UDC 343.14
DOI: 10.33270/01211203.28

Current Issues an Examination Computer Hardware and Software Productsduring the Investigation of Crimes in the Use of Computers (Computer) Systems, Computer Networks and Telecommunication Networks

Bronislav B. Teplytskyi*

National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine

■ **Abstract.** The purpose of the study is to investigate relevant issues of examination of computer equipment and software products during the investigation of crimes in the field of use of electronic computing machines (computers), systems, computer networks, and telecommunication networks. General and special scientific methods are used to achieve this goal. In particular, the method of analysis, system-structural, and statistical methods provided an opportunity to examine the place of the expertise of computer equipment and software products in the system of forensic examinations, and identify its tasks and varieties. The main subtypes of forensic expertise of computer equipment and software products are identified: an examination of computer equipment, software products, information, and information-computer research. The basic rules and requirements for the formation of questions for the forensic expert are proposed, an approximate list of issues that can be resolved during the research, and typical mistakes made by the initiators of conducting examinations of computer equipment and software products are highlighted. It is established that forensic examination of computer equipment and software products is a type of computer-technical forensic examinations that belongs to the class of engineering and technical forensic examinations and is internally divided into three subtypes. The basic requirements and rules for formulating questions for solving them within the framework of expertise of computer equipment and software products have been developed. Typical errors in the appointment of forensic examinations of computer equipment and software products are identified

■ **Keywords**: special knowledge; forensic examination; examination of computer equipment and software products; investigation of crimes; appointment of expert examinations

■ Introduction

The active introduction of computer equipment and computer technologies in the official activities of state bodies and private organisations is accompanied by the spread of a range of criminal offences related to their use.

Tens of thousands of criminal offences are committed annually in the world using computer technologies, software tools and other technological equipment. According to the authoritative American company McAfee, specialising in computer security, and the Centre for Strategic and International Studies (CSIS), illegal interference in the operation of electronic computing machines (computers), systems and computer and telecommunications networks during 2020 cost the world economy over a trillion dollars, or 820 billion euros. Compared to 2018, researchers report an increase of 50 per cent. One of the factors that contributed to the increase in the number of cybercrimes is that a substantial number of employees this year switched to remote work due to the pandemic caused by the spread of the SARS-CoV-2 coronavirus (COVID-2019), and have remote access to working computer systems [1].

The process of investigating criminal offences in this area often involves masking the illegal actions of offenders and other related persons. As elements of disguise, they use changing the virtual

■ **Suggested Citation:**
Teplytskyi, B.B. (2021). Current issues an examination computer hardware and software productsduring the investigation of crimes in the use of computers (computer) systems, computer networks and telecommunication networks. *Scientific Journal of the National Academy of Internal Affairs,* 26(3), 28-34. doi: 10.33270/01211203.28

■ *Corresponding author

■ Received: 23.06.2021; Revised: xx.xx.2021; Accepted: xx.xx.2021

addresses of personal computers, using dynamic IP addresses, changing the identification data of individual elements of computer systems, committing criminal offences through remote control of technical means, etc.

Such types of criminal offences are latent in nature, they leave a limited number of traces that are difficult to detect, fix, and collect. These circumstances make it necessary to use modern special knowledge in the field of computer and information technologies for the purpose of investigating criminal offences in the field of using electronic computing machines (computers), systems, computer networks and telecommunication networks. In the vast majority of cases, the appointment and conduct of computer-technical forensic examinations is a necessary condition for an effective investigation of criminal proceedings.

Problematic aspects related to countering, identifying, using special knowledge, and investigating crimes in the field of using electronic computing machines (computers), systems, and computer and telecommunication networks were investigated by such researchers as: V.V. Areshonkov, V.M. Atamanchuk, V.M. Butuzov, A.A. Vozniuk, V.G. Honcharenko, I.V. Hora, M.V. Hutsaliuk, A.V. Ishchenko, O.V. Kopan, O.V. Kravchuk, S.A. Kuzmin, V.I. Osadchyi, M.A. Pogoretskyi, A.A. Sakovskyi, Ye.D. Skulysh, O.A. Fedotov, V.G. Khakhanovskyi, D.M. Tsekhan, S.S. Cherniavskyi, Yu.M Chornous, V.P. Shelomentsev, M.G. Shcherbakivskyi, O.M. Yurchenko, and others.

