DOI: https://doi.org/10.34069/AI/2021.41.05.13

Criminological and forensic characteristics of forms of embezzlement committed through the use of information technology

Кримінологічна та криміналістична характеристики форм розкрадань грошових коштів, вчинених шляхом використання інформаційних технологій

Received: April 27, 2021 Accepted: May 30, 2021

Written by:
Mykhailo Dumchikov[42]
https://orcid.org/0000-0002-4244-2419
Web of Science researcher code: ABC-1338-2020
Oleksandr Yunin[43]
https://orcid.org/0000-0003-4846-2573
Web of Science researcher code: AAP-5453-2021
Nataliia Nestor[44]
https://orcid.org/0000-0003-4231-537X
Web of Science researcher code: AAP-5545-2021
Andrii Borko[45]
https://orcid.org/0000-0002-5498-1620
Web of Science researcher code: U-6786-2017
Oleksandr Yermenchuk[46]
https://orcid.org/0000-0001-5722-7183
Web of Science researcher code: AAP-5548-2021

Abstract

The article's purpose is the criminological and forensic characteristics of the forms of embezzlement of funds by the use of information technology and international and foreign experience in combating this destructive phenomenon. The object of this article is the relationship that arises in connection with the implementation and counteraction to theft in the field of information technology. The authors used various methods of scientific cognition to write this work. In particular, historical, observation, generalization, comparison and analogy, statistical, analytical, and others. The article emphasizes that the emergence and rapid development of new information technologies do not always positively affect criminals because criminals can transform positive qualities into crime. In particular, crimes of embezzlement through the use of information technology are now widespread. This article has tried to provide a criminological description of the three main forms of cybercrime against money: carding,

Анотація

Метою статті є кримінологічна та криміналістична характеристики форм розкрадань грошових коштів шляхом, вчинених використання інформаційних технологій та міжнародний і зарубіжний досвід протидії цьому деструктивному явищу. Об’єктом цієї статті євідносини, що виникають у зв’язку зі здійсненням та протидією розкраданню у сфері інформаційних технологій. Для написання даної роботи було використано різні методи наукового пізнання.Зокрема, історичний, спостереження, узагальнення, порівняння та аналогії, статистичний, аналітичний та інші.У статі акцентовано увагу на тому, що поява та стрімкий розвиток новітніх інформаційних технологій не завжди справляє позитивний ефект, адже злочинці можуть трансформувати позитивні якості у злочинні. Зокрема нині широкого поширення отримали злочини з розкрадання грошових коштів шляхом використання інформаційних технологій. У

[42] PhD in Law, Senior Lecturer, Department of Criminal Legal Disciplines and Procedure, Sumy State University, Ukraine.
[43] Doctor of Legal Sciences, Professor, Professor of the Department of Civil Law and Process of Dnipropetrovsk State University of Internal Affairs, Ukraine.
[44] Doctor of Scienceof Law, HonoredLawyerofUkraine, Kyiv Scientific Research Institute of Forensic Expertise, Ukraine.
[45] Doctor of Scienceof Law, Assotiate Professor, Admiral Makarov National University of Shipbuilding, Ukraine.
[46] Assotiate Professor, Assotiate Professor of the operative-searching department in National academy of internal affairs, Ukraine.

phishing, and embezzlement committed using NFC technology. In addition, emphasis was placed on the importance, role, tasks of computer and technical expertise in the investigation of embezzlement dedicated through the use of information technology. The importance of implementing international conventions and the positive experience of foreign countries in combating the embezzlement of funds committed through the use of information technology.

Keywords: cybercrime, carding, phishing, Near Field Communication, computer and technical expertise, foreign experience.

статті ми спробували надати кримінологічну характеристику трьом основним формам кіберзлочинів проти грошових коштів: кардингу, фішингу та розкраданням, що вчиняються за допомогою технології NFC. Крім того, акцентували на значенні, ролі, завданнях комп'ютерно-технічної експертизи під час розслідування розкрадань грошових коштів, вчинених шляхом використання інформаційних технологій. Наголошено на важливості реалізації міжнародних конвенцій та позитивного досвіду зарубіжних держав у контексті протидії розкраданням грошових коштів, вчинених шляхом використання інформаційних технологій.

Ключові слова: кіберзлочини, кардинг, фішинг, технологія «зв'язок на невеликих відстанях»,комп'ютерно-технічна експертиза, зарубіжний досвід.

