CRIMES RELATED TO INFORMATION TECHNOLOGIES AND PROSPECTS FOR COMBATING THEM

Matyozov Shodlikbek Ozodovich
Employee of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
https://doi.org/10.5281/zenodo.18721639

Abstract: This article presents various views and considerations on combating crime related to information and communication technologies in our country, addressing problematic issues and certain challenges in this area. It also highlights that a significant portion of crimes committed today occur in the field of information technology and, based on this, provides specific scientific terms related to cybercrime. The article examines all aspects of the issue, including trends in the development of information and communication technologies for combating crime and their future prospects.

Keywords: information and communication technologies, combating crime, development prospects, problems, cybercrime, internal affairs bodies.

Over the last five years, the number of cybercrimes in the republic has increased from 4,865 to 62,440. As a result, citizens have suffered damages amounting to 3 trillion 730 billion soums. Of this amount, 1 trillion 890 billion soums corresponds to the first 11 months of 2025. By the end of 2025, the total damage amounts to 1.9 trillion soums. The number of cybercrimes in Uzbekistan is on the rise. It is noted that between 2021 and 2025, the number of such crimes in the republic increased tenfold (from 4,865 to 62,440). Consequently, citizens incurred damages of 3 trillion 730 billion soums.

To gain experience in combating crimes in this field, a system has been established for exchanging information with foreign partners, involving their leading personnel, and training specialists. Specifically, the Ministry's Academy has launched a personnel training program in the "Combating Crimes in the Field of Digital Technologies" specialization, and starting this year, an additional 100 cadets have been enrolled. Furthermore, as part of the "One Million Uzbek Coders" project, a procedure has been established for admitting candidates who have successfully completed the program to this educational track at the Academy.

A digital laboratory for combating crimes in the field of information technology has been created. 483 malicious programs of the "phishing" type, aimed at illegally withdrawing funds from citizens' bank accounts, the most dangerous and causing damage to many citizens, were identified and their activities were suspended.

2,424 crimes related to violations of legislation in the sphere of crypto-asset turnover have been identified. Funds in the amount of 76 billion soums, obtained through criminal means, were prevented from being taken out of the territory of the republic in the form of crypto.

In cyberspace, 3,843 internet resources associated with promoting threats to public order, humiliation of the honor and dignity of the individual were blocked, and 1,508 malicious links promoting fraud were suppressed.

Crime related to bank cards accounted for 98%.

Here, to make it understandable to readers, we will highlight some terms related to cybercrime.

Cybercrime is crimes committed using electronic devices and computers. These crimes include the theft of personal data, fraud, and hacking of social networks.

a crime committed using information technologies - a crime committed using information systems, telecommunication networks, special software or hardware, as well as the World Wide Web, the beginning and end of which also occur in cyberspace;

"Hacker" (English hacker - intruder) - a polysemantic term in the field of computer technologies and programming. A "computer hacker" is a person who deliberately bypasses computer security systems.

Phishing is a type of fraud on the Internet, the purpose of which is to obtain the user's identification data (bank card numbers, logins and passwords) and their confidential information.

Smishing is a type of phishing that involves obtaining individuals' payment details related to online payment resources or obtaining personal information that allows access through SMS notifications.

Vishing - an attempt to obtain confidential information from the cardholder by introducing oneself by phone as a bank employee, a buyer, or another person, or to encourage certain transactions through an account (payment card).

Pharming is a type of phishing that directs users to fake sites to install malware, steal passwords, accounting data, or confidential information such as bank data.

Carding - carrying out transactions using a payment card without the participation of the owner.

Pretexting - the misappropriation of confidential information (date of birth, TIN number, passport or PIN number) without arousing interest, based on a pre-planned scenario, by introducing oneself as another person through a phone call or an SMS message sent to an email.

Dos, Ddos - a cyberattack aimed at refusing service, in which a person temporarily or indefinitely suspends host services connected to the network, making the machine or network resource unusable for serving users.

Malware - a set of software tools that, without the user's knowledge, enter the system and destroy or steal information that harms its operation. This includes viruses, Trojans.

SQL Injection - an attack on illegal access or manipulation of a database by ensuring that incoming text information from the user is executed directly as an SQL query.

