UDC 102/.148:343.982.9
DOI: 10.33270/04202002.8

Modern Capabilities of Forensic Examinations in the Investigation of Unauthorised Interference in the Operation of Computers, Automated Systems, Computer Networks or Telecommunication Networks

Bohdan Cherniakhovskyi

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

Abstract

The purpose of the study is to highlight the possibilities of using forensic examinations in criminal proceedings regarding unauthorised interference in the operation of computers, automated systems, computer or telecommunication networks. The study applies empirical and theoretical research methods. Empirical methods include a survey of employees of operational units of the cyber police and forensic experts of the Ministry of Internal Affairs system, analysis of data from the open part of the Unified State Register of Court Decisions. Theoretical methods include analysis and synthesis, analogy, comparison, and generalisation. A methodology for investigating the trace picture of a crime under Art. 361 of the Criminal Code of Ukraine is proposed, using the capabilities of forensic expert studies of various types to fix and examine physical traces of a crime, and the appointment of a comprehensive forensic examination of computer equipment, software, telecommunications systems, and their means. The necessity of improving regulatory acts in accordance with the methodology of computer equipment and software products research is substantiated. The results of forensic research are a key element of the evidence base of the prosecution in criminal proceedings regarding unauthorised interference in the operation of computers, automated systems, computer or telecommunication networks. The use of special knowledge in the pre-trial investigation of cybercrime is an integral part of achieving the tasks of criminal proceedings. Regulatory and legal support of forensic expert activities to meet the needs of pre-trial investigation must be improved based on modern leading methods of conducting expert research

Keywords:

computer; automated system; computer network; telecommunication network; unauthorised interference in the operation of computers; cybercrime; forensic examination

Article's History

Received: xx.xx.2021
Revised: xx.xx.xxxx
Accepted: xx.xx.xxxx

Suggest Citation:

Cherniakhovskyi, B. (2021). Modern capabilities of forensic examinations in the investigation of unauthorised interference in the operation of computers, automated systems, computer networks or telecommunication networks. *Law Journal of the National Academy of Internal Affairs*, 20(2), 81-89

*Corresponding author

Introduction

Activation of the processes of integration of information technologies into public relations is one of the most substantial indicators of expanding the opportunities for self-realisation of a citizen in the legal field of the state. This is provided by the rapid informatisation of both the private and public sectors of public life since most of the functions of enterprises, institutions, or organisations are performed using computers, computer systems or networks.

The development of information technologies expands the range of possibilities of cybercrime, provides a direct possibility of effective protection against them. Now the functioning of information and computer systems is becoming increasingly important for the proper functioning of the state. Therefore, unauthorised interference in the operation of computers, automated systems, computer networks provokes and deepens public crisis phenomena, weakens the image of the state on the world stage, negatively affects economic processes, hinders the establishment of a constructive dialogue between representatives of the state power and the public, destroys the foundations of the development of a democratic state governed by the rule of law.

None of the world's information systems had and does not have absolute immunity from cyber attacks and outside interference. Only the ways in which they are committed and the attitude of the state and society to such incidents change.

In this regard, ensuring an effective and high-quality investigation of crimes in the field of information technologies, the technical aspect of which is not yet a core basis in the system of training personnel for pre-trial investigation bodies, requires investigating these issues at an in-depth scientific level. However, considering the needs of the investigative practice and the constant hyperactive development of computer technologies, there is still an urgent need to regularly improve the system of knowledge and skills of investigators regarding the specific features of working with digital information during criminal proceedings, in particular regarding its fixation, seizure, and further research during forensic examinations.

The purpose of the study is to highlight the possibilities of using forensic examinations in criminal proceedings regarding unauthorised interference in the operation of computers, automated systems, computer or telecommunication networks.

It is necessary to solve the following tasks to reach the objective:

– conduct forensic characterisation of the collection of evidence, in particular in digital (electronic) form, their seizure and research within the framework of forensic expert research in the investigation of unauthorised interference in the operation of computers, automated systems, computer or telecommunication networks;

– determine the essence and features of forensic expert research of material and non-material (digital) components of the evidence base, coverage of methods of complex search and fixation of material (conventional) and digital (electronic) evidence;

– based on the analysis of existing practice, form practical recommendations for optimising and improving the quality of research on the traces of a crime under Art. 361 of the Criminal Code of Ukraine.

