


IRYNA OLEKSANDRIVNA TESLENKO,*Kharkiv National University of Internal Affairs;* <https://orcid.org/0009-0007-2622-0289>,*e-mail: iteslenko@ukr.net*

SPECIFIC FEATURES OF OBTAINING AND USING ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

The relevance and importance of this research is due to the fact that scientific and technological progress and rapid development of information technology in all spheres of public life have significantly influenced the emergence of new types of criminal offences. Criminals are using computer systems and other portable devices to commit unlawful acts with increasing frequency. Today, many criminal offences are being committed with the help of information technology around the world, ranging from simple online fraud to the threat of a territorial act. Therefore, one of the ways to record (document) such illegal activities effectively is to obtain (collect) electronic evidence by law enforcement agencies in criminal proceedings. In this regard, the key role is played by evidence, which helps to form an evidence base that makes it possible to notify a person of suspicion, send an indictment to the court and make a final court decision on the guilt (innocence) of a person in committing a particular criminal offence. Achievement of this objective undoubtedly necessitates a specific legal procedure for seizure of electronic evidence in criminal proceedings, which is not yet clearly defined in terms of its collection, leading to numerous cases of courts declaring such evidence inadmissible.

In the course of the scientific research, the author of the article analyses the views of scholars on the interpretation of the concept of electronic evidence; provides the legislative interpretation of this term (unlike the CPC of Ukraine, other procedural codes enshrine the concept of electronic evidence); studies the case law on the issue of electronic evidence being admissible/inadmissible; and identifies the main features of electronic evidence, etc.

Given the fact that the Russian Federation commits war crimes on the territory of Ukraine on a daily basis, the author states the need to collect and record evidence of such crimes from open sources, which will further ensure the prosecution of the perpetrators.

In the course of studying the specific features of obtaining and using electronic evidence in criminal proceedings, the author applied general scientific and special scientific methods, in particular, dialectical, formal and logical, and comparative legal methods. The interrelated use of these methods allowed for a comprehensive study, where each of these methods was used at a certain stage of the examination of the specific features of obtaining and using electronic evidence in criminal proceedings.

Key words: *process of proof, obtaining (collecting) evidence, sources of evidence, electronic evidence, digitalisation, collecting evidence from open sources.*

Original article

INTRODUCTION. Technological progress, the development of information technology and global achievements related to digitalisation are introducing new trends in all areas of our lives, including the legal sphere. These processes affect both the transformation of crime and the search for new means of exposing such activities, collecting evidence of criminal offences committed by certain individuals, and more. Therefore, the possibility of obtaining data from new sources within the criminal proceedings, such as unmanned systems, satellite communications, data from open and other sources, including the Internet, which have not been taken into account in the collection of evidence in criminal proceedings, is becoming increasingly important. This list is constantly being expanded.

It is worth noting that with Russia's full-scale military invasion of Ukraine, which is accompanied by the constant commission of war crimes, Ukraine's law enforcement agencies have faced new challenges in documenting and investigating them. In addition, during the ongoing hostilities, temporary occupation and annexation of Ukrainian territories, the prospect of conducting a proper pre-trial investigation is minimised or, in some cases, even impossible. For example, the analysis of footage from video cameras located in the occupied cities, combined with information obtained from browsing web pages, messengers, and social media, makes it possible to identify a war criminal or collaborator (Fomina, Rachynskyi, 2023, p. 208). In this regard, proper documentation of criminal offences, and especially

those committed under martial law, is very important, as civil society seeks to ensure justice, and its achievement is the main task of all subjects of the criminal procedure, who must take the necessary measures to identify the persons who have committed and/or continue to commit criminal offences. This can be ensured by providing the court with an adequate evidence base, and in view of this, when collecting the necessary evidence, pre-trial investigation authorities should use technical advances to conduct a prompt and complete pre-trial investigation. In this aspect, obtaining (collecting) electronic evidence, including from open sources, is important in the process of proving.

