UDC 343.983:004
DOI: 10.33270/04212202.30

Modern possibilities of forensic examination in the process of investigation of crimes in the field of computer systems and telecommunication networks

Bronislav B. Teplytskyi*

State Research Forensic Center of the Ministry of Internal Affairs of Ukraine
08130, 4 Velyka Okruzhna Rd., Kyiv, Ukraine

Abstract

The purpose of the study is to investigate the current issues of attracting special knowledge in the investigation of crimes in the use of computer systems and telecommunication networks. The methodological basis of the study is the use of a set of methods and methodological approaches, in particular: formal legal, structural-functional, system and comparative legal, analysis, synthesis, forecasting, etc. As part of the coverage of problematic issues in the fight against computer crime, negative factors that are common in Ukraine are highlighted. It is emphasised that computer crime as a new form of antisocial behaviour poses a serious threat to the security and normal functioning of society. Therefore, the main goal of the national policy in countering criminal offences in the use of computer systems and telecommunication networks is the interaction and coordination of efforts of expert structures with law enforcement agencies, and providing them with the necessary resources and facilities. Specialised expert research is fundamentally important for solving and investigating crimes in the field of computer technologies, telecommunication systems and networks. The correct definition of the object and purpose of the expert examination and the correct formulation of the expert's questions, which depend directly on the tasks of the expert examination, play an important role in the assignment of these types of expert examinations. In this regard, errors in asking questions to the expert constitute an error in determining the task that the expert examination should perform. Crimes in the use of computers and telecommunication networks are a complex anti-social phenomenon that covers almost all spheres of human life and directly concerns such a concept as information security. Effective detection and investigation of these criminal offences require, first of all, high-quality involvement of qualified specialists in the field of computer technology in the investigation process. Currently, almost no recommendations have been developed in forensic science that would relate to the specifics of investigating and conducting forensic examinations in these categories of cases. This is primarily conditioned by the novelty of the outlined problem, the availability and rapid increase in the number of varieties of computer and mobile devices, their services and mobile communication tools. Effective investigation of crimes in the field of information and computer technologies depends on timely and correct conduct of the necessary expert investigation. In addition to traditional forensic research, specialised expertise that implements a number of searches diagnostic and identification tasks related to the analysis of both electronic computing equipment and forensic information that they contain is important in the detection and investigation of crimes in the field of computer technology

Keywords:
electronic computer; forensic examination; criminal offence; computer crime; information security

Article's History:
Received: 20.09.2021
Revised: 02.11.2021
Accepted: 18.11.2021

Suggest Citation:
Teplytskyi, B.B. (2022). Modern possibilities of forensic examination in the process of investigation of crimes in the field of computer systems and telecommunication networks. *Law Journal of the National Academy of Internal Affairs*, 11(2), 30-37.

*Corresponding author

Introduction

Defining the main directions of the national policy in the field of information security is extremely relevant for modern Ukraine. Given the rapid progress in the development of ICT, it should be borne in mind that the life of society directly depends on the security of its information environment.

The search for new, more effective ways to detect and neutralise influences on information, in particular, in the world's open networks, is a natural defensive reaction of society, and Ukraine is no exception.

According to leading international organisations, the losses caused by criminal offences in the use of electronic computers and telecommunication networks can be compared with the income from illegal trafficking in narcotic drugs and weapons. In the United States alone, the annual economic losses from these types of criminal acts amount to more than USD 100 billion. Moreover, many torts in this area remain hidden, which indicates their high latency[1].

The purpose of the study is to investigate the current issues of attracting special knowledge in the investigation of crimes in the use of computers and telecommunication networks. The achievement of this goal involves completing the following tasks:

– to determine the main goal of the national policy on countering criminal offences in the field of computer technologies;

– to investigate the main form of using special knowledge in criminal proceedings during the investigation of crimes in the field of computer technologies;

– to analyse the object and main tasks of forensic research in the investigation of crimes in the field of computer technologies.