Results and Discussion

Countering crimes in the use of computer technologies requires active implementation and application of a set of new methods and tools for effective pre-trial investigation. One of the most common crimes in the field of information technology is unauthorised interference in the operation of computers, automated systems, computer or telecommunication networks under Art. 361 of the Criminal Code of Ukraine.

According to the statistics of the National Police of Ukraine, in 2017, as a result of massive cyber attacks of the PetyaA computer virus on Ukrainian infrastructure, the number of registered criminal offences with the above qualification was 2186 against 592 in 2016. Therewith, the indicators of registered criminal offences under Art. 361 of the Criminal Code of Ukraine over the past two years remain at a fairly high level, considering statistical data. Thus, during the eleven months of 2020, 1,174 criminal offences were registered, which is comparable to 1.289 criminal offences in 2019 [1].

According to its content, Art. 361 of the Criminal Code of Ukraine provides for unauthorised interference in the operation of automated electronic computers, their systems, or computer networks, which led to the distortion or destruction of computer information or carriers of such information, and the spread of a computer virus through the use of software and technical means intended for unauthorised entry into these machines, systems, or computer networks and capable of causing distortion or destruction of computer information or carriers of such information [2].

Experts in the field of informatisation and communications claim that cyber attacks, in particular, fall under the sanction of art. 361 of the Criminal Code of Ukraine, implemented by malefactors to violate the confidentiality, integrity, or availability of public information resources (or private ones) stored, processed, and circulated in a computer/information-telecommunication system. For this purpose, they mainly use the vulnerabilities of such systems, that is, their inability to resist the implementation of a certain threat or a set of threats [3].

It is necessary to use typical investigative situations of the initial stage of the investigation to outline the range of expert studies that allow covering and proving the fact of a crime under Art. 361 of the Criminal Code of Ukraine, namely:

– committing a crime by direct (physical) access of an attacker to the hardware of a computer, connecting to a computer network through connections on electric switchboard or wired lines, which are conducted, in particular, by secret entry into the premises;

– commission of a crime by remote access to a computer, computer or automated system through other computers using telecommunications or wireless networks.

The conclusions of forensic experts in the vast majority of criminal proceedings and other types of legal proceedings play the role of the most important evidence, without which it is almost impossible to resolve a certain case [4]. The effectiveness of the investigation, according to these situations, provides for the appointment and conduct of forensic examinations – investigations based on special knowledge in the field of science, technology, art, crafts of objects, phenomena, and processes to provide an assertion on issues that are or will be the subject of judicial review [5], depending on the specific circumstances of the initial stage of the investigation, tracological, biological, and main in the process of proof – computer-technical types of forensic examinations are appointed.

According to these investigative situations, to examine the traces of illegal access to the hardware of a computer, or a computer network, it is necessary to examine the traces of criminal actions that remained on objects and their surfaces, analyse the situation of the scene: to examine the places of the possible connection to the wired lines that lead to the premise, the state of connections in electric switchboards, the intactness of door locks, the presence of traces of hands, shoes (feet), other parts of the body, hair, smell traces in possible places of physical contact of the criminal with the elements of the crime scene, etc. The presence of such traces of crime must be in the centre of attention: traces of hands (papillary patterns), traces of shoes (feet) that the offender left during access to computer equipment, or traces of breaking locks, doors, seals on electric switchboards, etc.

Sharing the opinion of O.M. Dufenyuk [6], for the methodological support of forensic expert activity in criminal proceedings, the priority is algorithmisation of expert actions, which will allow for obtaining more accurate and reliable results with fewer resources and time.

First of all, the need to conduct a tracological examination of the identified traces is established, which is aimed at identifying or determining the generic (group) belonging of individually defined objects by materially fixed traces, in particular by the reflections of their trace-forming surfaces; diagnose the properties, condition of the object; establish the mechanism of trace formation (situational tasks), etc.