Notably, today there is a lack of thorough research on theoretical and practical issues related to using modern information technologies directly in forensic expertise during computer-technical forensic examinations, the definition of their tasks and objects.

The purpose of the study is to conduct a systematic analysis of the features of the appointment of forensic examinations of computer equipment and software products in the investigation of crimes with the use of electronic computing machines (computers), systems, computer and telecommunication networks. The following tasks were set to achieve this goal:

1) determine the place of examinations of computer equipment and software products in the system of forensic examinations, outline its varieties;

2) develop rules and requirements for the formulation of questions for a forensic expert when appointing an expert examination of computer equipment and software products;

3) identify typical errors in the appointment of forensic examinations of computer equipment and software products.

The main subtypes of forensic expertise of computer equipment and software products are identified: an examination of computer equipment, software products, and information-computer research. The basic rules and requirements for the formation of questions for the forensic expert are proposed, an approximate list of issues that can be solved within the framework of the study, and typical mistakes made by the initiators of conducting examinations of computer equipment and software products are highlighted.

Results and Discussion

Investigation into the use of electronic computing machines (computers), systems, and computer and telecommunication networks is the process of investigating, analysing, and recovering critical forensic digital data from networks involved in an attack. This can be the Internet and (or) a local network – to identify the authors of digital crimes and their true intentions.

Investigators of this category of criminal offences must be computer science experts who understand not only software, file and operating systems but also how networks and equipment work. They need to be sufficiently knowledgeable to determine how these components interact, form a complete picture of what happened, why it happened, when it happened, who exactly committed the crime, and how victims can further protect themselves from these types of cyber threats [2].

One of the most effective and, undoubtedly, decisive means (sources of evidence) in the investigation of such crimes is the examination of computer equipment and software products, which is actively used by law enforcement agencies in different countries.

To effectively use the capabilities of forensic examination of computer equipment and software products during the investigation of criminal offences, it is necessary, not only to have information about the possibility of solving a range of issues (which is also important) but also about its place in the system of forensic examinations.

In Ukraine, the implementation of forensic expert activities for conducting forensic examinations and expert research is regulated by the Constitution of Ukraine, the Law of Ukraine “On forensic expertise”, and other regulatory acts. Art. 1 of this Law states that forensic examination is a study based on special knowledge in the field of science, technology, art, crafts, etc. of objects, phenomena, and processes to provide an opinion on issues that are or will be the subject of judicial proceedings [3].

According to paragraph 1.2.2 of the Instruction on the appointment and conduct of forensic examinations and expert examinations, approved by the order of the Ministry of Justice of Ukraine of October 8, 1998, No. 53/5, the examination of computer

equipment and software products belongs to the class of forensic engineering-technical examinations [4].

Notably, another regulatory document, namely the Regulation on the Central Expert Qualification Commission under the Ministry of Justice of Ukraine and the certification of forensic experts, approved by the order of the Ministry of Justice of Ukraine No. 301/5 of March 3, 2015, defines the indices of expert specialities. In accordance with the provisions of this document, index 10.9 "Examination of computer equipment and software products" is defined, which is classified as a type of computer-technical forensic examinations [5].

Thus, according to the results of the analysis of regulatory documents, it is concluded that the forensic examination of computer equipment and software products is a type of computer-technical forensic examinations, which belongs to the class of engineering-technical forensic examinations.

In recent years, new ways of committing crimes in the field of using electronic computing machines (computers), systems, computer networks and telecommunication networks have become widespread, among which the following can be distinguished: the use of so-called ransomware programmes, through which attackers encode data and demand a ransom for their decoding, phishing and DoS attacks, theft of email accounts, the use of spyware, and the theft of cryptocurrencies, both through unauthorised access to virtual client wallets and through online interception of payments, etc.

The legal basis for conducting a forensic examination of computer equipment and software products is the decision of the investigator (prosecutor, detective), issued based on Art. 243 of the Criminal Procedure Code of Ukraine or the decision of the investigating judge to conduct this type of examination in cases where it is necessary to establish factual data relevant to the criminal offence under investigation and related to the use of computer equipment or equipment, with its help, certain actions are conducted that can be detected as a result of using special knowledge in the field of programming and computer technologies [6].

Notably, part two of this Article of the criminal procedure legislation also gives the defence the right to involve a professional forensic expert in conducting research, however, on contractual terms.

