UDC 343.140.02:004.77
DOI: 10.56215/04221204.28

Identification, collection, and investigation of electronic imagery as sources of evidence

Valerii Khakhanovskyi*
Full Doctor in Law, Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0001-5676-5641

Marharyta Hrebenkova
Adjunct
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0003-2184-8679

Abstract
Given the rapid pace of informatization of society, the number of criminal offences involving the use of computers, their software, as well as telecommunications systems is continuously growing. Such illegal actions are characterized by leaving traces, including electronic imagery. They can be evidence of the commission of criminal offences, which explains the development and improvement of methods for their detection, collection, and investigation by law enforcement agencies. However, today such methods of detecting, collecting, and investigating electronic imagery of evidence are separately contained in several scientific papers of Ukrainian and foreign scientists, which allowed comprehensively covering them in this study. The purpose of this study was to review the theory and practice of the activities of authorized entities for the detection, collection, and investigation of electronic imagery of evidence. The study uses a set of various methods, namely scientific cognition of real phenomena and their connections with the practical activities of authorized bodies for the detection, collection, and investigation of electronic imagery (dialectical method), as well as special and general scientific methods of legal science. The study showed as follows: usually, investigators and operational officers detect electronic imagery independently, or as part of an investigative task force during the investigation of criminal offences, or before their commission; the collection of electronic imagery occurs during procedural actions (usually law enforcement intelligence actions) both from technical devices with which a criminal offence was committed, and from those that were attacked. When extracting electronic imagery, it is advisable to involve a suitable specialist (if possible, a cyberpolice officer); an authorized investigator, specialist, and expert are authorized to examine electronic imagery. Expert research of electronic imagery belongs only to experts and is carried out using the following examinations: computer equipment and software products, telecommunications systems and tools, as well as technical and forensic examination of documents. The conducted review will help authorized practitioners restore the memory of knowledge about information about the tools for detecting, collecting, and investigating electronic imagery, which will ensure the effective implementation of the tasks of criminal proceedings

Keywords:
law enforcement intelligence actions; investigator; digital evidence; electronic document

Article's History:
Received: 22.08.2022
Revised: 18.10.2022
Accepted: 16.12.2022

Suggest Citation:
Khakhanovskyi, V., & Hrebenkova, M. (2022). Identification, collection, and investigation of electronic imagery as sources of evidence. *Law Journal of the National Academy of Internal Affairs*, 12(4), 28-39.

*Corresponding author

Introduction

Since the beginning of the 21st century, there has been a continuous development of information technologies. This is primarily explained by rapid progress, which is manifested in an increase in the functionality of their actions and the number of tasks they solve. Informatization has not spared the criminal world. Offenders are increasingly committing criminal offences, using information technologies as a means of committing and concealing such criminal offences. That is why law enforcement agencies should always be prepared for such actions of criminals and ensure a quick, complete, and impartial investigation of such facts.

In this regard, law enforcement agencies are increasingly faced with electronic imagery in their practical activities, which obliges them to collect and examine such factual data to form a high-quality evidence base.

In an effort to counteract cybercrime and collect digital evidence of criminal actions, these bodies introduce appropriate tools for analysing digital evidence into their law enforcement infrastructure, as well as use all the possibilities of computer forensic expertise (Belshaw & Nodeland, 2022). However, as practice shows, not all law enforcement officers who work with electronic imagery use advanced both Ukrainian and international practices, which led to the conduct of this study.

Today, there is no unified approach to the name of evidence that is available in electronic (digital) form. They are called "virtual traces", "electronic evidence", "electronic traces", "computer evidence", "digital evidence", "digital (electronic) evidence", "electronic imagery", etc. Earlier studies proved that the statement of scientists regarding the name "electronic imagery" is now quite well-founded, which is supported (Grebenkova, 2021). Electronic imagery is a system of information and/or computer instructions in an information network or technical medium that can be evidence of a fact or circumstances established during an investigation (Orlov & Chernyavskyi, 2017). Thus, this paper refers to the subject under study using the term specified above, and when referring to the scientific achievements of other scientists, this paper will use their concept, implying the term "electronic imagery" with certain features.

Considering the scientific studies of Ukrainian scientists, one can point out a certain intensification of scientific research aimed at solving certain issues of collecting and investigating electronic imagery. Among them, the following theses can be distinguished: A. Ratnova (2021), A. Skrypnyk (2021), Yu. Kohut (2021). However, a comprehensive review of the detection, collection, and investigation of electronic imagery as sources of evidence, using international practices, has not yet been carried out.

If one pays attention to the global scale of the subject under study, one can observe certain progress in the development of methods of detection, collection, and investigation of electronic imagery in the criminal procedural activities of certain countries (the United States of America, the Kingdom of Norway, Great Britain, the United Arab Emirates, etc.). First of all, this is explained by the fact that such states were among the first in the world to introduce electronic technologies in the activities of their state institutions. However, as determined by scientists from Australia (McCord *et al*., 2022), the Kingdom of the Netherlands (Stoykova *et al*., 2022), the Kingdom of Norway (Stoykova *et al*., 2022), the Republic of Estonia (Aksamitowska, 2021), the United States of America (Belshaw & Nodeland, 2022), (Holt & Dolliver, 2021), (Holt *et al*., 2020), Great Britain (Tun *et al*., 2020), Austria (Forgó *et al*., 2017), the Federal Republic of Germany (Hawellek *et al*., 2017), the Republic of Ecuador (Granja & Rafael, 2017), the Republic of Peru and other countries, such studies are not sufficient. Until now, it has not been fully clarified to what extent law enforcement agencies use the methodology and tools of digital criminalistics, how they implement recommendations and standards of digital forensic expertise, and how they receive, investigate, and analyse digital data sources (Stoykova *et al*., 2022). Cyberattacks on electronic media leave certain artefacts in the target device's storage that can detect a cybercriminal and its behaviour if handled and analysed correctly. Law enforcement agencies of the world use several digital forensic tools, both commercial and open source, to achieve digital evidence (Javed *et al*, 2022).