Presentation of Main Material

The Outlining the problematic issues of combating computer crime in the modern world, the following negative factors inherent in Ukraine were identified:

– lack of a well-established system of legal, organisational and technical support for the legitimate interests of citizens, the state, and society in the field of Information security;

– limited opportunities for budget financing of work on creating a legal, organisational and technical base for information security;

– inadequate coordination of actions in countering computer crime by law enforcement agencies and insufficient training of their personnel to effectively prevent, detect, and investigate such illegal acts;

– imperfect system of unified accounting of offences committed with the help of informatisation tools;

– the lag of the domestic information technology industry and their databases from the world level [2].

Computer crime as a new form of antisocial behaviour poses a serious threat to the security and normal functioning of society. Given this, the main goal of the national policy on countering criminal law violations in the use of computers and telecommunication networks should be to interact and coordinate the efforts of expert structures with law enforcement agencies, and provide them with the necessary resources and facilities.

The interaction of the relevant authorities is mainly reduced to an episodic exchange of information. The most important thing is missing – a complete system of continuous monitoring of the situation in the field of information security of various systems and timely (preventive) decision-making to identify and stop such types of criminal offences. Evidently, the creation of a complete system is impossible if effective interaction of domestic expert structures with expert and law enforcement agencies of foreign countries that fight computer crime is not established. In addition, any system, even the most technologically advanced, will not be able to achieve its goal if it is not provided with highly qualified personnel [3].

Unfortunately, law enforcement agencies in Ukraine do not have a sufficient number of specialists who understand modern technology and are able to quickly identify and solve crimes in the field of computer technology. Therefore, the creation of a holistic system of training and retraining of specialists in countering computer offences is a priority task of the law enforcement bodies.

Moreover, the processes of effective detection, investigation, and prevention of crimes committed using computer capabilities require the creation of all the necessary methodological and technical means [4]. Given the weak development of the relevant tools, this task is of paramount importance in the implementation of measures to adequately counteract computer crime. This area is closely related to the problem of improving the regulatory framework, the lack of development of which so far does not allow properly resisting illegal actions in the computer sphere.

In addition, the lack of a clear criminal legal qualification of crimes in the sphere of use of computers and telecommunication networks creates difficulties in interpreting and applying the provisions of the law, which restricts the actions of law enforcement agencies to implement tasks to counteract computer crime. Ultimately, one of the main tasks of effectively combating criminal offences in the use of computers and telecommunication networks is to conduct a complex of studies to improve and create software, hardware, and technical means that will ensure the effective protection of computer networks and their databases.

The results of the analysis of expert practice in Ukraine show that the tension of the criminal situation in the field of computer technology use is constantly

increasing. This circumstance gives rise to the assertion that:

– firstly, information becomes the subject of criminal encroachment, since its use, distribution, or sale gives high profits;

– secondly, expert and law enforcement agencies are gradually accumulating experience in combating these criminal offences, and therefore, they are developing more effective ways to detect, disclose, and stop them [5].

During the investigation of such high-tech crimes, it is necessary to identify and extract traces and physical evidence presented in the form of information in electronic computing, telecommunications systems, magnetic media, software products, and computer equipment. In this regard, there is an urgent need for investigators to attract special knowledge and skills in using the latest information technologies, that is, such scientific, technical, and other professional knowledge that is not generally known to the investigator, prosecutor, court, and other participants in the process.

In this regard, A. F. Koni in his book "Court – Science – Art" noted that judicial practice quite often necessitates the use of special studies, concentrating on them the core of the case and resorting to the involvement of experts from various special fields of knowledge, art, crafts [6]. In this context, B.M. Shaver in 1940 stated that effective detection and investigation of crimes directly depends on the use of knowledge and achievements of technical sciences in the investigation process [7].

