Problems of electronic funds theft investigation

Svetlana Mikhailovna Golyatina*

Volgograd Academy of the Ministry of Internal Affairs of Russia, Volgograd, Russia

Abstract. The number of thefts of electronic funds is growing each year. Regretfully this trend is observed not only in Russia but also in several foreign countries. Another surge in remote theft and fraud was triggered by the coronavirus pandemic, during which both large corporations and individual citizens became victims of cyberattacks. Scientists and various Internet sources note that today criminals are constantly developing new schemes for committing theft of electronic funds and are one step ahead of law enforcement. Since the number of crimes under consideration is increasing, and their detection rate remains extremely low, it can be assumed that the existing method of investigating electronic funds theft is not effective enough. In our opinion, to improve the situation, it is first of all necessary to identify the range of main problems that law enforcement officers face when investigating such crimes. By analyzing investigative practice, scientific literature, documents, and materials published on various websites, we have identified some of them and conditionally divided them into two groups that cannot be considered in isolation from each other: organizational problems (lack of interaction between departments of different countries, problems of the appointment and execution of computer-technical examinations, long time for obtaining information that has evidentiary value, the low competence of law enforcement officers and their minor experience of working with specific sources of evidentiary information, etc.) and problems directly related to the investigation of electronic funds theft, with the main one being the problem of establishing the crime scene.

Keywords: electronic funds, cybercrime, internet fraud, investigation

1 Introduction

The coronavirus pandemic has once again confirmed that today the Internet is one of the most popular and convenient platforms for doing business. While many were experiencing a lockdown incurring losses (tour operators, cinemas, airlines), online trading was gaining momentum. Thus, according to various estimates, the total audience of users of online stores in Russia alone has grown by 15-17 million people [1]. It is not surprising that the increase in the number of money thefts in the global network came along. In April 2020, in an interview with RIA Novosti, Deputy Chairman of the Board of Sberbank Stanislav Kuznetsov emphasized: “The COVID-19 virus has affected many countries and caused a surge in cybercrime. According to our data, since the beginning of the pandemic, scammers

*Corresponding author: svetlanagolyatina_6363@mail.ru

have registered more than 4000 domains with the words "coronavirus", covid, and so on. At the same time, the number of phishing emails increased by 30% compared to the previous quarter" [2]. European experts also indicate this. For example, the United Kingdom's National Fraud Alert Center, Action Fraud, notes that between September 2019 and September 2020, it received over 17000 fraud reports totaling £ 657.4 million, up 28% compared to the same period last year. At the same time, the number of such messages increased especially sharply from May to September 2020, when the country adapted to life after self-isolation [3]. However, it should be said that even before the pandemic, the damage from the actions of cybercriminals was great: according to the "Follow the Money" report by the SWIFT interbank payment system and BAE Systems Applied Intelligence, in 2019 "cybercriminals: from individuals to organized groups, often associated with a certain state, earned ... $1.5 trillion" [4].

Today, ways of stealing money on the Internet have become more sophisticated and knowledge-intensive [5-10]. Almost all of them say that criminals are constantly developing new schemes and are one step ahead of law enforcers. Even though specialized divisions have been created in many countries and regions for the disclosure and investigation of such crimes (such as the Administration "K" of the Ministry of Internal Affairs in Russia, the European Cybercrime Center in the countries of the European Union, and the Computer Crime and Intellectual Property Section (CCIPS) in the USA) and there are algorithms for investigating electronic funds theft, the number of crimes continues to grow, and it is not always possible to punish those responsible. We believe that the standard technique for investigating the theft of electronic funds is not effective enough. It is necessary, first of all, to establish the range of problems that law enforcement officers face when investigating these crimes to improve it.

2 Methods

The research is based on the dialectical method of cognition and the system of general scientific and private scientific methods based on it. Current work implemented: the method of logical comprehension (when presenting the material and formulating conclusions), the statistical method (when analyzing quantitative indicators, reviews of investigative and judicial practice), the comparative method (when analyzing the activities of law enforcement agencies in different countries), the method of sociological research (when studying documents).

3 Results

By analyzing the investigative practice, scientific literature, documents, and materials published on various Internet sites, we identified a range of main problems that law enforcement officers face when investigating the theft of electronic funds (Fig. 1).

