi, shaxsiy ma’lumotlarni himoya qilish, sanksiyalar, xalqaro tajriba, huquqiy takomillashtirish.

The current 21st century is called the "Year of Technology." Since the last century, the prestige and value of computers, the internet, and telephone devices have been growing day by day. Almost everyone on Earth uses these mobile devices, and we wouldn't be wrong to say that they have become a part of our lives. However, just as everything has its pros and cons, internet networks and mobile devices also have their pros and cons. While they help establish contact with distant individuals and facilitate faster information retrieval, these devices and the internet can cause material and financial harm to individuals. The rapid development of digital technologies and information and communication tools has led to fundamental changes in the life of modern society, and in this process, crime and its new types - cybercrimes - have emerged. Cybercrime is a complex of socially dangerous acts carried out primarily through information systems, computer networks, or digital devices [1]. This type of crime poses a significant threat on a global and national scale, and its social and economic consequences are fundamentally different from traditional crime. International legal standards call for a unified approach to the separate classification and regulation of cybercrimes. For example, the Budapest Convention is a comprehensive international agreement on cybercrime, calling on states to clearly define information and communication crimes in their codes [2]. At the same time, the UNODC (United Nations Office on Drugs and Crime) also calls on states to create special norms on cybercrime [3].

At the national level, the current Criminal Code of the Republic of Uzbekistan contains 278¹ and 278⁹ articles on cybercrimes (for example, illegal access to information systems, distribution of malicious files, and damage to computer systems). Furthermore, Articles 139-140 of the Criminal Code are called defamation and slander, and liability is provided for committing these acts using the Internet. At the same time, Article 141² on the protection of personal data is also included, according to which the dissemination of personal data through the Internet is punishable by a fine of one hundred to one hundred and fifty times the basic calculated value, or deprivation of certain rights for up to three

Date: 19th June-2026

years, or correctional labor for up to two years, in accordance with Part 1 of this article [4]. Today, cases of illegal withdrawal of money from plastic cards by cybercriminals using the Internet are also observed. This is also a component of cybercrime. However, due to the lack of a separate article for cybercrime, they will be held liable under Article 168, Part 3, Clause "g" of the Criminal Code. And for disseminating personal data using the Internet, they will be held liable under Article 141², and for illegal access to computer systems - under Article 278². From this, we can see that if cybercrime-related actions are committed, they can be regulated by various article norms, which can lead to a number of difficulties.

However, the concept of "cybercrime" is not explicitly defined in the legislation, and modern crimes such as cybercrime (e.g., phishing, APK files, Nigerian letters, various types of cybercrime, such as breaking into illegal telephone devices, and embezzlement) are not clearly covered [5]. These legal gaps create a number of difficulties in the process of detecting, investigating, and convicting crimes. Cybercrime involves not only financial damage but also factors affecting social and mental well-being, such as the disclosure of personal information, online bullying, and cybercrime. For example, cases of depression and social isolation have increased among young people due to cyberbullying [6]. Since cybercrimes are transnational, legal cooperation between countries is essential. For example, through the Budapest Convention and UNODC recommendations, countries cooperate in the extradition of cybercriminals, information exchange, and crime prevention. Writing this section enriches the article with scientific and global context. By including this section in the article, it is scientifically substantiated that cybercrimes not only cause financial damage but also have a broader impact on society.

As mentioned above, cybercrime is one of the global problems, not just Uzbekistan's. Some countries have established specific liability standards for this or have adopted separate legislation to combat and prosecute it. One of them is that cybercrimes in Great Britain are legally regulated by the "Computer Misuse Act 1990." This act designates unauthorized access to computer systems, alteration, or corruption of data as a separate crime. For example, according to Article 1 of the Act, unauthorized access to a system is considered a crime, and in this case, damaging information systems through illegal access by the perpetrator entails legal liability [7]. In some cases, if significant damage is caused as a result of a cybercrime, imprisonment for up to four years may be applied during the trial. These legal norms clearly define cybercrimes and allow the court to consider the crime as an act directed at computer systems. The United Kingdom's Computer Misuse Act, which regulates cybercrime by a separate article, indicates that technological crimes require a separate legal approach, as they are committed not within the framework of traditional criminal norms, but in information systems.

