Collection and research on electronic documents using specific expertise

Mykhailo Shcherbakovskyi * [a], Viktor Sezonov ** [b]

* Doctor of Law, Professor, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-1990-1231, e-mail: shcherbakovskyi@gmail.com

** PhD in Law, Docent, Kharkiv Scientific Research Forensic Center of the MIA (Ministry of Internal Affairs) of Ukraine, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0002-2580-2953, e-mail: sv26031985@gmail.com

[a] Writing – original draft, Project administration.
[b] Writing – original draft, Methodology.

DOI: 10.32353/khrife.3.2024.02 UDC: 343.98
Received: 13.06.2024 / Reviewed: 17.06.202 / Accepted for print: 25.09.2024 / Available online: 30.09.2024

This research paper purpose is to use modern general and special methods of scientific knowledge to investigate the essence, form of electronic documents and their carriers, the specifics of the involvement of specialists and experts in their search, recording and research. It has been proven that the essence of the concepts "electronic (digital) information", "electronic data", "electronic document" in the criminal procedural aspect should be considered identical. It is shown that in the broadest sense an electronic document is any information presented in electronic form, in a narrow sense it is a document with mandatory electronic details. It is argued that electronic documents are placed on physical or electronic media in the form of files. Physical media are digital devices on which electronic documents are stored, and electronic media (electronic environment) are global or local networks, cloud storage, various electronic registers. It is substantiated that in criminal proceedings physical media are physical evidence (Article 98 of Criminal Procedural Code of Ukraine) or appendices to the protocols of investigative actions in the form of carriers of copies of electronic documents (Article 105 of this Code), and documents removed from electronic media are evidence documents (Article 99 of

This article is translation of the original Ukrainian content, which source is available at the link: *https://khrife-journal.org/index.php/journal* (translated by Andriy Bublikov). The author acknowledges translation as corresponding to the original.

this Code). For admissibility of electronic documents as evidence in criminal proceedings during investigative actions for the search, detection and recording of electronic documents with the participation of an information technology specialist, it is recommended to necessarily record (in writing in the protocol or with the help of a video recording) all operations of the specialist with the carrier of electronic documents or appoint an electronic communications examination or a computer examination at the place of inspection (search).

Keywords: *electronic documents; electronic (digital) information; information carriers; electronic data; digital evidence; specific expertise; specialist; forensic expert; forensic science.*

Research Problem Formulation

Currently, the latest information technologies are actively used in everyday activities: they have become an integral part of modern society. At the same time, information technologies are used in illegal activities for creation of malicious programs, forged documents, interference in computers and computer networks, committing fraudulent actions, embezzlement and other offenses as a component of the method of committing crimes. Modern criminals are especially active in using the resources and capabilities of the Internet, social networks, e-mail and instant messaging services, means of anonymization and remote access, technologies for creating and disseminating unconfirmed facts, etc. Consequently, many evidences in criminal proceedings today have a digital (electronic) form requiring their collection, storage, processing and analysis during criminal proceedings. Information in electronic (digital) form includes virtual assets, websites, web pages, text and graphic images, plans, photographs, video and audio recordings, multimedia and voice messages, databases and other components that can be considered electronic documents.

There is no need to prove the need for innovations in the criminal procedural field, in methods and instrumental methods of searching, reviewing, extracting and researching electronic documents. Despite the presence of separate legislative acts, numerous scientific publications and methodological recommendations, in the criminal process there remain a number of problems related to the interpretation of the concepts of *digital information*, *electronic documents*, *electronic data*, *digital evidence*, which negatively affects investigative and judicial practice. Taking into account peculiarities of electronic documents, issues of turning them into evidence, developing rules for collecting, preserving, researching and using digital information in evidence based on specific expertise are urgent.

The issues of collecting and researching on electronic documents, created directly in computer tools and their systems, on information carriers, in a virtual environment are due primarily to the need to apply specific expertise. During investigation of criminal offenses, difficulties in working with electronic documents are caused by gaps in the legislation, insufficient knowledge of law enforcement officers in the field of computer technologies, the need to use complex licensed

equipment, and mandatory involvement of specialists of various profiles in conducting investigative (search) actions. In recent years, electronic documents have become objects of research in many types of forensic examinations which has caused a number of theoretical, legal and organizational problems, significantly influenced the methodology and methodology of forensic expert research, competence of forensic experts.

Article Purpose

Determine the essence, form of electronic documents and their carriers, specifics of involving specialists and experts in their search, recording and research..