In 2012, the Joint Technical Committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) developed the international standard ISO/IEC 27037:2012[1]. This standard provides recommendations for particular actions in working with digital evidence, which include identifying, collecting, extracting, and storing potential digital evidence that may have evidentiary value[2]. Such processes are necessary during a pre-trial investigation to ensure the admissibility and relevance of electronic imagery during court proceedings. After the publication of this international standard, the order of the State Enterprise "Ukrainian Research and Training Center for Standardization, Certification and Quality Assurance" (SE "UkrRTC") No. 400 was adopted[3]. Thanks to the latter, on January 1, 2019, the

[1]ISO/IEC 27037:2017. (2019). Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved from http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978

[2]Ibidem, 2019.

[3]Order of the State Enterprise "Ukrainian Research and Training Center for Standardization, Certification and Quality Assurance" No. 400. "On the adoption of national regulatory documents harmonized with European and international regulatory documents, cancellation of national regulatory documents, changes to national regulatory documents". (2017, December). Retrieved from http://www.leonorm.com.ua/P/NL_DOC/2017/Nak_400.htm.

state standard DSTU ISO/IEC 27037:2017[1] entered into force in Ukraine. The adoption of such standards indicates that the state aims to counteract cybercrime and those offences that are directly or indirectly related to the use of information technologies.

Considering the relevant international practice and the above-mentioned international and state standards for working with electronic imagery, it is advisable, according to the authors, to highlight modern methods of detecting, collecting, and investigating electronic imagery during the pre-trial investigation of criminal offences. Such a review will help familiarize authorized practitioners with a set of modern tools for detecting, collecting, and investigating electronic imagery, which in turn will effectively ensure a quick and complete investigation of criminal proceedings.

The purpose of this study was to review the theory and practice of the activities of authorized subjects for the detection, collection, and investigation of electronic imagery of evidence.

The objectives of this study are as follows: to analyse the scientific studies of scientists and the results of a survey conducted by investigators of the National Police of Ukraine on this subject.

Materials and Methods

Considering the purpose of the study, the specifics of the object and subject of the study, the relevant methodological framework was chosen. It was based on the method of scientific cognition of real phenomena and their connections with the professional activities of authorized subjects (pre-trial investigation and inquiry bodies), specialists and experts, as well as special and general scientific methods of legal science. Among the general scientific methods, the following methods were used: analysis (in the part of cognition of the following phenomena: detection, collection, and investigation of electronic imagery by law enforcement agencies, specialists, and experts), deductions (identification of common law enforcement intelligence actions during which electronic imagery is detected and collected), interpretation (of the above-mentioned international and state standards ISO/IEC 27037:2012[2] and the state standard of DSTU ISO/IEC 27037:2017[3], classification (identification of information carriers on which electronic imagery can be extracted). The system-structural method was also used, which allowed comprehensively analysing the provisions of the following regulations: the Criminal Procedural Code of Ukraine (the CPCU) dated April 13, 2012[4], the Law of Ukraine "On Forensic Examination" dated February 25, 1994 (Law No. 4038 -XII)[5], Order of the Ministry of Internal Affairs of Ukraine No. 575 dated 07.07.2017 (Order of MIAU No. 575)[6], Order of the Ministry of Justice of Ukraine No. 53/5 dated October 8, 1998 (Order of MJU No. 53/5)[7], as well as the practice of their application.

Apart from the general scientific methods, special methods were also used, namely comparative legal (determination of subtypes of examination of computer equipment and software products, their similarity and difference among different opinions of scientists).

The results of the latest fundamental research of Ukrainian and other scientists (Orlov & Cherniavskyi, 2017; Ratnova, 2021; Stoykova *et al*., 2021; Belshaw & Nodeland, 2022) from various countries (the United States of America, the Kingdom of Norway, the Islamic Republic of Pakistan, the Republic of India, Australia, Great Britain, the United Arab Emirates, the People's Republic of China) in the field of information technologies, cybersecurity, conducting examinations of computer equipment and software products, conducting law enforcement intelligence actions for collecting electronic imagery, etc. were used as the theoretical framework of the present study.

The empirical framework of the study is the results of a sociological survey of 113 investigators of the National Police of Ukraine (Kyiv, Lviv, Vinnytsia, Kirovohrad, Poltava regions), who were anonymously asked to answer several questions, specifically: "who most often detects electronic imagery during the investigation of a criminal offence, or before such investigation". Among the proposed answers were the following: a) citizens; b) employees of public and private enterprises, organizations, and institutions (11 people, which is 9.7%); c) investigators and operational workers (independently or as part of an investigative task force) – (79 people – 69.9%); d) police officers (23 people – 20.4%); e) other answers. It was also suggested to answer the question: "Do you have basic specialized knowledge in collecting and extracting electronic imagery (electronic evidence)?".

[1]ISO/IEC 27037:2017. (2019). Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved from http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978.
[2]Ibidem, 2019.
[3]Ibidem, 2019.
[4]Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.
[5]Law of Ukraine No. 4038-XII "Forensic Examination". (1994, February). Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12#Text.
[6]Order of the Ministry of Internal Affairs of Ukraine No. 575 "On the Approval of the Instructions on the Organization of the Interaction of Pre-Trial Investigation Bodies with Other Bodies and Units of the National Police of Ukraine in the Prevention of Criminal Offences, Their Detection and Investigation". (2007, July). Retrieved from https://zakon.rada.gov.ua/laws/show/z0937-17#Text.
[7]Order of the Ministry of Justice of Ukraine No. 53/5 "On the Approval of the Instructions on the Appointment and Conduct of Forensic Examinations and Expert Studies and Scientific and Methodological Recommendations on the Preparation and Appointment of Forensic Examinations and Expert Studies". (1998, October). Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

Results and Discussion

One cannot but agree with the statement of A. Amelina, S. Dementieva (2021) that "the use of information contained in electronic form on magnetic, optical, and other media in the evidentiary process is quite relevant today". This information can be used to determine the content of financial and economic activities carried out by business entities. This information can provide the understanding of the content of tax and accounting, the number of financial and economic operations, and methods of committing a criminal offence, etc.

