



Journal Website:
<https://theusajournals.com/index.php/ijlc>

Copyright: Original content from this work may be used under the terms of the creative commons attributes 4.0 licence.

METHODS AND MEANS OF THEFTING OTHERS' PROPERTY USING INFORMATION TECHNOLOGIES

Submission Date: November 16, 2023, Accepted Date: November 21, 2023,

Published Date: November 26, 2023

Crossref doi: <https://doi.org/10.37547/ijlc/Volume03Issue11-09>

Murodov Bakhtiyorjon Bakhodirjonovich

Head of the Department of “Preliminary Investigation and Criminalistics” Academy of the Ministry of Internal Affairs Doctor of Law, professor, Uzbekistan

Sultonov Muxsinjon Mukimovich

Independent applicant, Academy of the Ministry of Internal Affairs, Uzbekistan

ABSTRACT

The article discusses the methods, main elements and means of committing crimes of stealing someone's property using information technology, and also studies the legislation of foreign countries on crimes related to the theft of someone's property using information technology, the role of information technology in the process of theft of someone's property.

KEYWORDS

Information technology, information system, artificial intelligence, malware, technical devices, robbery, theft.

INTRODUCTION

The method of crime, the activities and actions of the suspect, methods of robbery are the main elements of the theft of other people's property using information technology.

According to the generally accepted approach, the method of crime is considered in the form of stages, consisting of a sequence of actions to prepare the crime, commit it and conceal the traces of the crime. According to everyone, adherence to this approach is

effective when using methods of stealing other people's property using information technology.

Criminologically important signs characterizing the method of theft of someone's property using information technology: the actions of the suspect (the use of information technology and devices and the practice of electronic money transfer), as well as the corresponding signs characteristic of the main forms and types of theft of someone's property.

The actions of a suspect in the theft of someone's property using information technology may include such signs as preparation for a crime, its commission and concealment, as well as the disposal of stolen property.

METHOD

The actions underlying the method of stealing someone's property using information technology can be divided into the following:

- 1) actions performed in the information environment;
- 2) actions typical for the use of devices and other means of theft related to the field of information technology.

In particular, actions in the information environment are illegal (unauthorized) use of computer information provided for in articles 169, paragraph b of the Criminal Code of the Republic of Uzbekistan, part three of Chapter XXI of the Criminal Code, that is, information in information and computing systems, networks and their components, the use, manufacture or transmission and distribution of special software or technical funds for the purpose of illegal (unauthorized) use of protected computer systems, as well as telecommunications networks, illegal modification of information, stored in information and computing systems, networks and their components of a computer system, its damage and deletion, as well as the creation of computer programs or making changes to existing programs for the purpose of intentionally entering false information into it, deleting, blocking, changing, copying or intercepting information stored or transmitted to the computer system without permission, and also the development of special virus programs, including their intentional use or intentional distribution and other actions. These

actions express information and methods of its processing.

Also, these actions can be carried out separately or together in the process of implementing the method of theft. In our opinion, despite the fact that they can be performed only with the help of information technology, they should be considered as a separate group of actions on the commonality of signs and the mechanism of their implementation, as well as a group of actions on the use of means and devices of the field of information technology.

When committing certain types of theft, actions in the field of information technology are often carried out in conjunction with their other type - illegal access to the information system. In our opinion, unauthorized access to the information system should be considered as theft committed with the help of information technology [1].

If, in the process of stealing someone else's property, signs of unauthorized access to an information system are discovered, this crime will be qualified in accordance with article 2782 of the Criminal Code of the Republic of Uzbekistan and the corresponding article, which provides for criminal liability for theft of wonderful property, depending on the presence of elements of the crime.

The use of information technology tools and devices by a suspect to rob someone's property can be assessed as a set of actions describing a method of stealing someone's property using information technology.

Since the use of techniques, methods, tools, devices (for example, special software, equipment, etc.) in the field of information technology for the purpose of theft is one of the important signs of the criminal aspect of the theft of other people's property with the

help of information technology, it is necessary to clarify the concept of these technologies.

According to the philosophical concept, technology is a dynamic system that includes information, knowledge, tools, devices, operations and management activities [2]. It is also possible to imagine information technology as a specific mechanism for processing information and working with it. Thus, information technology should be understood in a broad sense as a field of knowledge, including techniques, means and methods of processing information and working with it, as well as managing information processes using specially designed tools and devices. The legal definition of information technology is given in Law No. 560-II of December 11, 2003 "On Informatization", according to which it is noted that "information technology is a set of methods, devices, techniques and processes used to collect, store, track, process information and distribute it [3].

