ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.39 | *Nº 70*

2021

Cuestiones Políticas Vol. 39, Nº 70 (2021), 674-695
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Detection and Extraction of Electronic Information During Investigative (Search) Actions Under Ukrainian Legislation

DOI: https://doi.org/10.46398/cuestpol.3970.40

Oksana Khablo *
Dmytro Pysmenniy **
Oleksandr Halahan ***
Mykhailo Nykonenko ****
Olha Kubareva *****

Abstract

The article provides a comprehensive study of the features of detection and seizure of electronic information during investigative (search) actions under the laws of Ukraine. The methodological basis of the scientific article is the complex application of general scientific and special methods of scientific knowledge in their relationship, selected considering the purpose and objectives of the study, its object and subject. It is noted that the following information, which is contained in the form of electronic-digital mappings, can be obtained during investigative (search) actions, covert investigative (search) actions, as well as during temporary access to things and documents as a measure of criminal proceedings. It is established that the process of reviewing electronic documents in general corresponds to the generally accepted algorithm of actions: search and detection of documents; visual inspection of the external state without changing the conditions of perception; fixation; detection of handprints; detection of traces of changes in the original content; preparation for packaging; packaging. It is substantiated that the involvement of a computer technician in the investigation, search, other

* Candidate of legal sciences, Associate Professor, Professor at the Department of Criminal Procedure, National Academy of Internal Affairs, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-3923-275X. Email: hokana@ukr.net

** Candidate of legal sciences, Professor, Professor at the Department of Criminal Procedure, National Academy of Internal Affairs, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-7059-3935. Email: Krum.proces@ukr.net

*** Candidate of legal sciences, Associate Professor, Professor at the Department of Criminal Procedure, National Academy of Internal Affairs, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0001-5105-0022. Email: law54@ukr.net

**** Candidate of legal sciences, Associate Professor, Professor at the Department of Criminal Procedure, National Academy of Internal Affairs, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-7657-8672. Email: mnikonenko@ukr.net

***** Candidate of legal sciences, Associate Professor at the Department of Criminal Procedure, National Academy of Internal Affairs, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-2573-898X. Email: kubarevao@ukr.net

Recibido el 03/06/2021 Aceptado el 22/08/2021

procedural actions, aimed at solving the problems of contextual information retrieval, detection of electronic document management programs, viewing the history of visits to Internet browsers.

Keywords: digital research; criminal proceedings; electronic information; tests; investigative actions (search).

Detección y extracción de información electrónica durante las acciones de investigación (búsqueda) bajo la legislación ucraniana

Resumen

El artículo proporciona un estudio exhaustivo de las características de detección e incautación de información electrónica durante las acciones de investigación de conformidad con las leyes de Ucrania. La base metodológica del artículo fue la combinación compleja de métodos científicos generales y métodos especiales de conocimiento científico en su relación, seleccionados teniendo en cuenta la finalidad y objetivo del estudio, su objeto y tema. Se observa que la siguiente información, que está contenida en forma de mapeos electrónico-digitales, se puede obtener durante acciones de investigación, acciones de investigación encubiertas, así como durante el acceso temporal a cosas y documentos como medida de procesos penales. Se establece que el proceso de revisión de documentos electrónicos en general corresponde al algoritmo de acciones generalmente aceptado: búsqueda y detección de documentos; inspección visual del estado externo sin cambiar las condiciones de percepción; fijación; detección de huellas de manos; detección de rastros de cambios en el contenido original; preparación para envasado; embalaje. Se concluye que la implicación de un técnico informático es importante en la investigación, búsqueda y otras actuaciones procesales, encaminadas a solucionar los problemas de recuperación de información contextual, detección de programas de gestión documental electrónica y visualización del historial de visitas.

Palabras clave: investigación digital; proceso penal; información electrónica; pruebas; acciones de investigación (allanamiento).

Introduction

The development and introduction of modern information technologies in all spheres of public life and economy in Ukraine makes it possible to use

them, in particular, for selfish and other reasons. Information technology also provides new opportunities for criminal activity, the computer «provides» both new types of crimes and new ways of committing the usual illegal acts. Combating crimes committed with the use of information technology is a new challenge for law enforcement (Bolhov *et al.*, 2015). The use of telecommunications networks makes it possible to commit a crime without leaving home, office, without leaving the borders of their country, or simultaneously from the territory of several states. There is no form of control over information that opens unlimited opportunities for access to and use by criminals. This determines the transnational, organized, group nature of many cybercrimes (Husarov, 2013).

It should be noted the international importance of cybercrime, the level of which is directly dependent on the level of development and implementation of modern information technology. There is a consolidation of IT criminals into groups with their subsequent consolidation into criminal groups, criminal organizations that operate on a permanent basis - «professional cybercrime». There is also a rapid establishment and strengthening of links between criminal groups, which allows for the rapid exchange of information, the exchange of techniques and methods of committing crimes, methods of transferring electronic funds in cash, etc. (Shapochka, 2014). However, not only crimes in the field of use of computers, systems and computer networks and telecommunication networks, but also many «traditional» socially dangerous acts leave behind electronic traces in computer networks, on magnetic or optical media, monitor screens. As a result, there is a practical problem with the use of these traces during the pre-trial investigation (Muradov, 2013).

The investigation of cybercrime is also complicated by certain features: latency; the possibility of destruction or alteration of computer information that is evidence of a crime; the occurrence of a problem during the inspection of computer systems, removal and examination of traces stored in the memory of technical devices, in the electromagnetic field, on computer media; short-term storage of information that can act as evidence on the servers of companies - operators of telecommunications networks, etc. (Burbelo, 2013). That is why the challenge of modernity, which faced forensic theory and practice, is the need to clarify the forensic and procedural features of detection and recording of electronic trace information during the investigation of criminal offenses under the laws of Ukraine.

