DIGITAL EVIDENCE IN CRIMINAL JUSTICE: CHALLENGES OF UTILIZATION

Demidova Y., Latysh K., Kapustina M.

Introduction.

Our society global digitalization, digital technologies, such as computers, mobile devices, social networks and cloud services, etc., widespread use, including for criminal purposes, has led to a rapid increase in the number of digital traces left behind by various types of criminal offenses. The full-scale invasion of Russia exposed these problems further and became a significant factor in demonstrating the importance of digital evidence in criminal proceedings. Pre-trial investigations in the temporarily occupied territories are carried out mostly remotely, so evidence is collected using remote, mostly digital methods. Both war crimes and other ones leave not only material and ideal traces, which are more traditional for forensics, but also a significant amount of digital traces. These include geolocation data and IP addresses, telephone conversations and other electronic communications records, including email correspondence, audio, video, and photo materials, network traffic, various types of social media activity, and other digital information used to document such activity, as well as data from streaming services. In addition, when investigating cybercrime, "traditional" physical ("paper") evidence may not be available at all. However, there are no tactical and methodological guidelines for the search, collection and analysis of this type of traces, which is unacceptable given the need for further judicial perspective and evaluation of such evidence by the court.

On the one hand, the existence of digital traces simplifies investigations and greatly assists law enforcement agencies in detecting and solving criminal offences. For example, modern hardware, software, and scientific and technological developments provide the means for collecting, analyzing, and interpreting large amounts of digital data, which makes it possible to obtain evidence that used once to be virtually impossible to identify and examine. However, on the other hand, digital information growing use during criminal offenses investigation poses new challenges

and problems for scholars and practitioners that need to be addressed immediately, including: fragmentation of such information use legislative regulation in legal proceedings; uniform approaches lack as to ensuring their reliability and admissibility; the importance of human constitutional rights and freedoms non-violation while obtaining and using such information, etc.

Today, digital evidence-using problems are among the most relevant topics. Certain aspects of them have been subjects of consideration by A.V. Kovalenko, I.O. Krytska, V.V. Muradov, A.V. Skrypnyk, S.M. Stakhivskyi, V.M. Shevchuk, V.Y. Shepitko, M.V. Shepitko, A.V. Shylo, and others. However, due to the rapid development of technology, the legislation and practice of digital evidence using requires constant updating and improvement in order to provide prompt responses to new challenges of our time.

The purpose of the article is to analyze and highlight the problems arising in the course of digital evidence using in criminal proceedings. In particular, digital evidence collecting and examining peculiarities have been analysed, potential shortcomings and problems identified, and the ways and directions for improving their use to ensure a fair and objective trial have been found.

1. Digital information as a possible source of evidence.

A significant amount of valuable information is contained on electronic media and the Internet. At the same time, there exist problems in the legal sphere. Thus, according to part 1 of Article 84 of the CPC of Ukraine, evidence in criminal proceedings is factual data obtained in accordance with the procedure provided for by the Criminal Procedure Code, on the basis of which the investigator, prosecutor, investigating judge and court establish the presence or absence of facts and circumstances relevant to criminal proceedings and subject to proof. At the same time, part 2 of Article 84 of the CPC defines the following procedural sources of evidence:

testimony, material evidence, documents and expert opinions[1]. However, the range of possible evidence has been significantly expanded due to modern development of technology; these raises the question of defining the essence of digital information and its place among the sources of evidence. A part of the answer to this question can be found in Article 99 of the CPC of Ukraine, which defines a document as a material object specially created for the purpose of storing information, which contains information recorded by means of written signs, sounds, images, etc. that can be used as evidence of a fact or circumstances established in criminal proceedings. The documents, provided they contain the information forseen in part 1 of Article 99 of the CPC, may include: 1) materials of photography, sound recording, video recording and other data carriers (including computer data); 2) materials obtained as a result of measures taken in the course of criminal proceedings under applicable international treaties ratified by the Verkhovna Rada of Ukraine; 3) protocols of procedural actions and annexes thereto drawn up in the manner prescribed by the Criminal Procedure Code, as well as data storage media on which procedural actions have been recorded by technical means; 4) audit reports and inspection acts[2]. Thus, materials of photography, sound recording, video recording and other information carriers (including computer data) are classified as a source of evidence as documents. At the same time, part 2 of Article 98 of the CPC states that if documents contain the features specified in part 1 of Article 98 of the CPC, they are material evidence. So, digital (electronic) documents that were instrumental in a criminal offense commission, retained traces of it or contain other information that can be used as evidence of a fact or circumstances established in criminal proceedings, as well as things that were objects of criminal acts, money, valuables and others acquired by criminal means or obtained by a legal entity as a result of a criminal offense, are material evidence. In this regard, in practice, one may encounter different approaches to the application of

[1] Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

[2] Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

the relevant rules, i.e., recognizing them as either documents or material evidence, depending on the situation.

Digital evidence has certain peculiarities. For example, an electronic document cannot exist without an information carrier. In this case, the identification features of the storage medium (in particular, the name of the type, brand, model, individual machine media on which the document is recorded) become important; electronic evidence is invisible to the "naked eye" (without special tools), software and hardware are used to perceive and study it; it can be changed, damaged or destroyed during the operation of the device by the user or under physical factors influence (high humidity, high temperature, electromagnetic radiation, etc.); according to the stages of production, documents, including electronic ones, are divided into originals, duplicates, copies and extracts[3]. In addition, it should be noted that digital evidence, such as computer data, electronic messages, video, audio, photo, GPS tracker records, etc., differ in the nature of the information, i.e., they require a different format, namely, digital. This information is stored on various digital (electronic) media: hard drives, flash memory, CDs, cloud services, and other digital devices. Digital evidence origin is also different. It is created, transmitted and stored using digital technologies and information systems. Thus, digital evidence is essentially different from physical evidence and documents, so we support the position of scientists that it should be classified as a separate kind.

2. The ambiguity of terminology use in the field of digital information.

Thus, today, in the legislation and scientific literature, one can find such concepts as: "digital evidence", "electronic evidence", "electronic (digital) evidence", and "computer data". For example, Art. 5 of the Law of Ukraine "On Electronic Documents and Electronic Document Management" defines an electronic document as a document in which information is recorded in the form of electronic data, including mandatory

[3] Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рекомендації; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ, 2020. С. 6-7.

document details[4]. In 2022, the Criminal Procedure Code was amended to replace the term "electronic" documents with "computer data"[5]. At the same time, the Civil Procedure Code, the Commercial Procedure Code of Ukraine, and the Code of Administrative Procedure contain "electronic evidence" as a separate kind of evidence. So, according to Art. 100 of the Code of Civil Procedure, electronic evidence is information in electronic (digital) form containing data on the circumstances relevant to the case, in particular, electronic documents (including text documents, graphic images, plans, photographs, video and sound recordings, etc.), websites (pages), text, multimedia and voice messages, metadata, databases and other data in electronic form. Such data may be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, and other places where data is stored in electronic form (including the Internet)[6]. Similar data is mentioned in Article 96 of the Commercial Code of Ukraine[7] and Article 99 of the Code of Administrative Procedure[8].

The scientific literature has also different approaches to the definition of the relevant concept. For example, O.G. Kozytska, supporting the position on the need to use the concept of "electronic evidence", notes that, in its essence, electronic evidence is a digital object that was a mean or an instrument of a criminal offense, preserved electronic digital traces of a criminal offense, was the subject or object of a criminal offense, or contains other information that can be used as evidence of a fact or circumstances established in criminal proceedings[9]. Supporting the position on the

---

[4] Закону України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

[5] Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам» від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

[6] Цивільний процесуальний кодекс України від 18.03.2004 року № 1618-IV. URL: http://zakon3.rada.gov.ua/laws/show/1618-15.