Tasks and possibilities of forensic examinations in criminal proceedings on unauthorised interference in the operation of computers, automated systems, and computer or telecommunication networks are considered below. The subject of the investigation of tracological examination during the investigation of the crime under Art. 361 of the Criminal Code of Ukraine, there are two main groups of traces: 1) human traces (traces of the human skin, shoes, clothing (gloves, etc.); 2) traces of tools (traces of tampering, traces on mechanical locks, control devices, etc.). This list is not exhaustive, it is the basis for forensic knowledge of the situation by the investigator, so to identify other traces, it is recommended to inspect the scene with the involvement of a criminalist, expert.

The task of fingerprinting is to establish a person's identity based on a set of common and individual features reflected in the handprint. Instruction on the appointment and conduct of forensic examinations and expert research, approved by Order No. 53/5 of the Ministry of Justice of Ukraine of October 8, 1998, (as amended by the order of the Ministry of Justice of Ukraine of December 26, 2012, № 1950/5) (hereinafter referred to as the Order of the Ministry of Justice No. 53/5), defines a typical list of questions that are put for the expert's decision: whether there are traces of hands on the object; whether these traces are suitable for identification; whether the traces of hands left by a specific (one) person; whether the traces left by one person in different places; what features do the hands of the person who left the traces (absence of fingers, presence of scars, etc.); as a result of what action the trace was left (grabbing, touching, etc.); whether there were traces on the surface of a particular object; whether there are signs of transfer of the traces from one surface to another, etc. [7].

In the analysed category of criminal proceedings, tracological examinations are often appointed to examine shoe traces. The following questions can be asked to solve this expert study: whether there are traces of shoes on this surface (this object) and whether these traces are suitable for identifying shoes; whether the traces are left by shoes seized from a certain person; whether the same shoe leaves traces collected from different places; what kind of shoes leave these traces, what are its characteristics, distinguishing features (size, degree of wear, etc.); what is the approximate height of the person who left the traces, etc. [7].

The diagnostic task of such a study also provides an opportunity to determine the features of a person's movement, the size of their shoes, approximate height, etc. The investigator must inform the expert about the facts of wearing or repairing the shoes provided for research after the crime and before the appointment of the expert examination to ensure the objectivity of the study.

Expert examination of tampering traces allows for identifying a specific instance or type (features) of the used tool based on the traces of its direct action. This type of tracological examination solves issues related to the establishment of the mechanism (method) of tampering, the area in which the interference was broken (from the inside or outside), the type of product that left a trace, the possible method of its manufacture, etc.

The expert is asked the following questions to perform these tasks: whether tampering or another action was committed by this tool; what kind of tool was used to commit tampering; how the object was damaged (by cutting, sawing, drilling, etc.); what kind of tool damaged the object; whether traces of tampering, collected from different places of events, were left by the same tool [7].

The expert is preferably provided with an object with traces of tampering to conduct this examination. Sometimes it is recommended to provide casts from three-dimensional objects. The realities of practical investigative activity indicate that if there is no certainty that the seized tools correspond to the detected traces of tampering, it is necessary to inform the expert and ask questions about the method and possible auxiliary elements for the committed tampering. A separate investigative situation related to secret entry into a room with computer equipment consists of de-energising alarm systems and surveillance cameras due to blocking their signal by damaging cables.

In this case, the tracological examination of cables and tools provides an opportunity to resolve the following questions: how the cable was damaged (by cutting, sawing, snapping, etc.); whether this tool damaged the cable (the part of cable with damage trace is investigated); one or more tools damaged the cable (the part of cable with damage trace is investigated); whether the cable fragments collected during (separate) inspections of the crime scene were one (dates of procedural actions) [7].

The objects of expertise of locking and safety (control) devices (means) are locks and other locking devices, seals, and control devices (means). The task of this study is to establish the fact and method of unlocking (braking) the device, the type of object used for this purpose, and its identification. In the case of examining seals, it is possible to identify the seal vice, the fact of re-glueing paper control tools, etc. When examining locks, the expert, if possible, is sent lock picks and other items that could have been used to unlock or break the lock, and all the keys to these locks.