1. Methodology of the study

The methodology of the article is based on general and special methods of scientific knowledge, the use of which is determined by the purpose, object,

and subject of research (Vasylevych, 2021). General scientific methods are presented in the work mainly by methods of formal and dialectical logic (analysis and synthesis, methods of induction and deduction, ascent from concrete to abstract and from abstract to concrete, system-structural method, and others).

The appeal to the dialectical method provided consideration of the requirements and methods of detecting and preserving this type of material evidence in criminal proceedings, such as electronic information, from the standpoint of the integrity of the phenomenon and the interconnectedness of its individual elements. The formal-logical method was used in defining the basic legal concepts and categories that make up the content of a scientific article, to interpret the concepts of «sources of evidence», «electronic evidence», «review», to identify major problems that arise when collecting and extracting electronic trace information. The system-structural method provided an opportunity to develop the structure of the procedural mechanism for detecting and retrieving electronic sources of evidence and to characterize the procedure for their storage by separating its elements.

The analysis of the norms of the current criminal procedural legislation and the practice of its application, the interpretation of the provisions of the relevant normative legal acts and materials of judicial practice was carried out using formal-dogmatic and hermeneutic methods. The method of theoretical and legal modeling allowed substantiating the proposals aimed at improving the procedural order of collection and procedural consolidation of electronic evidence in criminal proceedings. The article uses a methodological system built on the vertical principle, which includes the following levels: philosophical, general, special-scientific, specific-scientific. The normative and legal basis of the dissertation research is the Constitution of Ukraine, acts of national criminal procedural legislation.

2. Analysis of recent research

Various aspects of the selected issues in the criminal process are the subject of research in the works of scientists of the modern period, among which it is appropriate to note V.V. Bilous (2012), V.V. Biryukov (2007), V.M. Bolhov, N.M. Hadion, O.Z. Hladun (2015) A.G. Volevodz (2001), A.V. Kovalenko (2017), B.B. Teplitsky (2019), Yu.Yu. Orlov, S.S. Cherniavskyi (Cherniavskyi, 2017) and others.

Despite the significant number of scientific papers and increased interest in the problems of evidentiary law in criminal proceedings, many issues related to electronic evidence in the criminal process of Ukraine, both doctrinal and purely applied, remain controversial or partially resolved. In

addition, the vast majority of research is based on previous legislation. At the same time, the potential for the use of electronic traces in the activities of investigative bodies for the search and identification of persons, crime prevention, etc., remains unacceptably low (Bilous, 2012).

The purpose of the article is a comprehensive theoretical and applied study of certain criminal procedural and forensic features of detection and seizure of electronic information during investigative (search) actions under Ukrainian law, development of proposals and recommendations of organizational, tactical, and legislative nature aimed at improving the use of digital sources of evidence in criminal proceedings.

3. Results and discussion

The urgent and most important tasks of investigators and operatives are to search, record, remove and provide the expert intact material objects - computer information carriers, which acquire the status of objects of expert research, and the correct definition of forensic computer and technical tasks Expertise (Teplitskyi, 2019).

During the pre-trial investigation, both material traces (fingerprints, micro-objects, etc.) and electronic ones (visits to relevant sites, user correspondence archive, management of electronic payment systems accounts, geolocation, etc.) can be detected, which contribute to the formation of a full evidence base and expose not only its user, but also other persons involved in the commission of a criminal offense. Electronic media, if it meets the definition of "evidence" (Article 98 of the Criminal Procedure Code of Ukraine, for example, if it is a material object), may be obtained by the prosecution, seized, taken under control by the prosecution in a certain procedural order, inspected, photographed, described, copied, attached to criminal proceedings, returned to the owner, saved, lost or destroyed, etc. (Zakharko, 2019).

Evidence obtained in the course of an investigation must meet the requirements of reliability, appropriateness and admissibility. The specified requirements are put forward both to the form of the received information, and their maintenance. These requirements also apply to electronic evidence. In order to properly document information from digital sources, it is needed to take into account the functional features of the technologies with which they were created, stored, transmitted, and so on.

Consolidation of electronic evidence obtained as a result of the Criminal Procedure Code, investigative or covert investigative (search) actions is carried out in compliance with several requirements for form and content. The first group of requirements provides for the procedural design of

relevant protocols, the involvement, if necessary, of specialists and witnesses, taking measures to properly preserve digital media important for the criminal process. The second group of requirements is put forward to the content of information, its qualitative and quantitative component. In the latter case, special attention should be paid to the completeness of the information obtained, so that they can be further presented both in court and submitted for examination by an expert (Vinakov, 2017).

Working with electronic trace information is a complex procedure that often requires special knowledge, and its result will depend on how quickly and efficiently the capture, storage and retrieval of trace information contained in electronic information systems or their parts, mobile terminals of communication systems information and telecommunication systems or parts thereof. Such actions must be performed with some systematization, starting with the inspection of the scene, electronic equipment, sources of external memory and ending with the extraction of data from electronic storage of information relevant to criminal proceedings.

Electronic traces and their media must be removed, recorded, and executed in accordance with the requirements of current criminal procedure legislation. It is extremely important to find out the procedural order of detection, seizure and storage of such information, given the possibility of its use in criminal proceedings (Marinin, 2015). Therefore, during the pre-trial investigation, they must be provided unchanged to ensure the possibility of examination. To search for electronic information, you need to use methods and tools that do not modify the first extracted information on the source of external memory.