Introduction

At the present stage of formation and development of the information society, digitalization is global, comprehensive, penetrating all spheres of public life. This is becoming one of the leading social development factors and essentially characterizes modern social dynamics (Babanina, Tkachenko, Matiushenko & Krutevych, 2021). World scientific and technological progress has led to the emergence of a large number of new technologies. Such technologies have introduced a large number of innovations into public life. An important point of development is the emergence of the first computers and computer networks, which opened up many opportunities for humankind. Considering all the features of progress and other factors, it is possible to view the emergence of a new criminal link in cyberspace. At the same time, along with the apparent positive effect of the use of information technology, there are accompanying negative manifestations (Kurmaiev, Seliverstova, Bondarenko & Husarevych, 2020). Cybercrime is a very pressing issue in society today. This is evidenced by news worldwide, criminal statistics, problematic issues in the science of criminal law, and problems in the criminal process. All this is because, as a phenomenon, cybercrime is a particular category that is constantly evolving in parallel with technological progress. This proves the lack of an effective mechanism for protection against this phenomenon (Utkina, Bondarenko & Malanchuk, 2021).

The urgency of issues related to criminal liability for theft committed with the use of information technology, because currently offenses that infringe on property relations, and directly related to computer technology and the Internet, have become widely spread acquired a prominent international character. In most cases, individuals do not know each other in real life, and their interaction is realized through virtual identification (Vorontsova, 2011).

Accordingly, information security requires a constant search for new mechanisms to combat cybercrime, including legal instruments, analysis of the causes, risks, and threats of high-tech criminal offenses against property. Cybercrime is a problem that needs to be taken seriously. This is because the impact of these unlawful encroachments is far-reaching and harms the economy. If left unchecked, these crimes will develop and require more attention from law enforcement and the legislature (Sujono, 2019).

New forms of crime are challenging our society. Until a few decades ago, there were only a few mentions of cybercrime, but in a short time, cybercrime has spread so that it not only poses a threat to individual states but has reached global proportions. The most common crimes in cyberspace are thefts committed by fraud, the scope of which allows us to talk about their types: payment fraud (theft using payment cards); skimming (crimes related to the use of ATM fraud); malicious payment software (theft through the development and use of malicious programs); social engineering (illegal obtaining of information for selfish purposes); phishing (gaining access to confidential personal data by sending e-mails); fraud in e-commerce (theft related to the vulnerability of payment systems of online stores, platforms for ordering tickets, car rental, and others); prepaid copy (a promise to provide services or deliver goods after prepayment).

This confirms the fact that the improvement of computer technology, the rapid development of information technology creates a qualitative change in criminal offenses in computer information, and today there is a specialization in this part of the criminal environment. For example, property crimes should no longer involve personal contact between the offender and the victim (Kunz and Wilson, 2014). Depending on which began to appear such types of criminals as carders, phishers (criminals who engage in computer fraud by obtaining illegal access to bank details, numbers of plastic payment cards, etc.), frackers (criminals who specialize in committing crimes in areas of telecommunications using confidential computer information and unique technology means for covert receipt of information from technical channels).

The purpose of scientific work is criminological and forensic characteristics of forms of embezzlement through the use of information technology and international and foreign experience in combating this destructive phenomenon.

Theoretical framework

Carding as a form of embezzlement through the use of information technology

Modern technology is firmly entrenched in our daily lives and is now an integral part of it. Speaking of the Internet, we can say that this area of human interaction is developing rapidly. Now there you can find any information, including criminal. And what about crimes committed on the Internet?

Unlike traditional types of crime, the history of which spans centuries, such as murder or theft, the phenomenon of cybercrime is relatively young and new, which arose almost simultaneously with the advent of the Internet.

In modern Ukraine, the terms "theft in the field of information technology" are not officially defined in regulations. At the same time, the concept itself was formed through the activities of law enforcement agencies of developed countries in Europe and the world, including crimes in the field of computer technology, illicit trafficking in electronic and special hardware, distribution of unlicensed computer software, and some other types. crimes (Bondarenko & Repin, 2018).

The most common crime on the Internet is theft. In the field of information technology, theft has developed quite well and therefore has many types. One of these is "carding," or in other words, theft associated with bank cards. An attacker can commit this act by hacking the servers of online stores, which store payment data, payment systems in general, or hacking a user's personal computer to obtain personal data of bank cards, accounts, etc.