Tracological examination of locks provides answers to the following questions: whether the lock is in good condition; what is the cause of the malfunction of the lock; whether there are traces of foreign objects on the surfaces of the lock; if so, what objects (tools) left them; whether the lock was unlocked with a lock pick, picked, or fake key; whether it is possible to unlock the lock with the provided key (lock pick); how (the picking of the provided lock was conducted) the lock was unlocked; whether the provided lock was picked by the provided tool, etc. [7].

As part of the tracological study of seals, considering the investigative situation of the investigation of the crime under Art. 361 of the Criminal Code of Ukraine, it is necessary to determine the following questions: whether the seal was compressed with these sealing vices; whether the seals were compressed with the same sealing vice; whether the seal was opened and re-compressed after it was compressed with a sealing vice; how and with what tool the seal was opened and re-compressed; whether it is possible to extract the material used for sealing (wire, twine, cord) from this seal, without damaging it; whether the seal was opened with the provided tools [7].

The expert must, in addition to the seal, provide the seal vice with which it was supposed to be sealed, or experimental seals compressed by this vice to establish the fact of opening the seal. It should be considered that during the examination in the process of conducting expert experiments, the expert can use over 10 non-compressed seals, similar to the investigated ones, and the same number of samples of materials (wire, twine, cord) that were used during sealing.

The analysis of investigative practice shows that in criminal proceedings under Art. 361 of the Criminal Code of Ukraine, there are cases in which accomplices of the main perpetrators of a crime enter the premises (Art. 162 of the Criminal Code of Ukraine) with computer equipment or a network in a rather primitive way – by breaking the glass of a window frame, plastic partitions, etc. In such cases, the subjects of the investigation should separately consider the possibilities of tracological expertise to establish the whole in parts.

This type of research provides an opportunity to determine whether the parts of the object (found fragments, pieces, etc.) have a common line (surface) of separation, that is, whether they previously formed a single whole. The expert can be faced with the following questions: whether the found parts

formed a single whole; how its parts were separated from the object; to what type does the object, part of which was removed from the scene belong [7].

All found parts that previously may have formed one item are submitted for examination. The list of issues resolved by forensic examinations, defined by the Order of the Ministry of Justice No. 53/5, is indicative and during the investigation of unauthorised interference in the operation of computers, automated systems, computer or telecommunication networks may require clarification or adjustment on the recommendations of a specialist or expert, depending on the specific circumstances of the case.

Increased attention during the recording of criminal actions under Art. 361 of the Criminal Code of Ukraine should be focused on the possibilities of examination of biological traces of a person, which are recorded during an investigative examination.

In this regard, during the investigation of a crime under Art. 361 of the Criminal Code of Ukraine, a forensic medical examination of material evidence is typical. Depending on the type of physical evidence of biological origin, the forensic medical examination is conducted by a separate specialised department of the bureau of forensic medical examinations, in accordance with the rules for conducting certain types of examinations approved by the order of the Ministry of Health of Ukraine No. 6 of January 17, 1995, (hereinafter referred to as the order of the Ministry of Health No. 6) [8].

Considering the typical investigative situations of the initial stage of the investigation of a crime under Art. 361 of the Criminal Code of Ukraine, physical evidence of biological origin includes: traces of blood, hair, skin epithelium, saliva, tear fluid, etc. The algorithm for investigating stated physical evidence covers, in particular, detection, description, photographing, extraction, and packaging of traces of biological origin; establishing the presence of blood, hair, other biological fluids and tissues (saliva, tear fluid, etc.) in the collected expert materials; establishing the specific, sexual, group affiliation of traces (in particular, according to isoserological and immune systems); excluding or establishing the affiliation of traces of biological origin to a specific person (the importance of molecular-genetic methods) [9].

The study of traces of biological origin is conducted in accordance with the methodology approved by the order of the Ministry of Health No. 6. The list of indicative questions that are put to the decision of a forensic medical examination is not fixed at the regulatory level.

However, the results of cooperation between investigators and forensic medical experts in the investigation of crimes allowed forming typical questions that are put to the decision of the forensic medical examination of material evidence.