Research Methods

During research, general and special methods of scientific knowledge were applied. Theoretical analysis and synthesis (induction, deduction, comparison, analogy, abstraction, classification) came in handy for summarizing content from literary sources, positions of authors on certain issues related to the research subject; examination and substantiation of the concept electronic documents, their importance while proof procedure was carried out by the system-structural method; the formal-legal method helped reveal the specifics and criteria for involving a specialist in investigative actions. The mentioned methods were used as interconnected and complementary, which contributed to research completeness and validity of formulated scientific conclusions and proposals.

Analysis of Essential Researches and Publications

The concepts, types, methods of collecting and researching electronic documents and digital evidence in the criminal process were analyzed by domestic scientists H. Avdieieva, D. Alieksieieva-Protsiuk, N. Akhtyrska, O. Bryskovska, O. Harasymiv, S. Honhalo, M. Hutsaliuk, I. H. Kalancha, A. Kovalenko, I. Krytska, S. Marko, Yu. Orlov, L. Ostapchuk, A. Ratnova, O. Riashko, O. Samoilenko, A. Skrypnyk, I. Smal, A. Stolitnii, I. Kharaberiush, V. Khakhanovskyi, A. Khytra, D. Tsekhan, S. Cherniavskyi, H. Chyhryna et al. A number of research papers by these and other authors were devoted, in particular, to the issues of involving expert witness in collection and research on electronic documents. However, certain aspects of the essence of electronic documents, specific expertise use regarding their detection, recording, extraction and research have not been fully analyzed that necessitates a more thorough analysis of outlined issues.

Main Content Presentation

Given the lack in the doctrine of criminal procedural law of Ukraine of a definition of the concept of *electronic documents* in the context of disclosing the purpose of our research, it is important to find out essence, specifics of these objects, relationship with other related categories of information technology.

In modern legislation, the concept of *document* is interpreted as “material object that contains information, the main functions of which are preserved and transferred to the world ” [1] or “material form of

1 Про інформацію : Закон України від 02.10.1992 р. № 2657-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (date accessed: 02.06.2024).

possession, saving, editing and expanding information recorded on the paper, magnetic, film, photo film, optical disk or other media" [2]. Another important concept of *document* in place of DSTU 2732:2004 (that has foregone DSTU 2732:2023) is "information recorded on a material basis, the main function of any "Save and transmit it in time and space" [3]. However, at different times, legislators gave different meanings: on the one hand, the document was perceived as material information, on the other hand, as the information itself. However, these concepts are not the same.

Information is defined as "any information and/or data that can be stored on tangible media or displayed electronically"[4]. Electronic (digital) information (digital content) is "any information or data in electronic (digital) form containing objects of copyright and/or related rights and can be stored and/or distributed in the form of one or more files (parts of files), records in a database on the storage devices of computers, servers, etc. on the Internet"[5].

The Criminal Procedural Code of Ukraine does not have the concept of *electronic digital information*, but mentions *electronic data*, the which review is carried out by the investigator, prosecutor in accordance with Art. 237 [6]. The concept of *electronic data* in the regulatory documents is defined as "any representation of facts, information or concepts in a form that is suitable for processing in a computer system, including a program that is suitable for causing the execution of certain function by a computer system, *data* is defined as information presented" [7], in a form suitable for processing by electronic means"[8], and *electronic data* is defined as any information *in electronic form* [9]. It is worth noting that, by its very nature, electronic (digital) information is a binary code written with zeros and ones and designed to be read, processed and transmitted by information technology. In its original form, it

2 Про обов'язковий примірник документів : Закон України від 09.04.1999 р. № 595-XIV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/595-14#Text (date accessed: 02.06.2024).

3 ДСТУ 2732:2004 Діловодство й архівна справа Терміни та визначення понять [Не чинний від 29.02.2024]. Київ, 2005. С. 2. URL: http://old.loga.gov.ua/netcat_files/4895/4106/h_7d602cb292dd3a86478915757d0425f9 (date accessed: 20.08.2024).

4 Про інформацію ... . URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (date accessed: 20.08.2024).

5 Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (date accessed: 02.06.2024).

6 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 20.05.2024).

7 Конвенція про кіберзлочинність : прийнята Ком. міністр. Ради Європи 08.11.2001 р. ; ратифік. Законом України від 07.09.2005 р. № 2824-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (date accessed: 02.06.2024).

8 Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (date accessed: 02.06.2024).

9 Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (date accessed: 02.06.2024).

is not suitable for human perception: only computer tools make it understandable for people.

Important characteristic of electronic documents is the way they are stored in a file format, which scientists propose to consider as a criminal procedural form of digital information [10]. There are various file formats used for preparing, processing, and storing electronic documents. File formats are usually divided into text ones (.txt, .rtf, .pdf, .doc (.docx), etc.), graphic (vector ones: .dxf, .tps, .cgm, etc.; raster ones: bmp, .tiff, .gif, .jpeg, etc.), spreadsheets, databases, video and audio, archival storage (.pdf, etc.) and so-called markup languagesthat allow displaying information about the document (.sgml, .html, .xml).

