Artículo de investigación

The specifics of the appointment of forensic examinations in the investigation of corruption-related crimes committed in cyberspace

СПЕЦИФІКА ПРИЗНАЧЕННЯ СУДОВИХ ЕКСПЕРТИЗ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ КОРУПЦІЙНОЇ СПРЯМОВАНОСТІ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

Recibido: 15 de octubre del 2019 Aceptado: 20 de noviembre del 2019

Written by:
Valerii Tishchenko[125]
ORCID ID: https://orcid.org/0000-0002-1609-6196
Larysa Bielik[126]
ORCID ID: https://orcid.org/0000-0003-2183-6635
Olena Samoilenko[127]
ORCID ID: https://orcid.org/0000-0002-8925-4116

Abstract

Relevance. The study is relevance due to the problem of cybercrime, including corruption-related crimes, which were caused by the rapid worldwide development of computer technology, as well as the widespread use of cyberspace networks and the digitization of information-sharing processes in society.
The object of the study is the public relations that arise in the process of judicial expertise in the investigation of corruption-related crimes committed in cyberspace.
Several research methods have been used in the writing of this research article. The dialectical method was the first and foremost method in the study of judicial expertise. The method of analysis, the synthesis method, and comparison method were used during the research process.
Research results. The authors of this scientific article came to the conclusion that the specific nature of the use of forensic investigations in the investigation of corruption offenses committed in cyberspace is one of the main forms of use of specialized knowledge in criminal proceedings and the result of which is the conclusion of expert opinion, which is the source of evidence in criminal proceedings. In addition, it was noted that all the issues that are solved by the examination of telecommunication systems

Анотація

Актуальність. Актуальність статті зумовлена ростом числа злочинів вчинених у кіберпросторі, вчиненні яких стало можливим через стрімкий загальносвітовий розвиток комп'ютерних технологій, поширення використання мереж кіберпростору та діджиталізація процесів обміну інформації у суспільстві, та злочинів корупційної спрямованості.
Об'єктом дослідження є суспільні відносини, що виникають у процесі проведення судових експертиз при розслідуванні злочинів корупційної спрямованості, вчинених у кіберпросторі.
У написанні даної наукової статті було використано кілька методів дослідження. Діалектичний метод був першим і головним методом вивчення процесу призначення судової експертизи. Окрім цього, у процесі дослідження використовували метод аналізу, метод синтезу, метод порівняння тощо.
Результати дослідження. Автори даної наукової статті прийшли до висновків, що специфіка призначення судових експертиз при розслідуванні злочинів корупційної спрямованості, вчинених у кіберпросторі представляється однією з головних форм використання спеціальних знань в

[125] Doctor of Legal Science, Professor, Corresponding Member of the National Academy of Legal Sciences of Ukrain, Head of Department of of Criminalistics of National University «Odesa Law Academy»
[126] Ph. D., Associate Professor, of Department of Criminalistics of National University «Odesa Law Academy»
[127] Ph. D., Associate Professor, of Department of Criminalistics of National University «Odesa Law Academy»

(equipment) and tools have a diagnostic nature, and a list of typical issues should be fixed in the appropriate instructions.

Keywords: Judicial expertise, crime investigation, corruption, cyberspace, corruption-related crimes, crime.

кримінальному процесі і результатом якого є складання експертного висновку, що є джерелом доказу у кримінальному провадженні. Окрім цього, було зазначено, що всі питання, які вирішує експертиза телекомунікаційних систем (обладнання) та засобів, мають діагностичний характер, а перелік типових питань доцільно закріпити у відповідній інструкції.

Ключові слова: судова експертиза, розслідування злочинів, корупція, кіберпростір, корупційні злочини, злочини.

Introduction

The rapid worldwide development of computer technology, as well as the widespread use of cyberspace networks and the digitization of information-sharing processes in society, unfortunately, are actively used actively to commit cybercrime, including corruption-related crimes.

Hiring an expert to conduct forensic examinations is one of the main procedural forms of the use of specialized knowledge in criminal proceedings for corruption offenses, including those committed using cyberspace. The qualitative and quantitative characteristics of such crime from the standpoint of high-tech offender conspiracy of its activity and its wide range of participants make it possible to conduct a wide range of forensics, among which the leading place is up to the expertise of computer hardware and software products and expertise of telecommunication systems (equipment) and facilities.