All means of stealing someone else's property using information technology, depending on the type of their device, can be divided into three large groups: 1) Hardware, 2) Hardware and software 3) software tools. In fact, there is no such clear separation, since it is believed that hardware, as a rule, has an information system associated with the software serving it.

In our opinion, based on the above, the means of stealing someone else's property using information technology can be classified as technical devices with software or hardware-software and software products or software tools.

Technical devices and software products used as means of committing a crime can be classified as officially authorized and licensed means, as well as unlicensed, but harmless means, as well as illegal,

malicious information technologies (for example, a computer virus). Official or legal types of information technologies (both software products and technical devices) must be licensed, certified in accordance with the procedure established by law, and also comply with certain standards. Therefore, signs such as the presence or absence of licenses, certificates, compliance with standards and technical requirements must be established for each individual hardware, hardware-software and software product.

These requirements are a guarantee of the full implementation of the principle of a unified approach to the regulation of cybersecurity, provided for in Article 7 of the Law "On Cybersecurity". After all, according to this principle, "a unified approach to the regulation of the cybersecurity industry is provided by the introduction of a unified state system of cyberbullying information systems and resources aimed at organizing the process of developing and implementing software and technical means for processing and protecting data, monitoring and controlling information technologies. Ensuring cybersecurity should be carried out on the basis of unified approaches when forming a system of legal, administrative and technical regulation of relations in this area [4].

Technical devices associated with various devices and software, the technical component of the field of information technology is a means of stealing someone's property using information technology, the principle of operation of which is based on the interaction of software with this mechanism of the technical device: personal computers, laptops, tablet personal computers, smartphones, mobile computers and other devices.

Modern research shows that theft of other people's property (article 169 of the Criminal Code), fraud

(article 168 of the Criminal Code) can be committed using malicious computer software.

Thus, the theft of funds using malicious computer programs and other means of payment is carried out as a means of committing crimes. There are two main types of such robberies with the help of malicious computer programs: theft of funds from bank accounts and robbery of electronic funds [5]. According to experts of the banking sector, such a type of malicious computer program as the Trojan computer program is a frequently used tool of robbery in the field of remote banking [6]. A Trojan computer program can be used to illegally obtain information outside the jurisdiction of the owner of a technical device, for example, to commit theft or fraud.

An electronic document should be created taking into account the possibility of perception of this document by participants of electronic document flow [7]. Thus, an electronic document should be defined as a complex structured object consisting of various types and forms of information.

A number of authors believe that based on the general concept of a document as a material object and the concept of documented data recorded on a material data carrier, an electronic document can be recognized as material evidence [8]. Material evidence may be objects and documents provided for by the Criminal Procedure Code. An electronic document is a type of document that can exist in relation to a material carrier. Thus, an electronic data carrier containing an electronic document should be considered as material evidence.

There are many classifications of types of electronic documents. Nevertheless, in the context of the mechanism of theft of other people's property, it is necessary to classify electronic documents according

to their purpose and structure. Thus, files are divided into: documents, database files, log files, temporary and system files, and other types [9]. The purpose and structure of a document or file depends on what digital traces remain in the process of using this crime tool and where to look for them.

Depending on the role of information technology in the process of plundering someone else's property, two types of committing these crimes can be distinguished:

- 1) the use of information technology as an additional means of committing a crime (in comparison with traditional forms of ownership);
- 2) the use of information technology as the main means of committing a crime (in relation to electronic means of payment).

Thus, information technologies that contribute to the hidden theft of someone's property are tools and devices that allow you to secretly acquire someone's property or provide access to information necessary for its acquisition.

When studying the legislation of foreign countries, we can see that the fourth part of article 188 of the Criminal Code of the Republic of Kazakhstan [10] for theft committed by unauthorized access to an information system or by changing information transmitted over telecommunications networks, article 177.2. .3-1 of the Criminal Code of the Republic of Azerbaijan for theft committed using information carriers or information technologies and the first part of article 158 of the Criminal Code of the Russian Federation, paragraph "d", establishes criminal liability for theft committed using bank accounts, as well as electronic means of payment (in the absence of signs of a crime provided for in article 159.3 of this Code).