Thus, forensic medical (immunological) examination of blood traces during the investigation of a crime under Art. 361 of the Criminal Code of Ukraine should answer the following questions: whether there is blood on the object; blood type; gender of the person it belongs to; whether that person is an adult or a child; what is the regional longevity of blood stain; what is the prescription of blood spots; whether the origin of blood from a particular person is possible [10].

Analysing the investigative practice, it was established that cases of collecting and analysing of hair found in places of physical access to the hardware of computers or servers is not uncommon. Such objects are sent for forensic medical (cytological) examination. In the departments of forensic cytology, studies are conducted to establish the presence of human tissue cells in traces and physical evidence, determining their specific, group, gender, and organ-tissue affiliation.

The study of hair is conducted during a forensic medical (cytological) examination, which asks the following questions: whether the provided object is hair; if so, whether it belongs to a person or animal; from what part of the body it originates; whether there is mechanical damage to it; what is the method of hair removal (dropped, torn); whether the hair has signs of chemical or thermal effects; whether there are diseases of the hair; what is its gender and individual affiliation, etc.

Comparative cytological examination based on the total characteristics establishes the similarity or dissimilarity of hair, and not its identity, since the hairs from the head of one person may differ, but the hair of different people may have the same characteristics [11]. Considering this feature, a complex of studies is conducted, which includes one of the variants of DNA analysis-polymorphism, which determines the source of hair origin. This study has the following names: DNA examination, molecular-genetic or genotyposcopic examination. The results of the molecular-genetic examination of mixed biological traces distinguish them and determine by individual characteristics the specific individuals who left them on the subject provided for research [9].

The possibility of using the examination of computer equipment and software products (in the forensic literature, the name "computer-technical expertise" is more common) and the examination of telecommunications systems and means are important while investigating criminal proceedings under Art. 361 of the Criminal Code of Ukraine. These studies are provided for in paragraphs 13 and 14 of the Order of the Ministry of Justice No. 53/5.

During the analysis of scientific sources, subspecies of expertise of computer equipment and software products are established:

– hardware examination (analysis of computer technical means);

– software examination (analysis of algorithms involved in the device and ensuring its performance);

– Information examination (installation, analysis of files operated by the user, evaluation of data functionality, their purpose, identification of belonging to the type of operational information).

The tasks of examination of computer equipment and software products are: establishing the working condition of computer-technical means; establishing circumstances related to the use of computer-technical means, information, and software; identifying information and software contained on the computer; establishing compliance of software products with certain versions or requirements for its development.

The expertise of telecommunications systems and tools was formed in the process of improving and deepening the methods of computer-technical expertise. This was due to the rapid development of types and forms of data transfer between individual computers. Mass connection of society to the global Internet, Wi-Fi and Bluetooth communication modules have determined the generally accepted norm of computer functionality. The need to examine routes and methods of information transmission formed tasks for the examination of telecommunications systems and means: determining the characteristics and parameters of telecommunications systems and means; establishing facts and methods of transmitting (receiving) information in telecommunications systems; establishing facts and methods of accessing systems, resources and information in the field of telecommunications; determining the quality of providing telecommunications services at the level of their consumption; establishing the configuration and working condition of telecommunications systems and means; establishing the type, brand, model, and other classification categories of telecommunications systems and means; investigating algorithms for information processing and protection in the field of telecommunications [7].

The Order of the Ministry of Justice No. 53/5 provides for an indicative list of questions that are put for solving by the examination of computer equipment and software tools: whether this medium contains information that interests the investigator, in what form; whether the medium of the computer under study contains information about certain user actions; whether the drive under study underwent certain procedures for the purpose of destroying information; whether the specified information could have been created on this computer, or it was transferred from another medium; how the information was transferred to the computer (medium) under study; what is the technology and chronology of creating a certain electronic document; what attributes (time of printing, editing, creating, deleting, etc.) of files containing information that interests the investigator; whether the hard drive of the computer under study contains certain software; what functional malfunctions this computer equipment or its individual components and devices have, how these malfunctions affect the operation of the equipment in general; whether it is possible to perform certain actions using this software product; whether this software product (programme code) implements the functions provided by the technical specification for its development [7].