Legal scholars and investigators often use the term computer-based expertise (hereinafter CBE). In theory, different types of CBE are distinguished, depending on the task, the specifics of the study, and the types of objects under study, such as hardware and computer expertise, software and computer expertise; examination of data (information-computer); computer network expertise; the complex of the mentioned expertise (Golubev, 2003; Panov, Shepitko, & Konovalova, 2003; Khatuntsev, 2010; Rossinskaya, & Usov, 2001). However, this separation is of theoretical importance, but the essence of CBE does not change. The investigation does not have a clear division of the objects of the study by CBE. The digital nature of information in cyberspace makes it impossible to delimit the study of the content of information from the material object that is its carrier. Research on telecommunication systems requires specialized knowledge related to understanding information processes in computer networks, communications networks, specialized telecommunication devices (Bobritskyi, 2008).

Methodology

Several research methods have been used in the writing of this research article. The dialectical method was the first and foremost method in the study of judicial expertise.

The method of analysis helped to identify the problematic issues and the efficiency of judicial examinations (computer-based expertise). The method of analysis also made it possible to study in detail the changes that have been made to the procedure for the appointment of judicial expertise in connection with the change of legislation.

The synthesis method was able to see ways to accelerate the process of computer-based expertise.

The comparison method made it possible to compare the new procedure for the appointment of forensics and the previous one, and to identify the positive and negative aspects of change.

Analysis of recent research

The analysis of the specialized literature on the topic of the research suggests that several domestic and foreign scientists have developed this problem. The works of following domestic for foreign scientists were used as the basis of this research Bobritskyi (2008); Golubev (2003);

Khatuntsev (2010); Lisichenko & Tsyrkal (1987); Panov, Shepitko, & Konovalova (2003); Rossinskaya, & Usov (2001); Teplitsky, Sharaj, Kovalev, & Kuzmin (2019).

Meanwhile, the development of cybercrime and changes in Ukrainian legislation create new problems that need to be solved. It is the analysis of recent changes in legislation and the resolution of practical problems that created this study.

Presentation of key research findings

Referring to the statistics of the State Scientific and Research Expert Forensic Center of the Ministry of Internal Affairs of Ukraine, we can see a union accounting of objects and the number of CBE (as of July 25, 2019, there were 1652 CBE in the structures of the Ministry of Internal Affairs Expert Service; 6239 objects of CBE was found in the study), similarly with regard to the examination of telecommunications systems (equipment) and facilities (20 expertise for 73 objects). Therefore, we aim to determine the specific purpose of the CBE and the expertise of telecommunication systems and facilities.

To achieve this goal, it is necessary to understand the current legal form of the appointment of judicial expertise in criminal proceedings. The essence of forensics is that the expert independently, based on specialized knowledge in science, technology, arts, crafts, etc., examines the objects, phenomena, and processes given to him to conclude issues that are or will be the subject of litigation (Law of Ukraine "On Forensic Examination", 2019). In the scientific literature, expert research refers to "the study of the objects and materials of the case provided to him by a knowledgeable person, to identify, analyze or compare the properties and features inherent, with the help of appropriate methods and techniques, to evaluate and formulate based on special knowledge the conclusions in the form of answers to the questions which were asked" (Lisichenko, & Tsyrkal, 1987).

In 2017, the lawmaker changed the traditional procedure for assigning an expert examination by the investigator – to involve a court expert in criminal proceedings, an investigator was required to refer to the investigating judge, and the reason for this referring was a decision on entrusting a judicial examination. At that time, many organizational aspects of its implementation remained unaddressed.

First, not all the decisions of the investigating judges included clarification for the expert on the further handling of all organizational matters about its execution by the investigator or the prosecutor. The organization of communication of the investigator with the expert through the investigating judge unreasonably increased the time limits for the examination.

Secondly, the initiation of a forensic examination by both the investigator and the defense party may have made it impossible for one of the experts to have access to the objects to be investigated. After all, the party of the process has already transferred them to another examination based on another decision or agreement. However, unfortunately, the prosecution party was not always the party that first applied to the investigating judge to request an examination.

