Вісник Тернопільського національного технічного університету
https://doi.org/10.33108/visnyk_tntu
Scientific Journal of the Ternopil National Technical University
2024, № 3 (115) https://doi.org/10.33108/visnyk_tntu2024.03
ISSN 2522-4433. Web: ***visnyk.tntu.edu.ua***

UDC 343.98

COMPUTER TECHNOLOGIES AS AN OBJECT AND SOURCE OF FORENSIC KNOWLEDGE: CHALLENGES AND PROSPECTS OF DEVELOPMENT

Valerii Muzh; Taras Lechachenko

Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

Abstract. *The article is dedicated to the examination of the impact of computer technologies on the development of forensic science as a whole, as well as their characterization as objects of forensic investigation. Within the scope of the research, an analysis of three main trends of forensic science in the field of information technologies is conducted. Computer technologies are considered as a means of obtaining evidence, the subject, and the instrument of crime. We conclude that computer technologies play a significant role in the process of forensic investigations, influencing the quality of criminal investigations, and consequently, the state of legality within the state.*

Key words: *Tool of a crime, cybercrime, computer forensics, computer technologies, forensic science, subject of a crime.*

https://doi.org/10.33108/visnyk_tntu2024.03.017 *Received 03.05.2024*

1. INTRODUCTION

The current pace of development of information technology requires constant renewal and modernization in various fields of scientific and practical knowledge. This process has not spared the field of criminal law and its practical aspect, such as forensic science, which is designed to develop and implement new and improved methods of fighting crime.

Of course, forensic science is understood as a legal science, but it can be considered one of the areas of jurisprudence that has a significant technical aspect, due to the development of technological means for detecting criminal offences.

The advancement of computer technology has created a new model of an offender with high intellectual qualities and high technological literacy. Therefore, the task of forensic science is the so-called modelling (forecasting) of future offences in the information sphere in order to develop methods for their timely detection and solving.

Moreover, computer technology can be both a means or object of a crime and a means for fighting such deviant behaviour, which in the worst case may develop into cyberterrorism.

Forensic science is designed to develop computer-based tools for detecting anti-social behaviour in order to prevent it and to introduce effective mechanisms for both pre-trial and judicial investigation. In addition, its task is also to monitor new technological developments as a means of committing offences in order to properly achieve the previous goal. And this requires the dynamics of its development to be adequate to scientific and technological progress.

In particular, for our country, which is entering a new stage of development of information technology, implementation of e-government and creation of databases of national importance, the issue of developing ways and means of fighting cybercrime is one of the priority tasks, where forensic technology is one of the key issues.

2. MAIN PART

2.1. Analysis of known research findings. In the paper [1], the authors discuss the challenges and importance of further developments in the Internet of Things (IoT) field of

Corresponding author: Valerii Muzh; e-mail: taras5a@ukr.net

digital forensics.. The textbook [2] covers digital forensics, including file systems and recovery of deleted files, timestamps, etc. In [3], a comparative analysis of various tools of digital forensics was carried out. In [4], the authors analyze the impact of cloud computing on computer forensics, in addition, [5] presents the Cloud Forensics Investigation Model for the investigation of cloud crimes. The authors in the study [6] define criteria for evaluating existing approaches to digital expertise for three main models of cloud services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In the study [7], scientists conduct an analysis of digital forensics in various areas and also consider anti-forensic computer methods. The article [8] explains the development and role of digital and cyber forensics in the investigation of cybercrimes. The chapter also focuses on processes and methods for preventing and investigating cybercrime. In work [9], scientists presented the current state of digital, cloud and IoT forensics. The study [10] provides an overview of the collection and analysis of digital forensic evidence. Analyzing presented works, it can be stated that computer forensics is actively developing taking into account the realities of the development of modern technologies. Let's explore the conceptual apparatus in more detail through the prism of domestic research.

