Western European Journal of Linguistics and Education
Volume 2, Issue 4, April, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed
This article/work is licensed under CC Attribution-Non-Commercial 4.0

FEATURES OF THE INVESTIGATION OF CRIMES OF THEFT OF OTHERS' PROPERTY COMMITTED WITH THE HELP OF INFORMATION TECHNOLOGY

Muxsinjon Sultonov
independent researcher of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Bakhtiyorjon Murodov
Head of the Department of "Preliminary Investigation and Criminalistics" Academy of the Ministry of Internal Affairs Doctor of Juridical Science (DSc), professor

ANNOTATION. The article highlights the features of interrogation of the victim and suspect, which are considered the most important investigative actions in the investigation of crimes related to the theft of other people's property using information technology. Opinions were also expressed on other investigative actions aimed at improving the quality of crime investigations.

KEY WORDS: information technology, theft, bank card, operational search activities, investigative actions, search, inspection, interrogation, information constituting bank secrecy.

The investigation of crimes related to the theft of other people's property using information technology differs from the investigation of other types of crimes by its particular complexity.

This, in turn, is due to the uniqueness of this type of crime and the fact that they can be committed in uncertain conditions, as well as be of an interregional and international nature.

The sufficiency and completeness of evidence play an important role in ensuring a high-quality investigation of crimes of theft of other people's property using information technology. In this case, operational search activities aimed at collecting evidence are of great importance [1].

At the same time, when carrying out investigative actions, it is necessary to approach the issue based on the meaning of the terms provided for by regulatory legal documents, international and national standards in the field of information technology.
In particular, Article 169[2] of the Criminal Code, part 3, paragraph "b" defines liability for committing theft through unlawful (unauthorized) access to or use of an information system.
In this case, it is necessary to pay attention to the content of the concept of information system, that is, it is assumed that the crime was committed not through the use of information technology, but through penetration or use of an information system.
The information system includes all organizationally organized information resources, information technologies and communication means that ensure the collection, storage, retrieval, processing and use of information [3]. Information technology is a set of methods, devices, techniques and processes [4] used to collect, store, search, process and disseminate information, and have a broader meaning compared to the concept of an information system.

Western European Journal of Linguistics and Education
Volume 2, Issue 4, April, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed
This article/work is licensed under CC Attribution-Non-Commercial 4.0

It should be noted that in accordance with the law[5], the investigator, prosecutor and official of the body carrying out the pre-investigation are obliged to initiate a criminal case in all cases where there are reasons and sufficient grounds that the crime of theft of other people's property using information technologies carried out within the limits of their powers.

For this purpose, applications from individuals, enterprises, institutions, organizations, public associations and officials, media reports, or any other information indicating the commission of a crime is a reason for the initiation of an investigation to determine the presence of signs of a crime. Once information indicating the presence of signs of a crime have been obtained, it then becomes a reason for initiating a criminal case [6].

The identification of signs of a crime is carried out by collecting evidence and information during pre-investigative actions before the start of the investigation.

However, in a number of cases it is necessary to additionally check whether the materials received by the inquiry and investigative bodies are sufficient grounds for initiating a criminal case. Therefore, some researchers [7] have proposed conducting investigative actions on crimes of theft committed with the help of information technology, based on the analysis of specific situations indicated below:

- a crime was reported by the victim, but the presence of signs of a crime was not fully proven;
- materials collected as a result of operational investigative activities have been transferred to the investigation and there are sufficient grounds to initiate a criminal case.

In investigative practice[8] in the manner established in relation to reports of crimes related to fraud:

- investigators will conduct an investigation and make a legal decision;
- documents on crimes in the field of information technology are initially studied by investigative authorities;
- based on the conclusion of the investigative authorities, an appropriate decision will be made.

In our opinion, the application of such investigative practice to the procedure for considering applications related to crimes concerning the theft of others' property using information technology may not be effective enough.

Because during the time elapsed before the submission of the conclusion by a higher authority, you can lose evidence exposing the crime and transfer the funds received to offshore accounts.