Third, the exclusion of the investigating judge from the approval of the questions raised by the investigator in the request prevented him from receiving the answers from the subject of special knowledge, since there was no mechanism to appeal against such a decision. The reason for the described situation could be the incompetence of the investigating judge in that area.

Fourth, the investigating judge, as the subject of the decision on conducting any expert examination, is not able to verify at the stage of the petition the main reason for the procedural changes - whether the relevant petition is directed to delay the pre-trial investigation or abuse of procedural rights.

Fifth, provided that the forensic examination was performed by an expert and the authorized person decided to close the criminal proceedings, there was a problem of the need to complete the investigation. The implementation of such a decision unreasonably increased the workload of the expert institution, since the decision remained mandatory for the expert.

Given the lack of time and lack of mechanisms to appeal against such a decision to the investigating judge, the legal registration of the judicial review process was a formal procedure, which led to numerous omissions and shortcomings in the examination process, and a negative impact on the course of the investigation. The investigator was not able to obtain evidence of probative value in time. This was the reason for the October 2019 return to the traditional practice of designation of examination) - the examination has since been conducted by an expert institution or experts involved by the parties to the criminal

proceedings or by an investigating judge at the request of the defense party in the cases and procedure provided in Article 244 of Criminal Procedure Code, if special knowledge is needed to clarify circumstances relevant to criminal proceedings (Part 1 of Article 242 of the Criminal Procedure Code) (On Amendments to Some Legislative Acts of Ukraine on Improvement of Certain Provisions of Criminal Procedure Legislation, 2019).

However, even these changes did not solve all the problems of the expert involvement process by the investigators. After all, the monopoly of state specialized institutions (Article 7 of the Law of Ukraine "On Forensic Examination" (2019)) on the issue of expertise in criminal proceedings also delays the process of conducting certain types of judicial expertise. Experts in some areas of knowledge are overwhelmed by the amount of expertise they have given, which makes it impossible to execute a court order on time. The only way to solve the problem for the investigator is to refer criminal proceedings for trial without obtaining the expert's opinion. Also, the investigator may involve an expert institution that will agree to violate the principle of adherence to the statutory regional service areas and to conduct an examination from another region. Besides, the involvement of foreign experts is still impossible, because the formalism of the appointment of the examination involves the determination in the resolution of the investigator only the state expert institution, the expert who is charged with the examination.

The foregoing aspects of the involvement of an expert in criminal proceedings indicate the need to clarify the specifics of the assignment of CBEs and the examination of telecommunication systems and facilities in the context of tactical recommendations aimed at optimizing the process of appointment and conduct of these types of expertise.

Computer-based expertise is conducted on the vast majority of criminal proceedings for cybercrime (99% of the material analyzed).
Analysis of the literature and regulatory sources allows to determine that computer-based expertise is a study of the technical properties of computer (digital) equipment, software, information contained on digital media, in order to establish factual data relevant to computer-related applications and applications, as well as knowledge-based in the areas of computer engineering and programming.

Subjects of the forensic examination are computers with storage media (any information storage media, hard disks, CDs, flashcards, etc.), software and other computer equipment (for example, mobile phones, ATMs, gaming machines, card readers, e-books, printers, equipment documentation).

The basic document for determining the indicative list of issues for conducting CBE is the Instruction on the Assignment and Conduct of Forensic Expertise and Expert Research, and Scientific and Methodological Recommendations on the Preparation and Assignment of Forensic Expertise and Expert Research (2019) (paragraph 13 of Section II of the Recommendations). Typical lists of such issues are also found in numerous scientific and methodological publications on the topic of investigating various types of cybercrime and crime related to cyberspace. But, in our opinion, the requirements for formulating are more important than simple lists of such questions today. Recently, a group of practitioners of the State Scientific and Forensic Expert Research Center of the Ministry of Internal Affairs of Ukraine has been offered clear requirements for the questions that should be resolved by CBE (Teplitsky, B.V., Sharaj, L.G., Kovalev, K.M., Kuzmin S.A. (2019). We will consider them with our own reasoning.

