European Journal of Innovation in Nonformal Education (EJINE)
Volume 4 | Issue 11 | Nov - 2024 ISSN: 2795-8612

Tactical Problems and Solutions for Exposing the Crime of Fraud, Which is Carried Out in Tashkent Using Information Technology

Muxammatqulov Shohruhbek Erkin ugli
Ministry of Internal Affairs Academy of the Republic of Uzbekistan "Department of Emergency Search" independent researcher

A B S T R A C T
This article deals with the tactical problem and solutions of exposing the crime of fraud carried out in Tashkent using information technology and problems of operational personnel with investigative, interrogators and specifics in exposing fraud committed using information technology, relevant conclusions and proposed interpretations on the disclosure of these crimes based on the opinions of specialists in this field on the effective conduct of cooperation.

A R T I C L E I N F O
Article history:
Received 20 Oct 2024
Received in revised form 21 Oct 2024
Accepted 22 Nov 2024

Keywords: technique-technology, information exchange, crime, fraud, cybercrime, cyberspace, cybercrime, internet fraud, experience, electronic address, account.

Introduction. On January 19, 2024, the law”on amendments and additions to the criminal, criminal procedure codes of the Republic of Uzbekistan and the administrative responsibility code of the Republic of Uzbekistan " came into force. At this point, the question arises, that is, what are the importance and important aspects of the law?

- Provided great facilities in finding Internet Information and necessary information.
- At the same time, it is no secret that this network is used even when carrying out some non-linear work.

At the next time, there are cases of blocking (blocking) the mobile devices of individuals as well as accounts or channels on social networks and messengers by sending malware, deleting, changing or withdrawing their data, demanding money or other material benefits. In particular, cases of falsification of the photo, voice and other biometric data of individuals using special programs are also missing.

This was facilitated by the fact that the legislation did not clearly express the state of the commission of a crime using information resources. In order to eliminate this gap, Article 165 of the Criminal Code (extortion) created the need to fill the disposition with the concept of “shameful fabrications”. To this end, the above-mentioned law was passed. The first part of Article 165 of the Criminal Code was supplemented with the words “to injure or destroy property or destroy it” and then “to destroy, change, withdraw or block the information resource of the victim, or to intimidate him with the distribution of shameful fabrications”.

Another important new norm in the law is associated with crypto – assets. Despite the fact that crypto-assets are recognized as property rights and there are relevant legislative acts regulating the industry, the codes on criminal and administrative responsibility for the illegal turnover of crypto-assets, in particular,

for the activities of illegal May, did not establish liability measures.

Due to the absence of a separate article in criminal law, in 2021-2022, 40 persons were charged with other articles of the Criminal Code in 15 criminal cases related to the activities of illegal turnover of crypto-assets, including illegal mining. Therefore, the codes of criminal and administrative responsibility were supplemented with new norms related to "violation of legislation in the field of crypto-asset turnover" and "unlawful implementation of May's activities", including the corresponding liability for the implementation of the activities of the secret may. According to him, in the code of administrative responsibility, violation of legislative documents in the field of crypto-asset turnover was defined as an administrative offense, and administrative responsibility was established for illegally obtaining, transferring or exchanging crypto-assets, carrying out the activities of service providers in the field of crypto-asset turnover without obtaining a license in the prescribed manner.

Analysis of the literature on the subject. Also, criminal liability was established in the event that these actions were committed after the application of administrative punishment. At the same time, in the code of administrative responsibility, it was established as an administrative offense to carry out May's activities in violation of the established procedure, as well as to carry out May's activities in a much larger and larger amount (from 300 to 500 times BHM) in violation of the established procedure.

In turn, if these actions were committed after the administration of administrative punishment, they will cause criminal liability, according to the appendix to the Criminal Code. In the development of this law, the legislation of Estonia, Georgia, Ukraine, Russia, Belarus, the Republic of Kazakhstan was studied and used. The law serves to fully direct all forces and means in exposing, combating, and investigating crimes committed using information technology.

Today, globalization has a certain influence on all processes in socio-political life in all regions of the Earth. The inhomogeneity of such influence is closely related to the political, economic, social, informational, spiritual capacities of the countries of the world and geopolitical factors. To reduce the negative impact of globalization on regions, and, on the contrary, to strengthen the positive impact, to deeper understand the essence of this phenomenon, the study of its own characteristics is one of the important requirements of today. Because, the possibilities of influence of globalization are clearly manifested against the background of global informatization, characterized by the fact that there is no barrier or limit to the spread of information flow in regions.

