DOI: https://doi.org/10.34069/AI/2021.41.05.14

Features of the initial stage of investigating fraud with financial resources in cyberspace

Особливості початкового етапу розслідування шахрайства з фінансовими ресурсами у кіберпросторі

Received: April 25, 2021 Accepted: June 15, 2021

Written by:
Oleg Reznik[47]
https://orcid.org/0000-0003-4569-8863
Web of Science researcher code: AAJ-3122-2020
Andrii Fomenko[48]
https://orcid.org/0000-0003-3517-1638
Web of Science researcher code: AAP-2665-2021
Andrii Melnychenko[49]
https://orcid.org/0000-0002-0719-2821
Web of Science researcher code: AAP-2675-2021
Natalia Pavlova[50]
https://orcid.org/0000-0002-1572-4648
Web of Science researcher code: AAP-2689-2021
Andrii Prozorov[51]
https://orcid.org/0000-0002-0905-7076
Web of Science researcher code: AAP-2986-2021

Abstract

The article aims to characterize the forensic features of the initial stage of investigating fraud with financial resources in cyberspace, its significance, analysis, and justification as a type of cybercrime that is dangerous for everyone, and prove the need for urgent measures to prevent and combat such criminal offenses. The authors used several methods of scientific cognition: logical-semantic, system-structural, analytical, formal-legal, forecasting, dialectical, interpretation, and hermeneutics. The article focuses on the general provisions of the forensic characteristics of Internet fraud with financial resources; analysis of the information model of the mechanism of committing fraud with financial resources in the field of computer information; coverage of the tactical features of individual investigative actions at the initial stage of the investigation of fraud with financial resources in cyberspace. It was concluded that

Анотація

Метою статті є характеристика криміналістичних особливостей початкового етапу розслідування шахрайства з фінансовими ресурсами у кіберпросторі, його значення, аналіз та обґрунтування як одного з видів кіберзлочинності, що є небезпечним для кожного, і доведення необхідності здійснення невідкладних заходів щодо попередження та протидії такому кримінальному правопорушенню. Об'єктом наукової статті є злочинна діяльність осіб, які вчиняють шахрайство з фінансовими ресурсами у кіберпросторі та пошуково-пізнавальна діяльність осіб, які ведуть розслідування даного виду кримінального правопорушення. Авторами було використано ряд методів наукового пізнання: логіко-семантчний, системно-структурний, аналітичний, формально-юридичний, прогнозування, діалектичний, тлумачення та герменевтики. У

[47] Doctor of Juridical Sciences, Associate Professor, Department of Administrative, Economic Law and Financial and Economic Security, Sumy State University, Ukraine.
[48] Candidate of Juridical Sciences, Rector, Dnipropetrovsk State University of Internal Affairs, Ukraine.
[49] Candidate of Juridical Sciences, Associate Professor of the Department of Criminal Procedure, Faculty of Training for Pre-trial Investigation, Dnipropetrovsk State University of Internal Affairs, Ukraine.
[50] Candidate of Juridical Sciences,Associate Professor of the Department of Criminalistics and Domestic Training, Dnipropetrovsk State University of Internal Affairs, Ukraine.
[51] Candidate of Juridical Sciences,Associate Professor of the Department "Organizations of information security with limited access" of the National Academy of the Security Service of Ukraine, Ukraine.

the effectiveness of combating Internet fraud and the level of cybersecurity in Ukraine is very low. Therefore, the investigation of fraud with financial resources in cyberspace requires in-depth specific knowledge from the subjects of the investigation.

Keywords: criminal offenses, cyberspace, fraud, financial resources, investigation.