In Ukrainian criminal procedure, special knowledge is used in three forms, namely:

– if specialists are involved in conducting certain investigative, procedural, or judicial actions (Article 71 of the Criminal Procedure Code of Ukraine);

– within the framework of conducting expert examinations (Articles 242-245, 332 of the Criminal Procedure Code of Ukraine);

– during the interrogation of the expert (Part 7 of Article 5, Part 7 of Article 101, Article 356 of the Criminal Procedure Code of Ukraine) [8].

The main procedural form for attracting and using scientific, technical, and other special knowledge in criminal proceedings is considered to be expertise, which is based on a special study and the corresponding qualified expert opinion directly related to pre-trial investigation [9]. For the first time in 1949, A.I. Winberg raised the issue of introducing such a procedural figure as a specialist into criminal proceedings together with an expert.

According to the Ukrainian criminal procedure legislation, a specialist is a person who has special knowledge and skills in using technical or other means and can provide advice during pre-trial investigation and judicial proceedings on issues that require appropriate special knowledge and skills (Part 1 of Article 71).

The specialist implements special knowledge in two forms, namely: non-procedural – oral explanations and methodological consultations on special issues; procedural – direct application of special knowledge and forensic technology, other scientific and technical means during the identification, seizure, consolidation, and analysis of evidence.

Conducting a forensic examination in Ukrainian legislation is regulated by: the Law of Ukraine "On Forensic Examination" of February 25, 1994, No. 4038-XII [10]; the Criminal Procedure Code of Ukraine (Art. 69, 70, 101, 102, 232, 242-245, 518) [8]; Civil Procedure Code of Ukraine (Art. 72, 73, 102-115, 255, 237, 239, 298) [11]; Regulation on the Expert Service of the Ministry of Internal Affairs of Ukraine of November 3, 2015, No. 1343 [12]; Instruction on the appointment and conduct of forensic examinations and expert research and Scientific and methodological recommendations on the preparation and appointment of forensic examinations and expert research of October 8, 1998, No. 53/5 [13]; Instruction on the specifics of the implementation of forensic expert activities by certified forensic experts who do not work in state specialised expert institutions of December 12, 2011, No. 3505/5 [14].

In accordance with the provisions of these regulations, forensic expertise is considered to be a research based on special knowledge in the field of science, technology, art, craft, etc., objects, phenomena and processes in order to provide an opinion on issues that are or may be the subject of judicial proceedings [10]. Based on this definition, it can be concluded that a forensic examination in criminal proceedings is appointed when the establishment of specific circumstances in a criminal proceeding requires specialised knowledge of the relevant persons, i.e., experts. This is also emphasised by the norm of Article 242 of the Criminal Procedure Code of Ukraine [15], which states that forensic expertise is carried out by the relevant specialised expert institution or certified forensic experts who do not work in these institutions, if special knowledge is needed to clarify the circumstances relevant to criminal proceedings [8].

Specialised expert research is fundamentally important for solving and investigating crimes in the field of computer technologies, telecommunication systems and networks [16]. Scientific and methodological recommendations on the preparation and appointment of forensic examinations and expert research, approved by the Order of the Ministry of Justice of Ukraine of October 8, 1998 No. 53/5, define: 1) expertise of computer equipment and software products; 2) expertise of telecommunications systems and equipment [6], including them to the class of engineering and technical expertise (that is, by origin electronic computer equipment belongs to engineering and technical developments).

Thus, the object of forensic research in the investigation of crimes in the field of using computer technologies is not only computer-based equipment but also the information contained in electronic media. Moreover, the development of mobile and computer technologies has given a wide range of digital and fully portable devices, their mobile applications, services, and mobile communication tools. As a result, this allowed carrying out operations for receiving, processing, and transmitting information in almost all spheres of human life. Consequently, the problem of information security has become more acute due to the processes of penetration of technical means of processing and transmitting information into almost all spheres of society's life. Therefore, the object of forensic examinations in the detection and investigation of crimes in the field of use of computers and telecommunication networks depends primarily on the method and mechanism of committing and concealing a crime.