Theft of details that identify users on the Internet as holders of bank credit cards, with their possible further use for illegal financial transactions (purchase of goods or money laundering) is called karting (Sachkov & Smirnova, 2015).

The increased interest of delinquents in increasing the number of online payments necessitates the improvement of legislation in combating carding. Moreover, this area's low level of resistance has turned carding into an independent measurement of criminal business with huge profits. The analysis of unique and scientific literature allows us to conclude that the scientific community pays attention to counteracting the theft of money from bank cards.

Tereshchenko L. K., Starodubova O. E defines carding as one type of fraud in which transactions are performed using someone else's payment card or its details that are not initiated or confirmed by its owner (Tereshchenko & Starodubova, 2017).

S. Usachev proposes to consider the theft of funds from payment cards, in other words, called carding and refers to the commission of various transactions directly through the use of the card itself or its details without the knowledge and permission of its official owner (Ermolenko, 2015).

M. Batiushkin notes that carding is an act of stealing someone else's property or acquiring the right to someone else's property by entering, deleting, blocking, modifying computer information or other interference in the operation of storage, processing, or transmission of computer information or information and telecommunications networks (Batyushkin, 2021). D. Grib notes that carding as theft is possible only with the help of computer manipulations, which consist in deceiving the victim or the person to whom the property is entrusted or under whose protection it was, using the information processing system (Grib, 2019).

In our opinion, "carding" should be defined as the theft of someone else's property, money, or rights to someone else's property by entering, deleting, blocking, modifying computer information or other interference in the operation of storage, processing, or transmission of computer information or information telecommunication networks.

Phishing is a form of embezzlement through the use of information technology

According to M. Mogunov, "phishing" is a particularly dangerous crime associated with erroneous messages from banks, payment system administrators, or sending messages on social networks. These messages often ask you to follow the link to change the password or other actions, thereby obtaining a valid login and user password. The purpose of such manipulations can be a bank account, an account in payment systems, e-mail, and social networks. Once scammers get what they need, they quickly apply it to access the user's bank account.

Phishing can be defined as the acquisition by deception or social engineering methods (hacking using the human factor) of personal data for selfish, criminal purposes. The implementation of phishing has two mechanisms: first, the intermediary receipt of personal data, and second, the receipt of personal data from their owner (Mogunova, 2020).

Near Field Communication (NFC)

L. Bondarenko, N. Yaroshevich, and A. Tarabinovych note that NFC, or Near Field Communication, translated from English, means "near field communication". It is this technology that allows two devices equipped with NFC chips to wirelessly exchange data at a distance of up to 10 cm (Bondarenko, Yaroshevich & Tarabinovich, 2019). In general, NFC technology is a logical continuation and extension of the ISO 14443 standard, which combines the interface of a smart card and a reader into a single device. This allows the measure to cover a broader range of tasks and standardize a much larger set of devices. Currently, NFC is actively used primarily in a considerable number of digital mobile devices, such as mobile phones. NFC chips are built into the default and are also used in public transport and payment systems. Contactless payment is one of the most valuable features of modern smartphones. With its help, it is enough to bring the gadget to the payment terminal or turnstile in public transport to pay for a purchase or trip. Mobile banking is another incredible invention that simplifies the lives of millions of users. However, how safe is it to store card data on a smartphone and pay for everything in a row using the gadget?

Methodology

Various methods of scientific cognition were used to write this work. In particular, the historical process is used to clarify historical moments in cybercrime and theft in information technology. The method of observation to get acquainted with the essence of theft in information technology and the difficulties it causes. The authors used the generalization method to define the general concept of theft in information technology and its significance for the economic security of the state and society. The way of comparison and analogy is used to identify some standard and distinctive features among the regulations of different countries. The statistical method made it possible to investigate and assess the scale of the development of theft in information technology. The analytical approach is used to study the individual components of theft in information technology: the causes and methods of its commission.

Results and discussion

General characteristics and types of theft through the use of information technology

Web carding: a description of the essence

Recently, web carding is gaining popularity, i.e., the theft of funds from payment card accounts, virtual accounts, cryptocurrency using the Internet. The low level of interaction between law enforcement agencies of different countries complicates counteracting webcarding. A person who steals money under a similar scheme is called a "carder" or a "web carder." Unemployed men are engaged in carding, as this kind of activity takes almost all the time. Age of malefactors from 18 to 40 years, not married. As a rule, these are people without education or have incomplete higher education, not previously convicted. These people have an increased ability to work because to commit theft, for example, from American payment cards, the last switch to a specific sleep mode, similar to the US time zone (conduct their "work" at night, sleep during the day) (Golovinov & Pogorelov, 2016).