According to Part 1 of Article 93 of the CPCU[1] "evidence is collected by the parties to the criminal proceedings, the victim, the representative of the legal entity in respect of which the proceedings are being conducted, in the manner prescribed by this regulation"[2].

The present paper specifically addresses the detection, collection, and investigation of electronic imagery by law enforcement agencies, i.e., the prosecuting party. Such authorized entities pursuant to Item 19 Part 1 of Article 3 of the CPCU[3] are the head of the pretrial investigation body, the investigator, the head of the inquiry body, the prosecutor, the interrogating officer[4].

According to Articles 36, 39, 40-1 of the CPCU[5], the specified entities are authorized to detect, collect, and investigate evidence, including electronic imagery. However, for the readability of a scientific article, as an authorized subject, the authors will indicate only the investigator.

Having surveyed 113 investigators of the National Police of Ukraine, the authors of this study found that electronic imagery is most often detected during the investigation of a criminal offence, or before such an investigation: by investigators and operational officers independently or as part of an investigative task force (69.9%), by other police officers (20.4%), by employees of public and private enterprises, organizations, and institutions (9.7%).

It is possible to detect electronic imagery during the investigation of any criminal offence or beforehand. At the same time, as practice shows, such evidence in most cases is found during the investigation of criminal offences in the sphere of official and professional activities; the use of electronic computers, systems, and computer networks and telecommunication networks; related to the provision of public services; entrepreneurial activities; as well as lately the circulation of narcotic drugs, psychotropic substances, their analogues, or precursors (Zelena, 2020). This indicates that electronic imagery in this category of criminal offences can be independent (main) sources of evidence, and not additional ones.

As the results of the survey indicate, quite often the investigator detects electronic imagery unassisted, or as part of an investigative task force (ITF). According to Item 1 Part 1 of the Order of MIAU No. 575[6], the investigator directs the actions of other ITF members and is responsible for the quality of the inspection of the crime scene; seizes things and documents relevant to criminal proceedings, and things that have been withdrawn from circulation, including material objects that are subject to proof, ensures their proper storage according to the established procedure for further dispatch for conducting an examination; together with other ITF members and other participants in criminal proceedings, records information about the circumstances of the commission of a criminal offence, etc[7].

As for the specifics of the ITF's activities in the above categories of criminal offences, this is partially presented in Sections XII and XV of the Order of the MIAU No. 575 dated July 7, 2017[8].

Thus, the investigator is authorized to seize electronic imagery independently, however, in most cases they do not have special knowledge of their collection. This is evidenced by the results of a survey of 113 investigators, which showed that only 8% of them have basic skills in this area.

Such skills can be obtained through the introduction of added disciplines in the preparation of applicants in higher education institutions in the speciality "pretrial investigation", during the organization of postgraduate education with investigators (completion of specialization, retraining, advanced training, internships), as well as conducting special trainings, webinars and practical classes with investigators with the involvement of relevant national and foreign specialists.

Apart from the above, according to Article 71 of the CPCU[9], detection and collection of evidence must be conducted by an authorized specialist who is involved by the investigator in the investigation procedure. According to Part 2 of Article 71 of the Criminal Procedure Code of Ukraine[10], a specialist may be involved in providing technical support (drafting diagrams, plans, drawings, photographing, sampling for examination, etc.) by the

[1]Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.
[2]Ibidem, 2012.
[3]Ibidem, 2012.
[4]Ibidem, 2012.
[5]Ibidem, 2012.
[6]Order of the Ministry of Internal Affairs of Ukraine No. 575 "On the Approval of the Instructions on the Organization of the Interaction of Pre-Trial Investigation Bodies with Other Bodies and Units of the National Police of Ukraine in the Prevention of Criminal Offences, Their Detection and Investigation". (2007, July). Retrieved from https://zakon.rada.gov.ua/laws/show/z0937-17#Text.
[7]Ibidem. 2007.
[8]Ibidem. 2007.
[9]Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.
[10]Ibidem, 2012.

court during the trial and by the parties to criminal proceedings during the pre-trial investigation, etc.[1].

When investigating a criminal offence, the investigator collects the evidence base using a certain algorithm of actions and certain tools. One of these tools is law enforcement intelligence actions.

As practice shows, quite often electronic imagery is detected during a search. It is correct to agree with the methodological recommendations of scientists that before carrying out this law enforcement intelligence action, it is necessary to find answers to the following questions: "What computer equipment and software can be at the place of search? How many devices can be detected? Who handles the equipment? How much data needs to be copied? Are data backups available, and where are they stored?" (Gutsalyuk et al., 2020). Notably, when conducting such a law enforcement intelligence action, it is advisable to involve an employee of the cyberpolice as a specialist because pursuant to the Order of the National Police of Ukraine No. 85[2], this department "takes part in the formation and implementation of the national policy on prevention and counteraction of criminal offences, the mechanism of preparation, commission, or concealment of which involves the use of electronic computing machines (computers), systems and computer networks and telecommunication networks"[3]. Only in extreme cases can other individuals who have the proper knowledge and are not cyberpolice officers be involved as specialists. This is explained by the fact that cyberpolice officers are full-time police officers who know, understand, and are aware of the consequences of disclosing information obtained during a pre-trial investigation, which cannot be said about civilians, to whom the usual warning by investigators about legal liability can be taken lightly.

Notably, if the investigator plans to use electronic information as evidence, then such information should be copied with the involvement of a specialist. However, if the information is needed for purposes other than proof, it is not necessary to involve a specialist. The specialist must be competent in information technology issues, knowledgeable in the techniques of verification of the integrity of information (Lytvynchuk et al., 2020).

When conducting the designated law enforcement intelligence action, the specialist is obliged to indicate to the investigator on the devices from which information can be extracted, on which devices it is advisable to do this and how to withdraw it (i.e., explain the methods of such information collection, which will affect the time of extraction and the amount of data received).

Typically, during a search, investigators decide to seize all technical equipment that contains evidentiary information. This allows the investigators to reduce the time of conducting this law enforcement intelligence action and give more time to the specialist in a calm environment, without making mistakes, to seize electronic imagery fully. Before investigators decide on the seizure of technical equipment, the specialist examines both their technical condition and the software.

