3 КРИМІНАЛІСТИЧНІ ВИДИ СУДОВИХ ЕКСПЕРТИЗ

DOI: 10.33994/kndise.2024.69.24
UDK 343.98

Yevheniia Oleksandrivna Murzo
Postgraduate student, lecturer of the Department of Criminal Procedure National Academy of Internal Affairs
ORCID: 0009-0000-4409-0560, e-mail: yevheniiamurzo@gmail.com

Victoria Serhiyivna Galchenko
Postgraduate student, lecturer of the Department of Criminal Procedure National Academy of Internal Affairs
ORCID: 0009-0000-7164-2949, e-mail: viktorya.galchenko99@gmail.com

Electronic document as an object of forensic examination during the investigation of marauding

The article is devoted to the study of the role and significance of electronic documents in forensic examination during the investigation of looting cases. The authors consider the technological aspects of storage, processing and transmission of electronic documents, and also highlight the main challenges that forensic experts face when analyzing these documents. The results of the research can be useful for improving judicial practice and increasing the efficiency of investigations in the field of looting with the help of modern technologies.

Keywords: *evidence*; *forensics*; *forensic examination*; *admissibility*; *criminal proceedings*; *pillage*.

Formulation of the problem. The relevance of the study is determined by the fact that the introduction of information technologies the society contributes to the emergence of new types of criminal offenses. In addition, the war on the territory of Ukraine showed how electronic tools for searching and collecting information are important for investigating crimes. One of these types is marauding.

In such a situation, the entire legal system of Ukraine faced new challenges that must be solved by forensic means. In order to establish the fact of looting, it is necessary to collect, investigate and submit evidentiary information to the court. In the process of proof, electronic evidence is of great importance that can be recorded by technical means. The Internet can include a huge amount of information about criminal events, as well as personal data about the person who committed the crime and their social connections.

The use of electronic evidence has become increasingly important as a modern technology in the investigation of looting. The digital environment has also a significant impact on crimes of this nature. In this regard, a forensic science loses its traditional form, and electronic documents become the main source of significant information from the point of view of forensics.

Analysis of recent research and publications. Divergent interpretations of the electronic document among scholars lead to the absence of a general and systematic approach to the study of this issue and its use in practical activities. Moreover, such issues are found in the scientific literature.

Ye. Khizhnyak proposes the definition of an electronic document as any information presented in the electronic form, which is important for the investigation of criminal offenses, the research of which is carried out with the help of special software and technical means [1, p. 84].

S. Chernyavskyi and Yu. Orlov point out that electronic documents as sources of evidence in criminal proceedings are not documents in the traditional sense. Due to this circumstance, as well as to avoid terminological confusion, they propose to use the concept of “electronic display” and to consider it as an independent source of evidence in criminal proceedings and a separate type of evidence [2, p. 19].

O. Metelev, investigating the problems of determining the admissibility and propriety of digital (electronic) evidence in the criminal process, noted that it is difficult to clearly classify digital evidence as physical evidence or documents [3, p. 224].

According to the Law of the Republic of Indonesia № 11 of 2008, there has been an expansion of the types of evidence in legal proceedings, namely (1) Electronic information and/or electronic documents and/or their printouts are valid legal evidence; (2) Electronic information and/or electronic documents and/or their printed results as specified in paragraph (1) are an extension of legal evidence in accordance with the applicable procedural law in Indonesia [4, p. 286].

A. Ratnova agrees with the opinion of scholars who believe that an electronic document is a method of recording and a separate type of evidence, proposing to understand an electronic document as the information in the electronic form that can be used as the evidence of a fact or circumstances established during criminal proceedings [5, p. 48].

Gongalo S. believes that from the point of view of using an electronic document as evidence, it can be divided into two groups — legal and technical. Legal documents contain the requisites prescribed by law, are drawn up by an authorized person and have legal force. Documents that do not have legal force should be classified as technical documents [6, p. 23]. That is, those elements that are most often encountered during a pre-trial investigation: photos and graphic images, video and audio recordings, websites, accounts in social networks, geolocation data, voice, multimedia and other messages, etc.

