Problems of Using Digital Evidence in Criminal Justice of Ukraine and the USA

Galina Avdeeva * [a], Elzbieta Żywucka-Kozlowska ** [b]

* PhD in Law, Senior Researcher, Academician Stashis Scientific Research Institute for the Study of Crime Problems of the National Academy of Sciences of Ukraine, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-4712-728x, e-mail: gkavdeeva@gmail.com
** PhD in Law, Assoc. Professor of Law, The University of Warmia and Mazury, Olsztyn, Republic of Poland, ORCID: https://orcid.org/0000-0002-6039-5580, e-mail: malerude@poczta.onet.pl

[a] Writing — original draft, Methodology, Formal Analysis, Project Administration, Resources.
[b] Methodology, Formal Analysis, Resources.

DOI: 10.32353/khrife.1.2023.07 UDC 343.98
Submitted: 15.02.2023 / Reviewed: 13.03.2023 / Approved for Print: 14.03.2023 /
Avialable online: 31.03.2023

Current issues of using digital evidence in criminal justice of Ukraine and the USA have been considered and proposals have been provided for their resolution. For this purpose, methods of theoretical analysis and synthesis, formal legal analysis, comparative legal method, and special methods of cognition have been applied. The concepts of "electronic evidence" and "digital evidence" have been differentiated. Analysis of 64 decisions of Ukrainian courts of criminal jurisdiction and 31 decisions of the US Court of Appeal and the Supreme Court has revealed certain challenges in recognizing information in digital format as admissible and veracious evidence. The experience of the US judiciary can be useful for reforming Ukrainian legislation and the development of methodological guidelines for digital evidence use. It has been proposed to amend the Criminal Procedural Code of Ukraine with regulations that would contain the definition for the digital evidence concept and its procedural media; differentiation of the concepts of "electronic evidence" and "digital evidence"; introduction of a detailed procedure for seizing digital information, its review, recording and storage

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 Daryna Dukhnenko). The authors acknowledge translation as corresponding to the original.

(with indication of the list of mandatory information on digital evidence which must be procedurally established); an algorithm for assessing veracity of digital evidence and an expert conclusion relying on certain criteria. It has been proved that a rapid change in technologies for detecting, seizing, recording and researching digital information has presented certain challenges for investigators, judges, prosecutors and employees of investigative agencies of Ukraine. It is recommended to improve the efficiency of using digital evidence in court proceedings by developing guidelines for working with such evidence and correspondingly improving qualifications of employees in law enforcement agencies.

Keywords: *digital evidence; electronic evidence; electronic devices; admissibility of evidence; sources of evidence; digital information; criminal proceedings; recording evidence.*

Research Problem Formulation

In the early 1990s, in view of advancement of digital and network technologies, law enforcement agencies started to work with evidentiary information in electronic (digital) format obtained from various electronic devices and telecommunication networks, namely: computers, phones, photo and video cameras, GPS-navigators, social networks, various Internet sites, etc. Particularly, *GPS* technology is helpful in establishing the presence of suspected persons at the crime scene, while the analysis of e-mails, text messages, digital photographs, audio recordings, and video recordings determines persons' involvement in illegal activities.

The development of information technologies, the emergence of new fields of their application and introduction of new electronic devices have led to an increase in the number of types of digital information and methods of its encoding and transformation. To view and research certain types of information, it is not enough to use ordinary computer equipment with standard software: specialized electronic devices as well as software are required for this purpose. This poses certain difficulties for investigators, judges, prosecutors, lawyers, forensic experts, etc.

The problem of using digital evidence in criminal proceedings became especially urgent after the open, full-scale armed invasion of the Russian Federation troops in the territory of Ukraine, which roughly violated the rights of Ukrainian citizens enshrined in Sec. I of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as *the Convention*) and its protocols, namely: right to life (Art. 2 of the Convention), prohibition of torture (Art. 3 of the Convention), prohibition of slavery (Art. 2 of the Convention), prohibition of discrimination (Art. 14 of the Convention), the right to property (Article 1 of Protocol No. 1), the right to education (Article 2 of

Protocol No. 1), the right to liberty and security (Article 5 of the Convention), the right to a fair trial (Article 6 of the Convention), no punishment without law (Article 7 of the Convention), etc. [1].

Ukrainian law enforcement agencies and human rights organizations from around the world have collaborated to create multiple electronic resources for collecting information on war crimes. According to the General Prosecutor's Office of Ukraine, digital information on approximately 70,000 such crimes [2] has been recorded as of December 2022, which will subsequently help not only to establish that these crimes were indeed committed but also to find out a connection between crimes and specific individuals (criminals) and charge them with reasonable accusations as well as ensure that they are brought to justice. However, investigators and judges often face difficulties in collecting and evaluating digital evidence due to the lack of its clear definition, as well as the lack of established procedures for its recording and evaluation in Ukrainian legislation. Also, Ukrainian courts sometimes do not recognize digital evidence as admissible, while investigative journalists frequently use developments of EU and US researchers and lawyers in this area. That is, Ukrainian legislation is not adequately keeping pace with the rapid advancements in information technologies, and gaps in legal regulation often require resolution through decisions made by the judiciary.

Analyzing positive experience of digital evidence use within the US judiciary will help to determine directions for overcoming the indicated problems in the Ukrainian judiciary.

Article Purpose

The Research Purpose is to analyze correlation between the concepts of *electronic evidence* and *digital evidence*, clarify the *digital evidence* concept, generalize judicial practice of Ukraine and the USA in order to emphasize problems that arise when using digital evidence in the criminal proceedings of both countries, conduct comparative analysis of Ukrainian legislation and the US one as to the use of digital information in the judiciary, determine ways to increase the efficiency of using digital evidence in Ukrainian criminal justice system. The authors also aim to provide suggestions for improving Ukrainian criminal procedural legislation in terms of studied problems.