Legislators define an electronic document as "document where information is recorded in the form of electronic data, including mandatory document details [11]." Scientists call an electronic document information in electronic (digital) form that can be used "as evidence of a fact or circumstance established during criminal proceedings" [12]. The analysis of the given wording gives reason to believe that in the criminal procedural aspect, the concepts: *electronic (digital) information*, *electronic data*, *electronic document* can be used as synonyms. However, from a practical and procedural point of view, it is advisable to distinguish the concept of electronic documents in a broad and narrow sense. In the first sense, an electronic document should be considered any information presented in electronic form, which formation and existence occurs thanks to special software and technical means [13]. It is worth noting that the concept of electronic document in a broad sense covers many different categories, namely: accounting and tax reporting documents, Internet pages, websites, audio and video recordings that are created, transmitted, received in electronic form, messenger pages, correspondence through e-mail, etc. In the narrow sense, an electronic document is a document that has electronic details: mandatory data (for example, an electronic signature or an electronic seal), without which it cannot be the basis for its accounting and will not have legal force. The visual form of presentation of an electronic document is a display of the data it contains by electronic means or on paper in a form suitable for human perception of its content [14].

Concept of electronic document is inseparable from its carrier, material object or environment capable of storing the entered information in its structure. A medium for storing electronic (digital) data is defined as "material medium used

10 Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. Вісник кримінального судочинства. 2023. № 1—2. С. 50. DOI: 10.17721/2413-5372.2023.1-2/42-53 (date accessed: 02.06.2024).

11 Про електронні документи … . URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (date accessed: 02.06.2024).

12 Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу. Прикарпатський юридичний вісник. 2022. Вип. 2 (43). С. 124. DOI: 10.32837/pyuv.v0i2.1028 (date accessed: 02.06.2024).

13 Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право*. 2017. № 4 (58). С. 81. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (date accessed: 02.06.2024).

14 Про електронні документи … . URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (date accessed: 02.06.2024).

for recording, storing and reproducing information processed by computer equipment" [15]. With the aim of more effective application of specific expertise for collecting and researching electronic document carriers and taking into account their nature, it is advisable to combine such carriers into two groups: material and electronic. Physical media during investigation are important as objects that directly contain forensically significant information in the form of electronic document files. Electronic documents in this case have evidentiary value when they are combined with a specific material medium seized in a specified place from a specific person under certain circumstances as evidence of a fact or circumstances that are being investigated during criminal proceedings. Tangible media can be: an object for storing digital data used in standard computers (hard, flexible, optical, magneto-optical disks; digital devices with similar functions); mobile phones, personal digital assistants (*PDAs*), personal electronic devices (*PEDs*), memory cards; mobile navigation systems; digital photo and video cameras (in particular, *CCTV*); a standard computer with network connections; networks based on *TCP/IP* and other digital protocols, as well as devices with functions similar to the above [16].

Electronic carriers of documents are the electronic environment: global and local networks, cloud storage, various electronic registers (weapons, property rights to real estate, ownership rights to real estate, mortgages, prohibitions on alienation of real estate objects, reimbursement of value added tax, etc. .). Due only to information they contain, electronic documents have an independent evidentiary value regardless of the physical medium. The proposed division of electronic document carriers correlates with the decisions of the Supreme Court of Ukraine, according to which the main feature of an electronic document is the lack of a rigid attachment to a specific material carrier that is only a way of preserving information and is relevant only when the electronic document is physical evidence. The same electronic document can exist on different media. All "copies of an electronic document that are identical in their content can be considered as originals and differ from each other only by the time and date of creation"[17].

Summarizing the above, we come to the conclusion that a certain material or electronic medium can contain an electronic document (digital information) in the form of corresponding file.

Electronic document acquires the status of evidentiary information only when it is found, and its content, special features and characteristics, etc. are documented and transformed into a written

15 ДСТУ 7448:2013 Інформація та документація. Бібліотечно-інформаційна діяльність. Терміни та визначення понять [Чинний від 01.07.2014]. Київ, 2014. 42 с. URL: https://lib.nure.ua/storage/app/media/nmbk/doc/dstu.pdf (date accessed: 02.06.2024).

16 ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) [Чинний від 01.01.2019]. Київ, 2018. 31 с. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (date accessed: 02.06.2024).