Considering the issues of objects of forensic examination of computer equipment and software products, now there is no clear opinion among both researchers and practising specialists on this issue.

On this occasion, M.H. Shcherbakovskyi believes that the object of expertise is a categorical concept that has a number of features. Classification of the object of expertise as a logical procedure involves the division of the concept, which results in the creation of a system of subordinate concepts and their distribution into classes. Such classification should be conducted on a certain basis according to the laws of logic; the basis should be substantial, essential for highlighting the essence of this concept as an integral system, which is the actual foundation for performing scientific and practical tasks [7].

According to V.G. Honcharenko & I.V. Hora, the objects of this type of research can be computer equipment with storage media (floppy disks, hard disks, CDR disks, flashcards, etc.), peripherals (printers, scanners, sound cards), and software products. The objects of this expertise can also be devices that are not computers in the classical sense of the word, for example, electronic cash registers, slot machines, card readers, etc. [8].

On the official website of The Independent Institute of Forensic Examinations, the objects of this type of expertise include computer equipment, "peripherals" (scanners, printers, plotters, etc.), various media (magnetic, optical, laser, etc.), software, other information stored on media and storage devices (permanent and operational), and organisers, pagers, mobile phones, and other devices that are manufactured and work based on technologies for building personal computers [9].

Representatives of the expert service of the Ministry of Internal Affairs of Ukraine to the objects of forensic examination of computer equipment and software products include hardware (computer system blocks, their components, servers, laptops, hard drives, flash drives, modems, routers, etc.), and software products (computer programmes, databases, etc.) [10].

In the vast majority of cases, the objects of forensic examination of computer equipment and software products in the investigation of crimes in the field of the use of electronic computing machines (computers), systems, computer networks and telecommunication networks are means of committing crimes. However, there are criminal offences in which the object of encroachment is not the actual material object, but the information contained in it, or on some medium, or software.

The objects of forensic examination of computer equipment and software products can be divided into three main types: hardware, software, and information objects [11].

Considering the types of objects of forensic expertise of computer equipment and software products under study, the features of the main tasks that are implemented, it is considered appropriate to distinguish three relatively independent subtypes of these forensic examinations:

– expertise of computer equipment (establishes circumstances and facts related to the functioning and operation of computer systems);

– expertise of software products (establishes circumstances and facts related to methodological, structural, and hardware features of software development and use);

– information and computer programmes expertise (establishes circumstances and facts related to information processing of the contents of file systems, their storage and reproduction on computer storage devices).

An important component of the successful outcome of the investigation of crimes in the use of electronic computing machines (computers), systems, and computer and telecommunication networks is the efficiency and completeness of the obtained sources of evidentiary information.

When appointing an expert examination of computer equipment and software products, it is necessary to focus on the stage of preparation for the appointment of a forensic examination, and also consider that due to incorrectly asked questions, difficulties may arise both in investigative and judicial practice, which, in turn, leads to the return of the decision to clarify the initiator of the expert examination or even a reasonable return of materials without their implementation.

Considering the above, persons initiating an expert examination should carefully and responsibly treat the initial stage of sending materials for expert research.

When determining the range of issues that should be clarified within the framework of a forensic examination, the initiator of the study must adhere to general rules and recommendations based on the classical principles of criminalistics, namely:

– not to go beyond the expert's special knowledge and not to have a legal nature;

– to be specific and concise;

– to have a logical sequence;

– to be characterised by completeness and have a complex character [12].

It is believed that when formulating questions for solution within the framework of expertise of computer equipment and software products, it is necessary to adhere to the following basic requirements and rules:

– use a generally accepted conceptual framework (do not use slang and semi-professional terminological units (for example,

“terabyter”,” logs and passes”,” iron”, etc.);

– the question should be formulated as clearly as possible, so that the forensic expert can provide an unambiguous answer. They should not concern the stages of Information research (description of the characteristics of information carriers and features of placing information on them, restoration and research of information among destroyed files is a mandatory stage of information research), have a legal area and go beyond the competence of a forensic expert of a certain expert specialty (special knowledge);

– adhere to the methodological sequence of questions (they must comply with the current methodological and technical base available for the forensic expert, be aimed at establishing the specific circumstances of the event related to the subject of proof, they should be formulated so that the costs (financial, technical, time, etc.) for conducting research when performing specific tasks of the investigation are minimal).