Research Methods

To fulfil set goals, 11 court orders, 9 decisions and 25 Resolutions of the Supreme Court of Ukraine (hereinafter referred to as *Ukraine SC*), 18 decisions of local courts of Kharkiv and Kharkiv region, 17 decisions of the Kharkiv Court of Appeal and the Court of Appeal of Kharkiv Region, 12 decisions of the U.S. Court of Appeals and 19 decisions of the US Supreme Court (hereinafter referred to as *the US SC*), posted on relevant official websites, have been studied in this research. What is more, results of analyzing judicial practice of the Kharkiv Court of Appeal on the use of electronic evidence have been studied, positions of the judges of the Criminal Court of Cassation as part of the Supreme Court of Ukraine (hereinafter referred to as *the CCC as part of Ukraine SC*) concerning the problem of admissibility

1 Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) : від 04.11.1950 р.; ратифік. Законом України від 17.07.1997 р. № 475/97-ВР; чинна для України з 11.09.1997 р. (зі змін. та доп.). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (date accessed: 02.02.2023).

2 Офіс Генерального прокурора / Офіц. сайт. URL: https://gp.gov.ua/ (date accessed: 08.02.2023).

of digital evidence have been analyzed, international and national standards for working with digital evidence have been carefully studied (ISO/IEC 27037:2012 [3] and ДСТУ ISO/IEC 27037:2017 [4]), research papers of domestic scientists and individual papers of the Scientific Working Group on Digital Evidence (USA) regarding the efficient use of digital information in court proceedings (in particular, the Berkeley Protocol on Digital Open Source Investigations) [5] (hereinafter referred to as *the Berkeley Protocol*), Guidelines for law enforcement agencies and prosecutors on the use of digital evidence in court (hereinafter referred to as *the Guidelines on Digital Evidence Use*) etc.). The analysis also includes the rules of domestic legislation (in particular, the Criminal Procedural Code of Ukraine) and the US Federal Rules of Evidence (hereinafter referred to as *FRE USA*) [6] on the use of digital evidence in criminal proceedings.

Methods of theoretical analysis and synthesis as well as scientific papers by both foreign and domestic researchers have been summarized to study the content of legal rules and concepts contained in legal regulations and court decisions. Individual issues required application of systems analysis method (primarily to clarify problems of assessing veracity of digital evidence in Ukraine and the USA and to determine ways to overcome them in Ukraine).

The formal and legal analysis of the legislation of Ukraine and the USA regarding the use of electronic (digital) evidence while court proceedings enabled to identify inherent deficiencies of legal acts and to provide suggestions for improving legal regulation (in particular, concerning improvement of efficiency of digital evidence use in criminal proceedings). With the help of comparative legal method, experience of using digital evidence in criminal proceedings in Ukraine and the USA has been studied. The solution of research tasks was also facilitated by application of special methods of cognition: formal-logical (to typify the grounds for recognizing digital evidence as inadmissible), functional (to establish dependence of efficiency of digital evidence use in court proceedings on the quality of its recording), etc.

Analysis of Essential Researches and Publications

In 2012, a special international standard ISO / IEC 27037:2012 [7] was adopted containing guidelines for working with digital evidence. By complying with this

3 ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (date accessed: 07.02.2023).

4 ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) : прийнято наказом ДП «УкрНДНЦ» від 06.12.2017 р. № 400. [Чинний від 01.01.2019]. Київ, 2018. 31 с. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (date accessed: 07.02.2023).

5 Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних / Управлін. Верховн. комісара ООН з прав людини та Центру з прав людини Каліфорн. ун-ту в Берклі, Юрид. шк., 2020. 119 с. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (date accessed: 11.02.2023).

6 Federal Rules of Evidence (FRE). Dec 1, 2020 / Legal Informational Institute. URL: https://www.law.cornell.edu/rules/fre (date accessed: 05.02.2023).

7 ISO / IEC 27037:2012. URL: https://www.iso.org/standard/44381.html (date accessed: 07.02.2023).

standard, investigative journalists of the *Bellingcat* Internet-edition based on the analysis of digital information (telephone conversations, video recordings, satellite images, etc.) established that specific military service members of the Russian Federation were involved in the passenger Boeing-777 MH17. The national standard of Ukraine ДСТУ ISO / IEC 27037:2017 [8] is the only official document in Ukraine that is applicable to digital evidence. It sets out guidelines for identification, collection, acquisition and preservation of digital evidence; however, these guidelines have not been legislated yet.

In 2020, The Office of the United Nations High Commissioner for Human Rights of Human Rights Center of the University of California, Berkeley presented a *Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law* including standards and methodological approaches to *"collection, preservation and analysis of publicly available information that can be presented as evidence in criminal proceedings"* [9]. *The Berkeley Protocol outlines the algorithms for searching, accumulating, analyzing and saving digital information from public sources in conformity with the principles of objectivity, competence, accountability, compliance with legislation, security, accuracy, independence, transparency, respect for human rights, etc. The authors of the Berkeley Protocol provide recommendations for determining boundaries of a task to be solved in order to save time and ensure the safety of witnesses and victims, as well as to protect hardware and software.*

Individual issues of using electronic (digital) evidence in criminal proceedings have been studied by the following domestic researchers: M. Hutsaliuk, Yu. Orlov, S. Stolitnii, V. Khakhanovskyi, D. Tsekhan, V. Shevchuk, V. Shepitko, and others. Employees of the U.S. National Institute of Justice (Shon E. Hudison, Robert K. Devis, Brian A. Jackson, Hari S. Kesler, Martin Novak, etc.) cite research findings on identification and prioritization of criminal justice needs associated with collection, management, analysis and use of digital evidence in their research papers. Despite a substantial number of published papers on the problems of using digital evidence in court proceedings, certain issues necessitate subsequent research. Specifically, the issues of legislative consolidation of the digital evidence concept, procedural regulation of its seizure, recording and storage, considering the US experience, remain unresolved.

Main Content Presentation

Current tasks of digital forensics are the search and analysis of digital traces, data analysis (in particular, metadata [10]), collection of evidentiary information in the digital environment. The most complex and extensive tasks are publicly available search and analysis of potential evidence sources: a wide range of publicly available video and audio recordings, photos and satellite images, texts, reports, posts in social media. Electronic devices are a repository of general and personal information, digital information about various events and phenomena, individual persons' actions, etc. Since modern phones are multi-functional (making and receiving calls, phone book and voice recorder, photo and video camera, creating and editing text

8 ДСТУ ISO / IEC 27037:2017. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (date accessed: 07.02.2023).

9 Протокол Берклі … . С. 6. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (date accessed: 11.02.2023).