Meanwhile, a systematic analysis of the CPC of Ukraine shows that:

firstly, the legislator does not separately distinguish electronic evidence from other types of evidence in this matter, but they are subject to general requirements for relevance and admissibility, which will ensure the presence or absence of facts and circumstances relevant to criminal proceedings and subject to proof;

secondly, the legislator does not separately distinguish electronic evidence as a source of evidence, and does not establish a certain form of evidence, but focuses on its content and compliance with the established criteria. We believe that the general principles of criminal procedure entitle the prosecution and the defence to provide the court with any appropriate and admissible evidence within the adversarial procedure, without limiting it by form or source, but subject to the general principles and requirements of its admissibility.

PURPOSE AND OBJECTIVES OF THE RESEARCH. The purpose of the article is to provide a theoretical comprehension of the specific features of obtaining and using electronic evidence in criminal proceedings. To achieve this purpose, the following tasks were solved: 1) to analyse the doctrinal approaches to understanding the concept of electronic evidence; 2) to review the current procedural legislation of Ukraine, the provisions of which define the concept of electronic evidence; 3) to present the practice of judicial authorities relating to the issues of recognition of electronic evidence as admissible.

METHODOLOGY. In order to achieve the purpose and objectives of the study, the author used modern methods of scientific knowledge. The study is based on a dogmatic analysis of scientific points of view, the provisions of the current procedural legislation and case law, which contributed to the formulation and substantiation of the following conclusions.

The research methodology was built on the basis of the dialectical method, which is an objectively necessary logic of the movement of cognition, and its application allowed to consider doctrinal approaches to the interpretation of the concept of electronic evidence. Using the dialectical method, the current state of legal regulation of collection of electronic evidence in criminal proceedings was analysed. The methods of analysis, synthesis and comparison were used to study the state of adaptation of the criminal procedure legislation of Ukraine in terms of regulating the procedure for collecting electronic evidence. The formal logical method made it possible to propose certain ways to solve the identified problems. In the course of the study, the comparative legal method was also used, which made it possible to compare the provisions of the current legal acts of Ukraine with the provisions of international documents containing recommendations on the collection and recording of electronic evidence.

RESULTS AND DISCUSSION. Currently, in the modern legal literature, one can find quite pluralistic methodological approaches to the definition of the category of “electronic evidence”, in particular, scholars interpret the latter as:

– a set of information stored in electronic form on any type of electronic media and in electronic means (Kotliarevskyi, Kitsenko, 1998). In this regard, the peculiarity of this evidence is that it cannot be perceived directly, but must be interpreted in a certain way and analysed with the help of special hardware and software (Muradov, 2013, p. 314);

– any data stored or transmitted by computer that supports or refutes a theory of how the criminal offence occurred or that relates to elements of the mechanism of the criminal offence, such as intent or alibi (Casey, 2011, p. 7);

– electronic data that confirm facts, information or a concept in a form suitable for processing by computer systems, including a programme for executing a computer system or other actions (Akhtyrskaya, 2016, p. 125);

– information in electronic form on facts and circumstances relevant to the case and recorded by means of electronic media provided for by law or transmitted via electronic communication channels (Vernydubov, Belikova, 2018, p. 301);

– actual data stored in electronic form on any type of electronic media and in electronic means, becoming available for human perception after processing by special technical means and software (Alekseev-Protstyuk, Bryzkovskaya, 2018, p. 250). In our opinion, the most important aspect of this definition is the reference to “data”, i.e. information stored in electronic form, such as text,

images, audio and video files, etc. It is the reference to information that makes it possible to cover all forms of evidence created or stored on the relevant device;

- 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) (Brown, Ovsyannikov, Shynkorenko, 2019);

- data on circumstances that are relevant to criminal proceedings and exist in an intangible form within a technical medium or communication channel and whose perception and study is possible with the help of technical means and software (Sirenko, 2019, p. 211);

- evidence that can be obtained in electronic form using electronic devices, computer storage media, as well as computer networks, including the Internet (Hutsaliuk et al., 2020, p. 5);

- information in electronic (digital) form, obtained in accordance with the procedure provided for by the criminal procedural law, which is relevant to criminal proceedings (Hutsaliuk, Antonuk, 2020, p. 44).

