The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.05 Issue12 2025
PAGE NO. 37-40
DOI 10.37547/ijlc/Volume05Issue12-09

Cybercrimes And Issues Of Protection Against Them: National And Foreign Experience

Djumayev Shokhjakhon Begimkul ugli

Senior lecturer of Training Institute for lawyers, PhD candidate of the Law Enforcement Academy of the Republic of Uzbekistan, Uzbekistan

Received: 30 October 2025; **Accepted:** 19 November 2025; **Published:** 26 December 2025

Abstract: This article examines cybercrime as one of the most serious challenges of the digital age, arising from the rapid development of information and communication technologies. It analyzes the concept and main forms of cybercrime, including hacking, phishing, malware distribution, financial fraud, and cyberterrorism, with reference to major international incidents such as the WannaCry attack and the Equifax data breach. Particular attention is paid to the national legal framework of the Republic of Uzbekistan, including criminal liability for cybercrimes under the Criminal Code and recent institutional reforms. The article highlights the significance of Presidential Resolution No. PR–153 of April 30, 2025, which introduces modern mechanisms for preventing and combating cybercrime, strengthens the responsibility of state bodies and financial institutions, and promotes cybersecurity culture. Furthermore, the study reviews international experience and legal instruments, such as the Budapest Convention, UN initiatives, and EU practices. The article concludes that an integrated legal, institutional, and technological approach is essential for effective cybercrime prevention and digital security.

Keywords: Cybercrime, cybersecurity, information technologies, criminal liability, personal data protection, international legal instruments, Budapest Convention, Uzbekistan legislation, digital security, cybercrime prevention.

Introduction: In the 21st century, the rapid development of information technologies, while providing humanity with numerous conveniences, has simultaneously led to the emergence of new threats, particularly cybercrime. Cybercrime is one of the most pressing problems of the modern era, posing threats to state security, economic stability, and the privacy of citizens.

With the development of technology, methods of committing crimes are becoming increasingly complex, and significant changes are occurring in human worldview.

Cybercrime is a socially dangerous act carried out through information technologies, computer systems, or the Internet.

Cybercrime activity refers to criminal activity aimed at abusing computers, computer networks, or network devices. Most of such acts are committed by cybercriminals or hackers for the purpose of obtaining illegal income.

In legal literature, the following types of cybercrime are distinguished:

- Hacking – unauthorized access to a computer or network;
- Phishing – obtaining users' personal information through fake websites or messages;
- Distribution of viruses and malicious software;
- Financial fraud (through online payment systems);
- Theft and dissemination of personal data;
- Cyberterrorism and attacks on state systems.

At the international level:

WannaCry virus (2017): More than 200,000 computer systems in over 150 countries worldwide were affected. Economic damage amounted to nearly 4 billion US dollars.

Equifax hacking incident (USA, 2017): Personal data of 147 million Americans were stolen.

In the Criminal Code of the Republic of Uzbekistan, liability for cybercrimes is established under the

following articles:

Article 278-1 of the Criminal Code: Violation of informatization rules – punishable by a fine of up to fifty times the basic calculation amount or corrective labor for up to one year;

Article 278-2: Illegal (unauthorized) use of computer information – punishable by a fine from one hundred to three hundred times the basic calculation amount or corrective labor for one to two years, or restriction of liberty for one to three years, or deprivation of liberty for up to three years;

Article 278-3: Preparation, transfer, or distribution of special tools intended for illegal (unauthorized) use of computer systems and telecommunication networks – punishable by a fine of up to two hundred times the basic calculation amount or corrective labor for up to one year;

Article 141-1: Violation of privacy (committed through various information technologies and gadgets) – punishable by a fine from fifty to one hundred times the basic calculation amount or compulsory public works for up to three hundred hours, or corrective labor for up to two years.

On April 30, 2025, the President of the Republic of Uzbekistan adopted Resolution No. PR–153 "On Measures to Further Strengthen Activities to Combat Crimes Committed Using Information Technologies," which can be considered an important step toward introducing modern mechanisms to combat cybercrime.

According to this resolution, the following provisions were established:

The Ministry of Internal Affairs is designated as the authorized body responsible for establishing a unified practice of combating cybercrime in the Republic of Uzbekistan, coordinating the activities of all relevant state bodies and institutions, and organizing targeted cooperation in this field;

Strict responsibility is imposed on all relevant state bodies, organizations, banks, payment system operators, and payment organizations to take all necessary measures to prevent cybercrime and enhance the population's cyber culture;

For banks, payment system operators, and payment organizations, ensuring the interests and financial security of their clients is defined as a priority task in organizing their daily activities;

The Ministry of Internal Affairs, together with interested ministries and departments, by the end of 2025, shall comprehensively study current practices, modern requirements, and advanced foreign experience, and develop a draft law "On Combating Crimes Committed Using Information Technologies," defining priority areas, operational mechanisms, and the specific responsibilities of state bodies, banks, payment system operators, and payment organizations in preventing and detecting cybercrime.