Brute Forse is an attempt to log in to the authentication system by sequentially automatically testing the user's name and passwords. This attack can also be applied to cryptographic functions.

Man in the middle - an attack carried out by illegally entering the communication channel between the user and the server, listening to, modifying, or resubmitting data.

Zero Day (hardware or software) is an attack that uses a vulnerability that is not detected or eliminated by the manufacturer, and it is impossible to detect it and take countermeasures. This attack will take place before security patches are released.

Cyberbullying is a set of aggressive actions carried out with the aim of continuously inflicting psychological or physical harm on a person in the form of insult, slander, threats,

harassment, or other forms using social networks, telecommunication networks, or other Internet capabilities.

Deepfake is fake media content (video, audio, or image) that imitates the appearance, voice, or movements of a person, created with the help of artificial intelligence or deep learning technologies, and is often used for the dissemination of false information, fraud, or other criminal purposes.

A financial pyramid is an illegal business model that involves paying income to previous participants in exchange for the funds of new participants, where the main income comes from attracting new participants[2].

More than 60% of cybercrimes are committed through malicious links and programs. One of the main methods is accessing victims' bank cards or phones with malicious links and mobile applications. It has become easier to collect, analyze, and transmit information about crimes, their perpetrators, and methods of combating them. It should be noted that the development of this mechanism is supported by the draft UN Convention on Combating the Use of Information and Communication Technologies for Criminal Purposes, approved by the UN General Assembly in December 2019 and adopted on June 29, 2021[3]. Information and communication mechanisms in the field of combating crime are systems used to collect, analyze, and transmit information about crimes and criminals, which also include various technologies such as databases, communication networks, and software used by law enforcement agencies to combat crime.[4]

The following main trends in the development of information and communication technologies can be identified:

1. Use of technology. The development of artificial intelligence (AI), the Internet of Things (IoT), and other technological resources is expected to increase the effectiveness and accuracy of crime control mechanisms. For example, AI can be used to analyze data and identify patterns of criminal behavior.

2. Data integration. With the advent of new technologies, more information from various sources, such as law enforcement agencies, medical and financial institutions, is expected to be integrated. This contributes to a more complete understanding of criminal behavior and the development of more effective strategies to combat it.

3. Improving communication.

Information and communication technologies can improve communication between law enforcement agencies and other actors involved in combating crime and contribute to more effective coordination of efforts. For example, mobile applications and other technologies can facilitate communication between police and other security agencies.

Thus, it is clear that information and communication technologies are gradually developing and are an excellent assistant in solving crimes, and further prospects for the development of this mechanism are expected. The following main directions for the development of cybertechnologies in the fight against crime can be distinguished:

- Robotization of the activities of entities maintaining public order;
- Forms of remote control and supervision of persons who may commit crimes;
- Use of artificial intelligence technologies and big data analysis;
- Use of mass media and other promising areas.

However, in the sphere of combating crime, there are some problems that hinder and complicate the development of information and communication technologies. For example, one of the most global problems is the lack of standardization and compatibility between different systems and databases. This problem threatens the impossibility of accessing data on an international scale.

The second most common problem is ensuring confidentiality and protecting personal data. Today, many people know how to use Internet resources and can hack any website, password, and database. Despite strict laws protecting personal data in other countries, this cannot stop criminals.

It is very important for combating crimes committed in the field of information technology, as criminals are finding new ways and means of committing them, and society and the state are suffering from cyberattacks. The lack of funds for the optimal development, development, and implementation of new technologies in the field of crime prevention is also an important problem.[6]

Today, the most common methods of committing cybercrimes in our country are as follows.

1. Persons who introduced themselves on the telephone, mainly in Russian, as employees of a bank or mobile payment system (employees of payment organizations such as "Click," "Payme," and other payment systems)

2. Coverage of "Interest-free online loan" in fake website links on the social networks "Telegram," "Instagram" and "Facebook" (for example, on behalf of "Asaka," "Anor" and other banks)

3. Stimulate interest by offering items at affordable prices on OLX and other platforms (Rental, phone, and other items).