When conducting an expert examination of telecommunications systems and means, the object of research is telecommunications systems, means, networks, and their components, the information that they transmit, receive, and process. The examination solves the following questions: what type, brand, model of the telecommunication means (system); whether the telecommunication means (object) is in working condition; what characteristics of connections to the network the telecommunication means has; whether the user of the telecommunication network changed the settings of individual devices, at what time, what are their values; what is the general nature of connections to the telecommunication network performed by the object (telecommunication system, means); through which software tools were connected to the telecommunication network; what is the topology of the hardware combined into the telecommunication system; whether the functioning of the telecommunication means (system) corresponds to the technical documentation; what technical characteristics (parameters) has the telecommunications mean (system); whether there is a fact of access to the telecommunications system and in what way; whether the use of resources and information in the telecommunications system, in what way; whether there is a fact of transmission (acquisition) of information in the telecommunications system and in what way; whether there are signs of interference in the operation of the telecommunications system; whether the hardware could be combined into a telecommunications network and by what signs; what data routing paths in the telecommunications system, etc. [7].

The proposed list is indicative, so depending on the circumstances of the crime under investigation, the questions should be adjusted, specified, and supplemented, considering the advice of a specialist or expert who will conduct the examination. According to O.V. Yakovlev [12], it is unacceptable

from a procedural standpoint to formulate general questions for the expert, for example: "is the provided object suitable for research?", since even within the same type of expertise, the examination can be identification, classification, diagnostic, situational. Procedural extremes are caused by the question: "Does the hard magnetic disk drive provided for research contain information related to criminal proceedings?" since the expert cannot know what information concerns the pre-trial investigation.

The existence of competition between non-governmental expert institutions conducting such types of research has a positive impact on the development and professional improvement of specialists in expert research of computer technology, software, telecommunications systems, and their means. This helps to expand the capabilities of computer-technical expertise and the list of issues that it solves.

The examination of investigative and expert practice, the analysis of scientific sources demonstrated that other issues that are not provided for by the Order of the Ministry of Justice No. 53/5 are also put on the solution of computer-technical examinations, which experts successfully solve, for example: whether information with keywords ".." is contained on the media provided for research; whether the media provided for research contained files that were subsequently deleted; if so, which files and what content; from which of the computers provided for research, access to the Internet was made, at what addresses, in what period of time; whether there are software products on the computer under study designed to crack the password and unauthorised access to computer systems; whether it is possible to perform a certain task using a software product (which one is indicated); what is the level of professional training in programming and working with computer equipment of the person who performed certain actions with the computer and software; whether the programming style of the software under study corresponds to ones of a certain person; whether the programming techniques and tools used in the creation of the software product under study correspond to the techniques and tools used by a certain person [13].

Along with the main tasks of complex forensic examination of computer equipment, software, telecommunications systems, and their tools, it is possible to solve issues of an auxiliary nature regarding the level of professional training of individuals in the field of programming and working with computer equipment. For example, identification of the user through keyboard style (by the speed of typing characters, the habit of using the main or auxiliary part of the keyboard, features of "double" or "triple" keystrokes, and favourite computer control techniques. Identification of keyboard style consists in selecting the appropriate standard from the list of standards stored in the computer's memory, based on evaluating the similarity of the handwriting parameters of one of the users who have the right to work to this standard [14].

The expediency of assigning a comprehensive forensic examination of computer equipment, software, telecommunications systems, and their means in criminal proceedings under Art. 361 of the Criminal Code of Ukraine is justified by the presence in the Register of methods for conducting forensic examinations of the Ministry of Justice of the appropriate methodology for this type of expert research. Therewith, this register does not contain a separate methodology for conducting research on telecommunications systems (equipment) and tools, in contrast to the methodology for investigating computer equipment and software products [15].