Skimming as a kind of carding

Let's turn to one of its most challenging to identify – skimming (such theft is carried out using special devices and tools that allow you to read payment card information (e.g., magnetic stripe). Ways to read information are currently different; continuous technical development, science, and technology determine the constant improvement of these methods by criminals.

Today, law enforcement agencies know such methods of reading magnetic strips of payment cards as the use of special devices that read the magnetic head and adapter to connect to a computer, allowing you to process the necessary data of the magnetic stripe cardreproduce it on a fake further. In addition, criminals use mini-video cameras, the task of which is to obtain data on the PINcodes of payment cards (Likholetov, 2016). The main problem of detecting these devices at ATMs or other terminals, gas stations, vending machines is their careful camouflage and lack of knowledge about the authentic appearance of these terminals among citizens. Yes, not a specialist in this field of expertise is unlikely to distinguish an ATM with the original elements from the receiving tray with a cover in the form of a magnetic head. First of all, such devices are not conspicuous, and the overlays have the original color, shape, and other external data.

The essence of the use of skimmers is the ability of such devices to concentrate criminally obtained information about payment cards, as well as transmit it through communication channels for further production of a duplicate card, both for cash and for various purchases without direct withdrawal funds from the card (Smagorinsky & Senchenko, 2016).

A significant problem in detecting such crimes is the relatively high level of development of the so-called "criminal electronics". Improving the methods of embezzling money from bank cards makes it difficult to create a particular algorithm of actions of law enforcement officers, which allows you to respond competently to such facts of illegal activities of criminals.

Phishing: characterization of the essence

The principle of "phishing" redirects the user to fake network resources created by attackers, outwardly no different from actual Internet pages.

By following the link attached to the letter, the user gets to a fake site that looks just like the accurate site of any bank, store, or social network. Once a user fills out a form with a login and password to log in to their account, they are detected by attackers. The criminal, gaining access to the login and password from the report to the Internet banking, transfers funds from the victim's account, thereby committing theft.

For example, there is a well-known cryptocurrency payment service www.myetherwallet.com. On such a service, you can create a virtual cryptocurrency wallet and buy and store cryptocurrency. In their messages or messages, intruders sending links to this site allegedly change several or even one letter to other characters to be invisible. For example, the actual link of this system is as follows: www.myetherwallet.com, and the attacker's link will look something like this: www.myetherwalIet.com (Decision of Appeal ruling of the Supreme Court of the Udmurt Republic, 2019). It should be emphasized that "phishing" does not affect the software on the victim's computer. The victim himself goes to the sent link and enters the login and password. In the future, the theft of funds is carried out using the received login and password, but not due to exposure to the victim's device.

Using NFC technology to steal money

Theft is associated with contactless payment, i.e., due to NFC, a wireless data transmission technology with a shortrange, which allows the exchange of data between devices at a distance of 4 centimeters. This technology is now present in almost every bank card and smartphone. Itenables you to pay for purchases up to a certain amount only by attaching a bank card without entering a password.

The essence of criminal activity is to intercept NFC signals using illegal readers. RFID interceptors are analogs of conventional contactless PIC card terminals with increased functionality that capture and process electromagnetic waves. Such a device is usually equipped with an antenna, a particular controller, connectors for extracting information from the reader, and pirated computer software, i.e., software. To receive money, the attacker is enough to be 10 centimeters from the bank card, which will get money and all its data. However, progress is not standing still, and today there are some ways to protect against attackers: many manufacturers have started selling unique aluminum card covers that dampen electromagnetic waves, thus limiting the use of the contactless payment, then there is an option to set a limit for contactless payment without entering a password and others.

The role and importance of computer forensics in the investigation of embezzlement through the use of information technology

It is worth emphasizing one of the achievements of recent years in the field of detection and investigation of criminal offenses, namely the emergence of computer science, which is included in the relevant list of genera (types) of forensic examinations performed in forensic departments.

With exceptional knowledge in computer technology, experts (experts) can contribute to the investigator's activities to establish the truth in the investigation of crimes (Shaevich, 2011).

The possibilities of forensic examination are challenging to overestimate. This fact is entirely accurateA. Vardanyan and O. Gribunov noted that current law enforcement practice is focused on the appointment and conduct of examinations that will reveal information about the mechanism of criminal activity, the identity of an unidentified offender, and other signs and properties, thereby serving as evidence in a criminal case (Vardanyan, Gribunov, 2016).