From the analysis of the content of Art. 93 of the Criminal Procedure Code of Ukraine, it follows those electronic reflections, as evidence, can be collected by conducting investigative (search) actions and covert investigative (search) actions, conducting other procedural actions. In particular, electronic reflections can be detected during a search, inspection, as well as during temporary access to things and documents as a measure to ensure criminal proceedings. For example, temporary access to electronic information systems or parts thereof, mobile terminals of communication systems is carried out by removing a copy of the information contained in such electronic information systems or their parts, mobile terminals of communication systems, without removing them. Thus Art. 159 of the Criminal Procedure Code of Ukraine it is established that such temporary access is possible only on the basis of the decision of the investigating judge. This norm can be interpreted as a means of ensuring the possibility of using copies of electronic reflections as sources of evidence in criminal proceedings.

In Part 2 of Art. 99 of the Criminal Procedure Code of Ukraine states that the materials, which recorded factual data on illegal actions of individuals

and groups of persons, can be collected by operational units in compliance with the Law of Ukraine «On operational and investigative activities» (Criminal Procedural Code Of Ukraine, 2012). These materials are mostly formed in the form of operational documents, as well as electronic displays (photographs, phonograms and videograms in modern digital format) and can be used in criminal proceedings as evidence, to be the objects of forensic computer science.

Trace information, which is contained in the form of electronic-digital mappings, can also be obtained during such covert investigative (search) actions as audio, video surveillance of a person, removal of information from transport telecommunications networks, removal of information from electronic information systems, location electronic means, surveillance of a person, thing or place, monitoring of bank accounts, audio, video surveillance of the place, control over the commission of a crime. In such cases, electronic-digital traces are issued as an appendix to the protocol of the relevant investigative (search) action (Criminal Procedural Code Of Ukraine, 2012).

Part 2 of Art. 93 of the Criminal Procedure Code of Ukraine contains an indication of another way of collecting electronic mappings: they may be required from public authorities, local governments, officials and individuals, enterprises, institutions, and organizations. Businesses that play a key role in ensuring the circulation of electronic images and have the technical capacity to store them are Internet service providers (ISPs) and mobile operators. Imperfect legal regulation of their relations with investigative bodies leads to numerous misunderstandings, unjustified seizures by investigators of network computer equipment from providers, which leads to violations of Internet users' rights and inadmissibility of evidence obtained by the court, as well as reluctance of (Cherniavskyi *et al.*, 2017).

Therefore, the issue of qualified collection of evidence in criminal proceedings committed with the use of electronic media (computer units, servers, laptops, mobile communications, memory cards, etc.) requires proper legislative regulation of the relevant procedural powers of the pre-trial authority's investigation.

Thus, one of the draft Laws of Ukraine "On Amendments to Certain Legislative Acts Concerning the Implementation of the Provisions of the Convention on Cybercrime and Improving the Effectiveness of the Fight against Cybercrime" proposed, inter alia, to amend the Criminal Procedure Code of Ukraine. authorities to carry out urgent storage of information, which will significantly increase the effectiveness of monitoring and prevention of viral attacks; opportunities in exceptional emergencies to provide temporary access to information held by telecommunications operators and providers, until the decision of the investigating judge, the

court; opportunities during the search to legally gain access to computer systems that are physically located outside the place of the search, to overcome logical protection systems, to obtain information about the peculiarities of the functioning of computer systems and the security measures applied to them; improving the procedure for conducting covert investigative (search) actions during the pre-trial investigation of crimes under Section XVI of the Criminal Code of Ukraine.

Any information transmitted through information and telecommunication systems is stored on special technical media (servers) and in a special form (log file). Internet service providers and other entities involved in the process of information and telecommunication data transfer and in the actual possession of the servers have the opportunity to extract the necessary log files, certify their content and provide them at the request of authorized participants in criminal proceedings. This method of gathering evidence, including electronic, is used in the investigation of criminal offenses by conducting appropriate covert investigative (investigative) actions.

Note that, in general, server owners are quite inactive in cooperating with law enforcement or ignoring requests, appealing against the lack of technical storage capacity. It should also be noted that modern messengers «WhatsApp» and «Viber» contain end-to-end encryption, which technically makes it impossible to decrypt correspondence for the company that owns the messenger, and all correspondence is under the control of users. It turns out that law enforcement agencies will not be able to obtain information about subscribers' correspondence in the traditional ways.

Vulnerability «of an electronic document necessitates the creation of special rules for recording electronic information, ways to store and attach them to the materials of criminal proceedings. In particular, at the level of traditional rules for handling documents, it is necessary to take into account the technical features of the collection, storage and use of information (Khyzhnyak, 2017).

During the search and inspection of the premises, local electronic reflections, which contain information relevant to criminal proceedings, may be detected: 1) in the searched (inspected) premises, on the ground: on an autonomous electronic medium (flash drive, autonomous electronic drive), on a specialized device (smartphone, digital camera, digital voice recorder, etc.) or on a memory device of a desktop computer (laptop); 2) on the Internet outside the searched (inspected) premises, terrain, namely on a remote server, the content of which is accessed from a computer located in the specified premises (Cherniavskyi *et al.*, 2017).

Any actions with electronic documents must be carried out in the manner prescribed by law by authorized persons using certified service equipment,

using licensed software. Use of uncertified hardware or unlicensed software may distort information obtained from an electronic document due to hardware and / or software failures and errors.

The process of reviewing electronic documents generally corresponds to the generally accepted algorithm of actions performed by the investigator during the review of ordinary documents. This set of actions should consist of the following: 1) search and detection of documents; 2) visual inspection of the external state without changing the conditions of perception; 3) fixation by photography; 4) fixation in the protocol of the corresponding investigative (search) action (all actions of officials, a condition of the document and the revealed traces are fixed); 5) detection of handprints (on a physical medium of an electronic document); 6) detection of traces of changes in the original content; 7) preparation for packaging; 8) packing (Biryukov, 2007).