At the doctrinal level, the use of the definitions of “digital evidence” and “electronic evidence” is also controversial among scholars. Thus, analysing these concepts, A. V. Kovalenko (2022, p. 49) notes that none of these terms is optimal from a technical point of view: today there are already coding systems that are not based on the use of numbers, as well as computing devices and modern means of information transmission that do not rely on the movement of electrons (quantum computers, data transmission using optical signals, etc.). Therefore, for information processed, transmitted or stored in the ways described, the use of the terms “digital” or “electronic” would be technically incorrect. It can be predicted that with the development of science and technology, other computer technologies will become widespread, which do not actually correspond to the terms under consideration.

In the context of the foregoing, it may be noted that electronic evidence occupies an independent place among the means of proof, but it cannot be classified as material or written evidence. In addition, according to the rules of formal logic, a concept has both specific and generic features. The term “evidence” itself is generic to

electronic evidence, the interpretation of which is enshrined in the provisions of Part 1 of Article 84 of the CPC of Ukraine. At the same time, electronic evidence is characterised by inherent features that distinguish it from other types of evidence (testimony, material evidence, etc.). Among the features of electronic evidence are the following: a) they have an intangible external expression; b) they can be transferred or copied to various technical means without loss or damage to the content; c) in order to reproduce such evidence in court, technical devices are required.

Further to the study, it should be noted that the concept of electronic evidence has been clarified at the legislative level. In particular, according to part 1 of Art. 96 Commercial and Procedural Code of Ukraine¹, Article 99(1) Code of Administrative Proceedings of Ukraine² and Article 100(1) Civil Procedural Code of Ukraine³ “Electronic evidence shall mean the information in electronic (digital) form containing data on the circumstances relevant to the case, in particular, electronic documents (including text documents, graphics, plans, photographs, video and audio recordings, etc.), websites (pages), text, multimedia and voice messages, metadata, databases and other data in electronic form. Such data can be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, other places of data storage in electronic form (including the Internet)”.

According to the Guidelines of the Council of Europe Committee of Ministers on Electronic Evidence in Civil and Administrative Proceedings, adopted by the Committee of Ministers on 30 January 2019 at the 1335th meeting of the Deputy Ministers, “electronic evidence” means any evidence contained in, or produced by, any device whose functioning depends on software or data stored or transmitted through a computer system or network⁴. Analysing the case law of the CCU of

¹ Verkhovna Rada of Ukraine. (1991). *Commercial and Procedural Code of Ukraine* (Law No. 1798-XII). <https://zakon.rada.gov.ua/laws/show/1798-12>.

² Verkhovna Rada of Ukraine. (2005). *The Code of Administrative Proceedings of Ukraine* (Law No. 2747-IV). <https://zakon.rada.gov.ua/laws/show/2747-15>.

³ Verkhovna Rada of Ukraine. (2004). *The Civil Procedural Code of Ukraine* (Law No.1618-IV). <https://zakon.rada.gov.ua/laws/show/1618-15>.

⁴ *Guidelines of the Committee of Ministers of the Council of Europe CM(2018)169 on electronic evidence in civil and administrative proceedings*. <https://minjust.gov.ua/m/rekomendatsii-parlamentskoi-asamblei-ta-komitetu-ministriv-radi-evropi>.

the Supreme Court on the admissibility of electronic evidence, Judge Nadiya Stefaniv (2022) noted that the above-mentioned document of the Committee of Ministers of the Council of Europe covers the basic principles that should be followed when collecting and processing electronic evidence, so that any evidence admitted to the trial is appropriate and admissible. Judges are also responsible for improving their own professional knowledge of the use of electronic evidence.