There are cases when experts recommend that the investigator seize electronic imagery on the spot, because their further removal may no longer be possible. For instance, a specialist will not be able to re-enable a technical device because its hard drives may be encrypted using BitLocker, or the data is located on the server.

When extracting electronic imagery, the following storage media can be used:

– drives on magnetic discs (hard disks);

– drives on optical discs (compact discs (CD-R; CD-RW), DVD discs, Blu-ray Disc and floppy discs);

– flash cards.

If items, valuables, and documents, in the opinion of the investigator, are of interest to the investigation process, they must be seized and properly packaged (attached labels with signatures of participants in the law enforcement intelligence action with the seal of the authorized body) (Gutsalyuk et al., 2020).

Apart from the fact that the investigator removes evidentiary information from electronic computers and electronic data carriers during the search of suspected individuals, they also decide on such removal during the examination of the attacked system of other electronic computers of the victims. As research objects of the attacked system, the following can be removed: "information carriers or their clones or bit images; RAM dumps; log files of services and applications; logging settings; files-reports of diagnostic utilities; configuration of diagnostic utilities; diagrams of the structure of automated systems, their integration into clusters, networks; schemes of internal networks (LAN, Local Area Network) and connection to the global network (WAN, Wide Area Network); setting up network equipment; setting up the software (system, server, user) of the automated system, specifically setting up remote access; email correspondence –primarily letters with attached files (potentially malicious software) or external links (potential sources of downloading malicious software)" (Nizovtsev & Omelyan, 2021).

Notably, during the seizure and examination of electronic imagery, the investigator, specialist, and expert must observe the confidentiality of private information of both the suspect and the victim. First of all, it is necessary to treat with the information seized from the suspect or victim with caution, since it also concerns third parties who are not involved in the commission of a criminal offence. It is clear that in some cases, access to such

[1]Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.
[2]Order of the National Police of Ukraine No 85 "On the Approval of the Regulations on the Cyber Police Department of the National Police of Ukraine". (2015, November). Retrieved from http://tranzit.ltd.ua/nakaz/.
[3]Ibidem, 2015.

information and its analysis can help the investigation. However, if such data is not of significant use for investigation, efforts should be made to limit their use. Authorized individuals having access to a digital device within the framework of any investigation should try to distinguish between "private information relevant to the investigation" and ordinary privileged information that does not affect the investigative procedure (Horsman, 2022).

After the investigator, together with a specialist, has seized (collected) electronic imagery during a certain law enforcement intelligence action, they analyse it, evaluate it, and decide on conducting a certain type of forensic examination. At the same time, the investigator may not send electronic imagery to the forensic examination but have it as reference information. However, in this case, this electronic imagery will not be eligible as evidence within the meaning of Article 84 of the CPCU[1].

According to Article 1 of the Law No. 4038-XII[2], "forensic examination is an investigation based on special knowledge in the field of science, technology, art, craft, etc., of objects, phenomena, and processes, intended to provide an opinion on issues that are or will be the subject of judicial proceedings"[3].

Forensic experts who meet the requirements defined in Law No. 4038-XII[4] are authorized to conduct forensic examinations. Other requirements for an expert in criminal proceedings and their opinion are covered in Articles 69, 70, 102, 103 of the CPCU[5].

If in criminal proceedings there is a question of expert examination of electronic imagery, then in such cases the investigator decides to send them for the following examinations: computer equipment and software products and telecommunications systems and tools. In some cases, a technical and forensic examination of documents may also be appointed, if the electronic document is materialized.

According to Item 13.1. of the Order of the MJU No. 53/5[6], the key tasks of examination of computer equipment and software products include: establishing the working condition of computer and technical means; determination of circumstances related to the operation of technical devices, information, and software; installation of information and software contained on technical devices; determining compliance of software products with certain versions or requirements for its development"[7].

As correctly noted by P.S. Mykhailov, M.P. Klymchuk (2020), before appointing a computer-technical examination, it is necessary to contact the appropriate specialist to clarify and draft a correct list of issues that can be resolved during the specified examination. Such a specialist can be an expert from the specified field of research. This is justified by the fact that one should not re-apply with a power of attorney to appoint an expert examination, delaying the time of the pre-trial investigation.

It should also be noted that the court's failure to provide a decision on the use of computer equipment and the information contained on it to commit a certain action is a typical mistake of the subjects of criminal proceedings. Messages stored on a seized device may be considered inadmissible evidence in the absence of declassified investigative measures or a separate resolution or approval to disclose the secrecy of messages in criminal proceedings. In addition, when downloading information from a hard disc, phone, or flash card, one cannot add anything, or extract messenger texts by "creating a screenshot" from the device, as this will change the data. The results of such investigations are recognized as inadmissible evidence if the expert immediately begins the examination with an "open" device, since a separate court order is required to "overcome the logical defence" (Knysh, 2019).

It is advisable to point out that today the verification of computer equipment and software products belongs to one expert speciality, which means that the presence of such two diverse branches does not lead to the need to appoint a comprehensive examination, when it is necessary to simultaneously verify both software and technical equipment. However, if it is necessary to involve several highly specialized specialists for an expert examination, a commission examination is carried out (Moussa, 2021). Furthermore, sometimes "apart from specialists in the field of expert research of computer technology and software products, the judicial practice still requires complex examinations with the involvement of experts in the field of telecommunication systems (equipment) and means (to establish the circumstances of the case, related with the dissemination of information on the Internet), etc." (Chvankin, 2021).

Objects of expertise of computer equipment and software products are conventionally divided into the following types: hardware, software, and information objects (Teplytskyi, 2019).