In our opinion, the inspection of objects, including electronic media (computer units, servers, laptops, memory cards), should be carried out at the place of their detection, usually during the inspection, with the participation of a specialist. It is the investigator who draws up a report on their detection, which records their individual characteristics (Vinitsky, 2009). Its main tasks when detecting and removing documents on computer media are: 1) to properly remove computer media and peripherals (if any) and record it in the protocol; 2) properly package all elements of the hardware and software complex and media; 3) send them for expert examination in the laboratory; 4) ensure the integrity of information and prevent its destruction or damage at all stages of work with it (Osyka, 2005).

It should be emphasized that the specific objects of search depend on the type of crime under investigation, the method of its commission, as well as the properties of the document and, accordingly, search and seizure. For example, the objects of search in the investigation of illegal actions with bank payment cards will be: a) blanks, stolen or manufactured cards;

b) computer information carriers with card details, software for generating card numbers, hacking databases, copying and recording card numbers; c) equipment for making cards or making changes to them (embossing machines, thermal printers, laminating machines, etc.); d) scanners; e) digital cameras; e) material for making cards (plastic, foil, magnetic film); g) mobile phones; g) maps or diagrams of settlements with ATM locations marked on them; h) pieces of paper with inscriptions, which may be passwords and access codes to e-mail and other information resources, etc. (Osyka, 2005).

When applying such a measure to ensure criminal proceedings as temporary access to things and documents (163 of the Criminal Procedure Code of Ukraine), electronic media may be inspected and their contents

copied. Also, the investigating judge, the court in the decision to grant temporary access to things and documents may order the possibility of seizure of things and documents, if the party to the criminal proceedings proves sufficient grounds to believe that without such seizure there is a real threat of alteration or destruction of things or documents. or such seizure is necessary to achieve the purpose of gaining access to things and documents (paragraph 7 of Article 163 of the Criminal Procedure Code of Ukraine).

As a rule, if the electronic digital information is stored on servers or hard drives of enterprises, institutions, organizations, you should make a bitwise copy of the media, because the seizure of property of these legal entities can lead to negative consequences. Identical copy of electronic information on technical media must be reproduced using special equipment, after which the physical media themselves are returned to the owners. Subsequently, the copied trace information may be submitted for examination in the event of a forensic computer forensic examination in criminal proceedings. It is also worth noting that a similar algorithm of action should be followed in case of need for forensic computer examination.

Given the peculiarities of the physical form of information contained on electronic media, the procedural rules governing the peculiarities of the formation of evidence on the basis of such information should ensure its preservation throughout criminal proceedings, including in cases where electronic media for certain reasons remains with the rightful owners.

It should also be emphasized that the features of the review of electronic trace information depending on the physical characteristics of the media that contains it. Given the specifics of each of these media, the features of detection and storage of information they contain, as well as the subject of the study, we will limit them to:

- electronic documents placed on a physical storage medium (external physical storage media of a computer) (hard disk - HDD, SDD; disk media - CD, DVD, Blue-Ray-disks, floppy disks; USB-disks); storage device, random access memory of peripheral devices (for example, a printer in the memory of which are documents in the «print queue»), random access memory, etc. (Volevodz, 2001); flash memory cards (SD, micro SD, etc. (Kovalenko, 2017);
- electronic documents located in the memory of cellular means.
- publications contained on the Internet.
- electronic documents placed in «cloud» storage services.

Prior to the physical inspection of the computer, the investigator must install the technical devices and technologies used at the facility to protect the information. This is established both by interviewing the persons responsible for the security of the facility and by studying the technical

documentation for the protection of information at the facility. The following circumstances are clarified:

1. whether the room in which the computer is located is blocked by an electronic access system or burglar alarm, and what technical means are used for this purpose.
2. whether special means for destruction of information in case of attempt of unauthorized access to it are installed in the computer; find out the location of the organization that installed this system.
3. whether the password (additional device - electronic key) is necessary for access to the information which is in the computer, or its separate parts, rules of its use.
4. whether the computers are connected (included) to the local network of the institution, organization, enterprise (firm), association, what is the scheme of the local network, the basic rules of its safe use (Examination Of Computer Equipment And Software Products Or Computer Technical Examination, 2019)?

If the computer is connected to the Internet, it is necessary to withdraw contracts from the head of the enterprise (firm) where the inspection will be conducted, immediately contact the network administrator - provider of the node to which the institution is connected (enterprise, organization), and organize by means of its extraction and storage of the electronic information belonging to the given enterprise or received to its address. In this case, it is appropriate to quickly determine whether the owner stores all its data in external storage, and if so, the information on local machines may not be detected and it is necessary to find out access to external storage.

5. the persons responsible for the backup and storage of protocols shall find out the location of the relevant documents and copies on magnetic media and take measures to remove and store them (Examination Of Computer Equipment And Software Products Or Computer Technical Examination, 2019);

During the physical examination it is necessary: to order the employees of the firm (enterprise) to move away from the computer means and place them in the room so that the possibility of using any means of communication is excluded. In the process of inspection do not accept help from employees of the firm (enterprise); to remove from the staff pagers, electronic notebooks, laptops, individual devices for disabling the car alarm, etc.; capture information on the screens of working computers by taking photos (detailed shooting); turn off the power of the mini-subscriber telephone service and seal it (if any); Draw a diagram of the connection of external cables to computer devices and mark the cables for proper reconnection in the future; to isolate computers from any communication from the outside: modem, local computer network, radio communication; The most effective

way to disconnect all computer equipment from power sources (including uninterruptible power supplies) (Examination Of Computer Equipment And Software Products Or Computer Technical Examination, 2019).