[7] Господарський процесуальний кодекс України від 06.11.1991 № 1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text.

[8] Кодекс адміністративного судочинства України від 06.07.2005 № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text.

[9] Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. № 8. 2020. С. 420.

need to use the concept of "electronic evidence", O. I. Garasymiv, S. I. Marko and O. V. Ryashko note that such electronic evidence has certain specific features that should be reflected in substantive and procedural legislation and prove that compliance with the requirements for the form of an electronic document forms its evidentiary value, the ability to put it in the basis of a procedural decision and refer to it in court[10]. At the same time, some scholars[11] do not distinguish between the concepts of "electronic (digital) evidence", "electronic proof" and "digital proof", using them in parallel, without focusing on their advantages or disadvantages.

Today, digital devices have completely replaced analog onesdevices, and the difference between analog and digital information is that analog information is continuous, while digital information is discrete[12]. G. K. Avdeeva, E. Zhyvutska-Kozlovska and N. Zozulia, distinguishing between the concepts of "digital evidence" and "electronic evidence", note that the term "digital evidence" is more accurate and "better reflects the cybernetic aspect of the transmission, processing and storage of information in view of the processes of information transformation using binary code", and "devices and machines that process and store digital information should be called electronic"[13]. It should also be noted that the term "digital evidence" is more adapted to the development of modern technologies, which allows to include new formats and sources of evidence that may become important in the future. Besides, in foreign scientific works, the term "digital evidence" is also used to define digital evidence, which is actually translated as "digital proof". The use of uniform terminology in the

---

[10] Гарасимів О.І., Марко С.І., Ряшко О.В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського національного університету.* Серія: Право. Том 2. № 75, 2023. С. 158-159.

[11] Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рекомендації; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ, 2020. С. 17.

[12] Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. Вип. 1 (30). С. 131.

[13] Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. Вип. 1 (30). С. 131; Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства. *Українське право*. URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva.

field of judicial proceedings helps to avoid misunderstandings and promotes more effective cooperation between law enforcement agencies of different countries. Therefore, in view of the above, we believe that it is more appropriate to use the concept of "digital evidence".

Moreover, it is necessary to correlate the concepts of "electronic document" and "electronic (digital) evidence", since not every electronic document, as well as not every digital information, can be qualified by the court as "electronic evidence".

When using digital evidence, it is important to establish the relevance, sufficiency, reliability and admissibility of the evidence, taking into account the specifics of such data. But the first question to arise, which has both theoretical and practical significance, is establishing their originality. For example, if it is necessary to establish whether the handwritten text in a document was executed by a certain person, it is mandatory to provide only the original document, in accordance with clause 3.5 of the Instruction on the appointment and conduct of forensic examinations and expert studies, approved by the Order of the Ministry of Justice of Ukraine No. 53/5 of 08.10.1998[14]. This is quite reasonable given the specifics of the relevant study, for which the signs remaining as a result of the person's direct actions on the relevant document are important. It is not possible to establish the relevant features from a copy of the document. This raises the question of determining the originality of an electronic document, taking into account the possibility of copying the relevant information without losing essential features. Thus, S. Gongalo notes that electronic documents are divided into originals, duplicates, copies and extracts according to the stages of production. At the same time, he also points out that this division is rather conditional, since in all these cases the electronic document remains the original[15]. We cannot generally agree with the relevant statement, since, for example, during diagnostic

[14] Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: затверджено наказом МЮ України від 08.10.98 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

[15] Гонгало С.Й. Електронні документи як об’єкти судової техніко-криміналістичної експертизи та їх класифікація. *Адвокат*. 2013. №1(148). С. 33-36.

studies of materials and means of sound and video recording, it is possible to determine whether files video-phonograms or phonograms are originals or copies. Besides, the methodology of conducting the relevant research on copies of records, without the availability of their originals, does not allow to establish the authenticity of the records[16]. Therefore, from an expert point of view, there is a difference between the original and a copy of such evidence.