The study of the use of computer technologies in forensics has been the focus of a wide range of scholars, such as V. P. Bakhin, R. S. Belkin, V. V. Biriukov, V. I. Galagan, V. G. Honcharenko, A. V. Ishchenko, R. A. Kaliuzhnyi, N. S. Karpov, N. I. Klymenko, V. P. Korzh, 1. 1. Kotyuk, V. S. Kuzmichev, E. D. Lukianchykov, M. A. Pogoretsky, O. V. Rybalsky, M. V. Saltevsky, V. K. Strynzh, V. V. Tishchenko, S. S. Cherniavsky, V. G. Khakhanovsky, V. Y. Shepitko and others.

However, computer technology is usually studied as a tool, an instrument of forensic science. In this article, we consider computer technology as an object of forensic knowledge, i.e. as an instrument and object of crime.

The objective of this research is to investigate the impact of computer technologies on the development of forensic science, and also to provide their characteristics as objects of forensic research.

2.2. Analysis results. Implementation of the achievements of natural and engineering sciences in the field of forensics, improvement of technical means, improvement of methods of their use are associated with complex technological operations, which results in the need to use not only forensic means, but also technologies. The work of modern law enforcement agencies is characterised by significant information content, a permanent need to obtain new data and keep previously obtained data up to date. The peculiarity of such activities is the constant receipt, processing and use of large volumes of various information. Ensuring a high level of these processes with a continuous increase in data volumes is an extremely difficult task, the solution of which becomes possible through the application of knowledge, development of methods and tools for working with information at the level of appropriate technologies [11].

Based on the aforesaid statements, we can distinguish three main areas of forensic science in the field of information, including computer technologies.

The first area is the use of computer technologies as a means of obtaining (collecting) evidence for the purpose of solving and investigating crimes.

The second area is the consideration of computer technologies as an object of forensic research, i.e. as an object of a crime.

The third is the consideration of computer technologies as an object of forensic research, i.e. as an instrument of a crime.

Today, the main ways to use information technology in pre-trial investigations are the formation and maintenance of criminal registers, the development and use of person profiles, and the use of Ukrainian legislation and other databases. Given the current requirements, investigators need information technology to improve the management of information support processes, automated search for data on any objects (persons, items, events), obtaining

knowledge from various databases available in the world, conducting statistical and geographical analysis of events, searching for specific objects and persons, etc. [12, p. 313].

Therefore, when analysing the first area, it is undeniable that computer technology is an auxiliary tool in the work of a criminalist. If in the last century it was used mainly for creating and processing databases of criminals, criminal case catalogues, etc., nowadays it is already being used in more complex forensic processes, in particular in such areas as fingerprinting and trace evidence analysis. Moreover, in the case of fingerprinting, technical means can be used as a fingerprint scanner and fingerprint database storage.

However, the creation of a fingerprint registration system in Ukraine is hampered by the lack of clear legal and regulatory framework that would ensure not only its creation, but also the effectiveness of its use with unconditional observance of human and civil rights and freedoms. Only under these conditions can the introduction of a fingerprint registration system in Ukraine be welcomed by both the population and other countries [13, p. 72].

In ballistics, hardware and software simulation of the bullet's flight path is becoming widespread, where it is possible to take into account almost all characteristics and physical processes (temperature, humidity, wind direction, etc.), i.e. to bring conditions closer to the real situation. It is important that the participation of a person (expert) in this process is minimised. It actually serves as a tool for initial input of elementary data.

In this respect, the scientific position of O. A. Sokyrynska on the development of forensic investigation is interesting and relevant. According to her, one of the trends is to improve the existing and create new technical means and technologies of human voice in all its variations (speaking, singing, paralinguisms, etc.), as well as, and most importantly, to develop perfect expert methods of individual identification of a person by these peculiar traces-reflections. It should be noted that this area will be developed outside the subject area of forensics, and by the efforts of representatives of computer science, physics, medicine, etc., but the knowledge obtained by specialists in these fields will be directly used in the tactics and practice of investigations and fact-finding in any field of legal regulation and therefore will become necessary and inseparable elements of certain forensic sciences, and also components of forensic theory [14, p. 57].