In support of this, there are different positions of the Supreme Court. For example, the first position: a printout of an electronic correspondence cannot be considered an electronic document (a copy of an electronic document) in the sense of the provisions of Part 1 of Art. 5 of the Law of Ukraine "On Electronic Documents and Electronic Document Management", that is, it cannot be considered as evidence, because it does not contain an electronic signature, which is a mandatory requisite of an electronic document, since in this case it is impossible to identify the sender of the message and the content of such a document is not protected from changes and distortion [7]. In contrast to this decision, in case № 753/10840/19 dated July 13, 2020, the Supreme Court admitted as evidence of domestic violence screenshots of correspondence between the ex-wife and the husband, in which the latter threatened her and the child, used obscene insults, threats and inappropriate language [8]. The evidence must be presented in a properly certified hard copy, and in case of doubt by the opposing party or the court, the original of such evidence must be provided, i.e. the device from which the copy was taken, such as a telephone or computer. In addition, electronic evidence in the form of a screenshot or copy is not considered as independent evidence, but only in the context of other proper and admissible evidence [9, p. 161].

Due to the development of technologies, it is possible to make changes to the informational content of a website or to create the appearance of messages on the Internet that never existed. Such electronic documents require careful verification of origin and authenticity. The examination can determine the authenticity of an electronic document and reveal signs of falsification. Methods of modern examination make it possible to determine whether an electronic document was created on a specific computer or copied from another medium. Such conclusions of experts are supported by circumstantial or evaluative evidence, such as: the information in the service options of the operating system regarding the properties of the file or testimony of witnesses, attempts by the user of a certain computer to destroy information on the Internet [10, Pp. 74—75].

However, according to the results of the survey of the employees of the National Police units, it was established that the main difficulties during the collection and research of information in electronic form arose during, in particular, the appointment of an examination (compilation of a list of questions, sending of evidence, duration of the examination) — 18.8% [11, p. 23].

The aim of the study. The determination of the peculiarities of the study of electronic documents within the framework of forensic examinations during the investigation of looting. Given the purpose of the research, ***the tasks*** should be identified:

- to find out the legal nature of electronic documents;
- to establish the types of forensic examinations that are recommended to be appointed during the investigation of looting.

Presentation of the main research material. The question of the place of an electronic document is not only of theoretical importance in the system of procedural sources. The choice of the most effective procedures depends on its solution, as well as the observance of human rights and freedoms during their implementation. The urgency and practical significance of the issue is confirmed by the lack of unity in law enforcement activities.

In accordance with Part 1 of Art. 99 of the Criminal Code of Ukraine, a document is a material object specially created for the purpose of preserving information, which contains information recorded with the help of written signs, sound, image, etc., which can be used as evidence of a fact or circumstance established during criminal proceedings [12].

There are no legal norms regulating the status of an electronic document in the current Code of Criminal Procedure of Ukraine.

However, the provisions of the Code of Civil Procedure determine that the documents may include photographic materials, sound recordings, video recordings and other media, including computer data.

Nowadays, the Law of Ukraine "On Electronic Documents and Electronic Document Management" establishes the basic organizational and legal principles of electronic document management and the use of electronic documents. According to Art. 5 of the aforementioned Law, an electronic document is a document in which information is recorded in the form of electronic data, including mandatory document details [13].

Among the general characteristics, experts indicate the following, that electronic documents:

- exist in intangible form;
- created by a person or a computer system;
- cannot exist outside the boundaries of a physical carrier or communication channel;
- do not have an inseparable connection with the material medium;
- move freely in the electronic network;

- perception and research of such documents can be carried out only with the use of special programs and devices;
- require a special collection, inspection and assessment procedure;
- have the ability to dubbing, i.e. copying or moving to another medium without losing its characteristics;
- the possibility of remote changes to them and their destruction [14, p. 252].