10 Metadata is data characterizing or explaining other data.

files and messages, Internet search and cloud storage use, e-mail and social media, messengers and communication services etc.), they store digital traces of using these functions and are a kind of personal information archives. Such information can become a component of the evidential base only if it is identified, seized, researched and procedurally consolidated with respect for human rights and taking into account personal data protection.

Researchers in criminal law field use the terms *electronic* and *digital* evidence interchangeably, although the terms are not identical. At present, digital devices have completely replaced analog devices, and the difference between analog and digital information is that analog information is continuous, while digital information is discrete. We should agree with N. Zozulia's viewpoint that the *digital evidence* term is more accurate and *"better reflects the cybernetic aspect of information transmission, processing and preservation in view of the processes of information transformation using a binary (binary) code,"* and *"devices and machines processing and saving digital information should be called electronic"* [11]. To be more precise, evidence is *"factual data obtained from proper sources, and their material basis is not the source itself, but an artificially created corresponding procedural medium. <...> Evidence is a unity of factual data and their procedural media"* [12].

D. M. Tsekhan understands digital evidence as *"factual data presented in digital (discrete) format and recorded on any type of medium and that become accessible for human perception after computer processing"* [13]. This definition needs clarification. In particular, not all media are capable of storing information in digital format (paper and magnetic tape are also information carriers). Also, decoding and researching some types of digital information do not require a computer, but specialized electronic devices with specific software (for example, for viewing records of flight recorders). Therefore, ***digital evidence*** *should be considered factual data which are presented as a binary code and contain information that is significant for objective case resolution.*

Unlike the Civil Procedure Code of Ukraine (Art. 100) [14], Commercial and Procedural Code of Ukraine (Art.

11 Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства. *Українське право*. 08.05.2018. URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva (date accessed: 02.02.2023).

12 Тертишник В. М. Кримінальний процес України. Загальна частина : підручник. Академічне видання. Київ, 2014. С. 288. URL: https://rd.ua/storage/lessons/434/512%D0%A2%D0%B5%D1%80%D1%82%D0%B8%D1%88%D0%BD%D0%B8%D0%BA%20%D0%92.%20%D0%9C.%20-%20%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%-D1%8C%D0%BD%D0%B8%D0%B8%CC%86%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%20%D0%A3%D0%BA%D1%80%D0%B0%D1%96%CC%88%D0%BD%D0%B8.%20%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%20%D1%87%D0%B0%D1%81%D1%82%D0%B8%D0%BD%D0%B0,%20%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA.%20%D0%90%D0%BA%D0%B0%D0%B4%D0%B5%D0%BC%D1%96%D1%87%D0%BD%D0%B5%20%D0%B2%D0%B8%D0%B4%D0%B0%D0%BD%D0%BD%D1%8F.pdf (date accessed: 02.02.2023).

13 Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 257. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58 (date accessed: 02.02.2023).

14 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: 02.02.2023).

96) [15] and the Code of Administrative Proceedings of Ukraine (Art. 99) [16], the Criminal Procedural Code does not include provisions on electronic (digital) evidence. Information in digital format is considered to be documents or electronic documents which are recognized as procedural sources of evidence (Part 2 of Article 84) [17]. The documents also include *"materials of photography, sound recording, video recording and other media (including computer data)"* (clause 1, Part 2, Article 99 of the Criminal Procedural Code) [18] and *"data media on which procedural actions have been fixed by technical means"* (clause 3, Part 2, Article 99 of the Criminal Procedural Code) [19]. The original of an electronic document is indicated as *"its representation, which is given the same weight as the document itself"* (Part 3, Article 99 of the Criminal Procedural Code) [20]. A duplicate of the document and copies of information in digital format produced by the investigator, prosecutor with specialist's involvement may be found by court to be the original of the document (Part 4, Article 99 of the Criminal Procedural Code) [21].

Documents as digital evidence are not only text documents, figures, photographs, audio and video recordings, but also computer programs and databases. They differ both in form and content, as well as in their source of origin. Some documents are created by a person, others emerge as a result of operation of electronic devices and systems and do not depend on human actions (information from navigation and monitoring systems, electronic digital signature, information from mobile service providers, network technological information, etc.).

Art. 237 of the Criminal Procedural Code regulates computer data examination, which *"is carried out by the investigator, prosecutor by reflecting in the examination protocol the information they contain in a way suitable for perceiving their content (using electronic means, photography, video recording, shooting and/or video recording of the screen etc. or on paper)"* (clause 2 Part 2) [22]. However, there is a lack of a mandatory list of information for recording digital evidence.

In recent years, digital evidence has gained significance as a research subject in Ukrainian courts; however, when considering cases in courts of various jurisdictions, judges encounter certain challenges in recognizing information in digital format as admissible and veracious evidence. Lawyers often file motions about inadmissibility of digital evidence in view of the fact that information was first copied from the phone to a computer and only later to an optical disc, which was further submitted to the court as procedural evidence medium. Defense counsels hold a belief that such a copy does not correspond

15 Господарський процесуальний кодекс України від 06.11.1991 р. № 1798-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text (date accessed: 02.02.2023).
16 Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text (date accessed: 02.02.2023).
17 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: 02.02.2023).
18 Ibid.
19 Ibid.
20 Ibid.
21 Ibid.
22 Кримінальний процесуальний кодекс ... . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 02.02.2023).

to the original because the file format changes when the media is changed [23]. This statement is misleading since one of the main features of information in digital format is that all its copies recorded on different media maintain identity with the original (a complete correspondence in all respects, including the file format). Despite this, in its ruling in case No. 397/2588/13-k, the Supreme Court of Ukraine upheld the decision made by the courts of the first and appellate instances and recognized the video and audio recording of the act of bribing a judge in his office, made during crime detection and investigation operations, as inadmissible evidence. The court ruled that records are copies and, subsequently, recognized protocols on the implementation of covert investigation (search) operations (hereinafter referred to as CISOs) as inadmissible evidence, which annex is this digital evidence, recording inspection protocol, where the investigator provided transcript of conversations about giving bribes, conclusions of three forensic examinations, as they are derived from this record. The accused was acquitted [24].