статі акцентовано увагу на загальних положеннях криміналістичної характеристики інтернет шахрайства з фінансовими ресурсами; аналізі інформаційної моделі механізму скоєння шахрайства з фінансовими ресурсами в сфері комп'ютерної інформації; висвітленню тактичних особливостей окремих слідчих дій на початковому етапі розслідування шахрайства з фінансовими ресурсами в кіберпросторі. Робиться висновок про те, що ефективність протидії інтернет шахрайству та рівень кібербезпеки в Україні на дуже низькому рівні. А відтак розслідування шахрайства з фінансовими ресурсми в кіберпросторі вимагає глибиних специфічних знань від суб'єктів розслідування, які, на жаль, не можуть бути ними здобутті з різних причин. Наприклад, застарілістю науково-практичної підготовки та техніки. Усе викладене, у свою чергу, ускладнює попередження та протидію незаконним діям, а це дозволяє їм існувати протягом такого тривалого періоду часу.

Ключові слова: розслідувння, шахрйство, фінансові ресурси, кіберпростір, кримінальні правопорушення.

Introduction

At the present stage of the formation and development of the information society, the process of digitalization is global, comprehensive, penetrating all spheres of public life. It is becoming one of the main factors of social development and largely characterizes modern social dynamics. Due to the process of society informatization, there are systemic changes, according to which all segments of society and each person are included in the global information space, becoming elements of the global information system and, accordingly, to some extent depend on it (Babanina, Tkachenko, Matiushenko, & Krutevych, 2021). The constant development of the market leads to the emergence of new financial instruments, goods, products and monetary surrogates (Dumchikov, Kononenko, Batsenko, Halenin & Hlushchenko, 2020).At the same time, accelerated scientific and technological progress, the global society computerization has led to significant changes, which are manifested in both positive and negative consequences for any sphere of public life. The positive consequences include the automation of most actions, which greatly facilitates the existence of each. The negative effects of computerization are expressed in the emergence of new types of cybercrime, characterized by high social danger. This means cases of violation of national and international law in cyberspace and/or with the use of information technology (Kurmaiev, Seliverstova, Bondarenko, & Husarevych, 2020). Today, this issue is very important to address and very relevant for discussion. Applying deterrent measures against cybercrime is important for domestic cybersecurity to protect the nation's critical infrastructure, as well as for individuals. In this regard, the main goal of the authorities is to prevent cyberattacks and protect the country's critical infrastructure. In addition, reducing vulnerability to cyberattacks is important to reduce and minimize damage and recovery time. To prevent criminal offenses in cyberspace, it is necessary to clearly understand the patterns of these criminally illegal acts in cyberspace and the online behavior of these criminals (Bhavna, 2016). In this regard, the peculiarities of the criminal offenses in cyberspace investigation are undoubted of particular scientific interest. This is due to the value of the subject of this criminal offense and, of course, the vulnerability of computer information. It is important to note that due to the large scale of non-cash payment, there are new types of criminally illegal acts, especially Internet fraud, which threatens the economic life of the country and its population. One of the main measures to combat this destructive phenomenon is to develop effective measures, methods, tactics, and techniques of its

investigation, which, of course, will ensure its prevention and active struggle.

The article aims to characterize the forensic features of the initial stage of investigating fraud with financial resources in cyberspace, its significance, analysis, and justification as a type of cybercrime that is dangerous for everyone, and prove the need for urgent measures to prevent and combat such criminal offenses. The object of the scientific article is the criminal activity of persons who commit fraud with financial resources in cyberspace and the search and cognitive activity of persons who investigate this type of criminal offense.

Theoretical firework

Cybercrime

With the development of information technology, the concept of "computer" is becoming commonplace. Currently, almost all gadgets have access to the Internet. With the growing statistics of computer users, the number of trusting consumers who are unable to refuse attractive offers, as well as those who use the Internet to commit illegal acts, is increasing. Computer and telecommunication systems not only open unique opportunities to meet the broadest demands of man in all spheres of his life and the functioning of the state but also create favorable conditions for all kinds of malicious actions.

The scale and structure of cybercrime in different countries vary considerably and depend primarily on the nature and level of information technology development, the extent of the Internet, the use of electronic services, and e-commerce. The authors also emphasize that so far the world community has not developed a single terminology and a single approach to the phenomenon and concept of cybercrime, which is used along with the concept of cybercrime.