B.B. Teplytskyi (2019) identifies three relatively independent subtypes of the mentioned expertise: "1) examination of computer equipment (establishes circumstances and facts related to the functioning and

[1]Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.
[2]Law of Ukraine No. 4038-XII "Forensic Examination". (1994, February). Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12#Text.
[3]Ibidem, 1994.
[4]Ibidem, 1994.
[5]Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.
[6]Order of the Ministry of Justice of Ukraine No. 53/5 "On the Approval of the Instructions on the Appointment and Conduct of Forensic Examinations and Expert Studies and Scientific and Methodological Recommendations on the Preparation and Appointment of Forensic Examinations and Expert Studies". (1998, October). Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text.
[7]Ibidem, 1998.

operation of computer systems); 2) examination of software products (establishes circumstances and facts related to structural, methodological and hardware features of software development and use); 3) information and computer expertise (establishes circumstances and facts related to information processing of the content of file systems, their storage, and reproduction on computer storage devices)".

First of all, the authors of the methodological recommendations "use of electronic (digital) evidence in criminal proceedings" distinguish the following subtypes of the examination under study: "hardware; software; information; network" (Gutsalyuk, 2020).

Comparing the above positions of scientists, such subtypes as examination of computer equipment and hardware; examination of software products and software, as well as information expertise are similar examinations, differing only in the name given by the author of the cited study. However, the team of authors of the above methodological recommendations identifies another subtype of this expertise – this is network expertise. According to the authors, this is a justified step because the expertise of telecommunications systems and tools does not solve the following tasks: whether the technical tool had access to the internet; how the technical tool was used to access the Internet; what software tools were used to connect the technical tool to the Internet; whether the technical tool contains files that were obtained through copying from the Internet, etc.

Furthermore, one of the key tasks of computer and network expertise is to identify software that was installed to hide the IP address. Common ways to replace a real IP address are as follows: connecting to a proxy server, using the TOR internet browser, and masking the IP address via a VPN. Today, attackers can use the following software to hide their IP address: "NordVPN, OpenVPN, ExpressVPN, PureVPN for Teams, ProtonVPN, NetMotion – programs that provide VPN service; TOR Browser, Tor Control (anonymity layer) for Firefox; ProxyCap, Proxyfier, Proxy Switcher – proxy programs". Thanks to the expert establishing all chains of IP addresses through which, e.g., monetary transactions or relevant files passed, it is highly probable that they will establish network traces that will help solve a crime (Kovalenko, 2020).

It is reasonable to note that the expertise of computer equipment and software products can not only solve issues of detecting electronic imagery, etc., but also of identifying the user using keyboard handwriting. Keyboard handwriting recognition involves the selection of a certain standard from the list of criteria stored in the computer's memory, based on an assessment of the similarity with this standard of the handwriting parameters of one of the users, among others who use the computer. A classic statistical approach to user identification using keyboard handwriting (a set of keywords) can reveal several features: the dependence of handwriting on letter combinations in a word, the presence of connections between a set of certain symbols, the presence of "delays" during the input of symbols, the dependence of the speed of typing words from their content, the time interval of pressing various keys. Another important feature of biometric identification is the password length. Practice shows that its length should be easy to remember and consist of 21 to 42 keystrokes. In this regard, the features of keyboard handwriting are manifested by two methods: typing "free" text and typing a key phrase (Borysova & Bilenchuk, 2020).

As V.V. Pavlov (2020) appropriately noted, when conducting procedural actions (inspection or hardware expertise), the electronic information carrier as material evidence will be connected to the expert's workstation, the performer should be careful when carrying out all manipulations and procedures. This statement is explained by the fact that experts who investigate electronic imagery contained on digital media are required to use those software tools that block the recording of any information from the media. That is, the software first examines such electronic imagery in the information viewing mode, preventing it from being recorded and making changes to the information contained on the digital storage medium.

Only after such an initial examination-research if the expert needs to examine such electronic displays, and they cannot do it without making changes, then they make a file-image of the information carrier, which is located on the disc space of the expert's workstation (Pavlov, 2020).

An approximate list of issues to be resolved by hardware examination is prescribed in Item 13.2 of the Order of the MJU No. 53/5[1].

It is a well-known fact that criminals exchange information among themselves during the commission of a particular criminal offence using both local computer networks and the Internet. Such information, which can be electronic imagery and, as a result, evidence of the commission of a criminal offence, can be established through the examination of telecommunications systems and tools.

As aptly noted by M.G Shcherbakovskyi, V.A. Korshenko (2019), telecommunications expertise is a fairly young, but very modern and progressive type of forensic expertise.

The main tasks of examination of telecommunication systems and means are as follows: establishment of facts and methods of transmission (reception) of information in telecommunication systems; determination

[1]Order of the Ministry of Justice of Ukraine No. 53/5 "On the Approval of the Instructions on the Appointment and Conduct of Forensic Examinations and Expert Studies and Scientific and Methodological Recommendations on the Preparation and Appointment of Forensic Examinations and Expert Studies". (1998, October). Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

of characteristics and parameters of telecommunication systems and means; establishment of facts and methods of access to systems, resources, and information in the field of telecommunications; research of information processing algorithms and its protection in the field of telecommunications; determination of the configuration and working condition of telecommunication systems and facilities; determination of the quality of provision of telecommunication services at the level of their consumption; determination of types, brands, models, and other classification categories of telecommunication systems and means[1]. However, despite the wide range of tasks solved by this examination, as practice shows, to identify the full extent of electronic imagery that will have evidentiary value in court, investigators appoint a complex forensic examination, which includes examination of both computer equipment and software products, and examination of telecommunication systems and means.

Notably, investigators, specialists, and experts need to remember that the detection, collection, and investigation of evidence must be accompanied by its pertinence and admissibility, which is prescribed in Chapter 4, Paragraph 1 of the CPCU[2]. In this regard, it is also advisable to focus on the practices of the people's Republic of China, where the review of evidence before the trial mainly lies in judging the use of evidence for the prosecution and defence. The content of the review includes the competence of subjects who withdraw evidentiary information and their evidentiary value. From the standpoint of legal requirements and technical norms, such rules can be constructed as follows:

– the content of the verification of electronic imagery mainly includes the subject's competence and qualification for their investigation;

– the content of verifying the evidentiary value of electronic imagery mainly includes their reliability and integrity;

– when proving, the participation of professional personnel must be accompanied by the appropriate permission to provide support during the trial (Du, et al., 2020).