It is worth noting that the judicial practice of Ukraine has also made attempts to clarify the concept of electronic evidence. For example, para. 68 of the resolution of the judges of the Joint Chamber of the Commercial Court of Cassation of the Supreme Court of 15.07.2022 in case No. 914/1003/21 states that “electronic evidence is any information in digital form that is relevant to the case”. On this basis, the Court noted that “messages (with attachments) sent by e-mail are electronic evidence”¹.

In the light of the above, as well as taking into account the provisions of Articles 84 and 99 of the CPC of Ukraine, it can be concluded that the characteristic of electronic evidence is its electronic (digital) form. In particular, the original document is the document itself, and the original electronic document is its reflection, which is given the same meaning as the document. As we can see, according to the CPC of Ukraine, an electronic document is a separate type of document that can be used as evidence in criminal proceedings, and according to DSTU 7157:2010 “an electronic document is a document in which information is presented in the form of electronic data and for the use of which computer equipment is required”². On this issue, referring to the practice of the Criminal Court of Cassation of the Supreme Court, we see that the latter states that “the identification of electronic evidence as a means of proof and the material carrier of such a document is groundless, since the characteristic feature of an electronic document is the absence of a strict link to a specific material carrier. ... The admissibility of an electronic document as evidence cannot be denied solely on the grounds that it has an electronic form. In accordance with the Law of Ukraine ‘On Electronic Documents and Electronic Document Management’, 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. The issues of identifying an electronic document as an original may be resolved by the authorised person who created it (using special software to calculate the checksum of a file or directory containing files (CRC-sum, hash-sum), or, if there are appropriate grounds, by conducting special research”³.

Consequently, it can be noted that in court practice, a comprehensive examination by the court of the procedure for obtaining (collecting) electronic evidence, its fixation and presentation as evidence in criminal proceedings is of great importance. In this regard, it is very important that the court does not declare the evidence inadmissible on formal grounds, because, as stated in the Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings, courts should take into account all relevant factors regarding the source and reliability of electronic evidence, and are aware of the value of electronic trust services in establishing the reliability of electronic evidence. And if it does not contradict the norms of the national legal system, and with the exception of a court decision, electronic data should be accepted as evidence, unless the authenticity of such data is disputed by one of the parties. It should be borne in mind that “intelligibility, accessibility, integrity, authenticity, reliability and, where appropriate, confidentiality and privacy should be components of electronic evidence during its storage. Electronic evidence should be preserved with standardised metadata so that the context of its creation is clear. The comprehensibility and accessibility of stored electronic evidence should be guaranteed over time, taking into account the evolution of information technology”⁴. Similar provisions are enshrined in part 4 of Article 69 of the Rome Statute of the International Criminal Court, which states that “the court may, in accordance with the Rules of Procedure and

¹ The Resolution of the judges of the Joint Chamber of the Commercial Court of Cassation of the Supreme Court dated 15.07.2022 (case No. 914/1003/21).

² State Consumer Standard of Ukraine. DSTU 7157:2010. Official edition. Kyiv, 2010. http://ksv.do.am/GOST/DSTY_ALL/DSTY1/dsty_7157-2010.pdf.

³ Resolution of the Joint Chamber of the Criminal Court of Cassation of the Supreme Court dated 29.03.2021 (case No. 554/5090/16-к). <https://reyestr.court.gov.ua/Review/95848991>.

⁴ *Guidelines of the Committee of Ministers of the Council of Europe CM(2018)169-add1final on electronic evidence in civil and administrative proceedings*. <https://minjust.gov.ua/m/rekomendatsii-parlamentskoi-asamblei-ta-komitetu-ministriv-radi-evropi>

Evidence, rule on the relevance or admissibility of any evidence, taking into account, inter alia, its strength and any prejudice which such evidence may cause to the conduct of a fair trial or to the fair assessment of the testimony of a witness”¹.

Undoubtedly, this issue is very important, since electronic evidence is part of the criminal proceedings, and the digitalisation of all social relations and technological progress lead to a constant increase in both the types of electronic evidence that can be used by the parties to the criminal proceedings and their share in the overall evidence base. Sources of evidence in electronic form may include: various storage media; monoblocks, mobile devices (mobile phones, tablet computers), digital cameras, routers, computer networks, the global Internet, sound and video recordings, etc. This means any electronic device, and this list may be significantly expanded over time. The information is stored on these devices in the form of information objects (data), which include: text and graphic documents; data in multimedia formats; information in database formats and other applications of an applied nature.

