BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg

INVESTIGATIVE USE OF SPECIALIZED KNOWLEDGE IN FRAUD CASES COMMITTED THROUGH INFORMATION TECHNOLOGIES

Amirkhon Nosirov
Independent Researcher,
Department of Criminalistics and Forensic Expertise,
Tashkent State University of Law
E-mail: a.nosirov.1111tsul@gmail.com
https://doi.org/10.5281/zenodo.20473447

ABSTRACT

This article examines the application of specialized knowledge in the investigation of fraud offenses committed through the use of information technologies. It explores the role of specialized expertise in investigating technology-enabled fraud, including investigative measures conducted by law enforcement agencies, as well as the procedures for appointing and conducting forensic examinations. The study also provides a comprehensive analysis of artificial intelligence technologies and cryptocurrency transaction monitoring systems used for the early detection of fraudulent activities, along with mechanisms of international cooperation in combating cyber-enabled fraud.

Keywords: computer forensic examination, forensic technical examination, digital evidence, crime traces, malicious software, artificial intelligence, cryptocurrency tracking, digital forensics, international cooperation.

During criminal investigations, an inquiry officer or investigator may involve a specialist or expert in procedural activities or appoint a forensic examination in order to apply specialized knowledge when conducting specific investigative actions. These legal forms of utilizing specialized knowledge are regulated by the Criminal Procedure Code of the Republic of Uzbekistan and the Law of the Republic of Uzbekistan "On Forensic Expertise."

In contemporary conditions, digital crime has undergone global transformation and continues to grow at a rapid pace. According to the analyses presented in the World Economic Forum's Global Risks Report 2023, "widespread cybercrime and cyber insecurity" ranks eighth among the most significant threats facing the global community over the next decade[1]. Furthermore, data from the U.S. Federal Trade Commission's Consumer Sentinel Network Data Book 2022 confirms the increasing severity of this threat. According to the report, consumers suffered financial losses amounting to USD 8.8 billion as a result of fraud, representing an increase of more than 30 percent compared to the previous year[2]. In the investigation of fraud offenses committed through information technologies, two principal types of forensic examinations are commonly employed: computer forensic examination and forensic technical examination[3]. Depending on the specific

[1] World Economic Forum. The Global Risks Report 2023, 18th Edition. — Geneva: World Economic Forum, 2023. — 98 p.
[2] Federal Trade Commission. Consumer Sentinel Network Data Book 2022. — Washington D.C.: FTC, February 2023.
[3] Мещерякова А.А. Особенности расследования преступлений, совершаемых с использованием пластиковых карт // Вестник криминалистики. — 2010. — №4. — С. 86

circumstances of the case, handwriting, dactyloscopic, and forensic economic examinations may also be appointed.

In the investigation of fraud offenses committed through information technologies, the main types of forensic examinations conducted are computer forensic examinations and forensic technical examinations. Depending on the specific circumstances of the case, handwriting, dactyloscopic, and forensic economic examinations may also be appointed.

One of the key types of forensic examination appointed in the investigation of fraud committed through information technologies is computer forensic examination. This type of examination is conducted to analyze digital devices and software, determine their relevance to the investigated crime, and examine digital traces associated with criminal activity. As noted by leading expert in digital forensics Eoghan Casey, digital evidence plays an increasingly central role in criminal investigations, and its lawful collection and preservation is a fundamental requirement for effective investigative practice[4].

The seizure and proper documentation of digital devices used in the commission of a crime are of critical importance in the investigative process. According to A.L. Osipenko, the specific nature of crimes committed via the Internet is reflected in the evidentiary process, where failure to timely formalize relevant information often results in the necessity of relying on alternative methods of proof and evidence collection[5].

Another distinctive feature of investigating crimes committed using digital devices and software is the possibility of changes in criminal charges due to the use of virtual and digital evidence. For instance, a criminal case initially initiated under Article 168 of the Criminal Code of the Republic of Uzbekistan may, during the investigation, be supplemented or reclassified under Article 278² (Unlawful Access to Computer Information) or Article 278⁶ (Creation, Use or Distribution of Malicious Software).