A. V. Gutnyk and A. Ya. Khytra are of the opinion that one of the main features of an electronic document should be a mandatory component of any electronic document — metadata. And they also offer their author's definition of the metadata of an electronic document, namely, that it is structured coded data that characterizes an electronic document and has evidentiary value in criminal proceedings [11, p. 36].

Thus, the resolution of the CMU № 833 dated November 10, 2017 "On the functioning of the system for recording administrative offenses in the field of ensuring road traffic safety in automatic mode" contains a definition of the concept of "metadata". According to the aforementioned resolution, metadata are structured data that contain the information about an event recorded using technical means (control devices), the characteristics of the recorded vehicle necessary for its identification, parameters of the functioning of technical means (control devices), as well as other data, necessary to record, search, evaluate and manage such information [15].

So, metadata are important in pretrial investigation because they can provide a valuable information about the origin, creation, changes, and other aspects of electronic documents or other digital files.

The use of metadata can greatly facilitate pre-trial investigations, helping to establish facts and relationships between various electronic objects.

One of the new areas of criminology is a digital criminology — forensics (computer criminology) acquires importance in relation to the use of electronic documents in criminal proceedings [16, p. 371].

This field allows for the development of effective tools for the investigation of criminal offenses, especially those committed in conditions of martial law, occupation of territories or armed conflicts, when there is a limited access to the scene of the incident or when it is impossible to get there at all.

The problem of this topic is the specificity of committing looting, the available traces of this crime, the features of identification of the criminal, the insufficient use of technical means, etc. In addition, it becomes difficult to collect and record evidence in the conditions of martial law.

Pillage, in accordance with the Criminal Code of Ukraine, is a theft on the battlefield of things that are with the killed or wounded [17].

Attackers can leave traces in the form of electronic data on mobile devices, such as: text messages, email, photos, videos, social media, and more. Law enforcement agencies can analyze these data to obtain important

information about a crime and possible individuals involved in it. Video recordings can serve as important evidence, where you can see the crimes themselves, as well as identify the perpetrators by their appearance or movements. The proper use of electronic evidence can greatly increase the effectiveness of investigations and help identify and prosecute looting criminals.

The main types of the electronic evidence in the investigation of looting can be:

1. Video and photo evidence: the latter can testify to the facts of looting, show the persons involved in the crime, or record other details. Such evidence can be obtained from surveillance cameras, mobile devices of witnesses or social networks.
2. Electronic communications: e-mail, messages on social networks, text messages and other forms of electronic communication may contain important information about criminals, their accomplices or their plans.
3. Online Trails: pillage can have an electronic trail in the form of activity on websites, forums, social media, etc. Such data can provide important information about the actions and motives of criminals [18, p. 51].

To successfully use electronic evidence in a burglary investigation, proper procedures must be followed to collect, analyze, and preserve the evidence so that it remains intact and reliable.

Digital forensics is of great importance in looting investigations, as digital traces can provide valuable information about the crime and the individuals involved [19, p. 188]. Digital forensics can include analysis of social media, communication records, email, cell phone and other digital traces that can help identify looters [20, p. 179]. Analyzing these traces can help to reveal the looters' ways of action, their communities, and information about possible targets and plans. Forensics can recover lost or deleted data from digital devices, such as: computers, mobile phones or media [21, p. 135].

This may include the recovery of photographs, videos, messages or other digital evidence that can be used to identify those involved in the looting or to trace their actions. They can also analyze network traffic passing through digital networks to detect exploits related to looting. The use of computer vision and artificial intelligence algorithms allows forensics to analyze photos and videos from surveillance cameras or mobile devices to detect looting [22, p. 201]. These tools help digital forensics to collect, analyze and interpret digital data related to looting. The use of these tools helps to gather independent, objective and convincing evidence that can be used in a legal process to bring looters to justice. Thus, digital forensics plays an important role in the investigation of looting, helping to identify the culprits and establish the truth [23].