Head of State Sh.Mirziyoev, in his work" strategy of New Uzbekistan", commented on the process: "under the influence of globalization and information attacks, various destructive ideas, threats and risks against our national self and spiritual values are growing. The risk of threats such as terrorism, extremism, transnationalism and cybercrime, human trafficking, drug trafficking is increasing. Harmful ideas, concepts and views that are completely alien to our national spirituality, without breaking the limit, without expressing, without saying, being an "uninvited guest", we cannot even turn a blind eye to our household, society, at worst, the Immaculate Heart and mind of our murgush children".

As noted above, the strengthening of the globalization process is ensuring that the impact opportunities of global informatization increase. In its place, global informatization is more manifested in ideological and ideological processes. "The transformation of Uzbekistan into a democratic country where law and justice are firmly established, the formation of an independent and strong sudhuquq system – was put on the agenda as one of our highest goals... It is known that the present time is a period when the entire world economy is undergoing a process of digitization, and "green" technologies and innovative development are gaining priority for the development of any sphere and business," the minister said. In fact, the information technology that serves for the development of our country is also becoming more and more updated today, which is developing rapidly. Indeed, in recent decades, Information Technology has penetrated into such important areas of state and human life, including communication, public services, the banking and financial system, health care, education. Naturally, this attracted criminals to this area. Because the possibility of committing this type of crime even at a long distance and the fact that an individual is unlikely to be identified is causing them to grow year after year in World coverage. This imposes the task of law enforcement agencies, including employees of investigative bodies, to prevent

crimes not only within the borders of our country, but also in its cyberspace, and to investigate crimes committed in information networks.

In this field, many processualist and criminalist scientists are conducting research today. The reason is that the new type of crime assumes the development of a new investigative methodology and new tactics for conducting investigative actions. In particular, from foreign scientists K. Brown, D. L'uis, F. Williams, B. Colin, D. Shinder, D. Dennings, and Ye from the CIS.A. Russkevich, G.R. Grigoryan, Ye.A. Markova and N.V. Letyolkin's carried out their research work in this field. While the above-named scientists in their research work focused mainly on crimes committed in the field of Information Technology and their legal description, within the framework of our study, issues of public cooperation in the investigation of crimes committed using information technology are studied.

Research methodology. The article explores the issue of further improving the bond of cooperation between investigative bodies and the public in order to effectively use the available forces and opportunities in society in identifying, exposing and preventing crimes committed using information technology at the pre-trial stage of the case. During the study, methods of analysis, comparative, deduction, logical, statistical, systematic approach were used. The results of the study show that, according to the International Organization Symantec Security for security in relation to cyber-attacks, now every second of every 12 people in the world are becoming victims of cyberattacks.

The types of cybercriminals are also increasing to kundankun. There are many views regarding the classification of crimes of this type. However, the most important of them is established through international legal documents. In particular, the Council of Europe Convention on Cybercrime (Budapest City, November 23, 2001) categorizes crimes committed in the field of information technology into 4 groups. On January 28, 2003, the adoption of an additional protocol to the convention in question in the city of Strasbourg added another 1 group of crimes to the classification of cybercrime.

In Uzbekistan, cybercrime has also increased 8.3 times in the last three years, accounting for 5% of total crime. For example, crimes related to cyberspace fraud increased by 13 times, theft by 20, and crimes related to extortion, slander and defamation by 4.9 times [13]. In Tashkent alone, there were 735 (10 in 2020) cases of fraud using computer equipment and mobile communications, 1,052 (24 in 2020) cases of unauthorized intrusion into personal account number management programs, a total of 1,787 (34 in 2020) crimes by the Investigative Department under the Iibb of Tashkent City during 2021.

The participation of specialists in conducting investigative actions is rightfully an indispensable condition for the effectiveness of the investigation. It must be involved in investigative actions in all cases where it is not only necessary to participate, but also possible to participate. Today in our practice there are also a number of problems with ensuring the participation of a specialist in investigative actions on crimes committed in the field of Information Technology. The reason is the identity of the specialist, the requirements for him and the procedure for involving him in the case are not sufficiently covered in Criminal Procedure legislation. This has been the subject of various controversies between scholars and practitioners. We found it necessary to dwell separately on the determination of competence of specialists involved in criminal proceedings. If it is possible to compare, the fact that when the chess piece reaches a certain stage, it becomes a Pharisee and, as if protecting its King, a specialist who is following a step on the Criminal Procedure board has reached a high level, serves to protect the truth in criminal proceedings, to ensure justice. Because a single word, a single argument can affect the final decision of a criminal case. Professional competence, on the other hand, is the acquisition by the Professional of the knowledge, skills and qualifications necessary to carry out professional activities and their high degree of application in practice. At the same time, one of the main reasons for insufficient use of the knowledge of specialists in criminal cases in this category can be considered as a lack of information about the specialty of specialists, their activities, where they conduct services. As its solution, a group of scientists suggested that investigators create reference books or registers with the address and telephone numbers of research institutions, higher education institutions, specialized institutions, public associations (cultural, historical, numismatic and other) through a service-use tariff. Other authors put forward the idea of creating a program that would determine when to call a specialist.