Consider the possibility of computer forensics as an essential aid in detecting and investigating criminal offenses related to the theft of funds from bank cards. Criminals, in most cases in terms of ways to commit illegal acts, use objects of electronic devices designed to intercept information about customers of remote banking systems.

The subject of computer-technical examination, which is conducted to establish the facts of theft of funds from payment cards, are the following categories: the establishment of factual circumstances relevant to the criminal case under investigation (1); establishing the actual occurrences associated with the use of electronic devices that allow you to seize the data of the payment bank card, as well as information about PIN-codes (2). Objects of computer and technical examination are unique devices and tools that allow you to read the statement of payment cards installed on the elements and nodes of the terminals of remote banking systems (ATMs), which are withdrawn directly from ATMs or during the inspection and searches (Pilipchuk & Dzioban, 2011).

The objectives of this examination, which is assigned in the investigation of criminal cases initiated on the facts of the investigated thefts, are: to determine the direct possibility of interception of information about customers, submitted for investigation equipment (1); diagnosing individual bank card numbers intercepted by them (2) (Golub, 2016).

Establishing these tasks will provide information about involvement in the crime and serve as the evidence in detecting compromised payment cards and determining the possible damage caused to the victim.

During the computer forensic examination, which is assigned to this category of crimes, the expert can answer the following questions: 1) whether it is possible to use the presented devices to obtain information available on plastic payment cards, as well as information about keystrokes on the ATM keyboard (including a number about PIN codes)? 2) does the presented objects contain data on plastic payment card numbers and their PINcodes? 3) in what way is it supposed to receive the presented equipment (device) data on the received information?

The relatively narrow list of issues to be resolved by experts is explained by the fact that this type of forensic examination is still relatively "young". The potential and opportunities of the study are not fully disclosed, which affects the formation ofthe quality evidence base in criminal cases.

Moreover, currently, there is no specialized method of producing such examinations, including all aspects of this activity, the exact algorithm, and ways to resolve disputes that arise at the stage of formulating conclusions. Continuous improvement of skills and abilities of criminals in terms of improving the concealment of traces of criminal activity on the proposed crimes indicates the need for constant monitoring of consumer radio technology, as well as the importance of developing new tools and methods to establish the facts of illegal actions, namely embezzlement—payment bank cards.

International and foreign experience in combating theft using information technology and computer information

The problems of counteracting such embezzlement are acute for the world community, which adequately assesses the current situation, recognizing the obligation to take urgent international action (Jahankhani, Al-Nemrat & Hosseinian-Far, 2014).

The UN makes a significant contribution to solving the problem of combating cybercrime. The UN Office on Drugs and Crime has conducted a comprehensive study of cybercrime to study the problem of counteraction and develop proposals for improving international legal measures and national legislation. At the request of the UN General Assembly (Resolution No. 65/230, 2011), the Commission on Crime Prevention and Criminal Justice set up an intergovernmental group of open-ended experts to identify the research topics and methodology, take note of the study itself, and take action. In response, the Member States, the international community, and the private sector, and in 2017 proposed a platform for further discussion of cybercrime issues to closely monitor new trends (United Nations, 2021).

Documents developed in the context of or under the auspices of the Council of Europe or the European Union, the Commonwealth of Independent States or the Shanghai Cooperation Organization, African intergovernmental organizations, the League of Arab States, and the United Nations (United Nations, 2021) are also necessary. First of all, it is essential to analyze the Council of Europe Convention on Cybercrime, adopted on November 23, 2001, also known as the Budapest Convention. It is currently the only global document at the international level that is mandatory for member states, which regulates actions to combat cybercrime (Council of Europe, 2001). Cybercrime in the Budapest Convention is divided into five groups: crimes against confidentiality, integrity, and availability of computer data and systems (illegal access, unauthorized interception, influence on data, influence on the functioning of the system, unlawful use of devices) (1); crimes for which a computer is used (forgery with the use of computer technology, fraud with the help of computer technology) (2); crimes related to data retention (child pornography) (3); crimes related to the infringement of copyright and related rights (4); crimes related to racism and xenophobia committed with the help of computer systems (5).

It is important to note that the Convention, as the primary document of international character, sets out the criteria for the development of national legislation defining the types of acts to be criminalized; fraud with computer technology has identified a separate crime.