In the Resolution of the Supreme Court of Ukraine dated December 18, 2019, in case No. 588/1199/16-k, the court declared inadmissible the protocol of audio and video monitoring of a person along with its annexes, media inspection protocol obtained during CISOs and the Resolution on their recognition as physical evidence. The grounds for such a decision was the motion of the defense counsel on non-issuance of the mandate to conduct CISOs by the accused in accordance with Art. 290 of the Criminal Procedural Code, in the course of which a video recording was made. This time, the official suspected of bribery was also acquitted [25].

The Supreme Court of Ukraine, in its Resolution in case No. 426/12149/17 on narcotic drugs, emphasized that *"the lack of original technical data carriers in the criminal proceedings materials, on which the procedural actions were recorded, serves as a basis to deem such evidence (video phonograms) inadmissible, according to the practice of the Supreme Court <...> the mandatory presence of original video recordings made during covert investigative (search) operations, in particular, control over crime commission, is intended to provide possibility of expertly establishing the veracity of information displayed in a video recording"* [26].

In case No. 675/1046/18 (Chapter 3 of Article 369 of the Criminal Code of Ukraine: providing an improper advantage to an official [27]) the Supreme Court of Ukraine, on the contrary, refused the defense's request to appoint a video and audio examination. The examination purpose was to assess whether the digital video recording of CISOs had been edited or altered. The Supreme Court independently reviewed and examined the video recording and

23 Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. 28.10.2021 / ВСУ. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/ (date accessed: 03.02.2023).

24 Ухвала ВСУ від 29.05.2018 р. Справа № 397/2588/13-к. Провадження № 51-3650км18 / Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/74475933 (date accessed: 05.01.2023).

25 Постанова ВСУ від 18.12.2019 р. Справа № 588/1199/16-к. Провадження № 51-3127км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/86505861 (date accessed: 06.01.2023).

26 Постанова ВСУ від 17.03.2020 р. Справа № 426/12149/17. Провадження № 51-112км20 / ЄДРСР. URL: http://www.reyestr.court.gov.ua/Review/88401663 (date accessed: 05.01.2023).

27 Кримінальний кодекс України від 05.04.2001 р. № 2341- III (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (date accessed: 02.02.2023).

found no grounds for examination appointment [28].

When considering bribery cases, in individual cases, the Supreme Court of Ukraine *"does not perceive any obstacles to presenting duplicates of protocols of procedural actions, as well as materials such as photography, sound recordings, video recordings, and other media (including electronic formats) that have been produced by the investigator or prosecutor with specialist's involvement. The court views these duplicates as the original documents"* [29].

In the case of abuse of power during forceful dispersal of protest actions by police, the Supreme Court of Ukraine recognized digital video recording of events as admissible evidence even without specifying who carried it out and how they were involved in criminal proceedings. This evidence became the basis for the official's conviction [30].

The Supreme Court of Ukraine also accepted copies of digital video recordings of a robbery at a pawnshop which was captured from CCTV camera (on DVD discs) as admissible evidence, although the Resolution does not specify how the investigation obtained copies of these recordings. Forensic examination conclusion as to identification of a person based on this video recording became the basis for issuing the guilty verdict [31]. In another robbery case, the court also a copy of the CCTV footage (on a DWD-RW disc), voluntarily submitted by an employee of a pawnshop, recognized as admissible evidence, despite the defense's objection. The court stressed that case files contain a request for video recording issuance, a cover letter submitted with a DVD disc and a protocol of its inspection, by which the disc was recognized as physical evidence (in the court's view: *"in the manner enshrined by the Criminal Procedure Code of Ukraine")* [32].

In case of illegal drug trafficking, civilians handed over a video recording showing crime commission to investigation. The investigator drew up a video inspection protocol, showing the video to the accused, his defense counsel and attesting witnesses. This procedural implementation helped the court to recognize the video recording as admissible evidence [33].

In one of the cases, the court recognized the video recording from two CCTV cameras as applicable evidence in a case involving violation of traffic safety rules, although technical characteristics of devices used to capture video recordings, their certification and the procedure for transferring information to the server were not established [34]. In another case, the court

28 Постанова ВСУ від 18.12.2019 р. Справа № 675/1046/18. Провадження № 51-3942км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/86505906 (date accessed: 05.01.2023).

29 E.g.: Постанова ВСУ від 15.01.2020 р. Справа № 161/5306/16-к. Провадження № 51-3498км19 / ЄДРСР. URL: http://www.reyestr.court.gov.ua/Review/87053591 (date accessed: 03.01.2023).

30 Постанова ВСУ від 20.02.2018 р. Справа № 750/4139/15-к. Провадження № 51-36км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72460327 (date accessed: 04.01.2023).

31 Постанова ВСУ від 27.02.2018 р. Справа № 759/8643/16-к. Провадження № 51-1031км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72642168 (date accessed: 03.01.2023).

32 Постанова ВСУ від 02.10.2019 р. Справа № 159/2377/17. Провадження № 51-4466км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/84788575 (date accessed: 03.01.2023).

33 Постанова ВСУ від 15.03.2018 р. Справа № 760/11451/15-к. Провадження № 51-727км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72909394 (date accessed: 22.12.2022).

34 Ухвала ВСУ від 25.03.2019 р. Справа № 754/2178/18. Провадження № 51-920ск19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/80716282 (date accessed: 27.12.2022).

recognized the copy of the CCTV camera recording and the automotive examination conducted on its basis as inadmissible evidence due to the fact that *"it is impossible to determine technological properties of the videogram from the copy in the absence of the original and the original device"* and the expert conclusion *"relies on inaccurate data obtained from video recording copies"* [35]

In criminal proceedings on theft, the court recognized a copy (on a DVD) of the video recording of an event as inadmissible evidence in connection with fact that investigation received it from the victim without the investigating judge's ruling [36]. The court did not recognize a copy of the theft video recording from a CCTV camera as admissible evidence in view of the fact that there is no request for discovery of this video recording and information about a person who received it in case files of criminal proceedings[37]. The court also recognized as inadmissible evidence a copy of a video recording from a CCTV camera on another theft since it is not an original [38].