The specialist promptly performs actions in accordance with the plan developed in conjunction with the investigator. The external inspection identifies specific circumstances related to the computer, the data of which are entered in the inspection report of the computer: the presence of the system unit, monitor, keyboard, printer, modem, uninterruptible power supply, speakers, etc., peripherals and multimedia devices.

According to the location of the parts of the devices on the front panel of the system unit, the specialist determines their types (storage devices, disk drives), as well as types of credit card readers, smart or chip cards, etc. Special attention should be paid to devices unknown to him. The location of the connectors on the back of the system unit determines the presence and types of built-in devices, network card, modem (whether it was connected to a telephone or other communication line), the presence of serial and parallel ports, whether they were connected to external communication lines (Examination Of Computer Equipment And Software Products Or Computer Technical Examination, 2019).

The protocol must provide a diagram of the connection of cables to the computer system. Disconnected cables must be marked to reconnect during the examination of computer hardware and software. The computer system unit, printer, detected floppy disks, magnetic tapes, and other computer storage media (such as printouts) are packaged and removed. Packaging of objects must prevent both accesses to objects and their damage during storage or transportation (Examination Of Computer Equipment And Software Products Or Computer Technical Examination, 2019).

Coordinated actions of the investigator and the specialist during the inspection and removal of material evidence from the scene will avoid irreversible loss of information contained on computer media.

Removal of electronic media from various sources of external memory during investigative (search) actions does not require the involvement of a specialist to examine and remove them. The Criminal Procedure Code of Ukraine does not require this either. However, it should be noted that in some cases, due to the peculiarities of the objects themselves, which are important in criminal proceedings, they can be found only by a specialist in a particular field. In the cases studied, it is best to use the help of a computer and software specialist.

In our opinion, such cases should include: copying information from electronic media to another electronic medium; establishing the presence of communication between computer equipment and telecommunication channels according to the schemes: «computer computer», «computer

server», etc.; the need to disconnect the local network from technical devices; the need to search the server itself, as it stores most of the computer information in its memory and manages the workstations of the local network.

The participation of a specialist in the seizure of electronic media and in investigative (search) actions, because of which such information is seized, will eliminate doubts about the authenticity of the evidence and is a guarantee of protection of the rights of participants in the process. It is fair to say that there is no such thing as a universal computer expert. It is possible to involve people with the following specialties as a computer expert: a) computer science and information technology; b) engineer for technical protection of information; c) computer engineering; d) systems engineering; e) software engineering; f) network technologies and system administration; g) computer systems analytics. Therefore, when going to the scene, it is important to find out what technology and what operating system you will have to deal with (Honcharenko, 2014).

Naturally, the growth of the level and intensity of the use of special knowledge leads to an increase in the requirements for the qualification of a specialist. Qualitative and full-fledged carrying out of investigative (search) actions with use of computer knowledge of the expert promotes establishment of specificity of the committed criminal offense, and also its timely detection, disclosure and investigation.

Therefore, when conducting an investigative inspection, search, and other procedural actions related to the seizure of various electronic media, investigators and other staff must carefully plan organizational and tactical actions, taking into account knowledge of the specifics of working with electronic media. First of all, you need to establish - this is the type of operating system. Not all computer systems are equally common, and there may be some problems. A Windows operating system specialist may not have the necessary knowledge to operate a machine with another operating system, such as UNIX, Linux, OS / 2, MacOS, and others. But, despite some difficulties, the specialist must determine whether he can personally work with this operating system or should involve another specialist in this field. In the latter case, actions with the equipment of the persons involved must be carefully recorded (Honcharenko, 2014).

Given the importance of forensic computer and technical examination of objects provided for research, we consider it appropriate to focus on the technical features of the extraction and storage of electronic trace information found during the investigative (search) actions.

There are two ways to obtain electronic trace information: 1) seizure of all detected means of computer and other equipment with further study of the information contained therein; 2) examination of all information

on electronic media directly during the inspection or search (if there are sufficient grounds). The latter option involves further copying of information of interest to criminal proceedings and (or) removal of magnetic media with such information.

Actions with electronic trace information have a certain algorithm. For example, when removing electronic equipment, you need to identify all possible sources of external memory both inside the electronic device and remotely connected via local area networks, using the capabilities of wireless information technology. There are cases when removing the system unit, operational staff did not take into account that the hard disk can be connected remotely with data transmission via radio, and sent for examination this unit without a hard disk drive, which was connected to the computer by radio and was in a car parked near the building (Kuvychkov, 2016).

The seizure of all computer equipment speeds up the investigation process, makes it possible to direct all efforts to search for other material traces related to the criminal offense (documents, technical means, etc.); reduces the psychological burden on citizens; does not require the involvement of a highly qualified specialist in the field of computer technology to directly participate in the search, as the competent seizure of computer equipment is quite accessible to a specialist «middle hand».

The undoubted advantages of this approach include the ability to further study in more detail, involving the necessary specialists, all the information available in computer memory. This virtually eliminates the possibility of omitting even professionally hidden information. However, on the other hand, in some cases there are purely technical difficulties in removing all computer equipment (integration into various networks, the possibility of losing information when disconnected, etc.) or such removal is simply impractical. It should also be borne in mind that the failure of computer banking systems and a number of enterprises can lead to a complete disruption of their work and significant material damage, which threatens their claims. Therefore, it is sometimes recommended to use another method: to extract information from computer equipment directly during the inspection or search. And here you cannot do without electronic copying of information using a laptop, flash drive, etc.