17 Постанова Верховн. Суду України від 10.09.2020 р., справа № 751/6069/19, провадж. № 51-1704км20 / ЄДРСР : офіц. сайт. URL: https://reyestr.court.gov.ua/Review/91722819 (date accessed: 02.06.2024) ; Постанова Верховн. Суду України від 26.01.2021 р., справа № 236/4268/18, провадж. № 51-3124км20 / Там само. URL: https://reyestr.court.gov.ua/Review/94905297 (date accessed: 02.06.2024).

and visual document available for unambiguous perception by all participants in the criminal proceedings. In order to use electronic documents as evidence during criminal proceedings, they should be obtained in accordance with the procedure provided by the law [18]. The need to use electronic documents (computer data, electronic (digital) information) in evidence has led to a lively discussion among scholars regarding identification of a new type of source: *digital evidence* [19]. It is necessary to support the proposal to legally enshrine the definition of *electronic (digital) evidence* in the Criminal Procedural Code of Ukraine, as formulated in Art.100 of the Civil Procedure Code of Ukraine [20] or the International Standard ISO/IEC 27037:2017 [21]. However, within the limits of current criminal procedural law, scholars and practitioners suggest considering electronic documents as evidentiary documents [22], as physical evidence [23], or as both of these categories [24]. Our approach is based on the proposed division of electronic document carriers, according to which documents extracted from electronic carriers should be considered evidence documents (Article 99 of Criminal Procedural Code of Ukraine), and physical carriers should be considered material evidence (Article 98 of Criminal Procedural Code of Ukraine) or appendices to the protocols of investigators and secret investigative (search) actions in the form of disks, flash drives

18 Авдєєва Г. К. Проблеми визначення достовірності цифрових доказів у кримінальному провадженні. *Вісник Луганського навчально-наукового інституту імені Е. О. Дідоренка.* 2024. Вип. 1 (105). С. 33—48. DOI:10.33766/2786-9156.105.33-48 (date accessed: 02.06.2024).

19 Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : кол. моногр. Львів, 2022. С. 34. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%d0%93%d1%83%d1%82%d0%bd%d0%b8%d0%ba%2c%20%d0%a5%d0%b8%d1%82%d1%80%d0%b0_%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f_21_06_2022.pdf (date accessed: 02.06.2024) ; Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : дис. … д-ра юрид. наук. Одеса, 2018. С. 154. URL: https://dspace.onua.edu.ua/bitstreams/94e3af63-a41b-4f31-8a68-07c2b8bc430b/download (date accessed: 02.06.2024) ; Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. … д-ра філос. у галузі права. Харків, 2021. С. 102.

20 Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (date accessed: 02.06.2024).

21 ДСТУ ISO/IEC 27037:2017. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (date accessed: 02.06.2024).

22 Бідняк Г. С. Використання спеціальних знань при розслідуванні шахрайств : дис. … канд. юрид. наук. Дніпро, 2018. С. 142 ; Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : дис. … канд. юрид. наук. Київ, 2013. С. 121.

23 Крицька І. О. Речові докази у кримінальному провадженні : монографія. Харків, 2018. С. 67 ; Гутник А. В., Хитра А. Я. Зазнач. твір. С. 25. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%d0%93%d1%83%d1%82%d0%bd%d0%b8%d0%ba%2c%20%d0%a5%d0%b8%d1%82%d1%80%d0%b0_%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f_21_06_2022.pdf (date accessed: 02.06.2024).

24 Остапчук Л. Г., Смаль І. А. Зазнач. твір. DOI: 10.32837/pyuv.v0i2.1028 (date accessed: 02.06.2024).

with copies of documents (Article 105 of the Criminal Procedural Code of Ukraine of Ukraine) [25]. We emphasize that, according to our concept, physical evidence is the physical medium itself and not the electronic document that is a peculiar sign, a characteristic of the medium and has no independent evidentiary value.

Despite the existing legal conflict, legislators provided for a certain list of investigative actions aimed at forming sources of evidence, which content are electronic documents, taking into account the characteristics of media and methods of working with them. Thus, electronic documents in the form of electronic data can be detected in case of temporary access to electronic information systems, computer systems or their parts, mobile terminals of communication systems (Article 160 of Criminal Procedural Code of Ukraine), search (Article 236 of the Criminal Procedural Code of Ukraine), inspection (Article 237 of the Criminal Procedural Code of Ukraine), removal of information from electronic communication networks (Article 263 of Criminal Procedural Code of Ukraine) or electronic information systems (Article 264 of Criminal Procedural Code of Ukraine) [26]. During procedural actions, complete copying of information from objects of inspection, search, access is allowed; if necessary, to reveal criminally relevant information, an examination is appointed under Art.242 of Criminal Procedural Code of Ukraine [27] (in our case, a computer-technical examination of seized physical evidence or carriers of copied information).