With regard to the second area of forensic science in the field of information technology, namely the consideration of computer technology as an object of forensic research, we are talking, as a rule, about information databases that have a certain value, as well as electronic bank account systems, i.e. everything that forms the motivational factors for committing a crime in the mind of the offender. In this aspect of the information sphere, we should not ignore the motives for marginal behaviour other than financial gain. A significant number of cyberattacks are accompanied not only by the goal of obtaining financial or other benefits, but also by the so-called «recognition», «praise», etc.

The third area of knowledge of computer technologies in forensics as a tool of crime received much attention in terms of legislation of this country. Thus, the disposition of Article 361 of the Criminal Code of Ukraine refers to unlawful tampering with computers, automated systems, computer networks or telecommunication networks, which leads to leakage, loss, forgery, blocking of information, distortion of the data processing process or violation of the established procedure for its transmission (routing) [15]. It is quite clear that today unauthorised interference should not be understood as physical destruction of computers, but rather more advanced ways of influencing information processing facilities, such as hacker attacks, phishing, etc., i.e. the use of one electronic computer to influence others. That is why in this case, computer technology is a tool for committing a crime, and in order to recognise it as such, it is necessary to conduct a specialised examination.

It should be noted that the commented article of the criminal law can also be used to analyse the second trend proposed by us. Of course, we are referring to information as the object of protection and the subject of the crime, but this information is still stored or processed by technical means.

In general, it can be argued that Chapter XVI «Crimes in the field of use of electronic computers, systems and computer networks and telecommunication networks» of the Criminal Code of Ukraine fully corresponds to the issue under study, and this indicates the absolute importance of the protected social relations in this area.

Based on the analysis of the three areas outlined above, we come to the conclusion that computer technology should be understood as a source and object of forensic cognition.

In addition, modern factors in the formation of the concept of «technology» in forensics are scientific and technological development, cyberneticisation of crime fighting practice, complication of the structure of criminal activity, compilation of management and organisation processes in the work of investigating crimes, algorithmisation and programming of the investigation process in general. The formation of the concept of technology in forensics is due to the allocation of new aspects of information and cognitive, organisational and managerial processes of investigation, the definition of which is not covered by the traditional system of concepts of forensics [16, p. 7].

Thus, it is necessary to distinguish a whole separate branch of forensic science that deals with these technologies. It can be called differently: «information forensics», «technological forensics» or «computer forensics». However, the first two concepts are not entirely correct, since general forensics is in any case related to the processes of obtaining information about the place, event, circumstances of a crime, etc., and its tools are various technical means that are not always related to computer technology. Therefore, the most appropriate name for this branch of criminalistics is «computer forensics».

Given the importance of computer technologies for the protection of public relations in the information sphere, as we have proved above, it is necessary to investigate the problematic issues that arise in their regulation.

The first problem we noted was the insufficiency of legal regulation. It applies not only to this area, but also to others, and consists in the failure to fulfil the predictive function of law (current positive law) and is a clear mistake of the subjects of rule-making, i.e. legal norms should, as they say, «keep up with the times», be oriented towards the future.

As mentioned by V. V. Semenogov, one of the promising areas for improving the effectiveness of crime detection and investigation should be considered the introduction of information technology into investigative activities, the definition of which is contained in the Law of Ukraine «On the National Informatisation Programme» [17, p. 335], but it is necessary to take into account how quickly changes can be made to a regulatory legal act adopted in a special manner by going through the procedure from legislative intent to its implementation.

The second problem we would like to draw attention to concerns education and is reflected in the poor or, more correctly, «outdated» training of specialists in the information sectors of the economy, i.e. the educational process «catches up» instead of «outstripping» real social relations.

In such circumstances, we believe that it is necessary to introduce new educational programmes for training specialists in the field of computer forensics. We are not referring exclusively to forensic experts, but also to specialists of the cyber police, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, etc.

At present, various private computer forensics laboratories (GROSS, CyberLab, etc.) are widely used, offering courses and trainings on this topic.