An important role in the appointment of an expert examination in the investigation of crimes in the use of computers and telecommunication networks is played by the correct formulation of questions to the expert, which directly depends on the tasks of expert research. In this regard, an error in stating questions to the expert is actually an error in determining the task performed by the expert examination. The range of tasks and questions that may be posed to the expert when appointing computer forensic examinations is sufficiently well covered in the forensic literature [17]. These recommendations may well be used when assigning an expert examination.

In particular, the main tasks to be considered are identification and non-identification (diagnostic or situational) tasks consisting of: setting the intended purpose and functionality of devices belonging to the computer; installation of the intended purpose and functionality of the software; establishing the fact of development and the chronology of software development; establishing the fact of development and chronological characteristics of the production of text documents; detection and recovery of deliberately destroyed text files of different formats or their fragments; establishing the facts of receiving and transmitting facsimile messages via modem connection, restoring texts and the chronology of information exchange; establishing the facts of the implementation of photomontage, editing of video and audio recordings; establishing authorship and chronological characteristics of the performance of these works; establishing the facts of the production of seals, stamps, letterheads, and other graphic products and determining the chronology of the production of graphic documents; establishing the facts of development, authorship and chronological characteristics of video products (video films, commercials, etc.) made using 3D technologies; restoration and analysis of low quality video information taken with insufficient exposure, insufficient illumination of objects or damaged for other reasons; restoration and analysis of low quality audio information recorded in high noise conditions, with insufficient microphone sensitivity, spoiled for some other reason; restoration and analysis of information contained in databases (information systems, accounting, directories, etc.); restoring intentionally deleted information or its fragments; recovery and analysis of information protected from unauthorised access (overcoming codes, passwords, etc.); setting the purpose and functionality of Internet applications; establishing technological sessions in the Internet, detection, analysis and recovery of information obtained under the protocols NTTR, FTP, UUCP, POP (files, e-mail messages, visits to internet sites, etc.); establishing the facts of software development intended for unauthorised access to computer networks; establishing the facts of software development for unauthorised access to distributed databases and database servers; establishing the facts of manufacturing or availability on the computer of software intended for unauthorised payment of credit cards in the e-commerce industries; establishing the facts of manufacturing and deliberate distribution of computer viruses and programmes that are dangerous from the standpoint of disruption of computer networks; establishing the facts of manufacturing information on the internet, the content and methods of distribution of which do not comply with the current legislation of Ukraine (pornography, videos, photos, texts, etc.); analysing the security of internet applications that use HTML, Java, VBA, XML, ASP, Sybase, Oracle, MS jet, PostgreSQL, etc.; establishing the facts of unauthorised access to information resources of corporate networks and the Internet; determining the computer from which unauthorised access to information resources is carried out, etc.

In some cases, when investigating crimes in the field of using electronic computers and telecommunication networks, comprehensive and commission examinations may be appointed. To perform tasks related to the economic and financial activities of institutions, a comprehensive computer-technical and forensic accounting expertise is carried out. In order to establish the device on which the document was executed and compare the document with the image in the file of institutions, a comprehensive computer-technical and forensic technical examination of documents is assigned. To investigate consumer properties, storage conditions, and the cost of computer tools and software, a comprehensive computer-technical and forensic commodity expertise is carried out. To establish the source of origin of software products, video and audio products, a comprehensive

computer-technical expertise and expertise of intellectual property objects are assigned.

In addition, research in recent years shows that more and more often during the investigation of crimes in the field of computer technology, the investigation faces the need for expert research of speech information transmitted by computer networks. In these cases, forensic scientists recommend appointing forensic linguistic examinations, the object of which, in their opinion, is speech (text) information recorded on a certain material medium. At the same time, additional opportunities for collecting the necessary evidence can be provided by both modern capabilities of traditional (forensic author's expertise) and relatively new recently formed examinations (semantic and textual expertise), in order to identify extremist statements, inciting national, religious and racial hatred, violation of intellectual property rights, etc.