Impossibility of direct perception of an electronic document and the need to use software and hardware for this is one of the most important features of this object, which distinguishes it from analog documents (documents on paper) and requires specific expertise use to provide such an electronic document with a form accessible to the participants in criminal proceedings. Peculiarities of searching, recording and copying computer data during investigative actions are widely covered in the forensic literature[28]. At the same time, a number of problems regarding the application of specific expertise for collection and research on electronic documents during criminal proceedings remain unresolved.

One of leading participants in investigative actions related to detection and seizure of electronic documents is a specialist (Article 71 of Criminal Procedural Code of Ukraine) [29], which is due to the need to

25 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 20.05.2024).

26 Там само.

27 Там само

28 Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія: юридичні науки*. 2023. Вип. 4. С. 53—58. DOI: 10.32999/ksu2307-8049/2023-4-9 (date accessed: 02.06.2024) ; Лісніченко Д. В. Особливості вилучення за допомогою технічних засобів інформації з мобільних терміналів зв'язку (смартфонів) під час кримінального провадження. *Південноукраїнський правничий часопис*. 2022. Вип. 1—2. С. 120—125. DOI: 10.32850/sulj.2022.1-2.22 (date accessed: 02.06.2024) ; Чигрина Г. Електронні документи: залучення спеціаліста до збирання та використання під час кримінального провадження. *Jurnalul juridic naţional: teorie şi practică*. 2017. № 3. С. 134—137. URL: http://www.jurnaluljuridic.in.ua/archive/2017/3/30.pdf (date accessed: 02.06.2024).

29 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 20.05.2024).

provide electronic documents with a form visually accessible to procedure participants, apply specific methods and technical means to detect and store the necessary information for the purpose of its further expert research. Like any participant in an investigative action, a specialist is endowed with special rights and obligations regarding specific expertise application. Information technology specialist is involved in the search, fixation and seizure of electronic documents.

The first thing to pay attention to is the situational nature of the involvement of specialist affecting the need to apply specific expertise, specialist choice, tools, techniques for searching, recording and saving electronic documents. The general algorithm for the inspection of a separate physical carrier includes the following stages: 1) external inspection and identification; 2) checking availability of cable or wireless connections (cell adapters, contactless communication, etc.), disconnecting cables and external devices; 3) overview of computer information (installed and used applications, file system, running processes) on the medium; 4) saving (copying) information from the RAM; 5) regular shutdown of the device and copying of permanent memory (hard media or hard magnetic disk); 6) compilation of the protocol and packaging of the removed, taking into account the type of media and the possibility of wireless control of it. Not all investigative situations require the involvement of an information technology specialist. In simple situations where the physical medium is in a disabled state and should be removed as physical evidence; when the medium is unlocked, the investigator knows exactly the name of the document (file, web page, etc.) and there is no need to search for it, it is possible to dispense with the involvement of a specialist. Viewing and capturing an image of a document is quite accessible to an investigator with basic computer skills. For stages 1, 2 and 6, a camera, portable work computer (laptop) of the investigator with a typical set of programs and a printed device (printer), forceps and a protective wrapper with packaging are sufficient. A difficult, problematic situation arises due to the lack of a password for access to work on a computer device; the unknown presence and name of a document relevant to the investigation; need to completely copy the information content of the tangible medium if it is impossible to remove the information medium itself or stop (turn off) automated systems. Implementation of stages 3, 4 and 5 requires the use of additional specific expertise and tools. In this situation, involvement of information technology specialist is mandatory.

The need for mandatory involvement of specialist is due to difficulties associated with the search and identification of electronic documents on media that are important for the investigation, which are especially relevant during the inspection (search) of large computer networks, which operation cannot be suspended due to their critical importance for production processes that cannot be interrupted. In addition, it is often technically impossible to remove them completely from the crime scene, and even if it were possible, large amount of information to be studied would make it impractical. In such a situation, specific devices with necessary information should be identified in the network, located and investigated separately. Computer system of even the simplest corporate network includes employee workstations, servers, including mail and proxy servers, domain controllers, routers, switches, and cabling. Elements of the network (cable and wireless, cor-

porate or local network and its whole segments) can be located not only in different premises of the building, but also in different geographical regions (for example, if the technology of virtual (logical) channels, cross-border, cloud system is used to organize the network , then processing of information, which is the most difficult during organization and conducting review, requires mandatory use of tools and methods). Similar situation can arise at the site of inspection (search) in case of detection of digital devices connected to a remote information storage, in particular a cloud one, or during an inspection of the premises of a hosting service provider that rents out computing power, servers that are physically located in different regions of the country or encrypted. In the relevant methodological recommendations, specialist was asked, for example, search for documents in a remote computer network resource, overcome computer blocking and to perform other manipulations [30]. Under such circumstances, role of a specialist, who no longer has to perform routine actions, increases many times over: now a long creative research work awaits him. In such a situation, the participation of a specialist in the field of information technologies during investigative actions consists in carrying out manipulations with computer means that are inaccessible and mostly incomprehensible to the participants of the investigative action: the investigator, witnesses, owners of the means.