Currently, social networks and publicly available web resources contain a large amount of information that can be used as evidence in criminal proceedings. However, electronic evidence has its own specifics, so its proper collection is crucial for the possibility of further use as admissible evidence in criminal proceedings. This is especially important in times of Russia’s full-scale invasion of Ukraine, which entails daily violations of human rights, war crimes, violations of the laws and customs of war, and international conventions ratified by Ukraine. Therefore, the issue of collecting and recording information in electronic form from open sources is very important. The use of data from open sources provides new opportunities for investigating criminal offences, exposing criminals, proving their guilt in court, and thus bringing them to justice and achieving the objectives of criminal proceedings in general.

Ensuring proper recording for the possibility of further authentication of the relevant electronic evidence, establishing its primary source, and the path of movement is the basis for the court’s perception of certain electronic evidence as admissible. At the same time, it is too complicated by the absence of a standard for collecting information from open sources at both the national and international levels.

¹ United Nations. (1998). *The Rome Statute of the International Criminal Court*. https://zakon.rada.gov.ua/laws/show/995_588.

It is worth noting that a large number of non-governmental organisations, such as Bellingcat, Human Rights Watch, conduct online investigations using publicly available online content known as open source intelligence (OSINT). Amnesty International’s Evidence Lab focuses on content that indicates attacks on civilian areas or infrastructure (hospitals, schools) or the use of prohibited weapons (e.g. cluster bombs). Amnesty claims to have collected thousands of videos of alleged atrocities in Ukraine to date. The laboratory uses geolocation, metadata, satellite imagery, weapons experts’ opinions and eyewitness testimony to confirm digital evidence. At the same time, the CPC of Ukraine does not provide for provisions on evidence obtained from open sources, but this does not lead to procedural obstacles to their use in criminal proceedings. After all, determining the content of evidence obtained from open sources and their legal assessment can be carried out on the basis of the provisions of § 1 of Chapter 4 “Evidence and Proof” “The Concept of Evidence, Relevance and Admissibility in Recognising Information as Evidence” and other paragraphs of Chapter 4, which regulate certain procedural types of evidence.

One of the most progressive steps in this regard was the adoption of the Berkeley Protocol on Open Source Investigations, which was developed by the Centre for Human Rights at the University of California, Berkeley. This is the first-ever guide to the effective use of open source information in international investigations of criminal and human rights violations, designed to set this standard². According to O. Yanovska, “The Berkeley Protocol defines the terminology and methodology of data, the procedure for collecting, analysing and storing digital information that is publicly available in compliance with professional, legal and ethical principles. The Berkeley Protocol has not been officially translated into Ukrainian, but this document is referred to in the letter of guidance of the Office of the Prosecutor General on the preservation of digital information from open sources of 28 August 2021”³.

² Matrix. (2020, January 28). *The Berkeley Protocol on Open Source Investigations*. <https://matrix.berkeley.edu/research-article/berkeley-protocol-open-source-investigations/>.

³ Supreme Court. (2021). *Judges of the CCS of the Supreme Court discussed problematic issues of admissibility of electronic evidence during court proceedings*. <https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/>; Yanovska, O. (2021, October 31). *The procedure for collecting and recording evidence must necessarily include computer*

The Berkeley Protocol describes professional standards to be applied in the identification, collection, preservation, analysis and presentation of digital open source information and its use in international criminal and human rights investigations. Open source information is information that any member of the public can observe, purchase or obtain, which does not require special legal status or unauthorised access. Digital open source information is publicly available information in digital format, usually obtained from the Internet. Open source digital information includes data created by both users and machines, and may include, for example: content published on social media; documents, images, video and audio recordings on websites and information-sharing platforms; satellite imagery; and government-published data¹.