1. When formulating the question, a well-established conceptual apparatus should be used, as well as to avoid semi-professional or jargon terms (such as a hard drive, flash drive, computer, etc.). The terminology from the laws of Ukraine, state standards and other normative legal acts should be used. Only in the absence of terms specified by legislative or regulatory acts, it is permissible to use the terms proposed directly by the developers of the technical means and software in the accompanying documentation.
2. The question should be as clear as possible and foresee the ability of the expert to give a clear answer. Often, objects that potentially do not and cannot contain information that is relevant to the proof are provided for CBE. For example, based on the requirement of completeness of the investigation of a crime, the investigator sends for the expert's examination all the computers that were temporarily removed during a search in the office from which the IP of the crime was

committed. It helps to avoid pre-screening and performing essentially sample work to identify a particular computer.

3. The wording of the question should not be related to the stages of information exploration (description of the characteristics of the storage media and the peculiarities of placing information on them, recovery and exploration of information among the destroyed files is a mandatory stage of the study).
4. Questions should not be legal (for example, about the lawfulness of a user's actions, counterfeit, license or cost of a software product) and should be meaningful, for example: what information, files, and folders are on the media; what is the content of the information contained on the media; what is the intended purpose of the information on the media; whether information on financial and economic activity is contained on a specific electronic medium; whether the storage medium contains information about automated system interference.
5. The questions must be directed at establishing the specific circumstances of the incident of the subject matter. The fully worded question helps to get the same answer. Therefore, the questions indicate a certain amount of time for the action, the essence of the action (printing, editing, creation, etc.), specific programs, their purpose, format files, sites, etc.
6. The questions should not go beyond the competence of a forensic expert of a particular expert specialty. In this sense, we note that a common misconception is to assign a single CBE decision to several sites that may require the involvement of specialists of different specialties or different specialties (for example, simultaneously using a computer and a mobile communication medium) which is of interest for the pre-trial investigation of the crime).
7. The questions should be consistent with the methodological and technical framework available to the judicial expert currently available. The investigator should understand that not all territorial divisions of the Expert Service of the Ministry of Internal Affairs of Ukraine or institutes of judicial expertise of the Ministry of Justice of Ukraine have the same software and hardware for conducting research. Usually, hardware and software complexes for making back-up copies of digital media that allow experts to completely or partially recover information that was lost accidentally or destroyed to conceal a crime, are now present in the MIA's expert units. However, if there is a need to investigate very large amounts of information, it is necessary to select the expert unit (with more sophisticated computer analytical systems) capable of researching at the appropriate technical level at the stage of the examination. Unfortunately, such services are not maintained in expert services. Only from the recorded data of the performance of the expert units can we conclude that in the territorial units, when updating the material and technical base for conducting CBE immediately increases the load on the experts, on average by 100%.
8. Questions should be formed so that the cost of research (financial, technical, time, etc.) for conducting research is minimal when solving specific investigative tasks.

For example, it is advisable to ask the following questions when conducting a CBE investigation of corruption offenses:

- Does the media contain the necessary information according to the questions and in what form? (For example, whether there is information on this medium about the implementation of a certain accounting transaction (transfer of funds, reporting, contracting, etc.).
- Does the test medium contain information about specific (specified) user actions? (For example, whether a particular user did certain activities (receiving or transferring funds, registering on certain sites)).
- Has the test drive been subjected to certain procedures for the destruction of information?
- Could this information have been created on this computer or has it been transferred from another medium? (For example, whether a specific document was created on a specified computer device or changes were made to a specific document on the specified computer device).

- What is the technology and timeline for creating an electronic document (indicate the name of the electronic document and its contents)?
- What are the attributes (when printing, editing, creating, deleting, etc.) of files containing the information which is searched?
- Do the media of the computer, which is under the test, contain some software (which is installed, not installed)? (for example, a specific Bank-client program, digital signature).