Conclusions

Digital evidence is diverse and rapidly improving. It varies in form and type and may include source data, monitoring systems in networks and servers, or electronic documents and digital signatures, or audiovisual recordings or attachments stored in email. The diversity of the electronic directory determines the breadth of its network. The development of several types of digital evidence is typical for the virtual world.

The present paper showed that:

– usually, investigators and operational officers detect electronic imagery independently or as part of the ITF during the investigation of criminal offences, or before their commission;

– the collection of electronic imagery takes place when conducting procedural actions (usually law enforcement intelligence actions) both from the technical devices using which a criminal offence was committed, and from those devices that were attacked. When extracting electronic imagery, it is advisable to involve the appropriate specialist (if possible, a cyberpolice officer);

– an investigator, specialist, and expert is authorized to investigate electronic imagery.

Only experts are authorized to conduct expert research on electronic imagery. Electronic imagery is investigated by conducting the following examinations: telecommunications systems and tools, computer equipment and software products, as well as technical forensic examination of documents (if the electronic document is tangible). Expert examination of electronic images must necessarily include updating the software with which they are investigated, focusing on the requirements of time and the development of criminal activities in this area. This is the prospect of further scientific research.

From the above overview, the world evidently aims to effectively combat "electronic crime", which is manifested in the development of international standards for the collection, identification, and storage of potential electronic images that can be evidence. This is also reflected in the improvement of practical skills of law enforcement agencies in working with them. Modern conditions point to the active informatization of society and the transfer of criminal activity to the information sphere, as well as to the fact that, according to the legislation of Ukraine, the investigator is authorized to extract trace information (electronic imagery) unassisted, which means that they must also possess the basic skills of collection, which is not always the case in practice.

References

[1] Aksamitowska, K. (2021). Digital evidence in domestic core international crimes prosecutions: Lessons learned from Germany, Sweden, Finland and the Netherlands. *Journal of International Criminal Justice*, 19(1), 189-211. doi: 10.1093/jicj/mqab035.

[2] Amelina, A.S., & Dement'eva, S.M. (2021). Documents as procedural sources of evidence in criminal proceedings. *Legal Scientific Electronic Journal*, 3, 243-246. doi: 10.32782/2524-0374/2021-3/62.

[1]Order of the Ministry of Justice of Ukraine No. 53/5 "On the Approval of the Instructions on the Appointment and Conduct of Forensic Examinations and Expert Studies and Scientific and Methodological Recommendations on the Preparation and Appointment of Forensic Examinations and Expert Studies". (1998, October). Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

[2]Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.

[3] Belshaw, S., & Nodeland, B. (2022). Digital evidence experts in the law enforcement community: Understanding the use of forensics examiners by police agencies. *Security Journal*, 35, 248-262. doi: 10.1057/s41284-020-00276-w.
[4] Borysova, L.V., & Bilenchuk, P.D. (2020). Examination as a means of establishing the facts and circumstances of the commission of transnational computer crimes. *Interdepartmental Scientific and Methodological Collection "Criminal Studies and Forensic Examination"*, 65, 230-239. doi: 10.33994/kndise.2020.65.22.
[5] Chvankin, S.A. (2021). Computer-technical expertise in civil proceedings. *Law and Public Administration*, 1, 45-51.
[6] Du, J., Ding, L., & Chen, G. (2020). Research on the rules of electronic evidence in Chinese *Criminal Proceedings. International Journal of Digital Crime and Forensics (IJDCF)*, 12(3), 111-121. doi: 10.4018/IJDCF.2020070108.
[7] Forgó, N., Hawellek, C., Knoke, F., & Stoklas, J. (2017). The collection of electronic evidence in germany: A spotlight on recent legal developments and court rulings. In *New Technology, Big Data and the Law* (pp 251–279). Singapore: Springer. doi: 10.1007/978-981-10-5038-1_10.
[8] Granja, F.M., & Rafael, G.D.R. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, 9(1), 1-18. doi: 10.1504/IJESDF.2017.081749.
[9] Grebenkova, M.S. (2021). Appropriateness and admissibility of electronic images as sources of evidence in criminal proceedings. *Legal Scientific Electronic Journal*, 12, 335-338.
[10] Gutsalyuk, M.V., Havlovskyi, V.D., & Khakhanovskyi, V.G. (2020). *Use of electronic (digital) evidence in criminal proceedings*. Kyiv: View of the National Academy Internal of Affairs.
[11] Holt, T., & Dolliver, D.S. (2021). Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes. *Forensic Science International: Digital Investigation*, 37, article number 301167. doi: 10.1016/j.fsidi.2021.301167.
[12] Holt, T.J., Clevenger, S., & Navarro, J. (2020). Exploring digital evidence recognition among officers and troopers in a sample of a state police force. *Policing*, 43(1), 91-103. doi: 10.1108/PIJPSM-07-2019-0119.
[13] Horsman, G. (2022). Defining principles for preserving privacy in digital forensic examinations. *Forensic Science International: Digital Investigation*, 40, 1-8. doi: 10.1016/j.fsidi.2022.301350.
[14] Javed, A.R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T.R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE* Access, 10, 11065-11089. doi: 10.1109/ACCESS.2022.3142508.
[15] Knysh, M. (2019). How do computer-technical examinations collapse? *Yuridychna Gazeta*, 45, 699-700.
[16] Kohut Y.I. (2021). *Anti-cyberterrorism as a threat to the information security of Ukraine*. Kyiv.
[17] Kovalenko, I. (2020). Certain types of examinations as mandatory investigative (research) actions during the investigation of fraud in the field of bank electronic payments. *Entrepreneurship, Economy and Law*, 12, 262-266. doi: 10.32849/2663-5313/2020.12.45.
[18] Lytvynchuk, O.I., Soroka, M.S., & Kolesnikov, I.V. (2020). *Electronic evidence. Search. Part 1*. Kharkiv: Factor.
[19] McCord, A., Birch, P., & Bizo, L.A. (2022). Digital displacement of youth offending: Addressing the issue. *Journal of Forensic Practice*, 24(3), 298-311. doi: 10.1108/JFP-03-2022-0012.
[20] Moussa, A.F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, 11, article number 20. doi: 10.1186/s41935-021-00234-6.
[21] Mykhaylov, P.S., & Klimchuk, M.P. (2020). Forensic computer-technical examination as a method of identifying the corruption component during the investigation of illegal influence on the results of official sports competitions. *Academic Notes of TNU named after V.I. Vernadskyi*, 31(70), 109-113. doi: 10.32838/2707-0581/2020.2-3/18.
[22] Nizovtsev, Yu.Yu., & Omelyan, O.S. (2021). Regarding the preparation and appointment of forensic examinations within the framework of the investigation of criminal offenses related to cyberattacks. *Forensic Herald*, 2(36), 59-68. doi: 10.37025/1992-4437/2021-36-2-59.
[23] Orlov, Y.Yu., & Chernyavskyi, S.S. (2017). Electronic display as a source of evidence in criminal proceedings. *Legal journal of the National Academy of Internal Affairs*, 1(13), 12-24.
[24] Pavlov, V.V. (2020). The practice of loading an operating system contained on a digital media in a virtual machine environment. *Bulletin of the Cherkasy State Technological University*, 1, 27-33. doi: 10.24025/2306-4412.1.2020.193369.
[25] Ratnova, A.V. (2021). *Criminal procedural and forensic basics of using electronic documents in evidence*. Lviv.
[26] Shcherbakovsky, M.G., & Korshenko, V.A. (2019). Comprehensive telecommunications and auto technical examinations. *Herald of KhNUVS*, 4(87), 179-186. doi: 10.32631/v.2019.4.18.
[27] Skrypnyk, A.V. (2021). *The use of information from electronic media in criminal procedural evidence*. Kharkiv.
[28] Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation*, 40, article number 301351. doi: 10.1016/j.fsidi.2022.301351.