In today's environment, it is important to have appropriate advice, recommendations and instructions on recording, preserving, archiving, and evaluating electronic evidence, as this will allow such evidence to be used in court. On this issue, the working group on the implementation of international humanitarian law and the provision of legal services to the population of the Territorial Defence Forces Command of the Armed Forces of Ukraine, together with the Ukrainian Legal Advisory Group, with the support of the AZONES law firm, prepared an illustrated guide for the military on documenting human rights violations and international humanitarian law. This manual describes how to document using video, conduct a basic survey, and what information to look for in shelling, places of detention, torture, etc. After all, proper recording, preservation and transmission are critical to ensure that the information collected becomes evidence in court, helps protect victims and ensures that perpetrators are brought to justice. It is important to understand who recorded the materials and in whose hands they ended up in order to verify them and check for possible distortions or alterations². Meanwhile, as O. Yanovska noted, "today

we cannot operate with an algorithm that would answer the question of what should be the sequence of saving data contained in open sources so that the court does not have questions about the reliability of such data. There are cases when it is impossible to comply with the principle of direct examination of evidence, since the transition to the relevant link on the Internet does not give any result or the link already contains other information"³. Given the public need to conduct pre-trial investigations in criminal proceedings for war crimes, the use of data from open sources provides new opportunities to establish the truth, recreate events, and identify persons involved in the commission of criminal offences in Ukraine. All of this clearly indicates that electronic evidence is a significant auxiliary tool in the implementation of the complex tasks currently facing the law enforcement agencies of Ukraine. The application of the Berkeley Protocol in this regard enables international organisations to participate in online investigations of war crimes committed on the territory of Ukraine, including by collecting evidence from open sources. This is possible through monitoring and further analysis of information from messengers (Telegram, Viber, WhatsApp, etc.), satellite images, recordings from drones (unmanned systems), CCTV cameras, ship navigation systems, etc. In this regard, we support the position of A. Bushchenko that the problem is not in the admissibility but in the reliability of electronic evidence. The judge is convinced that "information technology is a dynamic industry, and if we write in the law today how to collect, record and store electronic evidence, it may turn out to be wrong in the future development of information technology"⁴. There is no doubt that with the further advancement of scientific and technological progress, not only new sources of electronic evidence will appear, but also completely new categories of evidence. The scientific theory of procedural evidence in general and its criminal procedural part in particular, as well as the forensic doctrine of collecting, examining and using evidence, must keep pace with the times and be flexible enough to changes dictated by practice (Kovalenko, 2018, p. 242).

specialists. ADVOKAT POST. <https://advokatpost.com/protsedura-zboru-ta-fiksatsii-e-dokaziv-oboviazkovo-maie-vkliuchaty-fakhivtsiv-kompiuternykh-tekhnologij-suddia-ianovska/>.

¹ United Nations. (2020). *Berkeley Protocol on Investigations Using Open Digital Data. A practical guide to the effective use of publicly available digital information to investigate violations of international criminal law on human rights and humanitarian law*. <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>.

² Ready to Resist. (2023, August 21). *Directions on documenting violations of Human Rights and*

International Humanitarian Law. <https://tro.mil.gov.ua/yak-dokumentuvaty-porushennya-pravlyudyny-i-mizhnarodnogo-gumanitarnogo-prava/>.

³ Supreme Court. (2022, June 7). *Supreme Court judges discussed the admissibility of electronic evidence obtained from open sources with the experts*. <https://supreme.court.gov.ua/supreme/press-centr/news/1282146/>.

⁴ *Ibid*.

The analysis of investigative and judicial practice indicates that one of the problems is the fixation of electronic data during the process of proof, since, as M. V. Hutsaliuk and P. Ye. Antoniuk (2022, p. 118) point out, “information recorded in electronic (digital) form can be easily changed, destroyed, transmitted, copied. The specific nature of information in electronic form is that it is not directly accessible to a person, but only after processing it by special software tools (e.g., the text editor ‘Word’), which, in turn, operate under the control of an operating system on a particular computer device. In other words, the viewing of physically identical information in the form of bits (the minimum unit of information) on a hard drive by different software tools will result in different types of actual data on a monitor screen or printer printout”. In this regard, A. Zakharko (2020, p. 170) notes that “the problem of using electronic evidence is to carry out the process of authentication, i.e. to establish certain rules and methods by which the court and participants in

the process can be convinced of the authenticity of the evidence”.

