

ISSUES RELATED TO CRIMES COMMITTED ON THE
GLOBAL INTERNETPulatov Azizkhon Saidakbarovich^{1*}¹Associate Professor at the University, of Public Safety of the Republic of
Uzbekistan*azizpolatov6027@gmail.com | ORCID: <https://orcid.org/0009-0000-9214-800X><https://doi.org/10.5281/zenodo.23661640>

Abstract: This article analyzes issues related to crimes committed on the global internet network. The article also thoroughly examines issues such as the practical differences between cybercrimes and traditional crimes, methods, and the methodology of pre-investigation checks. In addition, issues related to cyber fraud are described.

Keywords: global internet, digitalization, electronic, criminal law policy, crime, cyber-crime, form, method, reforms, judicial practice, traditional, remote.

Today's modern society is fundamentally different from the traditional society of twenty years ago. These changes are primarily linked to achievements in science, information technology, and the digitalization policy pursued by the president. At the same time, it is difficult to imagine human life and activity without information technologies. This means that information technologies have already become an integral part of human life and activity.

It should be noted that the great achievements of human civilization, in turn, did not fail to have an impact on the criminal world. Previously, crimes related to theft, fraud, and psychotropic substances were committed mainly by traditional methods, i.e., by performing direct and active actions at the crime scene, but today, as a result of the rapid development of information and communication technologies, it is possible to commit and even manage crimes remotely. This, in turn, has led to an increase in cases of criminal encroachments on information (objects belonging to the individual, society, and the state) protected by the constitution and laws.

At a meeting held on March 12, 2026, President of the Republic of Uzbekistan Shavkat Mirziyoyev raised issues regarding increasing the effectiveness of combating cybercrime and organized crime, as well as preventing offenses committed using information technology. He noted that over the past six years, the number of appeals regarding cybercrimes in our country has increased 48 times. Last year, 82% of fraud crimes and 76% of theft crimes were committed in cyberspace. The material damage caused to individuals and legal entities exceeded 2 trillion soums¹.

Additionally, according to Gazeta.uz, the number of cybercrimes in Uzbekistan increased nearly 11-fold from 4,865 to 62,440 between 2021 and 2025. As a result, a total of 3 trillion 730 billion soums of damage was caused to citizens. Of these, 1 trillion 890 billion soums accounted for 11 months of the current year².

¹ <https://president.uz/uz/lists/view/9009>

² <https://www.gazeta.uz/uz/2025/12/24/cybercrime/>

ORCID: Saidakbarovich: <https://orcid.org/0009-0000-9214-800X>

According to A.A. Matchanov, due to the insufficient and incomplete level of protection of computer systems, the proliferation of personal computers, and the automation of almost all business processes, which cause damage to users, it is necessary to create modern programs to prevent risks³.

It is clear that the changes occurring in the forms and methods of crime in the digital world are raising the question of what solutions the state can use against modern crime. In particular, in the Decree of the President of the Republic of Uzbekistan No. UP-204 dated November 3, 2025, "On approval of the 'Digital Prosecutor's Office - 2030' Strategy and measures for its effective implementation," the issue of developing and implementing new approaches that meet modern requirements for the effective investigation and fight against crimes committed in the digital world has been prioritized⁴.

Thus, the state is improving criminal legislation to protect the interests of the individual, society, and the state. Specifically, by the Law of the Republic of Uzbekistan No. ZRU-1155 dated June 22, 2026, a clause "committed using an information system, including information technologies" was added to Clause "v" of Part 3 of Article 168 of the Criminal Code⁵. Also, in the Criminal Code, Chapter XX1 is dedicated to "Crimes in the field of information technology." The process of digitalization has also had an impact on the institution of proof in criminal procedural legislation. At the same time, the Code of Criminal Procedure has been supplemented with new articles 2041-2042 regarding electronic data and digital evidence⁶. Furthermore, the Decree of the President of the Republic of Uzbekistan No. PP-3723 dated May 14, 2018, "On measures to fundamentally improve the system of criminal and criminal procedural legislation," includes issues such as conducting criminal proceedings in electronic form.⁷

In general, the implementation of the idea of digitalization of criminal proceedings in Uzbekistan can be conditionally expressed in three main directions: 1) recognition of the priority of the model of electronic information and digital evidence in criminal procedural evidence; 2) development of legislative provisions defining the conduct of criminal proceedings in electronic form; 3) the use of artificial intelligence in judicial practice, that is, and the implementation of a software tool in sentencing, that is, the "electronic assistant" system.