In the protocol of investigative action (in accordance with Article 103 of Criminal Procedural Code of Ukraine) it is necessary to describe all operations and transitions carried out during examination (search) of the computer tool [31]. At the same time, as stated above, these actions are not obvious to the rest of the participants, and can last longer than a reasonable period of time for the investigative action, in addition, specialist makes changes in digital environment with his actions that are not related to a criminal offense.

Two methods can be recommended to ensure admissibility of electronic documents as evidence obtained during investigative activities involving an information technology specialist. The first is the recording of each specialist's action (video recording, printing, screenshots of web pages, etc.) so that, in case of doubts about the correctness of receiving electronic documents, each specialist's operation with physical or electronic media can be reviewed and checked. The second way (when the search for electronic documents both in physical media and in cyberspace requires complex manipulations with the use of software and technical means) is the appointment of a forensic examination at the place of inspection (search) [32]. In this case, the entire procedure of searching and fixing electronic documents is described in the research part of the expert's conclusion.

Another issue that has not received sufficient attention is the determination of

30 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Київ, 2020. Вид. 2-ге., допов. С. 23, 29. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content (date accessed: 02.06.2024).

31 Кримінальний процесуальний кодекс ... . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 20.05.2024).

32 Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : навч. посіб. Харків, 2010. 116 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/2b0c8656-bc78-4c21-8ff0-3808403f00ca/content (date accessed: 02.06.2024).

the competence of the specialist involved in investigative actions. In the field of knowledge "Information technologies" (in accordance with the decree of the Cabinet of Ministers of Ukraine), various specializations are acquired: *Software engineering*, *Computer science*, *Computer engineering*, *System analysis* [33], *Cyber security and information protection*, *Information Systems and Technology*, each of which has a specific subject related to software; software and technical means; information technologies; telecommunication systems, collection, presentation, processing, storage, transmission and access to information in computer systems, etc. Thereby, at preparatory stage of conducting investigative actions, the investigator should outline the purpose of the inspection (search), specifics of the carrier of electronic documents, their type and appearance, and determine the specialist's competence.

Forensic research on electronic documents is the main procedural form of application of specific expertise. Material evidence, which consists of electronic documents, as well as copies of these documents, which are appendices to the protocols of investigative actions, are procedural objects of research in such examinations: video and sound recording, linguistic, photo-technical, portrait, economic, technical documents. According to the provisions of forensic expertology, direct research objects of these examinations are, respectively, images, physical parameters of sound, oral speech, human appearance, accounting and other documents, etc. Electronic documents subject to expert examination in the said examinations are known in advance to the investigator, they are indicated in the questions to expert. Another situation concerns the forensic computer-technical examination, the typical task of which is to search and identify electronic documents (information, software) unknown to the investigator, contained in physical evidence, computer tools or media-applications for investigative actions [34]. We believe that such tasks can be set within the limits of examination of electronic communications to search for specific documents in an electronic medium, cyberspace [35]. Direct expert objects of these examinations are the content and parameters (metadata) of documents. Electronic documents discovered in this way can become the objects of further expert research on uniform or multidisciplinary examinations.

Conclusions

The concepts of *electronic (digital) information*, *electronic data*, *electronic document* are identical in their essence in the criminal procedural aspect. In a broad sense, an electronic document is any information submitted in electronic form, in a narrow sense; this is a document that has mandatory electronic details.

33 Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : затв. постанов. КМУ від 29.04.2015 р. № 266 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#n11 (date accessed: 02.06.2024).

34 Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень : затв. наказ. Мін'юсту України від 08.10.1998 р. № 53/5 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (date accessed: 15.08.2024).

35 Щербаковський М. Відкриті джерела кіберпростору як об'єкти судово-експертного дослідження. *Теорія та практика судової експертизи і криміналістики.* 2024. Вип. 2 (35). С. 10—27. DOI: 10.32353/khrife.2.2024.02 (date accessed: 02.07.2024).

