
# ANALYSIS OF THE CAUSES AND CONDITIONS ENABLING CRIMES IN THE FIELD OF INFORMATION TECHNOLOGIES

**S.S.Safarov**
Responsible officer of the Main Directorate of Personal Security of the Ministry of Internal Affairs of the Republic of Uzbekistan, Lieutenant Colonel
https://doi.org/10.5281/zenodo.15393870

**Abstract**. The article analyzes the causes and conditions of crimes committed in the field of information technology and concludes that regular study of these issues will serve to conduct general preventive measures in the city of Tashkent.

**Keywords**. Cause, condition, objective, subjective, factor, preventive measures.

Globally, attention to the legal and organizational aspects of effective operational-search activities by authorized state bodies, based on international law requirements, serves to reliably protect human rights, freedoms, and legitimate interests. In particular, it aids in promptly compensating for material damages caused to individuals and legal entities, and quickly solving crimes committed using information technologies in the context of modern globalization processes. According to data, cybercrimes are committed every 14 seconds worldwide, and between 2020 and 2024, $6 trillion in material damage is expected to be caused to individuals and legal entities globally[1], violating their property rights.

Research results from Europol experts show that the scale of crimes in the digital space is increasing, and the list of cyber threats is expanding. Currently, crimes using information technologies can involve both specific cybercrimes (phishing, spam dissemination, unauthorized access to computer data, computer sabotage, etc.) and other serious non-cyber crimes (money laundering, drug trafficking, human trafficking, arms trafficking, etc.).

This fact demonstrates that collecting electronic evidence is becoming increasingly relevant in combating information technology crimes and investigating any crime.

In the current era of rapid information technology development, the dissemination of false information that degrades personal honor and dignity, defamation, insults, and the spread of materials imbued with ideas of extremism, separatism, and fanaticism that threaten public safety and order, as well as the distribution of terrorist organization attributes or symbols, is becoming commonplace.

According to analysis, 1.6 percent of those subjected to cyberattacks today are damaged by banking trojans. Internet sources indicate that Uzbekistan is among the countries with the highest proportion of users who have fallen victim to banking trojans.

In the process of increasing globalization, major banks, financial companies, internet providers, government organizations, and even law enforcement agencies worldwide are suffering significant losses from such threats, attacks, and cybercriminal assaults.

Currently, the infrastructure of the Republic of Uzbekistan in the field of information and communication technologies is growing. In 2019, industry enterprises provided services worth 10.6 trillion soums, resulting in the industry's share of total services in the republic reaching 5.7 percent. In the first half of 2020, services worth 2.9 trillion soums were provided. In 2019, industry enterprises exported services worth $176.0 million, while in the first half of

2020, service exports by industry enterprises amounted to $36.9 million. The number of industry enterprises reached 8,277, of which 2,519 were software production companies. As a result, the number of Internet service users exceeded 22 million. Due to the convenience, speed, and economic efficiency of information and communication technologies, people's trust and need for these technologies are growing. It is precisely this need and trust that crimes, now termed cybercrime, are negatively impacting. According to statistics, about 7 billion people are currently covered by mobile communication networks, and the annual material damage caused by cybercrime amounts to 1% of the world's GDP[2].

In 2019, the damage caused by cyberattacks to companies worldwide increased 1.6 times compared to 2018, if in 2018 the amount of damage caused by cyberattacks amounted to 1.5 trillion dollars, then in 2019 this figure amounted to 2.5 trillion dollars. According to experts, the scale of cyberattacks will increase year by year, and by 2030, the world economy will suffer losses of $120 trillion. The main reason for this is the growing technological trends that can become targets of cyberattacks. In particular, in 2023, 1 trillion devices could be connected to the internet, and in 2024, 80% of people will have their own "avatars" (symbolic heroes) in the digital world[3].

The reasons that contributed to the commission of crimes in the field of information technology are understood as objective and subjective factors that contribute to the commission of crimes in this area.

The change taking place in society, the rapid development of the information technology sphere, and the lack of security measures in accordance with these processes are objective factors.

A subjective factor is the commission of crimes in the sphere as a result of indifference or insufficient cyber-hygienic literacy of citizens.

The causes of crimes related to the sphere committed in the city of Tashkent are:

accelerated development of information technologies and the Internet;

Increased interest of youth in information technologies;

the prevalence of uncontrolled or informal use of information technologies;

gain the trust of citizens only through economic interests;

Simplicity and quick-wittedness of individual citizens;

high motivation of individual citizens to obtain easy income;

citizens' interest in information technologies;

shortage of teachers teaching information technology;

Theft of citizens' property by persuading the person committing the crime through material gain;

citizens' interest in earning income without labor, easily, and easily;

disclosure of personal data, failure to use a protection system.

lack of formation of legal culture of citizens in the field of information technologies;

unfamiliarity of citizens with the protection of personal data;

a large number of cases of prepayment without any guarantees in online sales on social networks of the world Internet;

a high need for citizens to have access to information and financial interest through its dissemination;

easy dissemination of personal data through social networks and mobile applications;

today, in the era of globalization, as a result of the growing interest in information technologies, citizens are increasingly believing false information;

broad opportunities in information technologies and a high interest of citizens in online income generation and the use of fake websites;

provision of personal data (telephone passport, plastic card numbers) by citizens to unknown persons;

insufficient level of citizens' literacy in the field of information technologies;

among them is the addiction of young people to various internet games.