To control and prevent cybercrimes, researchers have attempt to understand the causion of ybercrime(Nguyen, 2020).

The term "cybercrime" is not defined in legally enforceable enactments. At the same time, the concept was formed due to the activities of law enforcement agencies of developed countries in Europe and the world and concerns criminal offenses in the field of computer information and telecommunications, illicit trafficking in electronic and special hardware, distribution of unlicensed computer software, and some other types of criminal offenses (Bondarenko & Repin, 2018).

In domestic and foreign scientific circles, criminal offenses committed in computer and telecommunications systems are nominated differently: computer crimes, crimes in the field of high technology, information crimes, cybercrimes, crimes in the field of computer information security, crimes in the field of computer information, criminal offenses in cyberspace, etc. (Vorobiev, 2014).

Crime on the Internet is often referred to as cybercrime and occurs because "the perpetrator uses expert knowledge of cyberspace" (Furnell, 2002).

However, the concept of "cybercrime" is semantically broader than "computer crime" and more accurately reflects the essence of such a global phenomenon as a crime in the information space. If the term "cybercrime" refers to both the use of computers and the use of information technology and global networks, the concept of "computer crime" mainly refers to crimes committed against electronic devices and stored data in them (Nomokonov & Tropina, 2013).

The existing variety of approaches to understanding this phenomenon was analyzed by V. Dulenko, R. Mamleev, and V. Pestrikov, in particular, they believe that cybercrime in the broadest sense - is any illegal act committed with or in connection with computer devices, including crimes such as illegal storage, supply or dissemination of information through the use of computer technology (Dulenko, Mamleev & Pestrikov, 2007).

According to I. Chekunov, cybercrimes are socially dangerous acts committed with the use of means and methods of computer and mobile (cellular) equipment, their software components for the information posted, used, processed, variable in the virtual space of the Internet (Chekunov, 2012).

According to M. McGuire and S. Dowling, cybercrime can be seen as a broad general term that encompasses cybercrime when computers and technology are used as an ancillary role, such as using a computer to send harassment messages. At the same time, the term "cybercrime" also includes computer-based crimes that are a direct result of computer technology and would not exist without them, such as the unauthorized intrusion of a computer system (McGuire and Dowling, 2013).

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Plumbing the depths of cyberspace from the standpoint of criminology, we note the most important methodological specifics of this science: it explores any objects of material and ideal macro and microworld. In other words, the composition of the tasks in the study of cyberspace and cybercrime is due to the infinite variety of investigative, forensic, and expert situations, due to which the methodological potential of studying virtual crime must necessarily embody the richness of general and special forensic knowledge.

The generalization of various aspects of the investigation of virtual crime, studied by many authors, suggests that cyberspace must be known through the field of interpenetration and interaction in the perspective of a systems approach as an object as a complex phenomenon formed from the elements between which it forms the relatively unchanged structure and ensure its integrity.

Methodology

To achieve this goal, a set of methods of scientific cognition was used in the article. With the help of the logical-semantic method, the conceptual apparatus of our research is generalized and improved. At the same time, the system-structural method helped to single out elements of the model of the mechanism of fraud with financial resources in the field of computer information. The analytical method allowed us to analyze statistical data and make reasoned conclusions based on them. The formal-legal method and the method of forecasting made it possible to clarify and single out the elements of the mechanism of the criminal offense of fraud with financial resources in cyberspace. It is necessary to dwell on the dialectical method, which was used to try to form some theoretical generalizations, in particular on the model of the mechanism of committing fraud with financial resources in the field of computer information. Also, the method of interpretation and hermeneutics was used in our study to ensure the definition of the conceptual and categorical apparatus of criminal offenses in cyberspace.