That is, under the same conditions, judges adopted contradictory decisions until recently. In individual cases, they recognized copies of digital records as permissible evidence, in others: inadmissible (especially regarding corruption crimes). However, lately judges have been trying to raise their level of awareness as to technical characteristics of digital evidence in order to avoid judicial errors. In particular, the judge of the Cassation Criminal Court of Ukrainian Supreme Court, Nadiia Stefaniv, highlights that *"judges are responsible for pursuing their own expertise in electronic evidence use. It's the judge's personal duty to stay informed about the latest news about documents and standards in order to apply them correctly within the framework of current procedural legislation."* [39]

Recently, judges of all jurisdictions have been trying to adhere to the Guidelines of the Committee of Ministers of the Council of Europe on Electronic Evidence in Civil and Administrative Proceedings [40]. Courts in Ukraine are increasingly rejecting motions from the defense counsel that seek to challenge the admissibility and veracity of copies of digital evidence, its inspection protocols, and forensic expert conclusions during consideration of cases across various categories. Judges carefully

35 Постанова ВСУ від 31.10.2019 р. Справа № 404/700/17. Провадження № 51-4451км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/85390646 (date accessed: 28.12.2022).

36 Постанова ВСУ від 12.04.2018 р. Справа № 366/1400/15-к. Провадження № 51-1528км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/73438093 (date accessed: 21.12.2022).

37 Постанова ВСУ від 04.09.2019 р. Справа № 369/3713/18. Провадження № 51-3536км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/84120855 (date accessed: 22.12.2022).

38 Постанова ВСУ від 15.11.2018 р. Справа № 140/2668/15-к. Провадження № 51-624км17 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/78110946 (date accessed: 23.12.2022).

39 Стефанів Н. Матеріальний носій — лише спосіб збереження інформації, який має значення тільки тоді, коли Е-документ виступає речовим доказом / Інформагентство «ADVOKAT POST». 02.11.2021. URL: https://advokatpost.com/materialnyj-nosij-lyshe-sposib-zberezhennia-informatsii-iakyj-maie-znachennia-tilky-todi-koly-e-dokument-vystupaie-rechovym-dokazom-suddia-stefaniv/ (date accessed: 02.02.2023).

40 Керівні принципи Комітету Міністрів Ради Європи CM(2018)169-add1final щодо електронних доказів у цивільних та адміністративних провадженнях : прийнято Ком. Міністр. 30.01.2019 р. на 1335-му засід. заст. міністр. / Мін'юст України. URL: https://minjust.gov.ua/m/rekomendatsii-parlamentskoi-asamblei-ta-komitetu-ministriv-radi-evropi (date accessed: 12.02.2023).

assess veracity of the forensic expert's findings and examine digital evidence directly (including information from phones) [41].

Court decisions of the last 2–3 years differ from previous ones in a more detailed consideration and explanation of digital evidence technical characteristics, which provides more chances for recognizing a copy of information in digital format as admissible evidence. In particular, in case No. 677/2040/16-к, the court rejected the cassation appeal of the defense counsel concerning non-recognition of copies of video recordings as admissible evidence and emphasized:

"According to Art. 7 of the Law of Ukraine No. 851-IV 'On Electronic Documents and Electronic Documents Circulation' dated May 22, 2003, each of the electronic copies shall be considered the original electronic document in a case of storing information on several electronic media.

A physical medium is only a way of storing information, which is important only when an electronic document is physical evidence. The main feature of an electronic document is the absence of a strict linkage to a specific material medium. The same electronic document (video recording) can exist on different media. All copies of an electronic document that are identical in their content can be viewed as originals and differ from each other only by the time and date of creation" [42].

The same decision includes the Resolution of the Cassation Criminal Court of Ukrainian Supreme Court in case No. 236/4268/18 dated 25.01.2021 [43] and the Order of the Supreme Court of Ukraine in case No. 756/8124/19 dated 19.08.2021 [44], in which the court rejected appeals of defense counsels on inadmissibility of digital information copies as evidence.

According to the results of practice generalization of cassation court on the issues of conducting and evaluating results of CISOs in criminal proceedings, it has been established that the reasons why digital audio and video recordings made during their conduct are not generally recognized as admissible evidence are as follows: providing copies of digital information to the court instead of the originals; conduct of CISOs by employees of operational subdivision without authorization from the investigator, the prosecutor and without the investigating judge's decision; non-issuance of the mandate to conduct CISOs to the defense counsel in conformity with Art. 290 of the Criminal Procedural Code; lack of procedural implementation of the investigator's or prosecutor's decision to involve "another person" in carrying out CISOs, non-fulfilment of requirements

41 E.g.: Вирок Дзержинського райсуду м. Харкова від 21.06.2019 р. Справа № 638/5928/18. Провадження № 1-кп/638/585/19. URL: https://zakononline.com.ua/court-decisions/show/82552131 (date accessed: 12.02.2023) ; Вирок Вищ. антикорупц. суду від 17.02.2022 р. Справа № 991/4996/20. Провадження № 1-кп/991/53/20. URL: http://iplex.com.ua/doc.php?regnum=103409303&red=1000033ab78a5efaf99e232b33e4b495c626d6&d=5#:~:text=%D0%B7%D0%B0%20%D1%87.,%D0%B2%D0%B8%D0%BA%D0%BE%D (date accessed: 22.02.2022).

42 Постанова ККС ВСУ від 22.10.2020 р. Справа № 677/2040/16-к. Провадження № 51-5738км19. URL: http://iplex.com.ua/doc.php?regnum=92458395&red=1000035e35a331e82f61d9818795df8ecd0762&d=5 (date accessed: 22.12.2022).

43 Постанова ККС ВСУ від 25.01.2021 р. Справа № 236/4268/18. Провадження № 51-3124км20. URL: http://iplex.com.ua/doc.php?regnum=94905297&red=10000347f1960a9ea9dcf00a1e2414ca33651f&d=5 (date accessed: 22.12.2022).

44 Ухвала ККС ВСУ від 19.08.2021 р. Справа № 756/8124/19. Провадження № 51-601ск21. URL: http://iplex.com.ua/doc.php?regnum=94874011&red=1000037c6dddd0bd0c253b026e82724e953e47&d=5 (date accessed: 22.12.2022).

outlined in Section 4, Article 271 of the Civil Procedural Code concerning the immediate drafting of a protocol based on the results of crime control in the presence of a person who was subject to CISOs, immediately after openly recording the final stage of crime control and his/her subsequent actual detention [45].