The scientific originality of the study is formed by the results of the analysis of the problems and features of fixing the traces of a crime in the investigation of unauthorised interference in the operation of computers, automated systems, computer networks or telecommunication networks, the object of encroachment is information stored in a computer, on a certain medium, and/or software. A set of measures for recording and working with material traces of a crime on the hardware component of computer equipment, and with information stored on their media and matters for pre-trial investigation, was considered. The features of using the capabilities of forensic research in the investigation of unauthorised interference in the operation of computers, automated systems, computer or telecommunication networks were highlighted, the object of encroachment is information stored in a computer, on a certain medium, and/or software. The expediency of considering the provisions of the methodology for investigating computer equipment and software products combined with the provisions of the Register of methods defined by the Ministry of Justice was substantiated. In such cases, the pre-trial investigation bodies should comply with the requirements of the current regulatory and administrative (departmental) acts of Ukraine, apply to the investigating judge with a request for the appointment of a comprehensive forensic examination of computer equipment and software products, examination of telecommunications systems and means. Such an expert statement will comply with the provisions of the Criminal Procedure legislation of Ukraine, and paragraphs 13 and 14 of the Order of the Ministry of Justice No. 53/5. Examples of storing or even hiding information of interest for pre-trial investigation on computer hard drives were considered to illustrate this position, leading to the investigation of a computer or computer network

as an environment in which unauthorised leakage, loss, forgery, blocking of information is conducted, its processing process is distorted or the established procedure for its routing is violated.

Conclusions

Pre-trial investigation of unauthorised interference in the operation of computers, automated systems, computer networks or telecommunication networks, considering the specific features of the crime and the methods of its commission, requires special training of the investigator, the presence of appropriate forensic knowledge, and skills and abilities. Therefore, the analysis of the possibilities of such examinations as tracological, fingerprint, forensic-medical examination of physical evidence, molecular-genetic, examination of computer equipment and software products, and examination of telecommunications systems and tools is important during the investigation of various manifestations of cybercrime in Ukraine.

References

[1] Arseniuk, T.M., Beliak, Yu.M., & Boiarov, V.I. (2005). *Examinations in judicial practice*. Kyiv: Yurinkom Inter.
[2] Boichenko, S.B., Boiarov, V.I., & Budko, T.V. (2015). *Expertise in the judicial process of Ukraine*. Kyiv: Yurinkom Inter.
[3] Borysova, L.V., Bilenchuk, P.D., & Malii, M.I. (2020). Examination as a means of establishing the facts and circumstances of committing transnational computer crimes. *Forensics and Forensics*, 65, 230-239.
[4] Dufeniuk, O.M. (2019). Ensuring forensic activity in criminal proceedings: A systemic paradigm. *Bulletin of Lviv University of Trade and Economics*, 8, 163-173.
[5] Kliuiev, O.M. (2019). Improving the expert support of justice: Theoretical, legal and organizational aspects. *Theory and Practice of Forensic Science and Criminology*, 19, 102-117.
[6] Criminal Code of Ukraine No 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14
[7] Marchuk, A.I. (1997). *Forensic medicine*. Kyiv: Heneza.
[8] Mishalov, V.D., Khokholieva, T.V., & Bachynskyi, V.T. (2018). *Forensic medicine*. Chernivtsi: Misto.
[9] Order of the Ministry of Health of Ukraine "Instructions for forensic examination" No. 6. (1995, January). Retrieved from https://zakon.rada.gov.ua/laws/show/z0254-95
[10] Order of the Ministry of Justice of Ukraine "Instructions on the appointment and conduct of forensic examinations and expert studies" No. 53/5. (1998, October). Retrieved from https://zakon.rada.gov.ua/laws/show/z0001-13#Text
[11] Disclosure of public information. (2020). Retrieved from https://www.npu.gov.ua/activity/zviti/oprilyudnennya-publichnoji-informacziji.html
[12] Register of methods of forensic examinations. (2020). Retrieved from http://rmpse.minjust.gov.ua
[13] 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.
[14] Yakovliev, O.V. (2019). The role of the prosecutor – procedural manager of the pre-trial investigation in the appointment of forensic examination and evaluation of its results. *Forensics and Forensics*, 64, 350-360.
[15] Law of Ukraine "About forensic examination" No. 4038-XII. (1994, February). Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12