Results and discussion

General provisions of the forensic characteristics of fraud with financial resources in cyberspace

Given the complex nature of the criminal activity considered by us, it should be noted that the method of committing fraud with financial resources has a certain structure. It consists of preparation for commission, implementation of the method of commission, as well as activities aimed at concealing the traces of this criminal offense. Consider them in more detail.

It should be noted that the specifics of fraud with financial resources in the field of computer information is that already at the stage of preparation, criminals carry out activities aimed at concealing the traces of a criminal offense. This is expressed, for example, in the creation of malicious programs that allow you to enter the victim's computer without informing him about it, remote access to the victim's computer, or communicate with him at a considerable distance using various programs.

In addition, depending on the chosen method, criminals develop appropriate sites where the victim receives information or sends malware or information that is used to involve the victim in fraudulent schemes. Similarly, depending on the method of committing fraud with financial resources, tools and means are selected (computer hardware, provider, computer network, etc.), as well as persons who, depending on the distribution of roles, perform the assigned duties on commission of fraud with financial resources. The peculiarity of the selection of these persons is that in certain cases they may not know the true purpose of their activities (development of a program that can then be used as malicious, courier services) (Rozsoliv, 2009). An analysis of investigative and forensic science, as well as scientific and legal literature, states that there is no single approach to the classification of methods of committing fraud with financial resources in the field of computer information.

It should be noted that in the authors' opinion, there is no numerus clausus of ways to commit this act. This approach, of course, can negatively affect the ability to qualify, in the event of new ways of committing fraud in the field of computer information. However, this is an inevitable situation to be prepared for.

This approach is the basis for the classification of the main ways of committing computer fraud in the Convention on Cybercrime, in Art. 8 which stipulates that to qualify in its national criminal law, following its domestic law, in the case of intentional and without the right to deprive another person of his property by a) any introduction, modification, removal or blocking of computer data; b) any interference with the operation of a computer system, fraudulent or dishonest intent to misappropriate economic benefits for oneself or another person (Council of Europe, 2001).

To date, a large number of different computer programs have been developed for the functioning of the computer network and its facilities and, accordingly, for the commission of corrupt criminal offenses in the field of computer information. According to O. Zuban, only according to the most modest estimates, Trojans are installed on several million machines around the world and can update their versions, receive instructions from pre-prepared (Zuban, 2003).

Thus, fully agreeing that without correlations between the elements there is no forensic characterization of any type of criminal offense, the above allows us to state with confidence that the interdependent (correlation) relationships between the elements of the forensic characterization of fraud with financial resources in the field of computer information are quite clearly visible in their detailed analysis, during the study of forensic practice and the provisions of science, which significantly has a positive effect on the possibility of preparing scientific provisions and developed on their basis practical recommendations for investigating this type of criminal activity.

The information model of the mechanism of committing fraud with financial resources in the field of computer information

Along with the forensic characteristics, in science, such a category as the mechanism of a criminal offense is quite actively developed. This is because the mechanism of a criminal offense characterizes the functional side of the act. The mechanism of a criminal offense is a system of elements of forensic characterization of criminal offenses, which reflects the process of preparation, commission, and concealment of a criminal offense, which leads to the formation of traces that are important for solving criminal proceedings. The forensic mechanism of a criminal offense includes elements of its forensic characteristics.

The mechanism of a criminal offense should be understood as a system of processes of interaction of the participants in this act, both direct and indirect, with each other and with the material environment associated with the use of appropriate tools, means, and other individual elements of the situation. In the scientific literature, it is rightly noted that the mechanism of a criminal offense naturally causes the emergence of criminologically significant information about the criminally illegal act, its participants, and results.