When conducting an investigative (search) operation related to the seizure of electronic media, the investigator must clearly know the specifics of the seizure and packaging of these objects to exclude any manipulation of the objects during their transportation. Therefore, at the preparatory stage of the investigative review, search, the investigator must take into account which electronic media will be the object of investigative (search) action. After all, during the inspection, the procedural person may encounter a personal computer, system units, cellular communications equipment,

video recorders and other computer equipment, as well as other objects, such as hard drives disguised as other objects, a non-standard form of flash drives with a USB input in the form of toys, jewelry, keychain.

Detection, fixation, removal, preservation, and research of any object are aimed at careful conduct of each stage. As practice shows, there are many cases of violation or poor performance of one of these stages of work with objects. This is usually the removal and storage of trace information, the completeness and quality of which is ensured by the packaging of the detected objects. The result of expert research depends on how correctly and competently the detected information carrier will be packed (Zinnurov, 2018).

When packed in a cardboard box, the areas that have access to the internal contents are pasted. In the absence of packages or boxes, the system units may be covered with sheets of paper to prevent access to the on / off / reset buttons, power connectors, and screws that secure the side and top walls to the chassis. In practice, forensic inspectors are faced with non-compliance with the rules of packaging system units: as a rule, it is a sheet of paper with the inscription, glued with transparent adhesive tape «tape» to the top cover. Such packaging does not meet the requirements of regulations and provides free access to all connectors and on / off / reset buttons.

The main requirement for the packaging of electronic media is to exclude access to information on the media and the possibility of making changes to the contents of the memory of the media after its removal. Thus, when a mobile phone is detected, experts recommend removing the object together with the network cable of the phone, packing it in cardboard boxes, using appropriate software and hardware to exclude any manipulation of the phone, namely, intentional, or unintentional turning on / off the phone change information in the memory of mobile devices (Zinnurov, 2018).

After a thorough inspection of computer equipment, a description of the software and hardware components of computers is made. The following software products can be used to describe computers: AIDA64, Everest. It is also possible to use the built-in utility «system information», for which in the program window «run» (start is performed by pressing the key win + r) type msinfo32 and press the Enter button. Information about the hardware and software components of computers is recorded in the inspection report of computer equipment and certified by two witnesses. It is advisable to keep the computer description document with the removed equipment. The case must be sealed. The seal is certified by the person initiating the seizure and the signatures of witnesses. Seal at the junction of the main body of the computer and the side removable covers. You must also seal the front of the computer (Zakharko, 2019).

The magnetic media on which the information is to be copied must be prepared (make sure that there is no information on it). Media should be stored in special packaging or wrapped in clean paper (do not use ordinary plastic bags). Keep in mind that information can be corrupted by humidity, temperature, or electrostatic (magnetic) fields (Zakharko, 2019).

Care should be taken when transporting computer equipment, as information on the hard disk may be damaged during transportation. Transport and special packaging should be prepared for the transportation of large computer systems. When removing and transporting computers, do not place them on top of each other or place any other objects on them. In addition, in the course of procedural actions, the objects of which are computer equipment, system units of personal computers, the investigator must clarify with the rightful owner, whether there is password protection on the media, if so, indicate it in the inspection report (search) and put this information in the packaging of the object, as the lack of this information will increase the duration of the expert study. It has specific features and packaging of these objects. The safest way is to pack the items in a plastic bag or box. The neck of the package is sewn with thread, the thread node is pasted with a tag with an explanatory inscription (Zinnurov, 2018).

DVRs as electronic media should be removed completely, without removing the hard disk drive due to the peculiarities of video recording. If you have to remove the storage device without a video recorder, then in this case it is necessary to display in the explanatory labels on the package the full name of the video recorder with markings.

When removing stationary DVRs, you should not remove the storage device from them, as DVRs use their file system to record and store video information. In addition, the drive removed from the DVR and then reinstalled may be reinitialized by the DVR and data may be lost. You also need to remove the power supplies of the DVRs.

When removing the server, you must completely remove the system unit, as the drives in the server can be combined in a RAID array of different configurations. The RAID settings are in most cases stored in the memory of the RAID controller, which is located inside the system unit. Extraction of some drives will lead to the fact that the expert will not know the configuration of the RAID-array and the study of information will be impossible or extremely difficult (Periakina, 2019).

When removing the cellular device, pay attention to its condition. If the phone is switched on, the best way to isolate it is to activate «offline mode» or «airplane» mode. Turning off the phone may activate security features (such as the SIM card PIN and / or security codes) that will be needed to access the device, making it impossible to perform an examination. If you have activated security features (for example, a «graphic key»), you should

immediately ask the phone owner about the unlocking algorithm. You should pay attention to the date and time indicated on the phone screen if it is turned on and compare them with the current time and date at the time of inspection, fixing discrepancies.

When extracting data from mobile applications, specialized software must be used as a source of electronic evidence. Examples of such applications are EnCase, Smartphone Examiner, MOBILedit, Forensic, Mobile Phone Examiner Plus and others. These tools are designed for law enforcement and information security professionals to collect evidence from mobile devices, they allow you to physically retrieve logical data from devices, get an image of the operating system, including the file system. After the analysis of mobile devices, it is possible to transfer the collected information to a specialized program FTK (Forensic Toolkit) for further study, for example, to recover deleted files. This integration also allows you to correlate the evidence collected on mobile devices with the evidence collected on computers (Sergeev, 2016).

The procedure for extracting evidence from mobile devices differs from the extraction of information from personal computers in that mobile electronic devices, compared to personal computers, have narrower tasks, excellent processor architecture, operating system, etc. In this regard, the methods and features of procedural actions must be individual, depending on the technical characteristics of the source of evidence (Sammons, 2015).