Due to the use of information processing tools as the main instrument of crime, the possibility of embezzlement of funds is created. For example, a group of individuals conspired to steal funds by secretly entering information obtained illegally using a copy of real computer data about bank card details. The technical instrument of the crime was a device designed to obtain computer data from a bank card [11]. In the example given, information about bank card details was a means of accessing transactions with property, and the technical device into which this information was copied was a means of information processing.

Electronic payment instruments, including contactless payment cards and electronic wallets, occupy a special place in this group of means of theft, as well as technologies for carrying out currency transactions (for example, electronic signatures, blockchain technology, etc.) require special attention.

According to article 34 of the Law of the Republic of Uzbekistan "On Payments and Payment Systems" No. LRU-578 dated 01.11.2019, a bank card or other electronic device containing information and allowing the payer to make a payment, as well as allowing other transactions stipulated by the agreement between the payer and the bank the issuer of an electronic means of payment is considered an electronic means of payment [12].

The most common means of theft committed using information technology is computer software. In addition to computer software, computer, mobile services and applications, it can also refer to universal means of theft committed using information technology systems. For example, most of the theft of other people's property using information technology is carried out using payment systems and services. In particular, this method is typical for such forms of theft

as fraud, embezzlement and theft. This method: 1) sending a payment order and using an electronic signature; 2) Theft by sending information (in the form of an SMS message) about the transfer of funds using the services "Mobile Banking", "Internet Banking".

The use of certain types of devices and other means of committing a crime may characterize certain types of this type of theft. For example, the use of a computer virus as a form of illegal computer software and actions through unauthorized access to the system characterize theft. The commission of theft by a person responsible for the disposal of property using utility computer programs is typical for the crime of misappropriation or embezzlement using information technology.

Since the theft of someone's property committed with the help of information technology can take the form of theft, fraud and embezzlement, the signs of this method of theft also include signs of methods of traditional forms of theft of someone's property, and this should be taken into account in the investigation process. The method of plundering someone's property with the help of information technology can be supplemented with such traditional signs as theft, fraud, abuse of trust, forgery.

The traditional method of fraud according to article 168 of the Criminal Code of the Republic of Uzbekistan is deception and the use of information technology to steal someone's property using various means: the Internet, e-mail, various instant messaging programs (messengers) to commit theft.

In our opinion, unlike the traditional form of fraud, this type of fraud, committed by deception using information technology, has a special element – a means of fraud, that is, information technologies that

differ from traditional oral and written means of committing fraud.

Some researchers attribute deception to a method of fraud committed using information technology, "conscious, illegal, unauthorized" use or violation of information [13], but, in our opinion, it is advisable that these actions of the criminal be qualified taking into account the consequences specified in Articles 168, 278² of the Criminal Code of the Republic of Uzbekistan, and not the concept of deception.

The Ukrainian [14] Criminal Code, Part Three of Article 190 establishes criminal liability measures for fraud committed by causing large-scale damage or by committing illegal actions (operations) with electronic computers, the Criminal Code of the Russian Federation [15] for fraud committed using electronic means of payment under Article 159.3, the Criminal Law (Code) Latvia [16] Article 177_1 defines criminal liability measures for fraud in automated data processing systems.

Deception as a method of fraud committed with the use of information technology is a psychological impact of the suspect in the form of a deliberate offer to the victim of false information with the help of information technology, which is perceived as the truth. Deception committed with the help of information technology means establishing a direct or indirect remote connection between the suspect and the victim. This remote method of fraud using information technology consists in virtual communication between the suspect and the victim through special technical devices and software as a means of communication.

In accordance with the resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan No. 17 dated June 23, 2023, according to article 168 of the

Criminal Code, the commission of fraud using an information system, including information technology (paragraph "d" of article 168 of part three of the Criminal Code), is understood to be theft carried out by deception manipulating the property of financial, banking institutions funds, etc. with the help of computer equipment, communications, tablet or other similar technical devices. Such fraud can be committed by changing the information processed in the computer system, stored on the appropriate media or transmitted over data transmission networks, as well as by entering false information into the computer system.

Another way of fraud committed with the help of information technology is the use of electronic means of payment. The method of fraud involves the active use of these means of payment, for example, a fake electronic payment order, a contactless payment method as a means of theft.