To investigate the information contained on computer media, the expert is provided with a computer media and a computer complex, which includes the media under study. In some cases, it would be sufficient to provide only a computer medium. If possible, an expert should be consulted in advance of such a study.

To determine the compliance of software products with certain parameters, and the cost of the software product, the expert is provided with a media with a copy of the software product under study and a reference (distribution) copy of the software product. If a distributive copy of a software product is not available, an examination should not be refused, as in some cases it can be carried out with a copy of the software product.

To investigate the technical condition and determine the cost of computer equipment, the expert is provided with computer equipment, as well as technical documentation for it. The removal of computer equipment blocks should be entrusted to an expert.

To establish the authorship of the software product under study, the expert is provided with programmes in the form of source texts, library, and executable modules, and programmes (source texts, library and executable modules) created by the person in respect of whom the version is being checked whether or not he is the author of the product under investigation

To determine which objects should be provided to the expert in each specific case, it is advisable to get advice from an expert (specialist) in the field of computer technology. Based on the results of the expert examination, the expert draws up and signs an expert opinion. This conclusion is important in the system of means of proof in criminal proceedings. Therefore, the specifics of the investigation of crimes in the computer sphere actualise the need for competent and effective work of the investigator to collect and study material evidence, documents, and other material information about the crime, which is mainly contained in certain electronic computing and software media. At the same time, the investigative bodies must fully obtain and document verbal criminally significant information in order to establish the involvement of a certain person in the crime committed.

As part of the coverage of problematic issues in the fight against computer crime, negative factors that are common in Ukraine are highlighted. It is emphasised that computer crime as a new form of antisocial behaviour poses a serious threat to the security and normal functioning of our society, and therefore the main goal of the national policy in countering criminal offences in the use of computers, systems, and computer and telecommunication networks is the interaction and coordination of efforts of expert structures with law enforcement agencies, and providing them with the necessary resources and facilities.

Specialised expert research is fundamentally important for solving and investigating crimes in the field of computer technologies, telecommunication systems and networks. The correct definition of the object and purpose of the expert examination and the correct formulation of the expert's questions, which depend directly on the tasks of the expert examination, play an important role in the assignment of these types of expert examinations. In this regard, errors in asking questions to the expert constitute an error in determining the task that the expert examination should perform.

Conclusions

A crimes in the use of computers and telecommunication networks are a complex anti-social phenomenon that covers almost all spheres of human life and directly concerns such a concept as information security. Effective detection and investigation of these criminal offences require, first of all, high-quality involvement of qualified specialists in the field of computer technology in the investigation process.

Currently, almost no recommendations have been developed in forensic science that would relate to the specifics of investigating and conducting forensic examinations in these categories of cases. This is primarily conditioned by the novelty of the outlined problem, the availability and rapid increase in the number of varieties of computer and mobile devices, their services and mobile communication tools. Effective investigation of crimes in the field of information and computer technologies depends on timely and correct conduct of the necessary expert research. In addition to traditional forensic research, specialised expertise that implements a number of search diagnostic and identification tasks related to the analysis of both electronic computing equipment and forensic information that they contain is important in the detection and investigation of crimes in the field of computer technology.