From the standpoint of a systematic approach, the mechanism of fraud with financial resources in the field of computer information is considered as a complex entity, the specificity of which is determined not so much by elements of its structure, but by the nature of relations and connections between elements (Ilyushin, 2007). As it is known, in the course of the investigating criminal proceedings, the activities of the investigator should be purposeful and aimed at clarifying the mechanism of the criminal offense. Knowledge of the most typical mechanisms of criminally illegal acts will allow forming an imaginary model of the mechanism of the offense, to determine the direction of research of available evidence and the place of search for new, missing information about the illegal act and its participants. The value of this approach is that it allows you to track the development of a criminal event in action and its consequences (and all its participants) from the origin of the criminal plan to its implementation, as well as the stages of formation of the mechanism of a criminal offense.

Thus, the basis for creating a model of the criminal offense mechanism is information about it. This fact allows the development of a model of the mechanism of fraud with financial resources in the field of computer information to take the statement of R. Belkin, who notes that "information about the mechanism of criminal offense and related circumstances arising from the formation of this mechanism and replenished throughout the time of its operation, occurs inevitably, and the process of its occurrence is natural" (Belkin, 2013).

The concept "mechanism of a criminal offense" focuses on the elements of its composition, relating to its subjective side. In the process of retrospective cognition, which is the investigation, the establishment of elements of the subjective side (purpose and motives, guilt and its forms) is possible only based on a single

"objective material" - the specific actions of the participants in the crime.

Within this framework, the main elements of the model of the mechanism of fraud with financial resources in the field of computer information, from the authors' point of view will be:

1) the activity of the subject of a criminal offense - a fraudster who commits theft by deleting, blocking, modifying computer information or other interference in the operation of storage, processing, or transmission of computer information or information and telecommunications networks (fraud or abuse) trust, as a rule, is characteristic at the stage of preparation for a crime) in cyberspace;
2) a set of actions, deeds of the victim of fraud with financial resources, committed in the field of computer information;
3) a set of actions, deeds of persons who were indirectly related to the criminal event;
4) elements of the situation used by the participants in the criminal event, including the subject of the criminal encroachment.

The information model of the mechanism of a criminal offense, created based on the analysis of the practice of investigation of this type of criminal offenses and scientific provisions, allows equipping the investigator with complex system knowledge that promotes optimization of all investigation process. In the process of investigating fraud with financial resources in the field of computer information, the investigator uses a typical model of criminal offense and, using such techniques of logical thinking as comparison and analogy, compares the information with the model, filling in the missing links due to the derived relationships between criminal the activities of the subject, the set of actions, deeds of the victim and persons who were indirectly related to the event of the criminal offense, as well as individual elements of the situation used by the participants in the criminal event.

Features of the opening of criminal proceedings on fraud with financial resources in the field of computer information and the initial stage of the investigation

A comprehensive model for investigating cybercrime is important (Ciardhuáin, 2004). Investigation of criminal offenses is a complex social activity that includes three subsystems: collection (receipt), examination of evidence and proof; search and obtain orienting information; use of office knowledge.

The initial stage of the investigation of any criminal offense is the stage of opening criminal proceedings. Its specificity is due to the peculiarity of a particular type of criminal offense and determines the algorithm of the investigator's actions in identifying signs of a particular criminal offense. These signs affect the choice of forces and means, as well as the entire course of further investigation. A study of investigative and judicial practice in criminal proceedings for fraud with financial resources in the field of computer information shows that in all cases, the investigation of this category of criminal offenses has changed its mind a special inspection. In 27% of cases, it lasted quite a long time (up to 30 days or more) (Rossinskaya, 2015).

Analysis of the materials of criminal proceedings on fraud with financial resources in the field of computer information shows that upon receipt of data on the committed criminal offense, a preliminary inspection by law enforcement agencies was conducted in all cases. From our point of view, this is due to several objective reasons. First, the signs of fraud with financial resources in the field of computer information (objective and subjective), as a rule, are not pronounced. Their detection requires certain, sometimes quite complex and consistent procedural and other actions (EMA de Ucrania, 2016).

Secondly, as noted earlier, the legislator went the way of maintaining the preliminary inspection in criminal proceedings. At the same time, to provide evidence of forensically significant information that indicates a criminal offense, significantly expanded the possibility of using various procedural and non-procedural means.