The method of fraud in mobile networks can also refer to a subtype of the method of fraud in the field of computer data, if there are no signs of the use of electronic means of payment. This fraud is sometimes called "hacker fraud" in the legal literature[17]. However, this name is applied to fraud committed using computer technology, software and special hacking skills.

In addition to the described methods, there may be other independent types of fraud methods using information technology: the use of an electronic document containing deliberately false information, the misuse of an electronic signature, the use of a malicious computer program.

The traditional method of appropriation and embezzlement with the help of information

technology makes it possible to distinguish the looting of someone's property from other types.

Firstly, the assignment or distribution is carried out by the person to whom the property is entrusted on the basis of a civil contract, an official or official position that provides the appropriate authority to manage, dispose of the entrusted property.

Secondly, the difference lies in the purpose of using information technology. For example, the use of an electronic document with changes made by a suspect during theft or embezzlement is a disguise, concealment of access to property and the very act of committing this type of theft.

CONCLUSION

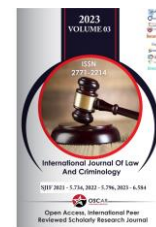
In conclusion, we can say that a group of interrelated elements of the mechanism of theft of other people's property using information technology can be called the actions of the suspect, the criminal means used by him and the method of committing this group of crimes. Actions carried out with the help of technical and software tools, information objects, individual actions or a set of actions in the field of computer data and other actions create a way of stealing someone's property using information technology. Taking into account the peculiarities of the forms of theft of other people's property, the methods of theft of other people's property using information technology are divided into theft, fraud, embezzlement and methods of embezzlement.

These signs describe some types of theft of someone's property, each of them is divided into separate types depending on the additional features of a certain method, while such signs as committing actions in the field of computer data using software products and software are theft of someone's property using information technology. These signs describe some

types of theft of someone's property, each of them is divided into separate types depending on the additional features of a certain method, while such signs as committing actions in the field of computer data using software are theft of someone's property using information technology.

REFERENCES

1. Жиноят кодекси 169- моддаси 3 – қисми “б” бандига қаранг.
2. Мальков Б.Н. История и философия науки: уч. пос. М.: РПА Минюста России, 2012. С. 330.
3. “Ахборотлаштириш тўғрисида”ги Ўзбекистон Республикаси Қонуни, Қонунчилик маълумотлари миллий базаси, 21.04.2021 й., 03/21/683/0375-сон
4. “Киберхавфсизлик тўғрисида”ги Ўзбекистон Республикаси Қонуни, Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон;
5. Пименов П.А., Горошко И.В. Организационные и правовые проблемы борьбы с хищениями денежных средств с использованием вредоносных компьютерных программ: монография. М.: Академия управления МВД России, 2015. С. 3.
6. Мошенничество в платежной сфере: Бизнес-энциклопедия. М.: Центр исследований платежных систем и расчетов. Интеллектуальная Литература, 2016. С. 15.
7. “Электрон ҳужжат айланиши тўғрисида”ги Ўзбекистон Республикасининг Қонуни, 29.04.2004 йилдаги 611-И-сон.
8. Полещук О.В., Шаповалова Г.М. Криминалистическое исследование следов при расследовании компьютерных преступлений: монография. Владивосток: Дальневосточный гос. ун-т, 2006. С. 18.



9. Иванов Н.А. Теоретические и методические основы комплексной судебной компьютерно-технической экспертизы и судебно-технической экспертизы документов: автореф. дис. ... канд. юрид. наук. М., 2005. С. 16.
10. Козоғистон Республикаси Жиноят кодекси
11. Мутахассислар тақдим этган маълумотлар.
12. Ўзбекистон Республикасининг 01.11.2019 йилдаги “Тўловлар ва тўлов тизимлари тўғрисида”ги ЎРҚ-578-сон Қонунининг 34-моддаси.
13. Звезда И.И. Расследование хищений в банковской сфере, совершенных путем мошенничества: автореф. дис. ... канд. юрид. наук. М., 2008. С. 9.
14. Украина Республикаси Жиноят кодекси
15. Россия Федерацияси Жиноят кодекси
16. Латвия Республикаси Жиноят кодекси
17. Андреев Б.В. Информационные технологии в расследовании преступлений, совершенных с использованием сотовой связи: учеб.-метод. пос. М.: Академия Генеральной прокуратуры России, 2009. С. 30.

OSCAR
PUBLISHING SERVICES