Thus, the state's priority policy in the field of priority criminal law in the context of digitalization is aimed at minimizing the risks and threats associated with the use of new information technologies in criminal proceedings by improving criminal and criminal procedure legislation, strengthening and developing procedural guarantees related to the interests of the individual, society, and the state.

As noted above, incidents related to cybercrime are mainly committed at a long distance from each other, even while being in different countries. Indeed, in practice, there are cases where participants in criminal proceedings are located in different regions, and in some cases,

³ Матчанов А.А. Кибержиноятлар тушунчаси ва уларга қарши курашишнинг ҳуқуқий асослари. EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES. Volume 2 Issue 12, December 6, Special Issue 2022. - Б. 115.

⁴ Ўзбекистон Республикаси Президентининг 2025 йил 3 ноябрдаги ПФ-204-сонли «Рақамли прокуратура — 2030» стратегиясини тасдиқлаш ва уни самарали амалга ошириш чора-тадбирлари тўғрисида»ги Фармони.

⁵ Ўзбекистон Республикасининг 2026 йил 22 июндаги ЎРҚ-1155-сонли Қонуни.

⁶ Ўзбекистон Республикасининг 2024 йил 21 ноябрдаги ЎРҚ-1003-сонли Қонуни.

⁷ Ўзбекистон Республикаси Президентининг 2018 йил 14 майдаги ПҚ-3723-сонли «Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида»ги Қарори

ORCID: Saidakbarovich: <https://orcid.org/0009-0000-9214-800X>

in different states. This, in turn, creates great difficulties for the officials of the pre-investigation (investigation) bodies involved in solving the crime (speed, labor, proof). Take, for example, the crime of cyberfraud, which is especially widespread today worldwide, committed remotely. Usually, a criminal, while abroad, performs an action via the Internet. One of the most common forms of Internet fraud is the attraction of consumers through advertising and various online offers, in which expensive goods are offered at unusually low prices, but after payment by the buyer, the goods are not delivered at all. Individuals are also promised the opportunity to win various competitions, receive a scholarship, or get a job, in exchange for which they are required to pay a certain amount of money in advance, a registration fee, or a guarantee. Another method of fraud involves offering housing at allegedly low prices, claiming regular installment payments, and issuing fictitious contracts. In addition, the sale of counterfeit or counterfeit goods, which are presented as genuine products, is also one of the most common types of online fraud. This situation deserves special attention, as it is widespread, and such violations can be committed not only on social networks, but also on other e-commerce and communication platforms on the Internet.

In this case, the victim of fraud must immediately report the crime to the internal affairs bodies as soon as they realize they have been deceived. The timely implementation of such an appeal is important for the prompt identification and recording of traces of the crime, the preservation of digital evidence, the identification of the person who committed the crime, and the adoption of measures to compensate for the damage caused.

In this case, the bodies conducting the pre-investigation check shall first obtain an explanation from the victim of the crime. In order to clarify the situation, it is necessary to inspect the digital information carriers in the victim's possession, usually a mobile phone. In such cases, the official conducting the pre-investigation check shall conduct an inspection of the mobile phone with the involvement of a relevant specialist.

One of the most important issues in this process is that the official conducting the pre-investigation check must take prompt measures related to the bank plastic card of the victim. In particular, the details of the bank plastic card belonging to the victim will be provided to the cybercrime unit within the internal affairs system, and measures will be taken to block it temporarily through the "cold block" system. As a result, operations carried out using this bank plastic card will be temporarily suspended and aimed at preventing the illegal transfer of funds to other accounts. Furthermore, the prosecution authorities will request information from the Central Bank regarding all monetary transactions made using the bank plastic card belonging to the victim of a crime. This information is of great importance in determining the circumstances of the crime, determining the direction of the movement of funds, and identifying the persons involved in the crime.

According to E.G. Kravets, "in order to ensure the prompt and effective fight against these types of crimes, it is important to integrate all regional internal affairs bodies with the system of control over monetary concepts. This approach appears as an effective solution that meets the needs arising in modern reality. The digitalization of investigative activities should primarily be based on the possibility of remotely collecting evidence and recording it in a procedural manner.