Indeed, as a general rule, in accordance with Part 3 of Article 99 of the CPC, a party to criminal proceedings, a victim, a representative of a legal entity in respect of which the proceedings are being conducted, are obliged to provide the court with the original document. The original document is the document itself, and the original of an electronic document is its reflection, which is given the same meaning as the document[17]. At the same time, according to Art. 7 of the Law of Ukraine "On Electronic Documents and Electronic Document Management", an original electronic document is an electronic copy of a document with mandatory details, including the author's electronic signature or a signature equivalent to a handwritten signature in accordance with the Law of Ukraine №2155-VIII "On Electronic Trust Services" dated October 05, 2017[18]. At the same time, the CPC also contains the concept of a "duplicate document" (part 4 of Article 99 of the CPC), i.e., a document made in the same way as its original. A duplicate of a document, as well as copies of information, including computer data contained in information (automated) systems, electronic communication systems, information and communication systems, computer systems, their integral parts, made by an investigator, a prosecutor with the involvement of a specialist, are recognized by the court as an original document [14]. It should be noted that the legislator has thus limited the range of entities having the right to produce the relevant documents so that they would be considered an original, and has not specified

---

[16] Експертиза відео-, звукозапису. *Офіційний сайт Київського науково-дослідного інституту судових експертиз*. URL: https://kndise.gov.ua/video-zvukozapysu

[17] Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

[18] Закону України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

the relevant knowledgeable person who should be involved as a specialist. In addition, no qualification requirements for such a specialist have been established (unlike in other cases of mandatory involvement of a specialist in criminal proceedings), which essentially devalues the role of the specialist involved and reduces his participation in procedural actions related to information copying to a formality [6, pp. 42-43]. That is, in fact, if the relevant copying was carried out in the presence of a specialist who was involved, for example, as a forensic expert to examine a corpse, the copies obtained will also be considered the original, regardless of the fact that this is beyond the scope of the expert's special knowledge. The question arises as to whether it is appropriate to use the relevant specialized knowledge. Thus, the lack of thoughtfulness and inconsistency of legal regulation in these aspects can be seen.

Important is the issue of the procedural consequences of technical media original copies absence and whether this will lead to the inadmissibility of such evidence. Thus, in part 3 of Art. 99 of the CPC, the legislator has determined that the original of an electronic document is not only the document itself, but also its display. At the same time, in accordance with part 1 of Article 99 of the CPC, a document is a material object specially created for information storage purpose, which contains information recorded with the help of written signs, sounds, images, etc. that can be used as evidence of a fact or circumstances established in criminal proceedings, including sound recording materials and electronic media. According to the legal position of the Supreme Court of Ukraine as part of the Criminal Court of Cassation, set out in the Resolution No. 554/5090/16-к dated 29.03.2021, the identification of electronic evidence as a mean of proof with its material carrier is groundless, since an electronic document characteristic feature is strict link to a specific material carrier absence. In order to fulfill the tasks of criminal proceedings, in view of the Law of Ukraine "On Electronic Documents and Electronic Document Management" provisions, an electronic document use as evidence cannot be denied solely on the ground that it has an electronic form (part 2 of Article 8). Pursuant to Article 7 of this Law, if an electronic document is stored on several electronic media, each of the electronic copies is considered an original electronic document. The same electronic document may exist on different media. All

copies of an electronic document identical in content may be considered as originals and differ from each other only in time and date of creation. Issues of identification of an electronic document as an original may be resolved by the authorized person who created it (using special programs to calculate the checksum of a file or directory with files (CRC-sum, hash-sum), or, if there are appropriate grounds, by special studies conducting[19]. In addition, it should be mentioned that an important issue when conducting forensic examinations in the field of information technologies is the legality of the use of a digital password by an expert to unlock a smartphone, computer or other technical medium[20].