Physical or electronic media contain electronic documents in the form of files. Physical media are digital devices which electronic documents are stored on . Electronic media is an electronic environment: global or local networks, cloud storage, a variety of electronic registers. In criminal proceedings, material carriers are material evidence (Article 98 of Criminal Procedural Code of Ukraine) or annexes to protocols of investigative actions in the form of carriers of copies of electronic documents (Article 105 of Criminal Procedural Code of Ukraine), and documents withdrawn from electronic carriers are evidence documents (Article 99 Criminal Procedural Code of Ukraine).

At the stage of preparation for the procedural action, depending on characteristics of the carrier of electronic documents, the investigator must determine the specialist competence in accordance with the specializations belonging to the field of knowledge: *Information Technology*.

For admissibility of electronic documents as evidence in criminal proceedings during investigative actions to search, detect and record electronic documents with the participation of information technology specialist, it is recommended to necessarily record (in writing in the protocol or by video recording) all operations of the specialist with the carrier of electronic documents or to appoint an examination of electronic communications or digital forensics examination at the place of inspection (search).

Збирання та дослідження електронних документів із застосуванням спеціальних знань

Михайло Щербаковський, Віктор Сезонов

Мета роботи — за допомогою сучасних загальних і спеціальних методів наукового пізнання дослідити сутність, форму електронних документів та їхніх носіїв, особливості залучення спеціалістів і експертів до їхнього пошуку, фіксування та дослідження. Доведено, що сутність понять «електронна (цифрова) інформація», «комп'ютерні дані», «електронний документ» у кримінальному процесуальному аспекті слід розглядати як тотожні. Показано, що у широкому значенні електронним документом є будь-яка інформація, представлена в електронній формі, у вузькому розумінні — це документ, що має обов'язкові електронні реквізити. Аргументовано, що електронні документи вміщено на речових або електронних носіях у формі файлів. Речовими носіями є цифрові пристрої, на яких зберігають електронні документи, а електронними носіями (електронним середовищем) — глобальні або локальні мережі, хмарні сховища, різноманітні електронні реєстри. Обґрунтовано, що у кримінальному провадженні речові носії є речовими доказами (ст. 98 Кримінального процесуального кодексу України) або додатками до протоколів слідчих дій у вигляді носіїв копій електронних документів (ст. 105 цього Кодексу), а вилучені з електронних носіїв документи — документами-доказами (ст. 99 цього Кодексу). Для допустимості електронних документів як доказів у кримінальному провадженні під час проведення слідчих дій з пошуку, виявлення та фіксування електронних документів за участі спеціаліста з інформаційних технологій рекомендовано обов'язково фіксувати (письмово у протоколі або за допомогою відеозапису) усі операції спеціаліста з носієм електронних документів або призначати на місці огляду (обшуку) експертизу електронних комунікацій чи комп'ютерно-технічну експертизу.

Ключові слова: *електронні документи; електронна (цифрова) інформація; носії інформації; комп'ютерні дані; циф-*

рові докази; спеціальні знання; спеціаліст; експерт; судова експертиза.

Financing

This research did not receive any specific grant from funding institutions in the public, commercial or non-commercial sectors.

Disclaimer

Founders had no role in the research design, data collection and analysis, decision to publish or manuscript preparation.

Participants

The authors have contributed solely to intellectual discussion underlying this document, case law research, writing and editing, and assumes responsibility for its content and interpretation.

Declaration of Competing Interest

The authors state that there is no conflict of interest relating to this topic; although Mykhailo Shcherbakovskyi is a member of the advisory board of the collection, he did not participate in the decision to publish, and this article has been subjected to a full peer review and editing process.

References

Avdieieva, H. K. (2024). Problemy vyznachennia dostovirnosti tsyfrovykh dokaziv u kryminalnomu provadzhennia [Problems of determining the reliability of digital evidence in criminal proceedings]. *Visnyk Luhanskoho navchalno-naukovoho instytutu imeni E. O. Didorenka*. Vyp. 1 (105). DOI: 10.33766/2786-9156.105.33-48 [in Ukrainian].

Bidniak, H. S. (2018). *Vykorystannia spetsialnykh znan pry rozsliduvanni shakhraistv* [Specific expertise use in the investigation of fraud] : dys. ... kand. yuryd. nauk. Dnipro [in Ukrainian].

Chyhryna, H. (2017). Elektronni dokumenty: zaluchennia spetsialista do zbyrannia ta vykorystannia pid chas kryminalnoho provadzhennia [Electronic documents: the involvement of a specialist in the collection and use during criminal proceedings]. *Jurnalul juridic naţional: teorie şi practică*. № 3. URL: http://www.jurnaluljuridic.in.ua/archive/2017/3/30.pdf [in Ukrainian].