As a result, it will not be possible to expose the suspect even if he/she agrees to initiate criminal proceedings in the future, or the quality of compensation for damages will decrease.

It should be noted that some investigative actions carried out for crimes of theft of other people's property committed with the use of information technology are of great importance in collecting evidence proving that a person has committed a crime.

According to experts, interrogation of the victim, interrogation of the suspect, interrogation of the accused, inspection of the scene of the incident, inspection of objects, documents, seizure, interrogation of witnesses of crimes committed, robbery of other people's property, committed using information technology through investigative actions in proving the guilt of persons. It gives a positive effect in more than 80 percent of cases.

So, let's dwell on the features of the interrogation of the victim and witnesses and its significance. During the investigation, the general rules of interrogation, the procedure for interrogating the victim and witness are observed in accordance with criminal procedural legislation.

Before starting the interrogation, in the process of finding out their personal data, it is necessary to pay attention to whether they have basic skills in using computers, mobile devices and technical

Western European Journal of Linguistics and Education
Volume 2, Issue 4, April, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed
This article/work is licensed under CC Attribution-Non-Commercial 4.0

means. Clarification of the following questions during interrogation is an important factor in fully disclosing the essence of the case and establishing evidence:
when the account was registered on an online trading platform, social media platform or email service;
the phone number connected to the personal account of interest, or whether a virtual number has been used;
placing advertisements on online trading platforms;
when and for what purpose a subscription to some dubious resources on the Internet and social networks has been made;
virtual friends, correspondence with them, whether they are familiar with one another in real life;
with whom and for what purpose was there a corrspondence on one's profile on the online platform;
the status of whether services should be sold or provided through online platforms;
the content of messages received on the device, including the presence of suspicious texts;
messages leading to a malicious link, information identifying the user who sent them (phone number, nickname, channels on which he is a member, correspondence and other personal information), message content;
advertisements posted online under an account used by the victim or witness, indicating a telephone number;
technical changes observed in the user's device after clicking on a malicious link (blocking, short-term shutdown, spontaneous shutdown, etc.);
redirection to other resources when entering via a malicious link, their URL stored in the memory of the web browser, as it looks, and its image saved as a screenshot;
information about the fact of cashing out funds from a bank card or electronic wallet, the amount of these funds, the resource to which the funds were sent;
that a bank card number and passwords have been disclosed to others;
that there has been an attempt to gain illegal access to an account in the past, and if so, when and by whom.
According to experts, it is important to establish a transaction of theft of funds, identify the device directing the funds (the person who ordered the operation), and its user in crimes of theft of personal property committed using information technology.
By answering the questions asked during the above-mentioned interrogation, conditions will be created to find out the device used by the suspect to divert funds.
To identify the devices to which the victim's bank card is connected, it is necessary to first obtain information about bank secrecy, as well as determine additional information associated with the real IP address.
In turn, during the investigation, the investigator himself has the right to obtain information directly related to bank secrecy. Therefore, a decision made on this matter can be presented to payment systems with the approval of the prosecutor.
However, the possibility of obtaining a response is limited to sending an investigative task to mobile operators to obtain information about the communication between subscribers or subscriber devices.
Nevertheless, according to the criminal procedure law, all enterprises, institutions, organizations, officials and citizens are obliged to execute written orders and decisions of the investigator in accordance with the law.[9]

Western European Journal of Linguistics and Education
Volume 2, Issue 4, April, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed
This article/work is licensed under CC Attribution-Non-Commercial 4.0

In our opinion, in these cases, one of the main criteria for ensuring law and order is to provide the authorities of inquiry and investigation with the authority to obtain information about connections between subscribers and subscriber devices in the process of their work.

To this end, we believe that the investigative action to obtain information about communications between subscribers or subscriber devices is reflected as a new norm in the legislation, and the procedure and conditions for its conduct are also defined, which ensures the quality of the investigation.