The Criminal Procedure Law contains guarantees for the legitimate rights and interests of the parties in criminal proceedings protection where Article 266 of the CPC sets out requirements for the storage of technical means used in the course of conducting the CID, as well as primary data storage devices, until the court verdict enters into force. If there are reasonable grounds, the storage media and technical means which the information was obtained with may be the subject to exam by relevant specialists or experts in accordance with the procedure provided for by this Code.

3. Digital evidence evaluation.

The practice also does not have digital evidence evaluation uniform approaches and varies depending on criminal offenses type being investigated. Thus, there have been cases where, in one case, electronic documents copies were not recognized as admissible evidence, and in another one - vice versa. An example is the Resolution of the Criminal Court of Cassation within the Supreme Court of March 11, 2020 in case No. 149/745/14, in which, based on an expert opinion, it was established that the video-phonograms (phonograms) referred to by the prosecution, recorded on optical disks, were copies, the court recognized them to be inadmissible evidence, and accordingly,

---

[19] Постанова Верховного Суду у складі Касаційного кримінального суду від 29.03.2021р. №554/5090/16-к https://verdictum.ligazakon.net/document/96074938

[20] Латиш К., Демидова Є., Домашенко О., Колеснікова І. Експертні помилки під час проведення окремих видів судових експертиз у сфері інформаційних технологій. Юридичний вісник. 2022. №2. С. 95. DOI: https://doi.org/10.32837/yuv.v0i2.2326

other evidence derived from them, were recognized inadmissible, too, including protocols of covert investigative (search) actions of audio and video control of a person, as stated in the court decisions[21]. A somewhat different approach was taken in the Ruling of the Criminal Court of Cassation of the Supreme Court of August 19, 2021 in case №756/8124/19, which states that in accordance with Article 7 of the Law of Ukraine №851-IV "On Electronic Documents and Electronic Document Management" of May 22, 2003, in the case of storing information on several electronic media, each of the electronic copies is considered the original electronic document. A material carrier is only a way of information storing that is relevant only when an electronic document is used as material evidence. The main feature of an electronic document is the absence of a rigid binding to a specific material carrier. The same electronic document (video recording) may exist on different media. All electronic document copies identical in content may be considered as originals and differ from each other only in creation time and date. As a result of the case, CDs with events circumstances video recordings which were made in connection with the need to provide relevant to criminal proceedings information, were attached to the case file as material evidence, were recognized as an independent source of evidence derived from information stored on a computer in electronic form in the form of files. And an electronic file in the form of a video recorded on an optical disk was considered to be the original (reflection) of an electronic document[22]. However, in all cases, an unconditional assessment of compliance with the traditional qualitative criteria of admissibility, sufficiency, reliability, and relevance is carried out. From a technical point of view, an original electronic document is one that is created and stored on a primary storage medium. For example, the original video recording from video surveillance cameras is stored on the storage medium on which the video is recorded. A copy of such a video is its transfer

[21] Постанова Верховного Суду колегією суддів Третьої судової палати Касаційного кримінального суду від 11 березня 2020 року, судова справа № 149/745/14. URL: https://reyestr.court.gov.ua/Review/88265263.

[22] Постанова Верховного Суду колегією суддів Третьої судової палати Касаційного кримінального суду від 9 серпня 2021 року справа № 756/8124/1911.URL:https://reyestr.court.gov.ua/Review/99088529?fbclid=IwAR2c3RBhiXTYBIPYqSPzTCCLhx5PQiCiS7TfsZwGdfO7YevBHkLT3NpVzbE.