References

[1] Computer crime in the United States. (n.d.). Retrieved from https://www.crime-research.ru/library/usa_crime.htm.
[2] Pashniev, D.V. (2007). The use of special knowledge in the investigation of crimes committed with the use of computer technology. (Doctoral thesis, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine).
[3] Meshcheriakov, V.A. (2002). *Crimes in the field of computer information: The foundations of the theory and practice of investigation*. Voronezn: Voronezh State University.
[4] Shcherbakovskiy, M.G. (2005). *Forensic examinations: Purpose, production, use*. Kharkov: Espada.
[5] Motliakh, O.I. (2005). *Questions of methods of investigation of crimes in the field of information technologies*. (Doctoral thesis, Academy of Advocacy of Ukraine, Kyiv, Ukraine).
[6] Koni, A.F. (1923). *Court – science – art (from the memoirs of a judicial figure)*. Petrograd: Polarnaia zvezda.
[7] Shaver, B.M., & Vinberg, A.I. (1940). *Criminalistics.* Moscow: Iuridiceskoe izdatelstvo NKIU SSSR.
[8] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from http://zakon0.rada.gov.ua/laws/show/4651-17.
[9] Rossinskaia, E.R., & Usov, A.I. (2001). *Forensic computer-technical expertise*. Moscow: Pravo i zakon.
[10] Law of Ukraine No. 4038-XII "On Forensic Examination". (1994, February). Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12#Text.
[11] Law of Ukraine No. 1618-VI "Civil Procedure Code of Ukraine". (2004, March). Retrieved from https://zakon.rada.gov.ua/laws/show/1618-15.
[12] Order of the Ministry of Internal Affairs of Ukraine No. 1343 "On the Statement of the Situation on Expert Service of the Ministry of Internal Affairs of Ukraine". (2015, November). Retrieved from https://zakon.rada.gov.ua/laws/show/z1390-15#Text.
[13] Order of the Ministry of Justice of Ukraine No. 53/5 "On Approval of the Instruction on Appointment and Carrying Out of Forensic Examinations and Expert Researches and Scientific and Methodical Recommendations Concerning Preparation and Appointment of Forensic Examinations and Expert Researches". (1998, October). Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text.
[14] Order of the Ministry of Justice of Ukraine No. 3505/5 "On the Statement of the Instruction on Features of Implementation of Judicial Expert Activity by the Certified Judicial Experts Who Do Not Work in the State Specialized Expert Institutions". (2011, December). Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text.
[15] Cherniakhovskyi, B.V. (2020). Features of the investigative review during the investigation of unauthorized interference in the work of computers, automated systems, computer networks or telecommunication networks. *Scientific Herald of National Academy of Internal Affairs*, 2(115), 58-68. doi: 10.33270/01201152.58.
[16] Palamarchuk, L.P. (2004). Forensic support for the investigation of illegal interference in the work of electronic computers (computers), systems and computer networks (PhD thesis, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine).
[17] Polishchuk, V.A. (2018). Features of expert experiment during forensic computer and technical examinations. *Forensic Bulletin*, 30(2), 116-121. doi: 10.37025/1992-4437/2018-30-2-116.

Список використаних джерел

[1] Комп'ютерні злочини у США. URL: https://www.crime-research.ru/library/usa_crime.htm.
[2] Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. … канд. юрид. наук: 12.00.09. Харків, 2007. 228 с.
[3] Мещеряков В. А. Преступления в сфере компьютерной информации : основы теории и практики расследования. Воронеж : Воронеж. гос. ун-т, 2002. 408 с.
[4] Щербаковский М. Г. Судебные экспертизы : назначение, производство, использование. Харьков : Эспада, 2005. 544 с.
[5] Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних технологій : дис. … канд. юрид. наук : 12.00.09. Київ, 2005, 221 с.
[6] Кони А. Ф. Суд – наука – искусство. Петроград : Полярная звезда, 1923. 68 с.
[7] Шавер Б. М., Винберг А. И. Криминалистика. Москва : Юрид. изд-во НКЮ СССР, 1940. 200 с.
[8] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL : http://zakon0.rada.gov.ua/laws/show/4651-17.
[9] Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. Москва : Право и закон, 2001. 416 с.
[10] Про судову експертизу: Закон України від 25.02.1994 р. № 4038-XII. URL : https://zakon.rada.gov.ua/laws/show/4038-12#Text.