The following proposals were approved:

(a) Establishing administrative and criminal liability for persons (drops) who allow the use of bank cards, bank accounts, SIM cards, and electronic wallets (electronic accounts) registered in their name for committing cybercrime;

(b) Improving existing norms establishing liability for non-compliance with information security and cybersecurity requirements, even in the absence of harmful consequences, from the perspective of the emergence of liability;

(c) Introducing procedures for compensation of material damage caused by cybercrimes committed as a result of non-compliance with information security and cybersecurity requirements by banks, payment system operators, payment organizations, and other organizations, at their expense;

(d) Strengthening criminal penalties for crimes in the field of information technologies and illegal activities involving the attraction of funds and other property;

(e) Establishing the use of information technologies in committing crimes as an aggravating circumstance affecting liability and punishment;

(f) Introducing procedures that define clear deadlines and simplify mechanisms and requirements for ensuring the execution of requests and decisions of law enforcement agencies related to bank secrecy.

Within the structure of the Prosecutor General's Office department supervising the execution of legislation in internal affairs bodies, a Cybercrime Legality Enforcement Division consisting of 6 staff units is to be established. Additionally, 44 staff units are allocated to establish its groups within regional prosecutor's offices and the Transport Prosecutor's Office. These structures will exercise prosecutorial supervision over the legality of investigations and detection of cybercrimes by internal affairs bodies.

Within the structure of the Digital Forensics Research Institute of the Law Enforcement Academy, a Center for Assisting in Combating Cybercrime and Digital Investigation is to be established, with the following main areas of activity:

(a) Developing substantiated recommendations and implementing them into law enforcement practice by studying pre-investigation materials, administrative offense cases, and criminal cases using scientific approaches to identify causes and conditions

facilitating cybercrime;

(b) Identifying existing problems in the practice of detecting and investigating cybercrimes and developing scientifically grounded proposals to eliminate them;

(c) Providing scientific and methodological support to improve the effectiveness of investigative activities and enhance the educational process in the field of cybercrime.

The following methods of protection against cybercrime are also recommended:

Using strong passwords.

One of the simplest measures is to use strong, unique passwords for all online accounts. Avoid common passwords such as “password” or “123456” that are easy for hackers to guess. Instead, create passwords using a combination of uppercase and lowercase letters, numbers, and symbols. Consider using a password manager to generate and store secure passwords.

Keeping software up to date.

Always keep device software up to date, including operating systems, web browsers, and applications. Developers regularly release security patches to fix vulnerabilities that hackers may exploit. Enable automatic updates whenever possible.

Being cautious with links and attachments.

A common method cybercriminals use to spread malware is through malicious links or email attachments. Be cautious when clicking links from unknown sources. Even if an email appears legitimate, hover over the link to check whether the URL matches expectations. Open attachments only if they come from trusted and expected sources.

Being cautious with public Wi-Fi networks.

Public Wi-Fi networks in cafes or airports may be convenient but pose security risks. Avoid accessing sensitive accounts such as banking or email services over public networks.

B y 2025, the total global cost of damage caused by cybercrime is expected to reach 10.5 trillion US dollars. In 2023, the United States recorded the highest average total cost of data breaches, amounting to 9.48 million US dollars.

The most important international legal instrument in combating cybercrime is the Council of Europe Convention on Cybercrime (Budapest Convention), adopted on November 23, 2001. This convention legally defines the concept of cybercrime and establishes mechanisms for criminal liability for offenses such as illegal access, data interference, computer fraud, and copyright violations. It also regulates rapid information exchange between states, the collection of electronic evidence, and extradition issues.

Within the framework of the United Nations, combating cybercrime is also a key area. In particular, the UN Convention against Transnational Organized Crime (2000) and its protocols treat cybercrime as a form of transnational organized crime and serve to strengthen legal assistance and cooperation between states. In addition, special expert groups under the UN General Assembly operate on issues of information security and cybercrime.

In the practice of the European Union, the NIS Directive (on Network and Information Security) and the European Cybercrime Centre (EC3) under Europol play an important role. These structures coordinate the activities of member states in detecting, preventing, and investigating cybercrime.

In the Asia-Pacific region, joint cybersecurity strategies have been developed within the frameworks of APEC and ASEAN, aimed at protecting information infrastructure and taking rapid measures against cybercrime.

CONCLUSION

In conclusion, combating cybercrime requires a comprehensive approach. This process involves legal regulation, implementation of international standards, development of public-private partnerships, and the application of scientifically grounded strategies, which serve as key factors in ensuring cybersecurity and strengthening the digital resilience of society.

REFERENCES

1. The Constitution of the Republic of Uzbekistan // URL: https://lex.uz/docs/-6445145
2. The Civil Code of the Republic of Uzbekistan // URL: https://lex.uz/docs/180552
3. The Criminal Code of the Republic of Uzbekistan // URL: https://lex.uz/docs/111453
4. The Code of Administrative Responsibility of the Republic of Uzbekistan // URL: https://lex.uz/docs/97664
5. Law of the Republic of Uzbekistan No. URL–547 dated July 2, 2019 “On Personal Data” // URL: https://lex.uz/docs/-4396419
6. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 570 dated October 5, 2022 “On Approval of Certain Regulatory Legal Acts in the Field of Processing Personal Data” // URL: https://lex.uz/ru/docs/-6225462
7. Resolution of the Cabinet of Ministers of the

Republic of Uzbekistan No. 71 dated February 8, 2020 “On Approval of the Regulation on the State Register of Personal Data Databases” // URL: https://lex.uz/docs/-4729730