Honhalo, S. Y. (2013). *Sudova tekhniko-kryminalistychna ekspertyza dokumentiv: suchasni mozhlyvosti doslidzhennia ta perspektyvy rozvytku* [Forensic examination of documents: modern research opportunities and development prospects] : dys. ... kand. yuryd. nauk. Kyiv. [in Ukrainian].

Hutnyk, A. V., Khytra, A. Ya. (2022). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv* u *dokazuvanni* [Criminal procedural and forensic bases for the use of electronic documents in evidence] : kol. monohr. Lviv. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%d0%93%d1%83%d1%82%d0%bd%d0%b8%d0%ba%2c%20%d0%a5%d0%b8%d1%82%d1%80%d0%b0_%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f_21_06_2022.pdf [in Ukrainian].

Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H. ta in. (2020). *Vykorystannia elektronnykh (tsyfrovykh) dokaziv* u *kryminalnykh provadzhenniakh* [Use of electronic (digital) evidence in criminal proceedings] : metod. rek. / za zah. red. O. V. Korneika. Kyiv. Vyd. 2-he., dopov. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content [in Ukrainian].

Khyzhniak, Ye. C. (2017). Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen [Peculiaritiea of the digital document review during the investigation of criminal offenses]. *Derzhava ta rehiony. Seriia: Ppavo*. № 4 (58). URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf [in Ukrainian].

Kovalchuk, S. O. (2018). *Vchennia pro rechovi dokazy* u *kryminalnomu protsesi:*

teoretyko-pravovi ta praktychni osnovy [The doctrine of material evidences in the criminal process: theoretical, legal and practical basis.] : dys. ... d-ra yuryd. nauk. Odesa. URL: https://dspace.onua.edu.ua/bitstreams/94e3af63-a41b-4f31-8a68-07c2b8bc430b/download [in Ukrainian].

Kovalenko, A. V. (2023). Orhanizatsiia i taktyka provedennia ohliadu komp'iuternykh danykh [Organization and tactics of computer data inspection]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia: yurydychni nauky*. Vyp. 4. DOI: 10.32999/ksu2307-8049/2023-4-9 [in Ukrainian].

Krytska, I. O. (2018). Rechovi dokazy u kryminalnomu provadzhenni [Physical evidence in criminal proceedings] : monohrafiia. Kharkiv [in Ukrainian].

Lisnichenko, D. V. (2022). Osoblyvosti vyluchennia za dopomohoiu tekhnichnykh zasobiv informatsii z mobilnykh terminaliv zv'iazku (smartfoniv) pid chas kryminalnoho provadzhennia [Features of extraction by technical means of information from mobile communication terminals (smartphones) during criminal proceedings]. *Pivdennoukrainskyi pravnychyi chasopys*. Vyp. 1—2. DOI: 10.32850/sulj.2022.1-2.22 [in Ukrainian].

Metelev, O. P. (2023). Tsyfrovi dokazy u kryminalnomu protsesi: vydova kharakterystyka [Digital evidence in criminal procedure: typological characteristic]. *Visnyk kryminalnoho sudochynstva*. № 1—2. DOI: 10.17721/2413-5372.2023.1-2/42-53 [in Ukrainian].

Ostapchuk, L. H., Smal, I. A. (2022). Do pytannia pravovoi pryrody elektronnoho dokumentu ta yoho mistsia u systemi dokaziv kryminalnoho protsesu [On the issue of legal nature of an electronic document and its place in the system of the criminal processevidence]. *Prykarpatskyi yurydychnyi visnyk*. Vyp. 2 (43). DOI: 10.32837/pyuv.v0i2.1028 [in Ukrainian].

Shcherbakovskyi, M. (2024). Open Sources of Cyberspace as Objects of Forensic Research. *Theory and Practice of Forensic Science and Criminalistics.* Is. 2 (35). DOI: 10.32353/khrife.2.2024.02.

Shcherbakovskyi, M. H., Pashniev, D. V. (2010). *Rozsliduvannia komp'iuternykh zlochyniv* [Investigation of computer crimes] : navch. posib. Kharkiv. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/2b0c8656-bc78-4c21-8ff0-3808403f00ca/content [in Ukrainian].

Skrypnyk, A. V. (2021). *Vykorystannia informatsii* z *elektronnykh nosiiv* u *kryminalnomu protsesualnomu dokazuvanni* [Use of information from electronic media in criminal procedural evidence] : dys.... d-ra filos. u haluzi prava. Kharkiv [in Ukrainian].

Shcherbakovskyi, M., Sezonov, V. (2024). Collection and research on electronic documents using specific expertise. *Theory and Practice of Forensic Science and Criminalistics.* Issue 3 (36). P. 10—23. DOI: 10.32353/khrife.3.2024.02.