[11] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 р. № 1618-VI. URL : https://zakon.rada.gov.ua/laws/show/1618-15.
[12] Про затвердження Положення про Експертну службу МВС України: Наказ МВС України від 03.11.2015 р. № 1343. URL: https://zakon.rada.gov.ua/laws/show/z1390-15#Text.
[13] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень: Наказ Міністерства юстиції України від 08.10.1998 р. № 53/5. URL : https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення 05.03.2021).
[14] Про затвердження Інструкції про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах : Наказ Міністерства юстиції України від 12.12.2011 р. № 3505/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text.
[15] Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. Т. 2. № 115. С. 58–68. doi : 10.33270/01201152.58.
[16] Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : дис. ... канд. юрид. наук : 12.00.09. Київ, 2004, 214 с.
[17] Поліщук В. А. Особливості експертного експерименту під час проведення судових комп'ютерно-технічних експертиз. *Криміналістичний вісник.* 2018. Т. 30, № 3. С. 116–121. doi: 10.37025/1992- 4437/2018-30-2-116.

Сучасні можливості судової експертизи в процесі розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Броніслав Броніславович Теплицький

Державний науково-дослідний експертно-криміналістичний центр МВС України
08130, Велика Окружна дорога, 4, Київ, Україна

Анотація
Мета статті полягає в дослідженні актуальних питань залучення спеціальних знань під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Методологічною основою дослідження є використання комплексу методів і методичних підходів, зокрема: формально-юридичного, структурно-функціонального, системного й порівняльно-правового, аналізу, синтезу та прогнозування тощо. У межах висвітлення проблемних питань боротьби з комп'ютерною злочинністю виокремлено негативні чинники, що поширені саме в Україні. Акцентовано, що комп'ютерна злочинність як нова форма антигромадської поведінки становить серйозну загрозу безпеці й нормальному функціонуванню нашого суспільства, а тому основною метою державної політики в протидії кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є взаємодія та координація зусиль експертних структур із правоохоронними органами, а також забезпечення їх необхідною матеріально-технічною базою. Принципово важливе значення для розкриття та розслідування злочинів у сфері використання комп'ютерних технологій, систем і мереж електрозв'язку мають спеціалізовані експертні дослідження. Важливу роль у призначенні цих видів експертиз відіграють правильне визначення об'єкта та завдання експертного дослідження, а також правильна постановка питань експерту, які безпосередньо залежать від завдань експертного дослідження. У зв'язку із цим, помилки в постановці питань експерту становлять помилку у визначенні завдання, яке має виконати

експертиза. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є складним антисоціальним явищем, що охоплює майже всі сфери життєдіяльності людини та безпосередньо стосується такого поняття, як інформаційна безпека. Ефективне розкриття та розслідування цих кримінальних правопорушень потребують передусім якісного залучення до процесу розслідування кваліфікованих фахівців у галузі використання комп'ютерних технологій. Нині в криміналістичній науці майже не розроблено рекомендацій, які стосувалися б особливостей розслідування та проведення судових експертиз за цими категоріями справ. Пов'язано це насамперед з новизною окресленої проблеми, доступністю та стрімким збільшенням кількості різновидів комп'ютерно-мобільних пристроїв, їх сервісів і засобів мобільного зв'язку. Результативне розслідування злочинів у сфері інформаційно- комп'ютерних технологій залежить від своєчасного та правильного проведення необхідних експертних досліджень. Крім традиційних криміналістичних досліджень, важливе значення в розкритті та розслідуванні злочинів у сфері використання комп'ютерних технологій мають спеціалізовані експертизи, які реалізують низку пошукових діагностичних й ідентифікаційних завдань, що стосуються дослідження як електронно-обчислювальної техніки, так і криміналістичної інформації, яка на них міститься

Ключові слова:
електронно-обчислювальна машина; судова експертиза; кримінальне правопорушення; комп'ютерна злочинність; інформаційна безпека