Currently, the timing of forensic examinations depends directly on the complexity of the study, the number of objects, the number of questions asked, and the workload of the specialists conducting the CBE. For example, according to clauses 14, 15 of the Instruction on the organization and conduct of expert proceedings in the units of the Expert Service of the Ministry of Internal Affairs of Ukraine for 30 days, examinations are conducted on materials that belong to the category of studies of medium complexity - this is subject to research from ten to twenty homogeneous and/or no more than ten different objects, solving no more than five questions and applying from three to five general scientific and/or specialized research methods (On approval of the Instruction on organization of conducting and registration of expert proceedings in the units of the Expert Service of the Ministry of Internal Affairs of Ukraine…, 2019). The analysis of the criminal proceedings concerning the investigated type of crimes indicates that the approximate duration of their conduct exceeds 30 days, since more than five questions are always asked for the expert's solution, and the presence on the study of one object is not an indicator of a small amount of work, the amount of information on a particular research object can "outweigh" the total amount of information on ten such objects. Therefore, in the practice of assigning CBE under the circumstances, the rule of "one object – one examination" may apply. Although, according to the statistics of the State Research Expert Forensic Center of the Ministry of Internal Affairs of Ukraine, the average of proportions looks like 1 examination for 5-6 objects.

To optimize the CBE process, the experts have developed the following algorithm for preparatory actions for the investigator (prosecutor):

1) To conduct a procedural review of sites involving experts (for example, the Expert Service of the Ministry of Internal Affairs of Ukraine) in order to determine the availability of data that can be of probative value in criminal proceedings and to decide on the expediency of further examination;
2) To pre-agree the list of questions on specific objects with experts (forensic experts) and optimize the number of questions;
3) To determine the research priorities of the objects submitted for examination;
4) To conduct examinations with differentiation by groups of research objects, and sometimes separate examinations for each research object (for the objective study of a large volume of various computer equipment (more than 10 units)) (Teplitsky, Sharaj, Kovalev, & Kuzmin, 2019).

Based on the analysis of forensic investigative practice, we consider it possible to supplement the specified algorithm of actions of the investigator (prosecutor) when engaging an expert to conduct CBE by the following measures:

1) To evaluate factual and documentary information that other examinations (or expert examinations) may have already been conducted in the case related to digital information research; the expert's requests received in this regard;
2) To evaluate the urgency of initiating the examination (whether the other party to the process is actually able to involve an expert under the contract before it is done in the pre-trial investigation);
3) To specify the quantity, quality, and list of objects to be provided for the trial expert (this will help to evaluate the real possibility of the examination in terms of time spent, its complexity and the value of future findings in the criminal proceedings).

Expert examination of telecommunication systems (equipment) and facilities was carried out in only 20% of the analyzed cybercrime cases. But an indicator could be much higher, the main reasons for this are the high cost of such expertise, the need for constant updating of the logistical support of the expert services for its implementation, as well as the lack of appropriate expert personnel in the system of the Expert Service of the Ministry of Internal Affairs of Ukraine.

The right to carry out forensic examinations is legally granted to forensic experts who have been entered in the State Register of certified forensic experts in their respective specialty. When working with the Register, it can be seen that as of October 1, 2019, 48 court experts are employees of state specialized institutions as of the specialty specialty "10.17 Research of telecommunication systems (equipment) and facilities". When working with their cards, it becomes clear that more than half of the experts are no longer valid for conducting such examinations, and the rest of the experts are released from the expert institutions of the Ministry of Internal Affairs of Ukraine. According to the State Scientific and Research Center of the Ministry of Internal Affairs of Ukraine, as of July 25, 2019 there are 6 vacancies in the expert services of the Ministry of Internal Affairs, with only 4 experts working in the state (in the State Research Expert Forensic Center, Vinnytsia and Chernivtsi Expert Forensic Centers), and 6 positions are vacant. The tendency for an increase in the number of objects being targeted for such studies (according to the State Scientific and Research Center for 2017, 69 objects were investigated, for 2018 - 224) indicates the necessity of obligatory resolution of personnel problems in this area of expertise.

Examination of telecommunication systems (equipment) and facilities is the study of telecommunication systems and facilities, networks, their components and the information transmitted, received and processed to establish the technical parameters and status of the object, to determine their functional purpose. This type of research requires some specific knowledge related to the understanding of information processes in computer networks, communications networks, specialized telecommunication devices (Bobritskyi, 2008), which necessitates a separate selection of relevant expertise.