From our point of view, the best way to connect the public with the investigative and investigative bodies in advance of the investigation is to draw up memorandums on mutual cooperation between the responsible organizations and the IIV, in which the specialists we need work. On the basis of this memorandum, it is necessary to create a single e-base with a recommendation of enterprises, organizations and institutions in the direction of Information Technology and information on specialists who can participate in investigative actions through the written consent of the individual, documents confirming their identity and competence, length of Service and activities, residence and working address, telephone numbers, electronic address. When a specialist is involved in a criminal case, it is necessary to be recorded directly through this base, to know if the employee of its head is actually participating in the investigation, to maintain the payment of the specialist for working hours and serve as the basis for the payment by the IIO for his participation in the investigation. The creation of such a base gives us a number of advantages:

First of all, before the investigation, the time of the employees of the investigation and investigative bodies is saved.

Secondly, the quality and effectiveness of criminal proceedings increases, since it is precisely where to look for a specialist whose participation is required and who to look for.

Thirdly, procedural outputs are reduced, since the search for a specialist begins in the area closest to the Department under investigation.

Fourth, this cooperation will prevent censorship from being allowed once it is structured on the basis of a memorandum between the responsible organizations.

If we also consider several problems that are encountered in practice in the investigation of crimes in the field of information technology, directly related to banking and payment systems.

First, when the bank, payment organizations and payment operators are presented with unsubstantiated request letters on the criminal case filed (with the sanction of the prosecutor), without fully responding to the request letters by the bank and payment system operators, the execution of the request letters is ensured from 10 to 15 days, which, in turn, causes serious difficulties in exposing these types of crimes from a hot.

Secondly, as a result of the absence of a centralized system for providing information about a bank plastic card or electronic money transfer, it is necessary to supply a request letter to 8-10 agencies such as payment system operators (Uzcard, HUMO), payment organizations (Click, PayMe, Orange) to obtain information on transactions of plastic cards in a single criminal case under prosecutor's sanction.

In order to eliminate these problems, as well as to further improve the cooperation of investigative agencies with the public, we offer the following:

First of all, a direct exchange of information should be established between the operators of the payment system, payment organizations, payment agents and subagents of the Ministry of internal affairs.

Secondly, it is advisable for the central bank to form a single automated system for providing information regarding a bank plastic card based on a request from law enforcement agencies.

Thirdly, the development of a mobile application reporting “SOS” on Lost and stolen bank plastic cards and the formation of a unified database on them will bring a number of facilities for exposing crimes.

Fourth, the involvement of public representatives, such as citizens engaged in electronic and Lute segregation, in the identification of an unknown person who committed the crime during an investigation into undisclosed criminal cases.

Conclusions and suggestions. In conclusion, it should be noted that in order to overcome the existing threats, when we all – both law enforcement agencies and citizens-head out of one collar and, if we are aware, tie our own destiny with the fate of the motherland and avoid indifference, chip in the implementation of the strategies and reforms set by our president, one body-it is one soul.

REFERENCES

1. Jinoyat va jinoyat-protsessual qonunchiligi tizimini tubdan takomillashtirish choratadbirlari to'g'risida [O'zbekiston Respublikasi Prezidentining Qarori, 14.05.2018 yildagi PQ-3723-son]. https://lex.uz/ru/docs/3735818
2. O'zbekiston Respublikasi Konstitutsiyasi. O'zbekiston Respublikasi qonun hujjatlari to'plami. 2007. - № 15. mod. 152; - 2008. - № 52. mod. 510; - 2011.- № 16. mod. 159; - 2014. - № 16. mod. 176; - 2017. - № 14. mod. 213, № 22. mod. 406, № 35. mod. 914.
3. O'zbekiston Respublikasining ayrim qonun hujjatlariga o'zgartish va qo'shimchalar kiritish to'g'risida [O'zbekiston Respublikasining Qonuni, 18.04.2018 yildagi O'RQ476-son]
4. O'zbekiston Respublikasi qonun hujjatlari ma'lumotlari milliy bazasi. https://www.uzavtoyul.uz/ru/page/hujjatlari malumotlari-milliy-bazasi.html
5. Кибальник А.ГОДА Современно международное уголовное право: понятия, задачи, принципы. - СПб., 2003. - С.188.
6. Иногамова-Хегай Л.В. Преступление по международному уголовному праву и его закрепление в национальном уголовном праве // Международное и национальное уголовное законодательство: проблемы юридической техники: Матер. III Медждунар. науч.-практика. конф. - М., 2004. - С.334.