The opening of criminal proceedings on the fact of fraud with financial resources in the field of computer information determines the procedure for carrying out actions (preliminary verification) aimed at identifying the circumstances of the act. We can say that the situation at the time of receiving information about the event (let's call it investigative), significantly affects the entire process of the investigator's activities due to the sources and nature of the information obtained (EMA de Ucrania, 2016).

In addition, the choice of means of preliminary verification is influenced by the situation that develops at the time of receipt by the investigator

of information about fraud with financial resources in the field of computer information. As the analysis of investigative and judicial practice shows, during this period there are two types (verification) situations.

1. Criminals continue to commit illegal acts, and there is a strong link between them and the person against whom the computer fraud is committed with financial resources (20% of cases studied).
2. The criminal offense is over and the connection between the person against whom it was committed and the fraudsters is absent (80% of cases studied).

In all cases, the investigator must document the nature and features of the activities of a legal entity that has suffered from fraud, as well as its legal status, features of protection of objects, access regime. Based on the results of the study of documents, security representatives and support staff should be interviewed, who could see outsiders who participated in the preparation and implementation of fraud with financial resources. In the presence of bandwidth or video recordings, during the study of the content of documents or video may be found constituent data of persons or their appearance in case of their penetration into the organization in preparation for fraud (repair of computer equipment, repair of electricity, etc. .).

When carrying out verification actions, it is necessary to take into account that the evidence obtained during it should be fully used in the course of further investigation, as it is impossible to obtain some of them in other ways in the future. This should be taken into account when conducting an investigation in criminal proceedings for fraud with financial resources in the field of computer information. In all cases, the results of the preliminary inspection affect the formation of investigative situations of the initial stage of the investigation of fraud in the field of computer information and the mechanism for resolving them (EMA de Ucrania, 2016).

The result of the inspection and determining the moment of its completion is the presence of the investigator's belief that the data obtained is sufficient to open a criminal investigation into fraud in the field of computer information. Given the specificity of a criminal offense, such data should indicate not only the impact on computer information but also the theft of specific financial resources. Only in this case can criminal proceedings be opened on the fact of committing fraud with financial resources. In all other cases, criminal proceedings must be instituted under other articles or a decision shall be made to refuse to institute criminal proceedings. The whole list of procedural and non-procedural actions listed above is aimed at obtaining data, which, ultimately, will be the basis for initiating criminal proceedings.

Tactical features of individual investigative actions at the initial stage of investigation of fraud with financial resources in cyberspace

Investigative actions are the cognitive tools of the investigator and universal means of obtaining evidence. Their production is due to the need to obtain criminally relevant information, which is important for establishing the circumstances of the investigated criminal event that constitute the subject (Uplan, 2017).

The structure and content of each investigative action, aimed at directly obtaining objective and complete information about the investigated event, and the whole system of investigative actions, in general, are not only formed on scientifically verified positions, but also aim to use the investigator in their work and scientific and technical tactical means, and the achievement of advanced scientific thought.

The process of investigating fraud with financial resources in the field of computer information requires the production of a significant number of legally regulated, investigative, and other procedural actions, and the tactics of their production directly depend on the specifics of the mechanism of a criminal offense.

Based on the authors' analysis of investigative and judicial practice, the following investigative and other procedural actions are most often carried out:

– inspection of the scene, an inspection of objects and documents (100% of criminal proceedings);
– interrogation of persons whose procedural status has been determined (100% of criminal proceedings). In most cases, this is the interrogation of victims and witnesses, and when identifying persons who have committed a criminal offense, it is the interrogation of suspects and accused. It should be noted here that the interrogation of these persons during their establishment may be carried out after a considerable period;
– appointment and production of forensic examinations (100% of criminal

proceedings). In 100% of cases, a computer examination was ordered; in 60% - ktyloscopic examination; in 55% of cases - forensic examination of documents; 25% - trasological examination; in 10% - psychological examination; in 5% of cases - others).