Based on a systematic study of these reasons, firstly, carry out constant explanatory and promotional work among the population; secondly, effective cooperation with mobile companies such as "UZMOBILE GSM," "Beeline," "UMS," "Usell" and "Perfectum," "UZMOBILE CDMA" in carrying out targeted and targeted general preventive measures. At the same time, it is necessary to introduce a filtration system in companies to identify suspicious subscribers and ensure that citizens do not answer suspicious calls by displaying on the phone screen, instead of a number, the message "a cybercriminal is calling." Mobile companies will introduce an additional fee for this service, which will prevent cyberattacks on funds in the client's bank card account. Of course, this issue should be implemented, first of all, by sending SMS messages to citizens (subscribers) in Uzbek, Russian, English, and other languages once by mobile companies with a full explanation; thirdly, when conducting general preventive measures, it will be beneficial to constantly explain to citizens in a simple, clear, and fluent way that they will turn off the SMS message service, such as receiving money on a bank plastic card, withdrawing it, or not responding to various SMS messages, and not telling anyone a secret code as an SMS message.

In addition, by placing videos on the topic "Prevention of crimes in the field of information technologies" in mahalla telegram groups by prevention inspectors serving 9255 mahallas of the republic, it is possible to increase the vigilance of citizens in the early prevention of crimes in this area to a certain extent. For example, 24.7 percent of the total population of 3 million 188 thousand 782 citizens living in the territory of the city of Tashkent joined the Telegram group of 585 mahallas.

By strengthening these preventive measures and including all citizens living and working in the administrative territory in Telegram groups, early prevention of crimes related to the sphere will be achieved, and the rights of citizens to property inviolability will be ensured.

Conditions enabling the commission of crimes in the field of information technologies are understood as favorable conditions created for the theft of citizens' property in cyberspace as a result of the failure to take the necessary organizational, legal, and technical measures.

The conditions that contributed to the commission of crimes in the sphere in the city of Tashkent are:

non-compliance of various Internet applications with established security requirements;

openness of personal data, a low level of protection;

insufficient level of security of applications of banks and payment systems (Uzcard and Humo), organizations (Payme, Click, Beepul, etc.);

Insufficient security measures in the information system;

the presence of legal gaps in the legislation;

ineffective organization of the activities of information security control bodies;

the presence of shortcomings in the "anti-fraud" system[4] in the information and software of most banks, that is, the absence of a client protection system;

the possibility of anonymity on the Internet creates difficulties in identifying and prosecuting criminals;

Failure of the heads of individual organizations with the status of a legal entity to take a serious approach to ensuring security in the field of information technologies and to cooperate with the relevant state bodies;

popularization of the internet and digital technologies;

insufficient provision of information security in the work of legal entities;

the possibility of opening two or more bank plastic cards in the name of one person;

the absence of geographical restrictions on the commission of crimes related to the sphere, that is, the possibility of the perpetrator moving from any point in the world;

the presence of legal nihilism in society, that is, the disobedience of some citizens to the law;

leakage of personal data from payment systems into social networks;

leakage by banks of their clients' personal data;

place personal data of individual citizens on social networks;

The lack of control by Telegram and Instagram messengers;

failure of commercial banks to take safety measures when issuing online loans to citizens;

entry of information by citizens through various false links;

excessive advertising on social networks;

crimes in the field of information technology are often committed on an international scale, however, due to the ineffectiveness of rapid information exchange between states, the question of the responsibility of persons who have committed crimes remains open;

the lack of a serious approach to ensuring cybersecurity for clients of enterprises, institutions, and organizations, including commercial banks, creates favorable conditions for committing crimes in the field of information technology.

Systematic analysis of the above-mentioned objective and subjective factors serves the purposeful and targeted implementation of general preventive measures, ensuring the early prevention of cybercrimes.

In conclusion, it should be noted that knowledge of the causes and conditions that allowed employees of internal affairs bodies to commit crimes in the field of information technologies contributes to the effective organization of their activities.

## References:

1.https://www.tadviser.ru/index.php/ Losses from cybercrime (accessed electronically: 11.04.2025).

2.A.K.Rasulev. Improvement of criminal-legal and criminological measures to combat crimes in the field of information technologies and security. Abstract of the dissertation of Doctor of Science in Law (DSc). - T.: 2018. - P. 5.

3.From the website Interpress.uz: The damage from cyberattacks is increasing. http://interpress.uz/archives/4170 (accessed electronically: 12.04.2025).

4.FRAUD-analysis is an innovative anti-fraud system that ensures the safety of remote customer service and protects against the actions of attackers.