4. In "E-Shop" online stores engaged in online trade (with prepayment)

5. Coverage of state bodies on fake website links in the social networks "Telegram," "Instagram," and "Facebook" (Provision of material assistance)

6. Increasing funds in a short time, registering through fake websites and transferring money to their accounts, as well as explaining investments in various types of fraudulent projects (scam projects) (Trade, USM Holding, MetaGo)

7. By contacting through fake accounts (profiles) in the social networks "Telegram," "Instagram," and "Facebook," you can claim that you have inherited a large sum of money or won a lottery (by stating that you or your spouse are originally from Uzbekistan and that there is a large prize).

8. Related to Internet games ("PUBG," "FreeFire" and other Internet games)

9. Informing those in need of charity posted on social networks "Telegram," "Instagram" and "Facebook," that they will supposedly give charity (having SMS codes claiming to transport money from Dubai, America and other countries)

The main reasons are:

- insufficient literacy of the population in the field of information technologies (insufficient cyber literacy);
- trustfulness (mentality) of the population;
- non-selectivity of territory and borders for committing crimes through the global Internet and telecommunication systems (transboundary);

- weak security measures (availability of gaps) in the programs of banks and other organizations;

- commission of crimes by persons with special skills using high-tech or modified programs (special subject);

- legalization (withdrawal of funds) of funds obtained by criminal means in electronic and crypto-wallets registered in foreign countries;

Recommendations include:

1) Do not answer incoming calls made through suspicious and unauthorized numbers.

2) Never trust people who introduce themselves as employees of a bank or mobile payment system, as they have no right to ask you for personal and bank plastic card information. Don't forget, if someone asks, it means they're a fraud!

3) Don't tell anyone about the special (5-digit) SMS code sent to you! SMS codes are requested only by fraudsters!

4) As soon as funds are withdrawn from your account for unknown reasons, immediately call the bank trust numbers on the back of your plastic card and block the card.

5) Do not register on social networks through suspicious links and do not enter bank plastic card details.

6) Don't believe false news through social media about large sums of money being inherited or about winning a lottery!

7) Don't trust scammers who promise to multiply your money in a short time!

8) Do not deposit the down payment before receiving the goods!

9) Before selling your phone, delete your mobile app account!

10) Do not issue a bank plastic card on your behalf to anyone in exchange for funds!

11) Every day, make sure that no additional (foreign) devices are connected in the mobile applications on your phone!

On December 23, 2025, the Board of the Central Bank of the Republic of Uzbekistan adopted Resolution No. 35/14 "On Minimum Requirements for Ensuring Information Security and Cybersecurity and Preventing Fraud Cases in the Provision of Remote Financial Services to Individuals by Credit and Payment Organizations, Payment System Operators." This resolution also strengthens the security of bank plastic card users and measures to protect their funds. However, this decision was set to take effect three months after the date of adoption of the approved decision.[7] Therefore, the security of bank plastic card users remains at the current level.

In conclusion, reforms in the field of information technology, the introduction of new systems, including artificial intelligence, play an important role in the fight against crime, as it contributes to the collection, analysis, and subsequent reporting of various data in the media or the exchange of information on an international scale. Thanks to the development of artificial intelligence, Internet technologies, and other resources, the level of crime detection is increasing, and the effectiveness and accuracy of mechanisms allow solving even the most complex cases.

References:

1. https://kun.uz/kr/news/2025/12/23/ozbekistonliklar-11-oyda-kiberjinoyatlardan-1-trln-890-mlrd-som-zarar-kordi. Date of application 06.02.2026.

2. B.A.Rajabov et al. Guide for employees of internal affairs bodies. Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan Tashkent 2025. Pages 125-128.
3. https://www.un.org/ru/documents/treaty/A-RES-79-243. Date of application 06.02.2026.
4. Ulyanov M.V. Fight against crime in the field of information and communication technologies in the context of quarantine measures / M.V. Ulyanov. Text: Law // National Security. - 2020. - P. 52-61.
5. Gribanov E. V. Prospective directions for the development of crime prevention in the field of cybertechnologies / E. V. Gribanov. Text: Law // Society and Law. - 2021. - No. 4 (78). - pp. 22-27.
6. Kumisheva M.K., Fedina L.M. Current Problems of Combating Crimes in the Sphere of Information and Communication Technologies / M.K.Kumisheva, L.M.Fedina. Text: Law // Education and Law. - 2022. - 8. - Б. 259-261.
7. https://lex.uz/uz/docs/8007760. Date of application 06.02.2026.