When conducting investigative actions, the presence of forensic information that was obtained during the preliminary inspection at the stage of opening criminal proceedings should be positively assessed. As noted earlier, during such an investigation, the investigator receives up to 40% of the evidentiary information. At the initial stage of the investigation, this affects the creation of a favorable investigative situation, as well as the process of further investigation. (Uplan, 2017).

Tactical and forensic support for the production of investigative actions in the investigation of fraud with financial resources is associated with the peculiarities of the mechanism of committing this criminally illegal act. Particular attention in the investigation of fraud with financial resources in cyberspace should be paid to such an investigative action as a survey of the scene. The specifics of this investigative action should also be taken into account when investigating fraud with financial resources in cyberspace.

Site inspection, as well as search, seizure, investigative experiments belong to the group of non-verbal investigative actions. They allow to form in the mind of the cognizer, the investigator an imaginary image of material objects based on sensory (visual), which is not expressed in verbal (conditional-signal) form. These actions are related to the personal perception of the persons conducting the investigation, the circumstances of the objective reality preserved in the trace. This is a different way of cognition, compared to verbal investigative actions, which has its pros and cons. But each of these methods is of great importance for establishing all the circumstances that are part of the subject of criminal procedure knowledge (Karchevskaya, 2017).

During the inspection of the scene, the investigator establishes, investigates, and records the situation at the scene, traces of the crime, the offender, and other facts that allow in conjunction with other evidence to conclude the mechanism of the crime:

- computer traces, as well as their objects - media (eg, computer or system unit, flash drives);
- traditional traces of the presence of a particular person at the scene;
- features of access, organization, operation, and devices of different types of networks, through which the fraud was committed;
- recording and video recording devices available on the territory of the institution or the territory adjacent to the crime scene.

Especially important for this category of criminal proceedings are the analysis of the previous activities of the suspect (labor and training), the appointment of forensic psychological and forensic psychiatric examinations and taking into account their findings, direct observation. The result of the analysis of various information about the interrogated during the preparation for interrogation should be the establishment by the investigator of the level of knowledge and information about computer technology possessed by the offender, what the crime was related to, whether the interrogated person could commit this crime or not. (Dovzhenko, 2019).

It should be noted that quite rarely (no more than 3% of cases) when individual criminals contributed to the investigation, investigative experiments were conducted to establish the principle of malware development, which were used to commit computer fraud with financial resources in cyberspace. In these cases, the presence of a specialist in the field of computer hardware and technology is required. In addition, the results of the production of such an investigative experiment are necessary to conduct a computer-technical examination (Uplan, 2017).

Thus, the production of investigative and other procedural actions in criminal proceedings on fraud with financial resources in cyberspace has certain features that are fully due to the mechanism of criminal activity, as well as the perpetrators. To achieve a positive result and the purpose of the investigative action, the investigator must carefully prepare, using a variety of tactics and the assistance of specialists.

Conclusions

Based on the above material, we can conclude that the current state of cybercrime poses great threats to society, and the number of cybercrimes is growing every year. Internet fraud with financial resources, in turn, poses a global threat to the economy of every country in the world. Today, the effectiveness of combating Internet fraud and the level of cybersecurity in Ukraine is very low, and therefore we should not neglect

such an important component as the Internet, as in advanced countries this area is a priority in domestic and foreign policy. But a comprehensive fight against this problem requires the joint efforts of the state, citizens, international cooperation, and relevant legislation. In addition, the sweetness of the investigation of fraud with financial resources in cyberspace is due to the manifestation of new methods and ways of committing the analyzed criminal offense and the lack of development of forensic techniques and tactics. Investigating financial fraud in cyberspace requires in-depth specific knowledge from the subjects of the investigation, which, unfortunately, cannot be obtained by them for various reasons. For example, the obsolescence of scientific and practical training and technology. All of the above, in turn, complicates the prevention and counteraction of illegal actions, and this allows them to exist for such a long period.