In addition to studying international regulations aimed at combating the theft of money through information technology, it is worth emphasizing the example of similar experiences in foreign countries.

In the French Criminal Code, the rules for liability for computer crimes are contained in two books. Thus, the second book, "On crimes and misdemeanors against the person, " includes the chapter "On encroachments on the person", including the composition of such crimes as illegal actions with personal data in telecommunications systems. The third book, "On property crimes and misdemeanors," contains a chapter "On encroachments on automated data processing systems", the rules of which provide for criminal liability for its misuse. It follows that personal data, as well as telecommunication systems, are subject to criminal law protection. The Criminal Code of France does not contain special rules on theft committed with the use of computer information (Criminal Code of the French Republic, 2020).

In the Criminal Code of the Federal Republic of Germany, computer fraud is a separate crime; paragraph 263a establishes liability for actions to obtain for themselves or a third party illegal property gain, which harms the property of another person by influencing the outcome of computer data processing compiling incorrect programs, using inaccurate or incomplete data, unauthorized use of data or other illegal influence on the data processing process. Computer information, in this case, is a way of committing theft (Criminal Code of the Federal Republic of Germany, 2013).

In 1986, the United States passed the Computer Fraud and Abuse Act. This law is one of the few components of federal law on theft using computer systems. Paragraph 1030 of Chapter 47, Section 18 of the U.S. Code, which establishes liability for committing fraud by accessing a computer, has become part of this law (Khilyuta, 2013). Under this rule, criminal liability arises for access to a computer that is carried out with fraudulent intent, and its use to obtain anything of value through fraud, including the illegal use of computer time worth more than $ 5,000 during the year, that is, without paying for the benefit of computer networks and services. Thus, US law separates computer fraud from the traditional, its essence - access to a computer and computer use.

The Swiss Criminal Code provides for liability for electronic espionage, perfect for selfish purposes. Thus, a person who, for his or her illicit enrichment or the enrichment of another, acquires for himself or another person data collected or transmitted electronically or in a similar manner is subject to criminal punishment. In addition, Article 147 criminalizes fraudulent abuse of a data processing facility (Swiss Criminal Code № SR 311.0, 2020).

Paragraph 2 of Article 278 of the Criminal Code of the Republic of Polandstates that a person who receives someone else's computer program to obtain property gain is subject to criminal punishment without the consent of an authorized person (Criminal Code of the Republic of Poland, 1997). In addition, paragraph 1 of Article 287 provides for criminal liability for unlawful receipt of property gain or wrongful infliction of harm to another person by influencing the automated conversion, collection, or transmission of information, its modification, deletion, or introduction of a new record on computer media (Criminal Code of the Republic of Poland, 1997). Crimes, which the legislator classified as a computer, in Poland are divided into groups depending on what the person's actions were aimed at - to obtain information or to obtain property benefits

The Turkish Criminal Code does not provide for computer fraud. Still, Article 504, paragraph 3, establishes liability for fraud using postal, telegraph, and telephone communications as a tool of crime (Penal Code of Turkey, 2016).

According to paragraph 279a of the Danish Penal Code, computer fraud refers to the unlawful alteration, addition, destruction of information or programs used for electronic data processing committed for illegal gain (Order No. 909, 2005).

The Criminal Code of the Republic of Korea contains Article 347-2 "Computer fraud", according to which a person who receives any benefit from the property or facilitates the receipt of such service by a third party through the use of information, input of erroneous or improperly processed data in technical means, including a computer, is subject to criminal punishment (Criminal Code of the Republic of Korea, 1998).