[29] Teplytsky, B.B. (2021). Current issues of appointment of examination of computer equipment and software products during the investigation of crimes in the field of use of electronic computing machines (computers), systems, computer networks and telecommunications networks. *Scientific Bulletin of the National Academy of Internal Affairs*, 3(120), 28-34. doi: 10.33270/01211203.28.
[30] Teplytskyi, B.B. (2019). Tasks, objects and issues of computer-technical forensic examination. *Legal Journal of the National Academy of Internal Affairs*, 2(18), 24-32. doi: 10.33270/04191802.24.
[31] Tun, T., Price, B., Bandara, A., Yu, Y., & Nuseibeh, B. (2017). Verifiable limited disclosure: Reporting and handling digital evidence in police investigations. *Proceedings – 2016 IEEE 24th International Requirements Engineering Conference Workshops, REW 2016*, 102-105. doi: 10.1109/REW.2016.43.
[32] Zelena, M.S. (2020). Research of computer equipment and software products in the investigation of crimes related to illegal trafficking of narcotic drugs, psychotropic substances or their analogues. *Theory and Practice of Forensic Examination and Criminology*, 22, 373-381. doi: 10.32353/khrife.2.2020.30.

Список використаних джерел

[1] Aksamitowska K. Digital evidence in domestic core international crimes prosecutions: Lessons learned from germany, sweden, finland and the netherlands. *Journal of International Criminal Justice*. 2021. No. 19 (1). P. 189–211. doi: 10.1093/jicj/mqab035.
[2] Belshaw S., Nodeland B. Digital evidence experts in the law enforcement community: understanding the use of forensics examiners by police agencies. *Secur J*. 2022. No. 35. P. 248–262. doi: 10.1057/s41284-020-00276-w.
[3] Du J., Ding L., Chen G. Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings. *International Journal of Digital Crime and Forensics (IJDCF)*. 2020. No. 12 (3). P. 111–121. doi: 10.4018/IJDCF.2020070108.
[4] Forgó N., Hawellek C., Knoke F., Stoklas J. The collection of electronic evidence in Germany: A spotlight on recent legal developments and court rulings. *New Technology, Big Data and the Law*. 2017. P. 251–279. doi: 10.1007/978-981-10-5038-1_10.
[5] Granja F. M., Rafael G. D. R. The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*. 2017. No. 9 (1). P. 1–18. doi: 10.1504/IJESDF.2017.081749.
[6] Holt T. J., Clevenger S., Navarro J. Exploring digital evidence recognition among officers and troopers in a sample of a state police force. *Policing*. 2020. No. 43 (1). P. 91–103. doi: 10.1108/PIJPSM-07-2019-0119.
[7] Holt T., Dolliver D. S. Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes. *Forensic Science International: Digital Investigation*. 2021. No. 37. doi: 10.1016/j.fsidi.2021.301167.
[8] Horsman G. Defining principles for preserving privacy in digital forensic examinations. *Forensic Science International: Digital Investigation*. 2022. Vol. 40. P. 1–8. doi: 10.1016/j.fsidi.2022.301350.
[9] Javed A. R., Ahmed W., Alazab M., Jalil Z., Kifayat K., Gadekallu T. R. A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access*. 2022. Vol. 10. P. 11065–11089. doi: 10.1109/ACCESS.2022.3142508.
[10] McCord A., Birch P., Bizo L. A. Digital displacement of youth offending: Addressing the issue. *Journal of Forensic Practice*. 2022. No. 24 (3). P. 298–311. doi: 10.1108/JFP-03-2022-0012.
[11] Moussa A. F. Electronic evidence and its authenticity in forensic evidence. *Egypt J Forensic Sci*. 2021. No. 20. doi: 10.1186/s41935-021-00234-6.
[12] Stoykova R., Andersen S., Franke K., Axelsson S. Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation*. 2022. Vol. 40. doi: 10.1016/j.fsidi.2022.301351.
[13] Tun T., Price B., Bandara A. Yu. Y., Nuseibeh B. Verifiable limited disclosure: Reporting and handling digital evidence in police investigations. *Paper presented at the Proceedings – 2016 IEEE 24th International Requirements Engineering Conference Workshops, REW 2016*. 2017. P. 102–105. doi: 10.1109/REW.2016.43.
[14] Амеліна А. С., Дементʼєва С. М. Документи як процесуальні джерела доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2021. № 3. С. 243–246. doi: 10.32782/2524-0374/2021-3/62.
[15] Борисова Л. В., Біленчук П. Д. Експертиза як засіб установлення фактів і обставин вчинення транснаціональних компʼютерних злочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 230–239. doi: 10.33994/kndise.2020.65.22.
[16] Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доповн. Київ : Нац. акад. внутр. справ, 2020. 104 с.