In addition to providing educational services, such laboratories conduct forensic investigations in the field of information technology at the request of legal entities and individuals. In particular, the GROSS Computer Forensics Laboratory is an organisation that provides professional services in the field of investigating computer crimes and information security incidents, and conducting computer forensics. The laboratory has a unique set of software and hardware tools for capturing, recovering and analysing data on various digital

media. They allow for the forensic examination of computer hardware, software, telecommunications equipment, data storage systems, mobile phones, etc. [18].

CyberLab is an independent forensic laboratory in Ukraine that provides services for computer and technical expertise, investigation of cybercrime, including fraud in Internet banking systems, response to information security incidents, and the extraction and examination of information from digital devices [19].

As we can see, the issue of training specialists (in particular, using advanced distance learning technologies [20]), providing various kinds of expert and security services in the field of computer forensics is becoming widespread in private sectors of the economy and is a promising area for further, as it goes beyond the scope of this article, scientific research on the quality indicators of such services with an analysis of their impact on the development of forensic technology in general.

However, at the state level, the problem of professional training of specialists in the field of computer forensics is not fully developed. Little attention is paid to distinguishing this area of forensics into a separate specialised field of knowledge. It is worth mentioning that there has been some progress in solving this problem. One of the first in our country, the Department of Cyber Security of Ternopil Ivan Puluj National Technical University introduced the discipline with the same name – «computer forensics» at the master's level.

3. CONCLUSION

Based on the above, we come to the conclusion that the problem of computer technology in forensics is important for a democratic, law-based state, since, it affects the state of law and order, and needs to be developed in at least two areas: law-making and educational.

The prospects for further scientific research on this topic lie in the correlation of forensic technology and the development of scientific and technological progress, in particular, in the field of prevention of recidivism.

References

1. Watson S, Dehghantanha A. Digital forensics: the missing piece of the internet of things promise. Computer Fraud & Security. 2016 Jun 1;2016 (6): 5–8. https://doi.org/10.1016/S1361-3723(15)30045-2
2. Lin X, Lin X, Lagerstrom-Fife. Introductory computer forensics. Springer International Publishing; 2018. https://doi.org/10.1007/978-3-030-00581-8
3. Barik K, Abirami A, Konar K, Das S. Research perspective on digital forensic tools and investigation process. Illumination of Artificial Intelligence in Cybersecurity and Forensics. 2022 Feb 8: 71–95. https://doi.org/10.1007/978-3-030-93453-8_4
4. Prakash V, Williams A, Garg L, Barik P, Dhanaraj RK. Cloud-based framework for performing digital forensic investigations. International Journal of Wireless Information Networks. 2022 Dec; 29 (4): 419–41. https://doi.org/10.1007/s10776-022-00560-z
5. Hemdan EE, Manjaiah DH. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimedia Tools and Applications. 2021 Apr; 80: 14255-82. https://doi.org/10.1007/s11042-020-10358-x
6. Schlepphorst S, Choo KK, Le-Khac NA. Digital forensic approaches for cloud service models: A survey. Cyber and Digital Forensic Investigations: A Law Enforcement Practitioner's Perspective. 2020: 175–99. https://doi.org/10.1007/978-3-030-47131-6_8
7. Paul Joseph D, Norman J. An analysis of digital forensics in cyber security. InFirst International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018 2019 (pp. 701–708). Springer Singapore. https://doi.org/10.1007/978-981-13-1580-0_67
8. Saharan S, Yadav B. Digital and cyber forensics: A contemporary evolution in forensic sciences. InCrime Scene Management within Forensic Science: Forensic Techniques for Criminal Investigations 2022 Mar 24 (pp. 267–294). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-16-6683-4_11
9. Ghosh A, Majumder K, De D. A systematic review of digital, cloud and iot forensics. The "Essence" of Network Security: An End-to-End Panorama. 2021: 31–74. https://doi.org/10.1007/978-981-15-9317-8_2
10. Mohammmed S, Sridevi R. A survey on digital forensics phases, tools and challenges. InProceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018 2020 (pp. 237–248). Springer Singapore. https://doi.org/10.1007/978-981-15-1480-7_20