CONCLUSIONS. Summarising the above, it should be noted that electronic evidence is of great importance in the process of proving and forming the evidence base in criminal proceedings. Their receipt provides new opportunities to ensure the effective investigation of criminal offences, increase the number of sources of evidence collection by the parties to criminal proceedings in order to prove the guilt or innocence of a person, and ensure a balance between fair trial and the inevitability of punishment. The development of the digitalisation of society gives impetus to all processes taking place in the country, and the use of technical achievements and achievements of society to fulfil the tasks of the criminal process is an important component of Ukraine’s development as a state governed by the rule of law and one of the guarantees of compliance with the provisions of Article 6 of the European Convention on Human Rights.

REFERENCES

1. Akhtyrskaya, N. (2016). The question probative cyberinformation in aspects of international cooperation in criminal proceedings. *Uzhhorod National University Herald. Series: Law*, 36(2), 123–125.
2. Alekseev-Protosyuk, D. O., & Bryzkovskaya, O. M. (2018). Electronic evidence in criminal proceedings: notions, signs and problem aspects of application. *Scientific Bulletin of Public and Private Law*, 2, 247–253.
3. Brown, S., Ovsyannikov, V. S., & Shynkorenko, S. V. (2019). *Application of Electronic Evidence in Corruption Cases: Collection of Training Materials for Judges* (N. G. Shuklina, O. P. Ishchenko, Eds). National School of Judges of Ukraine.
4. Casey, E. (2011). *Digital Evidence and Computer Crime* (3rd ed.). Published by Elsevier.
5. Fomina, T. H., & Rachynskiy, O. O. (2023). Electronic evidence in criminal proceedings: problematic issues of theory and practice. *Bulletin of Kharkiv National University of Internal Affairs*, 3(2), 207–220. <https://doi.org/10.32631/v.2023.3.43>.
6. Hutsaliuk, M. V., & Antoniuk, P. Ye. (2022). Procedural capacity of using electronic (digital) information as evidence in criminal proceedings. *Information and Law*, 2(41), 116–122. [https://doi.org/10.37750/2616-6798.2022.2\(41\).270373](https://doi.org/10.37750/2616-6798.2022.2(41).270373).
7. Hutsaliuk, M., & Antoniuk, P. (2020). The essence of digital information as a source of evidence in criminal proceedings. *Forensics Herald*, 33(1), 37–49. <https://doi.org/10.37025/1992-4437/2020-33-1-37>.
8. Hutsaliuk, M., Havlovskiy, V., Khakhanovskiy, V. et al. (2020). *The use of electronic (digital) evidence in criminal proceedings: methodological recommendations* (2nd ed.). National Academy of Internal Affairs Publishing House.
9. Kotliarevskiy, O. I., & Kitsenko, D. M. (1998). Computer information as material evidence in a criminal case. *Information technology and information protection*, 2, 70–79.
10. Kovalenko, A. (2018). Digital Evidences in Criminal Proceedings: Current State and Prospects for Use. *Bulletin of Luhansk State University of Internal Affairs named after E.O. Didorenko*, 4, 237–245.
11. Kovalenko, A. V. (2022, December 14). *Digital or electronic? On the issue of naming a new category of evidence and traces of a criminal offence* [Conference presentation abstract]. The Round Table “Application of information technologies in law enforcement”, Kharkiv, Ukraine.
12. Muradov, V. V. (2013). Digital evidence: criminalistical aspects of using. *Comparative and Analytical Law*, 3, 316–313.
13. Sirenko, O. V. (2019). Electronic evidence in criminal proceedings. *International Law Herald: Actual Problems of the Present (Theory and Practice)*, 14, 208–214. <https://doi.org/10.33244/2521-1196.14.2019.208-214>.
14. Stefaniv, N. (2022). *Judicial practice of the CCC of the Supreme Court on the admissibility of electronic evidence*. Supreme Court. https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf.
15. Vernyudubov, I., & Belikova, S. (2018). Electronic evidences: concept, features and problems of their study by the court. *European Political and Law Discourse*, 5(2), 299–305.