The British Association of Police Chiefs has developed guidelines for removing evidence from mobile devices (GOOD PRACTICE AND ADVICE GUIDE FOR MANAGERS OF E-CRIME INVESTIGATION, 2011). According to the proposed recommendations, during the procedural actions it is necessary to isolate the device from the mobile connection by turning off the device or thanks to special devices that muffle the connection, all the necessary procedures should be performed in a specially equipped room. The device must be fully charged in order to prevent the loss of information during procedural actions. You should take into account the feature of RAM (RAM) of the device, which requires uninterruptible power supply to store data, as opposed to non-volatile (ROM) memory. In order to preserve important information, the specialist must strictly follow the rules, do not allow software updates, as this may lead to data destruction. Along with the data of the applications on the mobile device, you must also request information stored on the servers of the application developers and the data of the Internet provider (Sergeev, 2016).

Modern smartphones, especially iPhones, often sync with a computer or laptop. Accordingly, it would be advisable to seize the owner of the smartphone computer or laptop. An alternative to removing your computer or laptop may be to check for Apple software on that device. Do not remove memory cards, SIM cards, or other hardware in your phone. The

packaging of a remote computer or storage device must, above all, ensure information integrity, i.e., exclude the possibility of connecting power cables or peripherals. The best option for packaging is to place the removed computer in its entirety in a plastic bag.

When describing computer devices that are seized and inspected, the information should be provided to the extent that will allow unambiguous identification of the seized device. In most cases, it is enough to specify the make, model, individual serial number of the device. If for some reason the mentioned information is not available, other individual features should be indicated: size, color, shape, etc. It is desirable to carry out the fixation not only procedurally, reflecting the seizure of electronic media in the protocol of the investigative (search) action, but also forensic, photographing the object of seizure (Periakina, 2019).

Conclusions

Thus, it should be summarized that electronic documents are an important source of evidence and guidance in criminal proceedings. Depending on whether such documents are placed on physical media, in the public domain on the Internet, or in cloud storage services, a specific procedure of their investigative review and preliminary investigation should be followed for further use in criminal proceedings, in particular in court proceedings. computer technical examination.

The following information, which is contained in the form of electronic-digital mappings, can be obtained during such investigative (search) actions as inspection and search, during temporary access to things and documents as a measure of criminal proceedings, as well as such covert investigators (search) actions: audio, video control of the person, removal of information from transport telecommunication networks, removal of information from electronic information systems, establishment of location of electronic means, supervision of the person, thing or place, monitoring of bank accounts, audio, video control of the place, control over commission crime.

In such cases, electronic-digital traces are issued as an appendix to the protocol of the relevant investigative (search) action.

The process of reviewing electronic documents generally corresponds to the generally accepted algorithm of actions: search and detection of documents; visual inspection of the external state without changing the conditions of perception; fixation by means of photography; fixation in the protocol of the corresponding investigative (search) action (all actions of officials, a condition of the document and the revealed traces are fixed);

detection of handprints (on a physical medium of an electronic document); detection of traces of changes in the original content; preparation for packaging; packaging. During the search and inspection of the premises, local electronic reflections, which contain information relevant to criminal proceedings, may be detected: in the searched (inspected) premises, on the ground (on an autonomous electronic medium, on a specialized device or on a memory device desktop computer); on the Internet outside the searched (inspected) room, area, namely on a remote server, the content of which is accessed from a computer located in the specified room.

Involvement in the investigation, search, other procedural actions, a specialist in the field of computer technology, who has knowledge of how to detect and extract relevant electronic-digital trace information, aimed at solving problems of contextual information retrieval, electronic document management programs, view the history of visits to Internet browsers (browsers), etc. In his activity, the specialist can use such tools as analysis of registry files, service files of applications, virtualization systems and complexes of recovery and analysis of remote data, the use of software and hardware, and so on. The use of this tool, although it requires much more time, it certainly has a positive effect on the effectiveness of detecting forensic information.

All actions with electronic documents must be carried out in the manner prescribed by law by authorized persons with the help of certified office equipment, using licensed software. When describing the computer tools that are seized and inspected, the information should be provided to the extent that will allow unambiguous identification of the seized tool. It is necessary to indicate such individual features as: size, color, shape, etc. Fixation should be carried out not only procedurally, reflecting the seizure of electronic media in the protocol of the investigative (search) action, but also forensic, photographing the object of seizure.

Bibliographic references

BOLHOV, Valentin; HADION, Natalia; HLADUN, Oleksandr. 2015. Organizational and legal support of counteraction to criminal offenses committed with the use of information technology: a scientific and practical manualNational Academy of the Prosecutor's Office of Ukraine. Kyiv, Ukraine.

HUSAROV, Serhii. 2013. "Investigation of cybercrime by the bodies of internal affairs of Ukraine: scientific and personnel support" In: Current issues of cybercrime investigation: materials of the international scientific-practical conference, Kharkiv, December 10, 2013. Kharkiv National University of Internal Affairs, pp. 14-18. Kharkiv, Ukraine.

SHAPOCHKA, Serhii. 2014. "On the issue of combating fraud, which is committed using the capabilities of the Internet" In: Legal Informatics. Ukraine. Vol. 3, No. 43, pp. 89-95.

MURADOV, Valentin. 2013. "Electronic evidence: forensic aspect of use" In: Comparative and analytical law. Ukraine. No. 3-2, pp. 313-315.

BURBELO, Bohdan. 2013. "Forensic bases of counteraction to cybercrime" In: Actual questions of investigation of cybercrimes: materials of the international scientific and practical conference, Kharkiv, December 10, 2013. Kharkiv National University of Internal Affairs, pp. 179-182. Kharkiv, Ukraine.