Also, when interrogating a suspect or accused, it is necessary to check their circumstances in detail, check their place at the time of the crime, whether they have a payment card in their name, when the bank account number was opened, which bank it belongs to, whether there is an SMS notification about bank transactions account, what phone number he or she is connected to, the amount of money coming in each month, how much money is spent, whether he or she has a social media account, when and on which social network he or she signed up, who else has the right to access this account, when they last logged into the account, through what device, phone, tablet or other device they logged in, their correspondence – all these circumstances must be made clear in the presence of the suspect or the accused.

Because fraud aimed at acquiring property is considered completed when said property passes into the illegal possession of the perpetrator or other persons and they have a real opportunity to use or dispose of it at their own discretion. According to the law, due to the fact that a person has the opportunity to actually manage funds in a bank from the moment they are received (transferred) to their bank account, transferring these funds to a bank account, or when a person or persons receive them from the account of the owner of funds through fraud or breach of trust, a crime should be considered complete from the moment of transfer [10].

In addition, investigation, search and seizure during the investigation of crimes of theft of other people's property committed by an investigator using information technology, inspection of a device, virtual treatment with the participation of an expert, stopping all banking operations, checking computer information of equipment or networks, appropriate verification is possible [11] .

In this case, it is necessary to pay special attention to maintaining the integrity of evidentiary information by limiting the possibility of remote access to devices that are the subject of the investigation.

From the above it is clear that criminals pay special attention to the use of modern technologies in order to ensure the anonymity of their socially dangerous acts.

This is especially clearly seen in the case of investigating crimes related to the theft of someone else's property using information technology. Therefore, when investigating crimes related to the theft of someone else's property using information technology, investigators are required to be "one step ahead" of the perpetrators of this type of crime, being aware of modern information and communication capabilities.

Also, in order to ensure the quality of the investigation and compensation for the harm caused to the victim, it is proposed to make the following changes and additions to the legislation:

- introduction of investigative actions for inquiry, inquiry of investigators to obtain information about connections between subscribers or subscriber devices in connection with the need to conduct an investigation against any person involved in a crime case;
- establishing the procedure for applying the existing practice of providing information constituting bank secrecy to the Accounts Chamber, the Ministry of Justice, justice authorities, law enforcement

Western European Journal of Linguistics and Education
Volume 2, Issue 4, April, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed
This article/work is licensed under CC Attribution-Non-Commercial 4.0

agencies, the tax service in cases under their control [12] and in the future also to internal affairs bodies in cases under their control;
- introduction of the practice of excluding the participation of impartial persons through the use of continuous video surveillance in the investigation and search for crimes related to the theft of other people's property using information technology.

References:

1. Комаров И.М. Проблемы расследования скимминговых преступлений // Преступность в сфере информационно - телекоммуникационных технологий: проблемы предупреждения , раскрытия и расследования преступлений: сборник материалов всероссийской научнопрактической конференции (Воронеж, 16-17 апреля 2015 г.) / под ред. д-ра юрид. наук А.Л. Осипенко. - Воронеж: Воронежский институт МВД России, 2015. С. 13.;
2. https://lex.uz/docs/111453;
3. https://lex.uz/docs/83472;
4. https://lex.uz/docs/83472;
5. https://lex.uz/docs/111460;
6. https://lex.uz/docs/111460;
7. Н.И. Малыхин, С.В. Кузьмин. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети интернет/Вестник Томского государственного университета. 2021. № 462. С. 238–247. DOI: 0.17223/15617793/462/29.;
8. Ўзбекистон Республикаси ИИВнинг 2017 йил 12 июндаги «Ўзбекистон Республикаси ички ишлар органларида суриштирув ва дастлабки терговни ташкил этиш тартиби тўғрисидаги йўриқномани тасдиқлаш ҳақида»ги 100-сонли буйруғи;
9. https://lex.uz/docs/111460;
10. https://lex.uz/ru/docs/6523582;
11. И. И. Файзуллаев Ахборот технологиялари соҳасидаги жиноятларни тергов қилиш хусусиятлари/ «Тергов амалиёти» журнали/3/2020. 11-сон. Б.6;
12. https://lex.uz/ru/docs/41760.