Based on the results of the analysis of forensic expert practice, a number of typical mistakes made by the initiators of conducting examinations of computer equipment and software products, which, as a result, complicates or makes it impossible to conduct it are distinguished. In particular:

– objects that do not and cannot contain information relevant for proof are submitted for examination;

– one resolution appoints forensic examinations for an excessive number of objects, making it impossible to examine them in a timely and proper manner;

– one resolution appoints expert examinations for various types of objects (servers and personal computers or mobile phones and “tablet” computers), for the study of which it is necessary to involve appropriate specialists;

– the forensic expert is provided with objects that, for objective reasons, cannot be properly examined (due to the lack of appropriate software, hardware, and devices).

Notably, computer systems (primarily servers) operate with so much information that their volumes can reach or even exceed university and academic libraries.

This means that the question of defining and installing an array of databases on it and the task of printing it out are incorrect

It should also be considered that the examination of computer equipment and software products does not solve the issue of the legality of user actions; licensing of software products; the cost of computer equipment and software products, since such issues go beyond the tasks facing this type of forensic examination.

Conclusions

It was determined that forensic examination of computer equipment and software products is a type of computer-technical forensic examinations belonging

to the class of engineering- technical forensic examinations, and is internally divided into three subtypes: examination of computer equipment, software products, and information-computer expertise.

The main requirements and rules for the formulation of questions for solving within the framework of the examination of computer equipment and software products were developed, including: the use of a generally accepted conceptual framework, clarity and unambiguity of formulation, methodological sequence of questions.

Typical mistakes made during the appointment of forensic examinations of computer equipment and software products are highlighted, namely: objects that do not contain and cannot contain information relevant for proof are provided for examination; within the framework of one resolution, examinations are appointed for an excessive number of objects; one resolution appoints examinations for various types of objects; objects are provided for the forensic expert, which for objective reasons cannot be properly investigated.

References

[1] State Research Forensic Center. (n.d.). Retrieved from https://dndekc.mvs.gov.ua.

[2] Honcharenko, V.H., & Hora I.V. (Eds.). (2015). *Expertise in the judicial process of Ukraine*. Kyiv: Yurinkom Inter.

[3] Computer-technical examination. (n.d.). nise.com.ua. Retrieve from https://nise.com.ua/it-ekspertyza.

[4] Criminal Procedure Code of Ukraine. No. 4651-VI. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#n2269.

[5] Kurylin, I.R., & Atamanchuk, V.M. (2020). Current issues of criminology and forensic science. In *Proceedings of the All-Ukrainian Scientific and Practical Conference* (pp. 461). Kyiv: National Academy of Internal Affairs.

[6] Lewis, J.A. (2020). *The hidden costs of cybercrime. Center for strategic and international studies*. Retrieved from https://www.csis.org/analysis/hidden-costs-cybercrime.

[7] Order of the Ministry of Justice of Ukraine "Instruction on appointment and conduct of forensic examinations and expert examinations". No. 53/5. (1998, October). Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

[8] Order of the Ministry of Justice of Ukraine "Regulations on the Central Expert Qualification Commission under the Ministry of Justice of Ukraine and certification of forensic experts" from March 3, 2015, No. 301/5. (n.d.). Retrieved from https://zakon.rada.gov.ua/laws/show/z0249-15#Text.

[9] Piaskovskyi, V.V., Chornous, Yu.M., & Samodin, A.V. (2020). *Forensics*. Kyiv: Pravo.

[10] Salnyk, S.V., Storchak, A.S., & Kramskyi, A.Ye. (2019). Analysis of vulnerabilities and attacks on state information resources processed in information and telecommunication systems. *Information Processing Systems*, 2(157), 121-128. doi: 10.30748/soi.2019.157.17

[11] Shcherbakovskyi, M.H. (2015). *Conducting and using forensic examinations in criminal proceedings.* Kharkiv: V dele.

[12] Teplytskyi, B.B. (2019). Tasks, objects and issues of computer-technical forensic examination., *Legal Journal of the National Academy of Internal Affairs*, 2(18), 24-32. doi: 10.33270/04191802.24

[13] Law of Ukraine "On forensic examination". No. 4038a-XII. (1994, February). Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12#Text.