One such foreign country, Tanzania, adopted the Cybercrimes Act in 2015, is a special law for cybercrimes, which clearly classifies offenses committed using the internet. The Cybercrimes Act defines the following as specific crimes:

- Unauthorized access to the computer system
- Destruction or modification of electronic data



Date: 19th June-2026

- Spreading false information online
- Online financial (material) fraud [8].

For example, Article 11 of this law establishes liability for unauthorized entry, and such an act may result in a fine or imprisonment for up to several years in court. The existence of such a special article allows for the legal consideration of cybercrime as a separate type in Tanzania. The Cybercrimes Act regulates cybercrimes separately from the general criminal code, detailing them and establishing specific sanctions. This not only simplifies the detection of cybercrimes but also further improves law enforcement practice. Today, national statistics show a rapid increase in the number of cybercrimes in the territory of Uzbekistan. Between 2024 and 2025, the number of cybercrimes in Uzbekistan increased significantly, resulting in a total of 3.7 trillion soums in damages to citizens. At the same time, cybercrimes occupy a high proportion in the overall crime structure - for example, it is noted that 42% of crimes committed in six months were cybercrimes [10].

These figures demonstrate the significant negative impact of cybercrime on society. Among cybercrimes, financial fraud using bank cards is particularly widespread. In 2024, cybercriminals stole 603 billion soums from citizens, a total of 1.9 trillion soums over three years. These circumstances clearly demonstrate the degree of economic damage caused by cybercrime and further strengthen the need to introduce a specific article for this type of crime into criminal legislation.

Moreover, not only financial damage but also the disclosure of personal data, cyberbullying and online psychological pressure, and the illegal withdrawal of money from plastic cards exacerbate the social and psychological consequences of cybercrime. Global scientific research has highlighted the emergence of depression, social isolation, and other mental health problems in society due to cybercrime. This requires the development of legal norms for cybercrimes that require not only technical but also social protection.

It is important to introduce a unified system of cybercrimes into the current legislation and define new types of crimes as separate articles. Specifically, the article "liability for types of cybercrime" should cover such situations as systemic psychological pressure, attacks on personal data or their disclosure, and illegal and unauthorized withdrawal of money from plastic cards. Thanks to this, crimes are clearly defined in the legislation, responsibility for them is clearly defined, and law enforcement practice is simplified.

Furthermore, there is a need for further differentiation of the sanctions system. For example, determining the punishment of a fine or imprisonment based on the material damage and psychological consequences caused by the crime, and making decisions based on mechanisms for compensating the victim for the damage caused should be considered in the legislation. If a person suffers minor material damage, I propose applying penalties such as fines or corrective labor. If a person suffers significant material damage or disseminates information discrediting their honor and dignity, I propose applying penalties such as restriction of liberty or imprisonment. This approach transforms relationships

Date: 19th June-2026

related to material and personal dignity into a more robust protective mechanism against cybercrime.

In conclusion, it can be said that cybercrimes pose a serious threat to modern society, and their consequences are significant at the legal, social, and economic levels. Therefore, improving the Criminal Code, creating separate articles and chapters for cybercrimes, dividing them into sections depending on the types of cybercrimes, updating existing articles, and introducing norms covering modern types of offenses will serve the full protection of the right. In the digital age, criminal law must also develop in accordance with modern requirements.

REFERENCES:

1. UNODC (United Nations Office on Drugs and Crime) site. https://www.unodc.org/documents/organizedcrime/UNODC_Cybercrime_Study_2013.pdf
2. Budapest Convention. November 23, 2001. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
3. UNODC (United Nations Office on Drugs and Crime) site. https://www.unodc.org/documents/organizedcrime/UNODC_Cybercrime_Study_2013.pdf
4. Criminal Code of the Republic of Uzbekistan. 22.09.1994. <https://lex.uz/docs/-111453>
5. European Union Agency for Cybersecurity, Threat Landscape Report <https://www.enisa.europa.eu>
6. UNICEF site. 2020. <https://www.unicef.org/reports/state-of-worlds-children-2020>
7. Computer Misuse Act.1990. <https://www.legislation.gov.uk/ukpga/1990/18>
8. Government of Tanzania, 2015, <https://www.parliament.go.tz>
9. <https://gov.uz/oz/iiv>
10. <https://gov.uz/oz/iiv>