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

Belkin, R.S. (2013). Forensics course. General theory of criminology. Moscow: Lawyer.

Bhavna, A. (2016). Exploring and analyzing Internet crimes and their behaviours. Perspectives in Science, 8, 540-542. Recovered from: https://www.sciencedirect.com/science/article/pii/S2213020916301537

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

Chekunov, I.G. (2012). Modern cyber threats. Criminal law and criminological classification and qualification of cybercrimes. Moscow: Jurist.

Ciardhuáin, S.Ó. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1). Recovered from: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

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

Dovzhenko, O. Yu. (2019). On the question of tactics of interrogations in cases of cyber crimes. Scientific Bulletin of the International Humanities University, № 37, 143-145. Recovered from: http://vestnik-pravo.mgu.od.ua/archive/juspradenc37/37.pdf

Dulenko, V.A., Mamleev, R. R., & Pestrikov, V.A. (2007). The use of high technology in a criminal environment. Fighting crimes in the field of computer information: textbook. help. Kyiv: Riv pres.

Dumchikov, M., Kononenko, N., Batsenko, L., Halenin, R., & Hlushchenko, N. (2020). Issues of regulating cryptocurrency and control over its turnover: international experience. Amazonia Investiga, 9(31), 10-20. https://doi.org/10.34069/AI/2020.31.07.1

EMA de Ucrania (2016). Safe Card: the first results were summed up at the Forum of Security of Settlements and Credits Source Recovered from: https://www.ema.com.ua/news/pervye-itogi-podvedeny-na-forume-bezopasnosti-raschetov-i-kreditov/

Furnell, S. (2002). Cyber Crime: Vandalizing the Information Society. London: Addison Wesley.

Uplan (2017) How are cybercrimes investigated in Ukraine? Recovered from: https://uplan.org.ua/analytics/iak-v-ukraini-rozsliduiut-kiberzlochyny/

Ilyushin, D.A. (2007). Peculiarities of initiating criminal cases on crimes committed in the sphere of providing Internet services. Visnyk of SamSU, № 1(51), 9-16. Recovered from https://cyberleninka.ru/article/n/osobennosti-vozbuzhdeniya-ugolovnyh-del-o-prestupleniyah-sovershaemyh-v-sfere-predostavleniya-uslug-internet/viewer

Karchevskaya, Yu. S. (2017). Carding as the most popular type of cyber crime of minors in the republic of Belarus. Theoretical and applied issues of combating crimes committed with the use of information technology, № 2, 17-20. Recovered from http://www.institutemvd.by/components/com_chronoforms5/chronoforms/uploads/20180103154844_Karchevskaja.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

McGuire, M., and S. Dowling (2013). Cybercrime: A Review of the Evidence. Home Office. Recovered from:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Nguyen, T.V. (2020). Cybercrime in Vietnam: An Analysis based on Routine Activity Theory. International Journal of Cyber Criminology, 14(1), 156-173. http://dx.doi.org/10.5281/zenodo.3747516

Nomokonov, V.A., & Tropina, T.L. (2013). Cybercrime: problems of struggle and forecasts. Forensic Library, Vol. 1, 148-159.

Rossinskaya, O. R. (2015). Computer crimes: criminal law and forensic aspects. Voronezh forensic readings, Vol. 3, 169-183.

Rozsoliv, I.M. (2009). Law and the Internet. Theoretical problems. Moscow: Norma.

Vorobiev, V. V. (2014). Crimes in the field of computer information: Legal characteristics composition qualification (PhD thesis), Syktyvkar State University named after Pitirim Sorokin, Russia. Recovered from: https://www.dissercat.com/content/prestupleniya-v-sfere-kompyuternoi-informatsii-yuridicheskaya-kharakteristika-sostavov-i-kva

Zuban, O.V. (2003). The problem of spam and its solution. Moscow: Norma.