J. Kanchauskene investigated computer forensics and electronic evidence in criminal justice in Lithuania in her work [24]. The Criminal Procedure Code of Lithuania primarily regulates the acquisition of electronic

data, supplementing the requirements of laws such as, but not limited to, the Criminal Intelligence Act, the Police Act and the Financial Crimes Investigation Service. The data are usually obtained in the manner prescribed by both the Criminal Intelligence Act and other laws prior to the commencement of a pre-trial investigation. After opening a pre-trial investigation, evidence is collected exclusively in accordance with the Code. Courts are especially careful to check whether evidence collected under the Criminal Intelligence Act is lawfully obtained. The requirement to obtain evidence is closely related to the requirement to obtain evidence legally in accordance with the procedure established by law [25, p. 162].

It is possible to view photos and videos of looting cases, collecting information from open sources, such as: social networks, news sites, blogs, etc. After the examination, the investigator should appoint *a forensic portrait examination* or *a photo-, video-, soundrecording examination,* in order to identify the person who committed the criminal offense by voice, face, etc. In order to avoid traces of editing and editing of photo, video and soundrecordings, it is worth appointing *a computer and technical expertise*. It is also possible to establish the origin and authenticity of an electronic document, the absence of signs of falsification in it, due to *a forensic technical forensic examination*.

In order to find out the value of the object of encroachment, it is necessary to appoint *a commodity expert*. Things that are the subject of looting can only be those objects of the material world in respect of which civil rights and obligations arise and which are related to ensuring the sphere of a person's personal life. Such things can include watches, wedding rings, pendants, etc. Therefore, one of the most important procedures in criminal proceedings related to the investigation of looting is conducting the above-mentioned examinations.

In our opinion, it is necessary to carry out examinations of electronic documents in all cases. This is an additional guarantee of the admissibility and reliability of such evidence during the trial of criminal proceedings from social networks.

In this context, the issues also remain unsettled:

- the possibility of obtaining information from sites in the form of a screenshot — an image obtained by a computer that reflects what the user sees on the monitor screen;
- the use of data from open electronic registers contained in the Internet in a criminal process. It should be also noted that practical employees of law enforcement agencies are not aware of the possibilities of obtaining official information about a specific person at the request of an authorized law enforcement agency.

Conclusions. As a result of the research, we can conclude that in modern digital world, electronic documents have become an indispensable component in the criminal process. The application of modern technologies and methods of forensic examination to these documents allows to increase objectivity and efficiency during the pre-trial investigation.

Electronic documents can be given to examination to confirm their authenticity, integrity and reliability. We recommend that the investigator/prosecutor appoint a forensic portrait examination or a photo, video, sound recording examination; computer and technical examination and technical and forensic examination during the investigation of criminal offenses related to pillage.

It is important to work with relevant security agencies, such as: the police, intelligence or military, to ensure that electronic evidence is properly collected and processed. This will help to ensure the legal aspect of the looting investigation.

Electronic documents, including electronic correspondence, data from various electronic devices and other digital traces, can serve as important evidence during the investigation of looting activities. The use of modern methods of analysis and extraction of information allows experts to obtain valuable conclusions regarding the involvement of persons in criminal acts, their intentions and other key aspects of the proceedings.

In general, electronic documents are an important object of forensic examination, contributing to the improvement of the effectiveness of the investigation in criminal proceedings regarding looting. The use of modern technologies is important in the forensic examination of electronic documents to ensure fairness and objectivity in the investigation of such crimes in the digital age.

Перелік посилань

1. Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Сер. Право*. 2017. № 4 (58). С. 80—85. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (дата звернення: 31.01.2024).
2. Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1 (13). С. 12—23.
3. Метелев О. П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2019. № 3. С. 224—238. URL: https://vkslaw.knu.ua/images/verstka/3_2019_METELEV.pdf (дата звернення: 31.01.2024).