16. Zakharko, A. (2020). Fixation of evidence in the course of proving. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*, 3, 168–173. <https://doi.org/10.31733/2078-3566-2020-3-168-173>.

Received the editorial office: 21 December 2023

Accepted for publication: 27 March 2024

ІРИНА ОЛЕКСАНДРІВНА ТЕСЛЕНКО,

Харківський національний університет внутрішніх справ;

ORCID: <https://orcid.org/0009-0007-2622-0289>,

e-mail: iteslenko@ukr.net

**ОСОБЛИВОСТІ ОТРИМАННЯ ТА ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ
У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ**

Актуальність і важливість проведеного дослідження обумовлені тим, що науково-технічний прогрес і стрімкий розвиток інформаційних технологій в усіх сферах суспільного життя суттєво вплинули на появу нових видів кримінальних правопорушень. Злочинці все частіше використовують комп'ютерні системи й інші портативні пристрої з метою вчинення протиправних дій. На сьогодні у всьому світі за допомогою інформаційних технологій вчиняється безліч кримінальних правопорушень – від звичайного шахрайства в мережі Інтернет до загрози терористичного акту. Саме тому одним зі способів ефективної фіксації (документування) вчинення такої протиправної діяльності є отримання (збирання) правоохоронними органами електронних доказів у кримінальному провадженні. У цьому питанні ключову роль відіграють докази, завдяки яким формується доказова база, що дає можливість повідомити особі про підозру, направити до суду обвинувальний акт і прийняти остаточне судове рішення про винуватість (невинуватість) особи у вчиненні конкретного кримінального правопорушення. Досягнення означеного завдання, безумовно, обумовлює необхідність здійснення специфічної процесуальної процедури вилучення електронних доказів у кримінальному провадженні, які наразі не знайшли свого чіткого закріплення в частині їх збирання, що призводить до непоодиноких випадків визнання судами таких доказів недопустимими.

Проаналізовано точки зору науковців щодо тлумачення поняття електронних доказів; наведено законодавче трактування цього терміна (на відміну від Кримінального процесуального кодексу України в інших процесуальних кодексах закріплено поняття електронних доказів); досліджено судову практику з питань визнання електронних доказів допустимими/недопустимими; виділено основні ознаки електронних доказів.

Зважаючи на щоденне вчинення російською федерацією на території України воєнних злочинів, констатовано необхідність збирання та фіксації доказової інформації щодо таких злочинів із відкритих джерел, що в подальшому забезпечить притягнення винних осіб до кримінальної відповідальності.

Під час вивчення особливостей отримання та використання електронних доказів у кримінальному провадженні застосовано загальнонаукові та спеціально-наукові методи, зокрема діалектичний, формально-логічний, порівняльно-правовий. Кожен з указаних методів був використаний на певному етапі вивчення особливостей отримання та використання електронних доказів у кримінальному провадженні.

Ключові слова: процес доказування, отримання (збирання) доказів, джерела доказів, електронні докази, цифровізація, збирання доказів із відкритих джерел.

Цитування (ДСТУ 8302:2015): Teslenko I. O. Specific features of obtaining and using electronic evidence in criminal proceedings. *Law and Safety*. 2024. No. 1 (92). Pp. 186–193. DOI: <https://doi.org/10.32631/pb.2024.1.17>.

Citation (APA): Teslenko, I. O. (2024). Specific features of obtaining and using electronic evidence in criminal proceedings. *Law and Safety*, 1(92), 186–193. <https://doi.org/10.32631/pb.2024.1.17>.