[17] Гребенькова М. С. Належність і допустимість електронних відображень як джерел доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2021. № 12. С. 335–338.
[18] Електронні докази. Обшук / [О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін.]. Харків : Фактор, 2020. Ч. 1. 80 с.
[19] Зелена М. С. Дослідження комп'ютерної техніки та програмних продуктів у розслідуванні злочинів, пов'язаних з незаконним обігом наркотичних засобів, психотропних речовин або їх аналогів. *Теорія та практика судової експертизи і криміналістики*. 2020. Вип. 22. С. 373–381. doi: 10.32353/khrife.2.2020.30.
[20] Книш М. Як розвалюють комп'ютерно-технічні експертизи? *Юридична газета online*. 2019. № 45–46. С. 699–700.
[21] Коваленко І. Окремі види експертиз як обов'язкові слідчі (розшукові) дії під час розслідування шахрайства у сфері банківських електронних платежів. *Підприємництво, господарство і право*. 2020. Вип. 12. С. 262–266. doi: 10.32849/2663-5313/2020.12.45.
[22] Когут Ю. І. Протидія кібертероризму як загрозі інформаційній безпеці України : дис. … канд. юрид. наук : 12.00.09. Київ, 2021. 258 с.
[23] Михайлов П. С., Климчук М. П. Судова комп'ютерно-технічна експертиза як спосіб виявлення корупційного складника під час розслідування протиправного впливу на результати офіційних спортивних змагань. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. 2020. Т. 31 (70). Ч. 3. № 2. С. 109–113. (Серія «Юридичні науки»). doi: 10.32838/2707-0581/2020.2-3/18.
[24] Нізовцев Ю. Ю., Омельян О. С. Щодо підготовки та призначення судових експертиз у межах розслідування кримінальних правопорушень, пов'язаних із кібератакими. *Криміналістичний вісник*. 2021. № 2 (36). С. 59–68. doi: 10.37025/1992-4437/2021-36-2-59.
[25] Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1 (13). С. 12–24.
[26] Павлов В. В. Практика завантаження операційної системи, що міститься на цифровому носії інформації в середовищі віртуальної машини. *Вісник Черкаського державного технологічного університету*. 2020. Вип. 1. С. 27–33. doi: 10.24025/2306-4412.1.2020.193369.
[27] Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філос. наук : 12.00.09. Львів, 2021. 248 с.
[28] Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. … д-ра філос. наук : 12.00.09. Харків, 2021. 369 с.
[29] Теплицький Б. Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 3 (120). С. 28–34. doi: 10.33270/01211203.28.
[30] Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2 (18). С. 24–32 doi: 10.33270/04191802.24.
[31] Чванкін С. А. Комп'ютерно-технічна експертиза у цивільному судочинстві. *Право та державне управління*. 2021. № 1. С. 45–51. doi: https://doi.org/10.32840/pdu.2021.1.7.
[32] Щербаковський М. Г., Коршенко В. А. Комплексні телекомунікаційно-автотехнічні експертизи. *Вісник Харківського національного університету внутрішніх справ*. 2019. Вип. 4 (87). С. 179–186. doi: 10.32631/v.2019.4.18.

Виявлення, збирання та дослідження електронних відображень як джерел доказів

Валерій Георгійович Хахановський
Доктор юридичних наук, професор
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0001-5676-5641

Маргарита Святославівна Гребенькова
Ад'юнкт
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0003-2184-8679

Анотація
З огляду на швидкі темпи інформатизації суспільства, щоразу зростає кількість кримінальних правопорушень, учинених з використанням електронних обчислювальних машин, їх програмного забезпечення, а також телекомунікаційних систем. Такі протиправні дії характеризуються залишенням слідів, серед яких й електронні відображення. Вони можуть бути доказами вчинення кримінальних правопорушень, що пояснює процес розроблення та вдосконалення методів їх виявлення, збирання та дослідження правоохоронними органами. На сьогодні такі методи виявлення, збирання й дослідження електронних відображень висвітлено в низці наукових праць національних та іноземних учених, що зумовило комплексне висвітлення їх у науковому дослідженні. Мета статті – здійснення огляду теорії та практики діяльності уповноважених суб'єктів щодо виявлення, збирання й дослідження електронних відображень. У роботі застосовано сукупність різноманітних методів, зокрема наукового пізнання реальних явищ та їхніх зв'язків з практичною діяльністю уповноважених органів щодо виявлення, збирання й дослідження електронних відображень (діалектичний метод), а також спеціальні та загальнонаукові методи юридичної науки. Дослідження засвідчило, що зазвичай слідчі й оперативні працівники виявляють електронні відображення самостійно чи в складі слідчо-оперативної групи під час розслідування кримінальних правопорушень або передування їх учиненню; збирання електронних відображень відбувається під час проведення процесуальних дій (слідчих (розшукових) дій) як з технічних пристроїв, за допомогою яких було вчинено кримінальне правопорушення, так і з тих, які було атаковано. До вилучення електронних відображень доцільно залучати відповідного фахівця (за можливості – працівника кіберполіції); досліджувати електронні відображення уповноважені слідчий, спеціаліст й експерт. Експертне дослідження електронних відображень здійснюють експерти шляхом проведення таких експертиз: комп'ютерної техніки та програмних продуктів, телекомунікаційних систем і засобів, а також техніко-криміналістичної експертизи документів. Проведений огляд допоможе відновити в пам'яті уповноважених практичних працівників знання щодо відомостей про інструментарій виявлення, збирання та дослідження електронних відображень, що забезпечить ефективне виконання завдань кримінального провадження

Ключові слова:
слідчі (розшукові) дії; слідчий; цифрові докази; електронний документ