Conclusions

In the investigation of crimes committed in cyberspace, the objects of this expertise are often the following: Internet IP nodes, web pages, radio receivers, switching nodes; primary communications networks, terrestrial satellite stations, circumstances (Internet addressing; radio transmissions; use of Internet domain names, etc.). The need for the appointment of this expertise in the case arises if the method of committing (concealment or preparation) of the crime is:

- Interference with the networks of telecommunication operators;
- Replacement, distortion, leakage, loss of traffic and distortion of the process of its processing;
- Violation of the established traffic routing order.

According to the departmental instruction " Assignment and Conduct of Forensic Expertise and Expert Research, and Scientific and Methodological Recommendations on the Preparation and Assignment of Forensic Expertise and Expert Research" (2019), the investigator formulates questions for expert investigation based on the material available in criminal proceedings and with compliance requirements for issues similar to those discussed above for CBE requirements.

Here is an example of issues that can be solved when conducting telecommunication expertise in the investigation of corruption offenses:

- What type, brand, a model of telecommunication facility (system)?
- Did the telecommunication network user change the settings of the individual devices, at what time, what are their values?
- What is the general nature of connections to the telecommunications network performed by the facility (telecommunication system, facility)?
- What software did you use to connect to the telecommunications network?
- Was there a fact of access to the telecommunication system and how?
- Was there any use of resources and information in the telecommunications system and how?
- Has there been a fact of transmission (receipt) of information in the telecommunication system and how?
- Are there any signs of interference with the telecommunication system?

Using the generally recognized in the theory of forensic division of questions into the identification and diagnostic, we consider all the issues that are solved by the examination of telecommunication systems (equipment) and tools, have a diagnostic nature, and a list of typical issues should be fixed in the appropriate instructions.

Therefore, the specific nature of the use of forensic investigations in the investigation of

corruption offenses committed in cyberspace is one of the main forms of use of specialized knowledge in criminal proceedings and the result of which is the conclusion of expert opinion, which is the source of evidence in criminal proceedings.

References

Bobritskyi, S.M. (2008). Methodological aspects of research of telecommunication systems (equipment) and facilities. Theory and Practice of Forensics and Forensics, 8, 445-449.

Golubev, V.O. (2003). *Information security: problems of fight against cybercrime.* Zaporizhzhia: ZIDMU.

Khatuntsev, N.A. (2010). On special knowledge required in the study of computer tools and systems. Actual problems of Russian law, 1, 332-339.

Law of Ukraine "On Forensic Examination" of February 25, 1994 No. 4038-XII. (2019). *Verkhovna Rada (Ukrainain Parlament).* Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12.

Lisichenko, V.K., & Tsyrkal, V.V. (1987). *The use of special knowledge in investigative and judicial practice.* Kyiv: KGU.

On Amendments to Some Legislative Acts of Ukraine on Improvement of Certain Provisions of Criminal Procedure Legislation. (2019). *Verkhovna Rada (Ukrainain Parlament).* Retrieved from https://zakon.rada.gov.ua/laws/show/187-20#n6.

On approval of the Instruction on organization of conducting and registration of expert proceedings in the units of the Expert Service of the Ministry of Internal Affairs of Ukraine: Order of the Ministry of Internal Affairs of Ukraine 17.07.2017 No. 591. (2019). *Verkhovna Rada (Ukrainain Parlament).* Retrieved from https://zakon.rada.gov.ua/laws/show/z1024-17?find = 1 & text =% F1% F2% F0% EE% EA # w12.

On Approval of the Instruction on the Assignment and Conduct of Forensic Expertise and Expert Research, and Scientific and Methodological Recommendations on the Preparation and Assignment of Forensic Expertise and Expert Research: Order of the Ministry of Justice of 08.10.1998 No. 53. (2019). *Verkhovna Rada (Ukrainain Parlament).* Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=%EA%EE%EC%EF%27%FE%F2%E5%F0#w110.

Panov, M.I., Shepitko, V. Yu., & Konovalova, V.O. (2003). *Investigator's Handbook.* Kyiv: In Yure Publ. House.

Rossinskaya, E.R., & Usov, A.I. (2001). *Forensic computer-technical examination.* Moscow: Law.

Teplitsky, B.V., Sharaj, L.G., Kovalev, K.M., & Kuzmin, S.A. (2019). *Crimes in the use of electronic computers (computers), systems and computer networks and telecommunication networks.* Kiev: Palivoda.