The use of digital evidence is less "regulated" in US law. Even at the end of the 20th century digital evidence in the USA was treated as a category of evidence due to peculiarities of its creation, storage, detection, research and evaluation of its admissibility and veracity. In 1995, law enforcement agencies of the USA, Canada, and some European countries jointly created the *International Organization on Computer Evidence (IOCE)* [46], and in 1998, the *Scientific Working Group on Digital Evidence* (SWGDE) [47] that brings together law enforcement, academic, and commercial organizations actively engaged in the field of digital forensics to develop cross-disciplinary guidelines and standards for the recovery, preservation, and examination of digital evidence. The SWGDE group has developed basic standards and principles for working with digital evidence ensuring relevance and admissibility of this evidence in court proceedings. Particular attention was drawn to procedural recording of all operations with such evidence, ensuring access to it by all participants in procedure, allowing only qualified IT specialists to examine digital evidence in order to maintain its integrity [48].

The Federal Rules of Evidence of the USA (FRE USA) [49], which were adopted in 1975 and which regulate the work with evidence in civil and criminal proceedings in US federal courts, had been repeatedly amended and supplemented to address digital evidence, given the standards developed by researchers and methodological approaches to collection, preservation and analysis of digital evidence [50] as well as recent court decisions involving digital evidence. Specifically, Clauses 13 and 14 have been added to Rule 902 [51] in *FRE USA*. These clauses outline the procedure for determining the authenticity of certain digital evidence (excluding witness statements) and providing the parties involved in a case with the opportunity to verify (challenge) the veracity of certified records generated using electronic systems and data, as well as copied from electronic devices or

45 Узагальнення практики суду касаційної інстанції з питань проведення та оцінювання результатів НСРД у кримінальному провадженні (*оновлено*). Тренінговий центр прокурорів України. 2021. С. 51. URL: https://ptcu.gp.gov.ua/wp-content/uploads/2021/11/uzagalnennya_praktyky_sudu_po_nsrd_z_qrkodamy_1.pdf (date accessed: 12.02.2023).

46 International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648 (date accessed: 02.02.2023).

47 Scientific Working Group on Digital Evidence (SWGDE). URL: https://www.swgde.org/ (date accessed: 12.02.2023).

48 Kessler G. C. Judges' Awareness, Understanding, and Application of Digital Evidence. *Journal of Digital Forensics, Security and Law*. 2011. Vol. 6. No. 1. Art. 4. Pp. 54—72. DOI: 10.15394/jdfsl.2011.1088 (date accessed: 12.02.2023).

49 Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre (date accessed: 05.02.2023).

50 Протокол Берклі … . URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (date accessed: 11.02.2023).

51 Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre (date accessed: 05.02.2023).

mediums. Clarifications to these clauses further explain that when it comes to challenging the veracity of digital evidence, technical information obtained by involving a forensic expert or a specialist from the IT industry may be necessary. Additionally, Rule 702 allows for the engagement of forensic experts who possess not only knowledge and skills in technology and science, but also who are experienced in specific fields (doctors, bankers, architects, physicists, etc.) [52]. At the same time, expert testimony and conclusions must be veracious (meet the *Daubert standard* [53]) and admissible under the principles of Rule 104(a) [54] of *FRE USA*.

US courts ascertain authenticity (accuracy, veracity) of digital evidence in compliance with Rule 901 [55] of FRE USA. In particular, the court checks the information to ascertain whether the digital evidence *"was obtained from a specific computer or other electronic device"* or *"whether a complete and exact copy of it was recorded and has remained unchanged since the moment of recording."* [56] Veracity of a large array of data in digital format often necessitates the examination of a complete copy of the data from the electronic device, which is created by a forensic expert or specialist specifically engaged for this purpose. Such a copy preserves the logical structure of information storage, including even deleted files. This enables to carry out additional examination as well as re-examination later [57].

Authenticity of a separate file, its part or a group of files is checked using their hash code (a unique code for each such object). The same hash code values for the original file (especially from an exact disk copy) and the file being checked testify to their identity [58]. To compare files by hash code, a forensic expert or an IT specialist is involved, and veracity of the expert's testimony or conclusions is checked according to the *Daubert standard* (Rule 702).

The court can ascertain the authenticity of digital evidence by relying on witnesses' statements, even in the lack of relevant data in case files or protocols [59]. Such witnesses, in particular, can be law enforcement agencies who seized electronic devices or

52 Federal Rules of Evidence ... . URL: https://www.law.cornell.edu/rules/fre (date accessed: 05.02.2023).

53 *Daubert standard* was developed on the basis of three legal cases — Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U. S. 579 (1993). URL: https://supreme.justia.com/cases/federal/us/509/579/ (date accessed: 07.01.2023); General Electric Co. v. Joiner, 522 U. S. 136 (1997). URL: https://supreme.justia.com/cases/federal/us/522/136/ (date accessed: 07.01.2023) and Kumho Tire Co. v. Carmichael, 526 U. S. 137 (1999). URL: https://supreme.justia.com/cases/federal/us/526/137/ (date accessed: 07.01.2023) is intended to establish veracity of the expert's testimony and conclusions.

54 Federal Rules of Evidence ... . URL: https://www.law.cornell.edu/rules/fre (date accessed: 05.02.2023).

55 Ibid.

56 United States v. Budziak, 697 F.3d 1105 (2012) / Caselaw Access Project. URL: https://cite.case.law/f3d/697/1105/ (date accessed: 07.01.2023).

57 United States v. Burdulis, 753 F.3d 255 (1st Cir. 2014). URL: https://casetext.com/case/united-states-v-burdulis (date accessed: 05.01.2023).

58 United States v. R. Burke. 633 F.3d 984 (10th Cir. 2011). URL: https://casetext.com/case/united-states-v-r-burke (date accessed: 03.01.2023).

59 United States v. Bush. 727 F.3d 1308 (11th Cir. 2013). URL: https://casetext.com/case/united-states-v-bush-30 (date accessed: 02.01.2023).

recorded (copied) information in digital format [60].

Researchers from the US National Institute of Justice underline the importance of detailed recording of authentication processes (authenticity determination) and all other actions taken with digital evidence (seizure with a detailed description of an electronic device, indicating its owner and persons who had access to it, methods and means of information seizure, copying on an external medium, research with outline of methods and means involved, etc.). This enables to prove the fact of storing information in its original format [61]. The prosecution has an obligation to timely disclose digital evidence to the defense counsel otherwise the court may return materials for further investigation.