to another storage medium[23]. In other words, the original is actually the primary source of information from which copies and duplicates of such a document may be derived. At the same time, copies and duplicates do not differ from the original in their essence (provided that no changes have been made to them), which is due to the digital way they are made. The information copied in this way may also have the procedural value of the original if it is collected by the investigator with the involvement of a specialist (part 4 of Article 99 of the CPC of Ukraine). Thus, the seizure of digital information during a search and inspection should be carried out by copying it from the information space or digital storage medium and should be carried out in several stages: 1) extraction (copying) of digital information from the place of its detection to a digital storage medium; 2) presentation of the detected digital information to witnesses, a specialist and other participants in the investigative actions; 3) reflection in the protocol of investigative actions of the time, place and environment of the detected information; 4) packaging and sealing of digital storage media containing the desired digital information[24].

In criminal proceedings, the collection of evidence in electronic form is a rather complex process due to the complexity of the objects and the fact that every action on a digital device leaves certain traces, including viewing and copying, because most programs automatically generate reports and have a registry. performed actions (logs)[25].

Conclusions

[23] Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. С. 45.

[24] Метелев О.П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. *Науковий вісник Ужгородського національного університету*. Серія: Право. № 60, 2020. С.179.

[25] Білоус В., Латиш К. Судові експертизи радіоелектронних засобів як форма використання спеціальних знань під час розслідування корупційних кримінальних правопорушень. Наукові праці Міжрегіональної Академії управління персоналом. Серія: Юридичні науки. 2022. Випуск 1(61). С. 5-11.

From our point of view, the procedural formalization of relevant digital copies production is important, as the correctness of this process determines the procedural consequences in the form of assessing the reliability of such evidence by the court in the future. This procedure has become most relevant due to the relevant amendments to the Criminal Procedure Code of Ukraine in 2017, which were adopted to prevent unjustified blocking of enterprises, especially in the IT industry, through the seizure of computer equipment, phones, servers, etc. Temporary seizure of electronic information and other electronic systems is carried out in exceptional cases and only if they are specified in a court order. Preference should be given to copying information from telecommunication, information and telecommunication and other systems rather than seizing it. I.G. Kalancha and A.M. Harkusha proposed a procedural scenarios system of four blocks when it is necessary just to copy information: the first block is devoted to cases of copying during such investigative (search) actions as inspection and search (for example, when there are no grounds for temporary seizure of property; or due to organizational (structural) complexity, physical cumbersomeness of information systems; or when it is impossible to seize an information system due to the risks of interruption of the production process; as well as in case of inappropriate copying). The second block of the procedural scenarios system concerns the situation when there is a need to make a copy of electronic information being already in the possession of the prosecution. This is necessary, for example, for preventive purposes (to prevent loss) or to transfer to another party (for example, to the owner of this information in accordance with Part 3 of Article 100 of the CPC of Ukraine The third block of the system is provided for in accordance with part 1 of Article 159 of the CPC of Ukraine, when temporary access to things and documents is carried out exclusively by making a copy of information if the court has granted access to electronic information systems or parts thereof or communication systems mobile terminals. The fourth block provides

for making a copy of information in electronic form as a backup copy of technical information carriers original copies (part 3 of Article 107 of the CPC of Ukraine)[26].

Thus, the digital evidence use in criminal proceedings requires a conscientious attitude to their procedural design in order to ensure such evidence reliability and admissibility. Copies of electronic documents should be used as evidence, but their authenticity, verification and authenticity of information must be clearly documented and verified. When copying digital information to a specific technical medium, it is important to comply with the following rules: 1) electronic documents must be created during the course of this investigative (detective) action: the creation time and circumstances must coincide with those specified in the investigative action protocol; 2) the subject must be authorized.

Summary

Rapid technological development poses new challenges for law enforcement agencies and the judiciary. Effective use of digital evidence in criminal proceedings requires a comprehensive approach. The development of rules and standards for collecting digital evidence, effective ways and methods of obtaining it is an important aspect of ensuring trial fairness and objectivity, which requires additional research. In addition, it is important to train and retrain professional staff, adapt their knowledge, skills and abilities to modern needs, in terms not only digital technologies use, but also global trends in digital technologies development in their use for the needs of the judiciary.