[14] Zybin, S.V. (2007). Model of information security object and model of information leakage channels. *Ukrainian Information Security Research Journal*, 4(36), 9. doi: 10.18372/2410-7840.9.4127.

Список використаних джерел

[1] Державний науково-дослідний експертно-криміналістичний центр. URL: https://dndekc.mvs.gov.ua.

[2] Експертизи у судочинстві України: наук.-практ. посіб. / за заг. ред. В. Г. Гончаренка, І. В. Гори. Київ: Юрінком Інтер, 2015. 504 с.

[3] Комп'ютерно-технічна експертиза. URL: https://nise.com.ua/it-ekspertyza.

[4] Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n2269.

[5] Курилін І. Р., Атаманчук В. М. Тактичні особливості допиту в провадженнях про кіберзлочини. *Актуальні питання криміналістики та судової експертизи:* матеріали Всеукр. наук.-практ. конф. (Київ, 19 листоп. 2020 р.). Київ: Національна академія внутрішніх справ, 2020. 461 с.

[6] Lewis J. A. The hidden costs of cybercrime. Center for strategic and international studies. 2020

[7] URL: https://www.csis.org/analysis/hidden-costs-cybercrime.

[8] Інструкція про призначення та проведення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

[9] Положення про Центральну експертно-кваліфікаційну комісію при Міністерстві юстиції України та атестацію судових експертів: наказ Міністерства юстиції України від 3 берез. 2015 р. № 301/5. URL: https://zakon.rada.gov.ua/laws/show/z0249-15#Text.

[10] Криміналістика: підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Самодін; за заг. ред. В. В. Пясковського. 2-ге вид., переробл. і доповн. Київ: Право, 2020. 752 с.

[11] Сальник С. В., Сторчак А. С., Крамський А. Є. Аналіз вразливостей та атак на державні інформаційні ресурси, що обробляються в інформаційно-телекомунікаційних системах. Системи обробки інформації. 2019. Вип. 2. № 157. С. 121–128. doi:10.30748/soi.2019.157.17.

[12] Щербаковський М. Г. Проведення та використання судових експертиз у кримінальному провадженні: монографія. Харків : В деле, 2015. 560 с.

[13] Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. Вип. 2 № 18. С. 24–32. doi: 10.33270/04191802.24.

[14] Про судову експертизу: Закон України від 25 лют. 1994 р. № 4038а-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text.

[15] Зибін С. В. Модель об'єкта захисту інформації і моделі каналів витоків інформації. *Ukrainian information security research journal*. 2007. Вип. 4. № 36. doi:10.18372/2410-7840.9.4127.

Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку

Броніслав Броніславович Теплицький

Національна академія внутрішніх справ
03035, Солом'янська площа, 1, м. Київ, Україна

■ **Анотація**. Мета статті полягає в спробі дослідити актуальні питання проведення експертизи комп'ютерної техніки та програмних продуктів під час розслідування злочинів у сфері використання електроннообчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. Для досягнення поставленої мети використано загальнонаукові та спеціальні методи, які є засобами наукового пошуку. Зокрема, метод аналізу, системно-структурний і статистичний методи надали можливість дослідити місце експертизи комп'ютерної техніки та програмних продуктів у системі судових експертиз, виокремити її завдання й різновиди. Визначено основні підвиди судової експертизи комп'ютерної техніки та програмних продуктів: дослідження комп'ютерної техніки, дослідження програмних продуктів, інформаційно-комп'ютерні дослідження. Запропоновано базові правила й вимоги до формування питань судовому експерту, а також орієнтовний перелік питань, що можуть бути вирішені під час дослідження, виокремлено типові помилки, яких припускаються ініціатори проведення експертиз комп'ютерної техніки та програмних продуктів. З'ясовано, що судова експертиза комп'ютерної техніки та програмних продуктів є видом комп'ютерно-технічних судових експертиз, що належить до класу інженерно-технічних судових експертиз і внутрішньо поділяється на три підвиди. Розроблено основні вимоги та правила формулювання питань для вирішення в межах експертизи комп'ютерної техніки та програмних продуктів. Визначено типові помилки під час призначення судових експертиз комп'ютерної техніки та програмних продуктів

■ **Ключові слова**: спеціальні знання; судова експертиза; експертиза комп'ютерної техніки і програмних продуктів; розслідування злочинів; призначення експертиз