In order to prevent mistakes when working with digital evidence, US police academies have expanded the digital evidence curriculum based on guidelines for working with this kind of evidence [62]. Authors of Guidelines stress that digital evidence is useless without determining its veracity and detailing the "chain of custody" over the evidence, so they developed an algorithm for recording actions taken with digital evidence and listed issues that should be noted in protocols [63].

Authors of the guidelines place particular emphasis on the following issues:

- the need to enhance advanced training for investigators and prosecutors on technical aspects of digital evidence; [64]
- advice on verifying e-mails authenticity; [65]
- procedural significance of information printouts from a computer, explanation of the concepts of *original*, *copy* and *duplicate* related to digital information; [66]
- procedure for determining authenticity of digital photographs, etc. [67]

Until 2014, US law enforcement agencies would seize individuals' phones during their arrest and examine information stored on them. However, the US SC ruled that searching and seizing digital information from a phone without a warrant contradicts the US Constitution and violates citizens' rights [68]. In addition, the situation with obtaining information from mobile phones was complicated by the

60 Goodison S. E., Davis R. C., Jackson B. A. Digital Evidence and the U. S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. RAND Corporation, 2015. P. 11. URL: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf (date accessed: 25.12.2022).

61 Ibid. P. 13.

62 Hagy D. W. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. U. S. Department of Justice. Office of Justice Programs. National Institute of Justice. Washington, Jan 2007. 81 p. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors (date accessed: 23.12.2022).

63 Ibid. Pp. 15—17.

64 Ibid. P. 23.

65 Ibid. P. 31.

66 Ibid. P. 33.

67 Ibid. P. 50.

68 Riley v. California, 573 U. S. 373 (2014). URL: https://supreme.justia.com/cases/federal/us/573/373/ (date accessed: 23.12.2022).

refusal of representatives from *Apple* and *Google* to grant access to user information even at the official requests from law enforcement agencies. This encourages litigants to focus on digital traces left by mobile devices on the Internet. The task of subjects of proof is to carefully record such digital evidence, analyze its integrity, authenticity and reliability, as well as assess admissibility and veracity.

Researchers from the US National Institute of Justice, by interviewing employees of law enforcement agencies, found that respondents face multiple problems when working with digital evidence. Specifically, they lack expertise in mastering technical characteristics of digital information and understanding the rules for its seizure and storage. Investigators require sets of scientific and technical tools to effectively work with digital evidence, such as Faraday bags, which are used to isolate electronic devices. With the rapid development of technologies of digital devices and methods of extracting digital information from them, significant difficulties arise when evaluating digital evidence by the criterion of veracity (its compliance with the *Daubert standard*) [69]. Researchers argue that prosecutors (due to insufficient knowledge of the digital evidence technical characteristics) try to seize more information than needed and overload forensic experts with unnecessary work, and some judges lack expertise in methods of processing and seizing digital evidence. Police officers and detectives often lack knowledge on how to properly record and store digital evidence; whereas, forensic experts require up-to-date research methodologies. We propose to solve these problems by developing guidelines for working with digital evidence (separately for each department) and improving qualifications of all employees of law enforcement agencies who handle digital evidence in their work [70].

Consequently, when working with digital evidence, investigators, judges, prosecutors, security officers and forensic experts in the United States face similar challenges when working with digital evidence as their counterparts at all levels of Ukrainian criminal justice. At the same time, in contrast to the Criminal Procedural Code, FRE USA contains an extensive system of amendments that relate to the procedure for seizure of digital evidence, its recording, storage, authentication (authenticity verification), evaluation of admissibility and veracity, etc. Veracity of digital evidence, scientific testimonies of specialists and expert opinions about it in the USA is determined according to the *Daubert standard*. When handling digital evidence, US criminal justice officials at all levels are guided by the Berkeley Protocol and Guidelines for the Use of Digital Evidence.

The Criminal Procedural Code does not contain a specific definition for the *digital evidence* term, nor does it offer a comprehensive procedure outlining the steps for its seizure, examination, documentation, and storage. This may lead to errors when working with digital information and to not recognizing it as admissible and veracious evidence in court.

The above demonstrates that the US judiciary has more opportunities for efficient application of digital evidence in contrast to the Ukrainian judiciary.

69 Goodison S. E., Davis R. C., Jackson B. A. Op. cit. P. 16. URL: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf (date accessed: 21.12.2022).

70 Ibid. P. 25.

Conclusions

Currently, analog devices have been completely replaced by digital ones (that is, continuous information has been replaced by discrete). Therefore, the *digital evidence* term is more accurate and better reflects the essence of information in digital format (in the form of a binary code); whereas, devices, tools and machines that create, transmit, process and store digital information should be called electronic. ***Digital evidence*** *should be considered factual data that is presented in the form of binary code and contain information that is essential for objective case resolution.*

Investigators, judges, prosecutors, employees of crime detection and investigation authorities and forensic experts of Ukraine and the USA encounter certain challenges when handling digital evidence due to the rapid development and change in digital device technologies and, as a consequence, changes in technologies for detecting, seizing, recording and researching digital information.

Courts of Ukrainian criminal jurisdiction oftentimes take conflicting decisions as to recognition of digital information as admissible evidence under the same conditions. Reasons for not recognizing digital information as admissible evidence by the court: providing the court with a copy of digital information instead of the original; conducting CISOs and obtaining digital information without a mandate from the investigator, prosecutor and without the investigating judge's decision; failure to disclose to the defense counsel of the mandate to conduct CISOs; lack of procedural implementation of the investigator's or prosecutor's decision to involve "another person" in CISOs, etc.

The US judiciary has more options for efficient application of digital evidence than the Ukrainian judiciary. Legal regulations and methodological literature on digital evidence use (used in the US judiciary), are a worthy reference point for reforming Ukrainian legislation and developing methodological guidelines on outlined issues.

As it depends on competence and accurate decision of employees within law enforcement agencies (investigators, judges, prosecutors, operative officers) whether a particular piece of digital evidence will play a crucial role in solving a specific case, these employees should know the basic technological characteristics of digital devices and digital information. Therefore, appropriate methodological and reference literature should be developed and added to professional development programs separately for each category of such employees.