In computer forensic examinations, when analyzing seized devices such as computers, laptops, and flash drives, experts are typically asked the following questions:

1. Does the provided storage device contain information related to the production of bank cards or the use of their details?

2. Is the software intended for the production of bank cards, or has it been previously installed on the submitted computer?

3. Is there software installed on the computer that enables unauthorized access to computer information?

4. Has communication been conducted via this computer, through which applications, and what is its content?

Experts use software such as “EnCase,” “FTK,” and “Pasco” for the reconstruction of criminal digital traces[6]. According to the methodology of file system forensic analysis developed by Brian Carrier, specialized tools play a crucial role in reconstructing all operational traces on digital devices.

Another important type of forensic examination in the detection of such crimes is forensic document examination, which is conducted in cases where the authenticity of documents is in

[4] Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd edition. — Orlando: Academic Press, 2011. — 840 p.

[5] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. — М., 2004.

[6] Калмыков И.А., Пелешенко В.С. Компьютерная криминалистика. — Ставрополь: СКФУ, 2017. — 84 с.

doubt. Forensic technical examination is appointed to determine document forgery, the original condition of documents, subsequent alterations, authenticity of seals and stamps, methods of production, writing instruments used, and the materials of documents.

Handwriting examination may also be appointed in the investigation of such crimes. It is particularly useful in cases involving bank cards bearing cardholder signatures, payment slips for goods and services, checks, application forms for issuing or obtaining bank cards, and forged identity documents[7].

For seized bank cards, as well as materials used in their production, forensic examination of materials and substances may also be appointed. In forensic practice, due to scientific and technological development, document examination is increasingly conducted using advanced technical equipment[8]. These include devices such as the DVS-Portable video scanner, the "VSC-2000" video spectral comparator, the "ESDA" system, Leica DMK microscopes, and the "VSC-6000" video spectral device developed by the British company Foster & Freeman, among others[9].

With the development of modern technologies, artificial intelligence (AI) and machine learning methods are increasingly being applied in fraud detection systems. AI technologies are effectively used in digital forensics for automated analysis of large datasets, detection of anomalies, real-time monitoring of suspicious financial transactions, and prediction of fraud patterns. This approach significantly accelerates and enhances the effectiveness of traditional investigative methods.

In modern conditions, perpetrators of bank card fraud increasingly use new financial instruments such as cryptocurrencies. Cryptocurrency tracing is an important area of digital forensics, focusing on tracking and analyzing the flow of cryptocurrencies through blockchain networks[10]. In many cases, criminals convert funds into different currencies and transfer them across jurisdictions, which complicates investigations and creates issues related to jurisdiction and extradition.

During urgent investigative operations, law enforcement officers request data from telecommunication companies, banks, and electronic payment operators to collect personal information. Mobile operators provide data such as registered SIM cards, IMEI numbers, incoming and outgoing calls, and SMS records[11].

Similarly, banking data plays a crucial role in apprehending offenders. This includes personal identification data, financial transaction records, online banking activity, and currency conversion information. According to M. Conti and A. Dehghantanha, one of the most challenging issues in modern digital forensics is the lawful collection and preservation of electronic evidence from cloud technologies and mobile applications in compliance with legal standards[12].

---

[7] Волкова Г.П., Махова И.В., Чистова Л.Е. и др. Расследование отдельных видов мошенничества: учебное пособие. — С. 64.

[8] Филиппов М.Н. Особенности расследования краж и мошенничеств, совершённых с использованием банковских карт и их реквизитов: монография. — М. — С. 124.

[9] Калмыков И.А., Пелешенко В.С. Компьютерная криминалистика. — Ставрополь: СКФУ, 2017. — 84 с.

[10] Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G.M., Savage S. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names // Proceedings of the 2013 Internet Measurement Conference (IMC'13).

[11] Лаврушкина А. А. Типичные следственные действия в рамках методики расследования мошенничества с исползованием сети Интернет и средств мобилной связи . 2018. Т. 4. No 4. S. 447–451.