Список використаних джерел

[1] Експертизи у судовій практиці : бюлетень / Т.М. Арсенюк, Ю.М. Беляк, В.І. Бояров та ін. ; за заг. ред. В.Г. Гончаренка. Київ: Юрінком Інтер, 2005. 480 с.
[2] Експертизи в судочинстві України : наук.-практ. посіб. / С.Б. Бойченко, В.І. Бояров, Т.В. Будко та ін. Київ : Юрінком Інтер, 2015. 504 с.
[3] Борисова Л.В., Біленчук П.Д., Малій М.І. Експертиза як засіб установлення фактів і обставин вчинення транснаціональних комп'ютерних злочинів. *Криміналістика і судова експертиза*. 2020. № 65. С. 230–239.
[4] Дуфенюк О.М. Забезпечення судово-експертної діяльності у кримінальному провадженні: системна парадигма. *Вісник Львівського торговельно-економічного університету*. 2019. № 8. С. 163–173.
[5] Клюєв О.М. Удосконалення експертного забезпечення правосуддя: теоретичні, правові та організаційні аспекти. Теорія та практика судової експертизи і криміналістики. 2019. № 19. С. 102–117.
[6] Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

[7] Марчук А.І. Судова медицина: курс лекцій. Київ: Генеза, 1997. 143 с.
[8] Судова медицина : підручник / В.Д. Мішалов, Т.В. Хохолєва, В.Т. Бачинський та ін. Чернівці: Місто, 2018. 575 с.
[9] Інструкція про проведення судово-медичної експертизи: наказ Міністерства охорони здоров'я України від 17 січня 1995 р. № 6. URL: https://zakon.rada.gov.ua/laws/show/z0254-95.
[10] Інструкція про призначення та проведення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 8 жовтня 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0001-13#Text.
[11] Оприлюднення публічної інформації. Національна поліція. URL: https://www.npu.gov.ua/activity/zviti/oprilyudnennya-publichnoji-informacziji.html.
[12] Реєстр методик проведення судових експертиз. Міністерство юстиції України. URL: http://rmpse.minjust.gov.ua.
[13] 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.
[14] Яковлєв О.В. Роль прокурора – процесуального керівника досудовим розслідуванням у призначенні судової експертизи та оцінці її результатів. *Криміналістика і судова експертиза*. 2019. № 64. С. 350–360.
[15] Про судову експертизу: Закон України від 25 лютого 1994 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12.

Сучасні можливості судових експертиз у розслідуванні несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Богдан Вікторович Черняховський

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

Анотація
Метою дослідження є висвітлення можливостей використання судових експертиз у кримінальних провадженнях щодо несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. У статті застосовано емпіричні й теоретичні методи дослідження. Серед емпіричних методів використано опитування працівників оперативних підрозділів кіберполіції та судових експертів системи Міністерства внутрішніх справ, аналіз даних відкритої частини Єдиного державного реєстру судових рішень. З-поміж теоретичних методів застосовано аналіз і синтез, аналогію, порівняння, узагальнення. Запропоновано методологію дослідження слідової картини злочину, передбаченого ст. 361 Кримінального кодексу України, з використанням можливостей судово-експертних досліджень різних видів для фіксації та дослідження фізичних слідів злочину, а також призначення саме комплексної судової експертизи комп'ютерної техніки, програмного забезпечення, телекомунікаційних систем та їх засобів. Обґрунтовано необхідність удосконалення нормативних актів відповідно до методики дослідження комп'ютерної техніки та програмних продуктів. 1. Результати судово-експертних досліджень є ключовим елементом доказової бази сторони обвинувачення в кримінальних провадженнях щодо несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. 2. Застосування спеціальних знань у досудовому розслідуванні кіберзлочинів є невід'ємною складовою для досягнення завдань кримінального провадження. 3. Нормативно-правове забезпечення судово-експертної діяльності для забезпечення потреб досудового розслідування потребує вдосконалення на підставі сучасних провідних методик проведення експертних досліджень

Ключові слова:
комп'ютер; автоматизована система; комп'ютерна мережа; мережа електрозв'язку; несанкціоноване втручання в роботу комп'ютерів; кіберзлочини; судова експертиза