4 Discussion

The presented problems can be conditionally divided into two groups: 1) organizational problems; 2) problems directly related to the investigation of crimes. Both cannot be considered in isolation from each other.

Since today Internet theft is often transnational, the problem of interaction between divisions of different countries comes to the fore and becomes the main one. E.S. Shevchenko notes: "The difficulties of cooperation in the investigation and disclosure of cybercrimes with law enforcement agencies of foreign states are aggravated by the fact that different countries

have established their legislation standards concerning computer crimes, developed their approaches to the appointment and execution of computer forensics" [11, p. 35]. The participants of the European Commission used to speak about the same. In their opinion, the chance of detecting cybercriminals is extremely low. They see the reasons for this situation in the lack of information exchange between countries, different possibilities for investigations and forensic examinations, uncoordinated cooperation between law enforcement agencies and other participants possessing valuable information about the crimes committed (providers of payment systems and cellular communications) [12]. Besides, in Russia, the appointment of computer-technical forensic examinations is associated with several difficulties, such as the insufficient number of experts having access to their execution, the duration of execution, and the high cost of examination in non-governmental organizations.

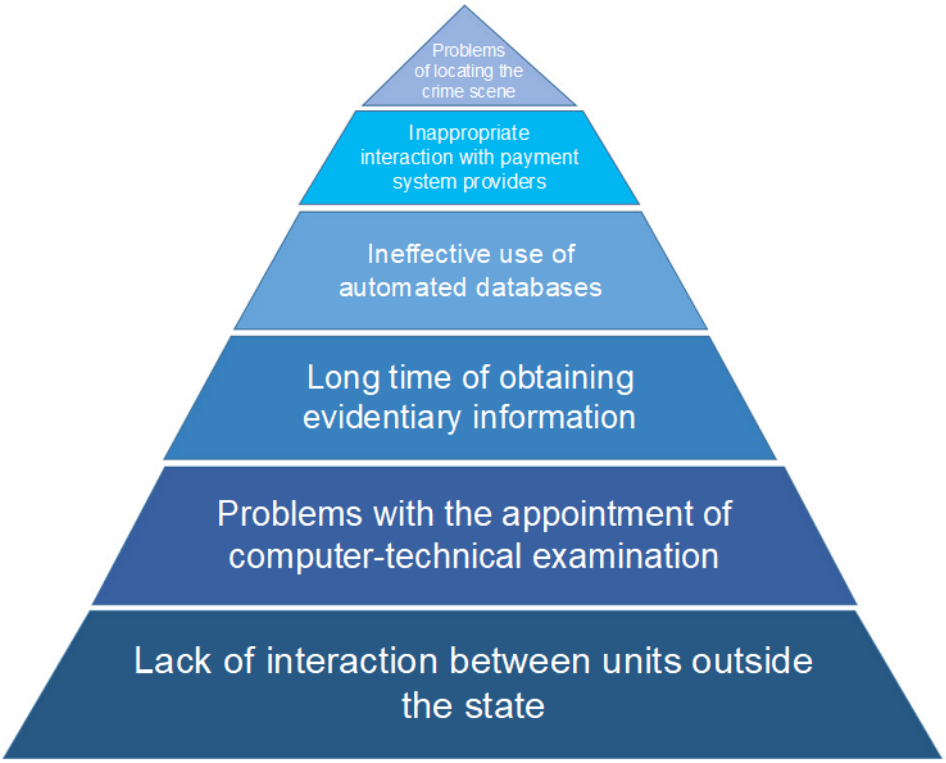

Fig. 1. The main problems arising during the investigation of electronic funds theft.

Some authors consider the low competence of law enforcement officers and their little experience of working with specific sources of evidentiary information in electronic digital form as electronic messages, pages, sites among the organizational problems [13]. According to A.S. Shatalov, "... here, like nowhere else, there is a high probability that the evidence that had been nevertheless discovered may be unintentionally changed and even lost as a result of mistakes made in recording or, for example, withdrawing, and during the investigation. Preparation of evidence of this kind in the course of pre-trial proceedings in a criminal case to be further presented in court requires not only thorough professional training, but also regular updating of existing knowledge among investigators, interrogators, operatives, and, of course, specialists and experts" [14].