[12] Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things security and forensics: Challenges and opportunities // Future Generation Computer Systems. — 2018

However, operational and investigative measures do not always yield the expected results. This is mainly due to the fact that offenders often use specialized software to erase traces of their activities, SIM cards registered under third parties, and bank cards, accounts, or electronic wallets belonging to unrelated individuals. In combating cybercrime effectively, international cooperation plays a decisive role. In particular, the Council of Europe's Convention on Cybercrime (Budapest Convention, ETS No. 185), which entered into force on 1 July 2004, aims to harmonize national legislation, improve investigative methodologies, and strengthen international cooperation in combating cybercrime[13].

Determining the place of occurrence in fraud cases committed using information technologies is significantly more complex than in traditional crimes. In many cases, offenders commit crimes from foreign jurisdictions, convert funds into different currencies, and transfer them across borders, creating additional complications related to jurisdiction and extradition.

CONCLUSION

In conclusion, improving the identification of the place of occurrence in fraud investigations, enhancing international information exchange between investigative bodies, and addressing issues related to jurisdiction and extradition are essential tasks that require fundamental improvement.

Legal reforms, international cooperation (Budapest Convention), the development of advanced digital forensic capabilities, the implementation of artificial intelligence technologies, increased public awareness, and technological innovation represent key prospects for the development of digital forensics in the modern era. As stated in the World Economic Forum's Global Risks Report, cybercrime continues to intensify year by year, making a proactive approach an unavoidable necessity.The effective utilization of these opportunities and the active resolution of crime-related challenges associated with digital technologies are essential for ensuring justice and security in the modern technological era, where legal systems are continuously evolving alongside technological advancement.

REFERENCES

1. Meshcheryakova, A.A. (2010). Features of the investigation of crimes committed using plastic cards. *Bulletin of Criminalistics*, No. 4, p. 86.
2. Filippov, M.N. *Features of the investigation of thefts and frauds committed using bank cards and their credentials: a monograph*. Moscow, p. 125.
3. Osipenko, A.L. (2004). *The fight against crime in global computer networks: International experience: A monograph*. Moscow.
4. Volkova, G.P., Makhova, I.V., Chistova, L.E., et al. *Investigation of certain types of fraud: a textbook*, p. 64.
5. Filippov, M.N. *Features of the investigation of thefts and frauds committed using bank cards and their credentials: a monograph*. Moscow, p. 124.
6. Kalmykov, I.A., & Peleshenko, V.S. (2017). *Computer Forensics*. Stavropol: NCFU, 84 p.
7. Lavrushkina, A.A. (2018). Typical investigative actions within the methodology of investigating fraud using the Internet and mobile communications. Vol. 4, No. 4, pp. 447–451.

[13] Council of Europe. Convention on Cybercrime. ETS No. 185, Budapesht , 23 November 2001. Entered into force 1 July 2004.

8. World Economic Forum. (2023). *The Global Risks Report 2023*, 18th Edition. Geneva: World Economic Forum, 98 p. ISBN: 978-2-940631-96-5. URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
9. Federal Trade Commission. (2023). *Consumer Sentinel Network Data Book 2022*. Washington D.C.: FTC. URL: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2022
10. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd edition. Orlando: Academic Press, 840 p. ISBN: 978-0-12-374268-1. DOI: 10.5555/2021194.
11. Carrier, B. (2005). *File System Forensic Analysis*. Upper Saddle River, NJ: Addison-Wesley Professional, 600 p. ISBN: 0-321-26817-2.
12. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., & Savage, S. (2013). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. *Proceedings of the 2013 Internet Measurement Conference (IMC'13)*. Barcelona: ACM, pp. 127–140. DOI: 10.1145/2504730.2504747.
13. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, Vol. 78, pp. 544–546. DOI: 10.1016/j.future.2017.07.060.
14. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. ETS No. 185, Budapest, 23 November 2001. Entered into force 1 July 2004. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185