It is advisable to supplement the Criminal Procedural Code with the following novel provisions: adding the definition for the digital evidence concept and its procedural media; differentiating the concepts of *electronic evidence* and *digital evidence*; adding a detailed procedure for the seizure of digital information, its examination, recording and storage (with a list of mandatory information on digital evidence which should be procedurally established); the procedure for assessing admissibility and veracity of digital evidence and the expert conclusion according to certain criteria.

Проблеми використання цифрових доказів у кримінальному судочинстві України та США

Галина Авдєєва,
Ельжбета Живуцька-Козловська

Розглянуто актуальні проблеми використання цифрових доказів у кримінальному судочинстві України та США й надано пропозиції щодо їх розв'язання, для

чого застосовано методи теоретичного аналізу й синтезу, формально-юридичного аналізу, порівняльно-правовий метод, спеціальні методи пізнання. Розмежовано поняття «електронний доказ» і «цифровий доказ». Аналіз 64 рішень українських судів кримінальної юрисдикції та 31 рішення Апеляційного й Верховного Суду США показав, що визнання допустимими та достовірними доказами інформації у цифровій формі спричиняє певні труднощі. Досвід судочинства США може стати в пригоді реформуванню законодавства України й розробленню методичних рекомендацій із використання цифрових доказів. Запропоновано доповнити Кримінальний процесуальний кодекс України нормами, які б містили визначення поняття «цифрові докази» і їх процесуальних носіїв; розмежування понять «електронний доказ» і «цифровий доказ»; докладний порядок вилучення цифрової інформації, її огляду, фіксування і зберігання (із зазначенням переліку обов'язкової інформації щодо цифрових доказів, яку має бути процесуально закріплено); алгоритм оцінювання достовірності цифрового доказу й висновку експерта за певними критеріями. З'ясовано, що швидка зміна технологій із виявлення, вилучення, фіксування й дослідження цифрової інформації спричиняє певні труднощі для слідчих, суддів, прокурорів і співробітників оперативно-розшукових органів України. Поліпшити ефективність використання цифрових доказів у судочинстві рекомендовано шляхом розроблення настанов щодо роботи із ними та відповідного підвищення кваліфікації співробітників правозастосовних органів.

***Ключові слова**: цифрові докази; електронні докази; електронні пристрої; допустимість доказів; джерела доказів; цифрова інформація; кримінальне провадження; фіксація доказів.*

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 study design, data collection and analysis, decision to publish, or manuscript preparation.
Participants
Authors contributed solely to the 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 declare no conflict of interest.

References

Federal Rules of Evidence (FRE). Dec 1, 2020 / Legal Informational Institute. URL: https://www.law.cornell.edu/rules/fre.

International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648.

ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html.

Hagy, D. W. (2007). Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. U. S. Department of Justice. Office of Justice Programs. National Institute of Justice. Washington. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors.

Kessler, G. C. (2011). Judges' Awareness, Understanding, and Application of Digital Evidence. Journal of Digital Forensics, Security and Law. Vol. 6. No. 1. Art. 4. DOI: 10.15394/jdfsl.2011.1088.

Protokol Berkli z vedennia rozsliduvan z vykorystanniam vidkrytykh tsyfrovykh danykh (2020) [The Berkeley Protocol on Digital Open Source Investigations]/ Upravlin. Verkhovn. komisara OON z prav liudyny ta Tsentru z prav liudyny Kaliforn. un-tu v Berkli, Yuryd. shk. URL: https://

www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf [in Ukrainian].

Scientific Working Group on Digital Evidence (SWGDE). URL: https://www.swgde.org/.

Stefaniv, N. (2021). Materialnyi nosii — lyshe sposib zberezhennia informatsii, yakyi maie znachennia tilky todi, koly E-dokument vystupaie rechovym dokazom [Physical medium is only a way of storing information, which is important only when the E-document acts as physical evidence]/ Informahentstvo «ADVOKAT POST». URL: https://advokatpost.com/materialnyj-nosij-lyshe-sposib-zberezhennia-informatsii-iakyj-maie-znachennia-tilky-todi-koly-e-dokument-vystupaie-rechovym-dokazom-suddia-stefaniv/ [in Ukrainian].

Tertyshnyk, V. M. (2014). Kryminalnyi protses Ukrainy. Zahalna chastyna [Criminal Procedure in Ukraine. General Part]: pidruchnyk. Akademichne vydannia. Kyiv. URL: https://rd.ua/storage/lessons/434/512%D0%A2%D0%B5%D1%80%D1%82%D0%B8%D1%88%D0%BD%D0%B8%D0%BA%20%D0%92.%20%D0%9C.%20-%20%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%-D1%8C%D0%BD%D0%B8%D0%B8%CC%86%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%20%D0%A3%D0%BA%D1%80%D0%B0%D1%96%CC%88%D0%BD%D0%B8.%20%D0%97%D0%B0%D0%B3%D0%B0%D0-%BB%D1%8C%D0%BD%D0%B0%20%D1%87%D0%B0%D1%81%D1%82%D0%B8%D0%BD%D0%B0,%20%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA.%20%D0%90%D0%BA%D0%B0%D0%B4%D0%B5%D0%BC%D1%96%D1%87%D0%BD%D0%B5%20%D0%B2%D0%B8%D0%B4%D0%B0%D0%BD%D0%BD%D1%8F.pdf [in Ukrainian].

Tsekhan, D. M. (2013). Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia [Digital evidence: concepts, characteristics and place in the proof system]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Yurysprudentsiia.* Vyp. 5. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58 [in Ukrainian].

Zozulia, N. (2018). Elektronni chy tsyfrovi dokazy: udoskonalennia zmin do protsesualnoho zakonodavstva [Electronic or digital evidence: improving amendments in procedural legislation]. *Ukrainske pravo.* URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva [in Ukrainian].

Avdeeva, G., Żywucka-Kozlowska, E. (2023). Problems of Using Digital Evidence in Criminal Justice of Ukraine and the USA. *Theory and Practice of Forensic Science and Criminalistics.* Issue 1 (30). Pp. 126—143. DOI: 10.32353/khrife.1.2023.06.