Analyzing the international and foreign experience in combating computer theft, it should be noted that agreement on this issue has not been achieved at any level. In our opinion, it is worth developing a concept that would include the following segments: 1) a review of the activities of international organizations allows us to conclude that the world community is actively taking measures to combat cybercrime, making efforts to reform legislation. However, recognizing that effective confrontation is possible only with joint complex, coordinated actions, it has not yet achieved positive results in this direction. The adopted documents of international and regional organizations are characterized by a certain degree of fragmentation in the criminalization of acts. Some address the problem of cybercrime in the broadest sense as a growing threat to international security, including information terrorism, information warfare, and do not contain provisions relating to criminal justice, including crime and procedural powers. Other guidance documents containing these provisions do not provide a single approach, particularly addressing the criminalization of acts committed in cyberspace. Such differences can significantly impact how the requirements of international law will be taken into account in national legislation. At the same time, most countries of the world community recognize that the fight against cybercrime requires the strengthening of legal measures, improvement of legislation, including in the field of criminal law; 2) currently in foreign countries in terms of criminalization of theft committed with the use of computer information, different approaches are used. Several countries, such as the United Kingdom, France, and Georgia, use general rules on cyber theft with provisions that reflect components of acts such as unauthorized access, intrusion into personal data, and other information security crimes. In addition, an approach is being implemented in which the use of computer technology is envisaged as a qualifying feature of property crimes (Turkey). In other countries, such as the United States, Germany, Japan, Switzerland, Sweden, Poland, Denmark, Korea, China, Belarus, Armenia, thefts committed with computer information are allocated to separate warehouses in the system of property crimes. Such acts are mostly recognized as either theft or fraud and are prohibited by either the fundamental criminal law of the country, or unique, or both.

Conclusions

The emergence and rapid development of new information technologies do not always positively affect criminals because criminals can transform positive qualities into crime. In particular, offenses related to the theft of money through information technology are now widespread. This article has tried to provide a criminological description of the three primary forms of cybercrime aimed at stealing money: carding, phishing, and embezzlement committed using NFC technology. In addition, emphasis was placed on the importance, role, and implications of computer and technical expertise in the investigation of embezzlement through information technology. The importance of implementing international conventions and the positive experience of foreign countries in combating the embezzlement of funds committed through the use of information technology.

Bibliographic references

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. Amazonia Investiga, 10(38), 113-122. https://doi.org/10.34069/AI/2021.38.02.10

Batyushkin, M. V. (2021). "Phishing" – a computer fraud? International scientific journal "symbol of science", 1, 90-93. Recovered from: https://cyberleninka.ru/article/n/fishing-kompyuternoe-moshennichestvo/viewer

Bondarenko, L. P., Yaroshevich, N. B., & Tarabinovich, A. B. (2019). Practice of Using Contactless Payments in Ukraine and the World. Effective economy, No. 2, Recovered from: http://www.economy.nayka.com.ua/pdf/2_2019/54.pdf. DOI: 10.32702 / 2307-2105-2019.2.52

Bondarenko, O. S., & Repin, D. A. (2018). Cybercrime in Ukraine: causes, signs and countermeasures. Comparative and Analytical Law, No. 1, 246–248. Recovered from: https://essuir.sumdu.edu.ua/bitstream-download/123456789/67982/1/Bondarenko_Repin_KIberzlochinist.pdf

Council of Europe (2001) Convention on Cybercrime on 23. XI.2001. No 185. Recovered from: https://rm.coe.int/1680081561

Criminal Code of the Federal Republic of Germany. Federal Law Gazette Bundesgesetzblatt I, 24 de septiembre de 2013, p. 3322, Recovered from:https://www.legislationline.org/documents/section/criminal-codes/country/28/Germany/show

Criminal Code of the Republic of Korea, National legislative bodies / National authorities of Jan. 1, 1998. Recovered from: https://www.refworld.org/docid/3f49e3ed4.html

Criminal Code of the Republic of Poland, Principios de responsabilidad penal, of 6 June 1997. Recovered from: https://www.legislationline.org/download/id/7354/file/Poland_CC_1997_en.pdf

Criminal Code of the French Republic, Legislative part, January 01, 2020. Recovered from: https://www.legislationline.org/documents/section/criminal-codes/country/30/France/show

Ermolenko, O. M. (2015). Banking Innovation as a Trend of Increasing Competitiveness of Credit Institutions at The Present Stage of Functioning. Scientific Bulletin of YIM, No. 1, 49-55. Recovered from: https://cyberleninka.ru/article/n/kriterii-razvitiya-rynka-bankovskih-kart-na-sovremennom-etape-funktsionirovaniya-bankovskogo-sektora/viewer

Golovinov, O. N., & Pogorelov, A. V. (2016). Cybercrime in the modern economy: state and development trends. Innovation Economics, Issues, 6(1), 73-88. doi: 10.18334 /vinec.6.1.35353

Golub, A. (2016). Cybersecurity in all manifestations: see, heritage and ways to fight. Resource Center GURT: website. Recovered from: http://www.gurt.org.ua/articles/34602

Grib, D. (2019). Theft Of Property Through The Use Of Information Technology In The Criminal Code Of The Russian Federation And The Republic Of Belarus: A Comparative Aspect. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia, No. 4, 76-80. DOI 10.24411/2073-0454-2019-10199

Jahankhani, H., Al-Nemrat, A., Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. Cyber Crime and Cyber Terrorism Investigator's: Handbook. London: Waltham.