BILOUS, Vasyl. 2012. "Electronic traces as an actual direction of forensic research" In: Legal life of modern Ukraine: materials of the international scientific conference, Odessa, Vol. 2, pp. 425-427.

TEPLITSKYI, Bohdan, 2019. Tasks, objects and issues of computer-technical forensic examination. In: Legal Journal of the National Academy of Internal Affairs. No. 18, pp. 24-32.

ZAKHARKO, Andrii; HARKUSHA, Alina; ROHALSKA, Viktoria; KRASNOBRYZHYI, Ihor; BRIAHIN, Oleh. 2019. The use of electronic media with media content as sources of evidence: guidelines. Dnipropetrovsk. State un.-tvnutr cases. Dnipro, Ukraine.

VINAKOV, Andrii; MANZHAI, Oleksandr; 2017. Some issues of recording electronic evidence. In: Topical issues of combating cybercrime and human trafficking. Kharkiv, Ukraine.

MARININ, Serhei. 2015. Legal and organizational-tactical foundations for identifying, documenting and solving crimes committed in the field of illegal gambling business using computer technology and the Internet: monograph. AT the Ministry of Internal Affairs of Russia. Novgorod, Russia.

CRIMINAL PROCEDURAL CODE OF UKRAINE: LAW OF UKRAINE. 2012. № 4651-VI. Available online. In: http://zakon.rada.gov.ua/laws/show/4651-17#n384. Consultation date: 10/03/2021.

CHERNIAVSKYI, Sergey; ORLOV, Yuri. 2017. "Electronic reflection as a source of evidence in criminal proceedings" In: Bulletin of criminal proceedings. No. 2, pp. 112-124.

KHYZHNYAK, Evhen. 2017. "Peculiarities of review of electronic documents during the investigation of criminal offenses" In: Series: Law. Vol. 4, No. 58, pp. 80-85.

BIRYUKOV, Volodymyr. 2007. Forensic document science. Palivoda AV Ukraine. Kyiv, Ukraine.

VINITSKY, Lev; MELNIK, Svetlana. 2009. Expert initiative in criminal proceedings. Exam. Moscow, Russia.

OSYKA, Ihor. 2005. "The concept of the method of forgery of documents used in committing crimes in the field of entrepreneurship" In: Law and Security. T. 4. No. 6, pp. 92-94.

VOLEVODZ, Aleksandr. 2001. Countering Computer Crimes: Legal Foundations of International Cooperation. LLC "Yurlitinform". Moscow, Russia.

KOVALENKO, Artem 2017. "Peculiarities of electronic document review tactics during the pre-trial investigation of encroachments on the life and health of a journalist" In: Bulletin of the National Academy of Legal Sciences of Ukraine. Vol. 1, No. 88, pp. 182-191.

EXAMINATION OF COMPUTER EQUIPMENT AND SOFTWARE PRODUCTS OR COMPUTER TECHNICAL EXAMINATION. 2019. Available online. In: http://centrservis.com.ua/ekspertiza-komp-yuternoyi-tehniki-i-programnih-produktiv-abo-komp-yuterno-tehnichna-ekspertiza. Consultation date: 10/03/2021.

HONCHARENKO, Vladlen; HORA, Irina. 2014. Expertises in the judicial process of Ukraine: scientific and practical manual. Yurinkom Inter. Kyiv, Ukraine.

KUVYCHKOV, Serhei. 2016. "On modern problems of forensic computer examinations during the preliminary investigation" In: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. Vol. 2, No. 34, pp. 293-298.

ZINNUROV, Foat; KHAIYRULLOVA, Elvira. 2018. "Features of working with electronic media as sources of evidence during investigative actions" In: Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. T. 9. No. 2, pp. 274–278.

PERIAKINA, Marina; UNZHAKOVA, Svetlana; SHYSHKINA, Natalia. 2019. Procedural and forensic aspects of the seizure of electronic media in the light of protecting the rights of participants in criminal proceedings. In: Siberian Legal Bulletin. No. 3/861-2019, pp. 81-85.

SERGEEV, Mihail. 2016. "Criteria for proving electronic crimes when using mobile applications. Features of their withdrawal" In: Actual problems of economics and law. T. 10. No.2, pp. 264-272.

SAMMONS, John; BRUNTY, Josh 2015. "Mobile device forensics: threats, challenges and future trends" In: Digital Forensics: Threatscape and Best Practices. Syngress, Waltham. P. 69.

GOOD PRACTICE AND ADVICE GUIDE FOR MANAGERS OF E-CRIME INVESTIGATION, 2011. Available online. In: http://www.acpo.police.uk/documents/ crime /2011/201103CRIECI14.pdf. Consultation date: 10/07/2021.

VASYLEVYCH, Vitalii; MOZOL Stanislav; POKLONSKYI, Andrii; POKLONSKA, Olena; ZELENIAK Polina. 2021. "Regulatory framework for the fight against corruption in the National Police of Ukrain" In: CUESTIONES POLÍTICAS. Vol. 39, No. 68, pp. 682-695.

CHERNIAVSKYI, Serhii; BABANINA, Viktoria; MYKYTCHYK, Oleksandr; MOSTEPANIUK, Liudmyla. 2021. "Measures to combat cybercrime: analysis of international and Ukrainian experience" In: CUESTIONES POLÍTICAS. Vol. 39, No. 69, pp. 115-132.

UNIVERSIDAD DEL ZULIA

CUESTIONES POLÍTICAS

Vol.39 Nº 70

Esta revista fue editada en formato digital y publicada en octubre de 2021, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org