11. Bilous V. V. Information technologies in forensics: setting the problem, Problems of legality, no. 121, pp. 160-170. (In Ukrainian).
12. Rogatyuk I. V. The use of information technologies in pre-trial investigation: current state and development prospects, Scientific Bulletin of the National Academy of Internal Affairs, 2013, no. 3, pp. 312–320. . (In Ukrainian).
13. Polyanska Yu. V. Theoretical and legal aspects of improving dactyloscopic registration, Criminal Bulletin, no. 1, 2014, pp. 70–74. . (In Ukrainian).
14. Sokyrynska O. A. Forensic and procedural issues of human identification by traces of reflection: diss. Ph.D. legal Sciences: 12.00.09, Kyiv, 2004, 198 p. . (In Ukrainian).
15. Criminal Code of Ukraine: Voice of Ukraine dated June 19, 2001, no. 107. . (In Ukrainian).
16. Bartsytska A. A. Forensic technologies: essence and place in the system of forensic science: autoref. thesis for obtaining sciences. candidate degree legal Sciences: spec. 12.00.09 “Criminal process and criminology; forensic examination; investigative activity” Odesa, 2011, 19 p. . (In Ukrainian).
17. . Semenogov V. V. Concepts and types of forensic technologies during the investigation of crimes. URL: http://www.pap.in.ua/6_2014/104.pdf. (In Ukrainian).
18. Available at: https://g-ross.com.ua/kryminalistyka.html.
19. Available at: http://cyberlab.com.ua/.
20. Pikuliak M., Lazarovych I., Usyk M. Progressive web technology-based improvement of the distance learning adaptive system. Scientific Journal of TNTU (Tern.), 2022, vol. 105, no. 1, pp. 118–127. https://doi.org/10.33108/visnyk_tntu2022.01.118

УДК 343.98

КОМП’ЮТЕРНІ ТЕХНОЛОГІЇ ЯК ОБ’ЄКТ І ДЖЕРЕЛО КРИМІНАЛІСТИЧНОГО ПІЗНАННЯ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Валерій Муж; Тарас Лечаченко

Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

Резюме. *Присвячено дослідженню впливу комп’ютерних технологій на стан розвитку криміналістики як науки в цілому, а також їхня характеристика в якості об’єктів криміналістичного дослідження. Проведено аналіз трьох основних напрямків криміналістики в сфері інформаційних технологій, у тому числі комп’ютерних. Розглянуто комп’ютерні технології як засіб отримання доказів, предмет та знаряддя злочину. Перший напрямок полягає у використанні комп’ютерних технологій як засобу отримання (збирання) доказів з метою розкриття та розслідування злочинів. З’ясовано беззаперечний факт, що комп’ютерна техніка є допоміжним інструментом у роботі криміналіста. Другий напрямок – це розгляд комп’ютерних технологій як об’єкта криміналістичного дослідження, тобто як предмета злочину. Встановлено, що другий напрямок криміналістики у сфері інформаційних технологій полягає в розгляді комп’ютерних технологій як об’єкта криміналістичного дослідження, тобто інформаційних баз даних, які мають певну цінність, а також про електронні системи банківських рахунків. Тобто все те, від чого у свідомості порушника формуються мотиваційні чинники до вчинення злочину. Третій – це розгляд комп’ютерних технологій як об’єкта криміналістичного дослідження, тобто як знаряддя злочину. Третій напрямок дослідження проаналізовано під призмою національного законодавства. Зокрема, розглянуто статті Кримінального кодексу України, які проливають світло на дану проблему. Таким чином, необхідно виокремлювати цілу галузь криміналістики, яка стосується цих технологій. Називати її можна по-різному: «інформаційна криміналістика», «технічна криміналістика» чи «комп’ютерна криміналістика». У даній статті дійшли висновку, що комп’ютернії технології займають важливе місце у процесі криміналістичних досліджень, чим впливають на якість кримінального слідства та відповідно на стан законності в державі.*

Ключові слова: *знаряддя злочину, кіберзлочинність, комп’ютерна криміналістика, комп’ютерні технології, предмет злочину.*

https://doi.org/10.33108/visnyk_tntu2024.03.017 *Отримано 03.05.2024*