Khilyuta, V.V. (2013). Computer theft or computer fraud? Criminalist Library, No. 5(10), 55-65

Kunz, M., & Wilson, P. (2004). Computer Crime and Computer Fraud. Report to the Montgomery County Criminal Justice Coordinating Commission. Recovered from: https://www.montgomerycountymd.gov/cjcc/resources/files/computer_crime_study.pdf

Kurmaiev, P., Seliverstova, L., Bondarenko, O., & Husarevych, N. (2020). Cyber insurance: the current situation and prospects of development. Amazonia Investiga, 9(28), 65-73. https://doi.org/10.34069/AI/2020.28.04.8

Likholetov, A. A. (2016). Responsibility for the theft of funds in the bank accounts of citizens in the context of reforming criminal legislation. Bulletin of the Volgograd Academy of the Ministry of Internal Affairs in Russia, No. 1(36), 59-63. Recovered from: http://va-mvd.ru/vestnik/arhiv/36.pdf

Mogunova, M. M. (2020). Implementation technology and legal regulation of illegal seizure of personal bank data (phishing). Bulletin of the Saratov State Law Academy, No. 4, 135-141. Recovered from: https://elibrary.ru/item.asp?id=43846129

Order No. 909, Criminal Code of Denmark, of September 27, 2005. Recovered from:https://www.legislationline.org/documents/section/criminal-codes/country/34/Czech%20Republic/show

Penal Code of Turkey. European commission for democracy through law, Council of Euope, 15 February 2016. Recovered from: https://www.legislationline.org/documents/section/criminal-codes/country/50/Tajikistan/show

Pilipchuk, V. G., Dzioban, O. P. (2011). Theoretical and state-legal aspects of anti-information terrorism in the minds of globalization. Strategic priorities, No. 4(21), 12-17.

Resolution No. 65/230 of Twelfth United Nations Congress on Crime Prevention and Criminal Justice. April 1, 2011. Recovered from: https://undocs.org/en/A/RES/65/230

Sachkov, D. I., Smirnova, I. G. (2015). Ensuring information security in government: textbook. Irkutsk, NovaPravo.

Shaevich, A. A. (2011). Features of use of special knowledge in the field of computer technologies at investigation of crimes: monograph. Irkutsk: Vost.- Sib. in-t M-va vnutr. Affairs of Russia.

Smagorinsky, B. P., & Senchenko, P. P. (2016). Features of detecting thefts committed using payment cards. Volgograd Academy of the Ministry of Internal Affairs in Russia, No. 4 (39), 102-106. Recovered from: http://va-mvd.ru/vestnik/arhiv/39.pdf

Sujono, I. (2019). Cybercrime Law Reconstruction in the National Cybersecurity Concept. http://doi.org/10.5281/zenodo.3462123

Swiss Criminal Code № SR 311.0. The Federal Assembly of the Swiss Confederation, 3 de marzo de 2020. Recovered from: https://business-swiss.ch/zakonodatel-stvo-shvejtsarii/ugolovnoe-pravo/ugolovny-j-kodeks-shvejtsarii/

Tereshchenko, L. K., & Starodubova, O. E. (2017). Mysteries of information law, Journal of Russian law, 1, 156-161. Recovered from: https://cyberleninka.ru/article/n/zagadki-informatsionnogo-prava/viewer

Utkina, M., Bondarenko, O., Malanchuk, P. (2021). Patent Trolling and Intellectual Property: Challenges for Innovations. International Journal of Safety and Security Engineering, 11(1), pp. 69-77. https://doi.org/10.18280/ijsse.110108

United Nations (2021). Global Program on Cybercrime. Recovered from: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

United Nations (2021). Comprehensive Study on Cybercrime Recovered from: http:///www.unodc.org

Vardanyan, A. V., & Gribunov, O. P. (2016). Forensic examinations assigned in the investigation of thefts at transport facilities. Theory and Practice of Countering Crime in the Asia-Pacific Region, No. 1 274-277 Recovered from: http://journals.tsu.ru/uploads/import/1800/files/437_205.pdf

Vorontsova, S. V. (2011). Cybercrime: masalah kualifikasi tindakan kriminal (criminal act qualification problema). Russian journal of economy, 2, 14-15.