Other no less significant problems in the investigation of electronic money theft are the following: the duration of obtaining information (ranging from 1 to 3 months) that has

evidentiary value in criminal cases; ineffective use of automated information bases and the lack of an information storage system in investigative departments; limited periods of information storage in banks and payment systems [15]. All this slows down the investigation and allows criminals to destroy traces and hide.

Among the problems directly related to the investigation of the electronic funds' theft is the problem of establishing the crime scene. Since online fraud and theft are often carried out remotely, law enforcement officers need to locate a specific technical device with which the victim's funds were accessed. Then, after establishing the IP address of the device, the provider needs to be contacted to find out the individual the contract for the provision of communication services was concluded with. Finally, it is necessary to prove that it was this person who used this technical device to commit illegal actions. It can be aggravated by the fact that the IP address can be registered in the territory of another state. O.A. Naumenko notes: "A free and uncomplicated way of using foreign IP addresses, servers and resources (for example, mailbox servers @google.com, @yahoo.com, @aol.com), which are outside the jurisdiction of the Russian Federation, almost completely excludes the possibility of obtaining the necessary information by employees of the Ministry of Internal Affairs of Russia. Therefore, a serious obstacle in the investigation of crimes of this category is the lack of agreements between Russia and some foreign states on the provision of legal assistance in the investigation of criminal cases" [15]. This brings us back to the problem of interaction between divisions of different countries. Therefore, in our opinion, it is precisely the one that requires an immediate solution.

5 Conclusion

To increase the efficiency of investigating electronic funds theft, first of all, it is necessary to solve organizational problems, to establish interaction between the relevant divisions of different countries and providers of payment systems and cellular communications. This will allow receiving the necessary information on time and speed up the investigation. Also, it is worthwhile to regularly generalize the results of the practice of investigating electronic funds theft in Russia and foreign countries and, on this basis, to constantly improve the standard method of investigating the crimes in question; to introduce new forensic and technical methods and means into practice; to improve the competence of law enforcement officials.

References

1. The pandemic has seized online commerce. Accessed on: October 05, 2020. [Online]. Available: kommersant.ru
2. Stanislav Kuznetsov: the coronavirus has spawned new fraudulent schemes. Accessed on: October 05, 2020. [Online]. Available: ria.ru
3. Action Fraud warns of rise in investment fraud reports as nation enters second lockdown. Accessed on: October 05, 2020. [Online]. Available: https://www.actionfraud.police.uk/news/action-fraud-warns-of-rise-in-investment-fraud-reports-as-nation-enters-second-lockdown
4. Follow the Money. Accessed on: October 05, 2020. [Online]. Available: swift_bae_report_Follow-TheMoney.pdf
5. V.G. Lyuban, A.Y. Molyanov, E.N. Khazov, Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia **1**, 190 (2019)
6. I.A. Mikhailenko, Siberian Criminal Procedural and Criminalistic Readings, **5(13)**, 98 (2016)

7. A.Y. Sypachev, Nauchno-metodicheskiy Elektronnyi Zhurnal “Kontsept” [Concept Scientific and Methodological Electronic Journal], **10**, 71 (2015)
8. B.P. Smagorinsky, A.V. Sycheva, Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia, **53(2)**, 111 (2020)
9. M. Offei, F.K. Andoh-Baidoo, E. Ayaburi, D. Asamoah, *Understanding Internet Fraud: Denial of Risk Theory Perspective*, in ICT Unbounded, Social Impact of Bright ICT Adoption, IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2019, June 21-22, Accra, Ghana (2019). https://doi.org/1 10.1007 / 978-3-030-20671-0_28/
10. D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, N. Díaz-Castaño, European Societies, **1** (2020). https://doi.org/10.1080/14616696.2020.1804973
11. E.S. Shevchenko, Tactics of executing certain investigative actions in the investigation of cybercrimes, PhD thesis in Law (Moscow, 2016)
12. Frequently Asked Questions: the new European Cybercrime Center. Accessed on: October 05, 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_12_221
13. S.A. Nesterovich, Bulletin of Science and Education, **2(8-44)**, 46 (2018)
14. A.S. Shatalov, Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia, **3(32)**, 7 (2018)
15. O.A. Naumenko, Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia, **3(45)**, 60 (2019)