ORCID: Saidakbarovich: <https://orcid.org/0009-0000-9214-800X>

One of the most important factors in the rapid detection of digital crimes is, first of all, the modern material and technical equipment of law enforcement agencies, as well as the provision of necessary software and information systems to ensure their activities. In this regard, special software and technical means that allow for the rapid search, collection, recording, storage, and analysis of digital data in the process of identifying, solving, and investigating crimes are of great importance.

This criminal act must be qualified under paragraph "v" of part three of Article 168 of the Criminal Code of the Republic of Uzbekistan. This provision provides for an aggravating circumstance when fraud is committed using an information system, including information technology. Cyber fraud and similar criminal acts, unlike traditional fraud, are committed not by directly deceiving a specific person or abusing their trust, but by unauthorized access to a computer system and performing certain actions on it. As a result, such actions lead to the secret seizure of another's property or the acquisition of rights to another's property. The objective side of cyber fraud consists of actions aimed at obtaining another's property or the right to it using information technologies, information systems, or telecommunications means. An important point here is that unauthorized access to any computer does not automatically mean cyber fraud. If a person enters the information system and seizes another's property or acquires the right to it through this action, a causal link exists between the property result and the method of the act. Cyber fraud, as a rule, is committed with direct intent. The perpetrator is aware of the socially dangerous nature of their actions, knows that they are illegally seizing another's property or property right, and wants such a result to occur.

In this case, the primary goal is self-interest, i.e., the seizure of another's property or the acquisition of another's property right. For example, a person convinces the victim that he is a fake bank employee, obtains an SMS code from him, and transfers funds from his account to his own account using this code.

In conclusion, based on the analysis of crimes committed using information and telecommunications networks and in the field of computer information, the following main features can be identified:

the latent level of crimes in the field of computer information is high, which is primarily due to the complexity of their detection, as well as the rapid development and use of new information technologies for criminal purposes;

the level of education and specialized knowledge of persons committing this type of crime is one of the characteristics of these crimes;

a high level of special technical knowledge and skills is not always required to commit many crimes committed using information and telecommunications networks;

crimes committed using information technologies increasingly increase threats to the security of information related to citizens' financial data, bank details, and other funds.

Based on the above analysis, it can be concluded that in the investigation of fraud and other property crimes committed in the virtual space, the cardlock system can be an important technological tool for the rapid detection of the movement of funds and the prevention of their subsequent illegal transfer. However, its practical effectiveness is closely linked not only to the blocking of cards or the restriction of account operations, but also to the possibility of identi-

lying funds obtained as a result of a crime, determining their legal status, and restoring the violated property rights of the victim.

Therefore, one of the urgent tasks is to develop a special procedural mechanism for returning temporarily restricted funds to the victim through the cardlock system, ensure its compliance with the norms of the Criminal Procedure Code on the return and seizure of property, and improve electronic cooperation between banks, payment organizations, and law enforcement agencies.

In our view, the establishment in the Criminal Procedure Code of a special procedure for identifying, storing, seizing, and returning to the legal owner funds transferred to bank accounts as a result of a crime and temporarily restricted by authorized bodies, as well as ensuring the rights of third parties in this process, is a promising direction for improving legislation in this field. This procedure serves to accelerate the compensation of damage caused by a crime, prevent the concealment and distribution of funds obtained from criminal activities, and ensure a balance between legality and the protection of property rights in criminal proceedings.

References / Foydalanilgan adabiyotlar / Литература

1. <https://president.uz/uz/lists/view/9009>
2. <https://www.gazeta.uz/oz/2025/12/24/cybercrime/>
3. Матчанов А.А. Кибержиноятлар тушунчаси ва уларга қарши курашишнинг ҳуқуқий асослари. EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES. Volume 2 Issue 12, December 6, Special Issue 2022. - Б. 115.
4. Ўзбекистон Республикаси Президентининг 2025 йил 3 ноябрдаги ПФ-204-сонли «Рақамли прокуратура - 2030» стратегиясини тасдиқлаш ва уни самарали амалга ошириш чора-тадбирлари тўғрисида»ги Фармони.
5. Ўзбекистон Республикасининг 2026 йил 22 июндаги ЎРҚ-1155-сонли Қонуни.
6. Ўзбекистон Республикасининг 2024 йил 21 ноябрдаги ЎРҚ-1003-сонли Қонуни.
7. Ўзбекистон Республикаси Президентининг 2018 йил 14 майдаги ПҚ-3723-сонли «Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида»ги Қарори