References

1. Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. Вип. 1 (30). 2023. С. 126-143.

[26] Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. №8. С. 337.

2. Білоус В., Латиш К. Судові експертизи радіоелектронних засобів як форма використання спеціальних знань під час розслідування корупційних кримінальних правопорушень. *Наукові праці Міжрегіональної Академії управління персоналом. Серія: Юридичні науки.* 2022. Випуск 1(61). С. 5-11.

3. Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рекомендації; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ, 2020. 104 с.

4. Гарасимів О.І., Марко С.І., Ряшко О.В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського національного університету.* Серія: Право. Том 2. № 75, 2023. С. 158-162.

5. Гонгало С.Й. Електронні документи як об'єкти судової техніко-криміналістичної експертизи та їх класифікація. *Адвокат*. 2013. №1(148). С. 33-36.

6. Господарський процесуальний кодекс України від 06.11.1991 № 1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text.

7. Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерела доказів в кримінальному провадженні. *Криміналістичний вісник.* 2020. № 1(32). С. 37- 49.

8. Експертиза відео-, звукозапису. *Офіційний сайт Київського науково-дослідного інституту судових експертиз*. URL: https://kndise.gov.ua/video-zvukozapysu

9. Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам» від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

10. Закону України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

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

12. Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: затверджено наказом МЮ України від 08.10.98 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

13. Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. №8. С. 337.

14. Кодекс адміністративного судочинства України від 06.07.2005 № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text.

15. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. № 8. 2020. С. 418-421.

16. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

17. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. 204 с.

18. Латиш К., Демидова Є., Домашенко О., Колеснікова І. Експертні помилки під час проведення окремих видів судових експертиз у сфері інформаційних технологій. Юридичний вісник. 2022. №2. С. 93-99. DOI: https://doi.org/10.32837/yuv.v0i2.2326

19. Метелев О.П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. *Науковий вісник Ужгородського національного університету*. Серія: Право. № 60, 2020. С.177-180.

20. Постанова Верховного Суду колегією суддів Третьої судової палати Касаційного кримінального суду від 11 березня 2020 року, судова справа № 149/745/14. URL: https://reyestr.court.gov.ua/Review/88265263.

21. Постанова Верховного Суду колегією суддів Третьої судової палати Касаційного кримінального суду від 9 серпня 2021 року справа № 756/8124/1911.URL:https://reyestr.court.gov.ua/Review/99088529?fbclid=IwAR2c3RBhiXTYBIPYqSPzTCCLhx5PQiCiS7TfsZwGdfO7YevBHkLT3NpVzbE.

22. Постанова Верховного Суду у складі Касаційного кримінального суду від 29.03.2021р. №554/5090/16-к https://verdictum.ligazakon.net/document/96074938

23. Цивільний процесуальний кодекс України від 18.03.2004 року № 1618-IV. URL: http://zakon3.rada.gov.ua/laws/show/1618-15.

Information about the authors:

Demydova Yevheniia,

PhD in Law,

Associate Professor at the Criminalistics Department,

Yaroslav Mudryi National Law University,

77, Pushkinska street, Kharkiv, 61002, Ukraine

Latysh Kateryna,

PhD in Law, Associate Professor,

Assistant Professor at the Criminalistics Department,

Yaroslav Mudryi National Law University,

77, Pushkinska street, Kharkiv, 61002, Ukraine

MSCA4Ukraine postdoctoral fellow, Vilnius University,

Saulėtekio al. 9 - I rūmai, 10222, Vilnius, Lithuania

Kapustina Mariieta,

PhD in Law,

Associate Professor at the Criminalistics Department,
Yaroslav Mudryi National Law University,
77, Pushkinska street, Kharkiv, 61002, Ukraine