References

Khizhnyak, E.S. (2017). Peculiarities of reviewing electronic documents during the investigation of criminal offenses. *State and regions*. № 4 (58). Pp. 80—85. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (access date: 31.01.2024) [in Ukrainian].

Chernyavskyi, S.S., Orlov, Yu.Yu. (2017). Electronic display as a source of evidence in criminal proceedings. *Legal journal of the National Academy of Internal Affairs*. № 1 (13). Pp. 12—23 [in Ukrainian].

Metelev, O. P. (2019). Problems of determining the admissibility and propriety of digital (electronic) evidence in the criminal process. *Herald of criminal justice*. № 3. Pp. 224—238. URL: https://vkslaw.knu.ua/images/verstka/3_2019_METELEV.pdf (access date: 31.01.2024) [in Ukrainian].

4. Mariyam S., Zabidin (2022). Power of Proof Electronic Document Evidence in the Court. *Proceedings of the International Conference On Law, Economics, and Health (ICLEH 2022)*. Pp. 285—297. DOI: 10.2991/978-2-38476-024-4_31 (access date: 31.01.2024).

5. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філософії. Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3747/1/ratnova_d.pdf (дата звернення: 31.01.2024).

Ratnova, A. V. (2021). Criminal procedural and forensic basics of the use of electronic documents in evidence. (Candidate's thesis. Doctor of Philosophy, Lviv University of Internal Affairs). URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3747/1/ratnova_d.pdf (access date: 31.01.2024) [in Ukrainian].

6. Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : автореф. дис. … канд. юр. наук. Київ, 2013. 21 с.

Gongalo, S. Y. (2013). Forensic technical and forensic examination of documents: modern research opportunities and development prospects : autoref. thesis … candidate legal Sciences. Kyiv. 21 p. [in Ukrainian].

7. Постанова Верховного Суду від 11.06.2019 у справі № 904/2882/18, постанова Верховного Суду від 24.09.2019 у справі № 922/1151/18, постанова Верховного Суду від 28.12.2019 у справі № 922/788/19, постанова Верховного Суду від 16.03.2020 у справі № 910/1162/19.

Resolution of the Supreme Court of June 11, 2019 in case No. 904/2882/18, Resolution of the Supreme Court of September 24, 2019 in Case No. 922/1151/18, Resolution of the Supreme Court of December 28, 2019 in Case No. 922/788/19, the decision of the Supreme Court dated March 16, 2020 in case No. 910/1162/19 [in Ukrainian].

8. Постанова суду № 753/10840/19 від 13.07.2020. Про видачу обмежувального припису, заінтересована особа — ОСОБА _2, за касаційною скаргою ОСОБА_2 на рішення Дарницького районного… Касаційний цивільний суд Верховного суду. URL: http://iplex.com.ua/doc.php?regnum=90385050&red=100003f71a6e5ec4dff7a575c38330807b6b30&d=5 (дата звернення: 31.01.2024).

Court ruling No. 753/10840/19 dated 07/13/2020. Regarding the issuance of a restraining order, the interested person is PERSON _2, according to the cassation appeal of PERSON_2 against the decision of the Darnytskyi District…Cassation Civil Court of the Supreme Court. URL: http://iplex.com.ua/doc.php?regnum=90385050&red=100003f71a6e5ec4dff7a575c38330807b6b30&d=5. (access date: 31.01.2024) [in Ukrainian].

9. 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 університету. Сер. Право*. 2023. Вип. 75. С. 158—162. DOI: 10.24144/2307-3322.2022.75.2.25.

Garasimov, O. I., Marko, S. I., Ryashko, O. V. (2023). Digital evidence: some problematic issues regarding its concept and use in criminal justice. *Scientific Bulletin of Uzhhorod University*. Iss. 75. Pp. 158—162. DOI: 10.24144/2307-3322.2022.75.2.25 [in Ukrainian].

10. Школьніков В. І., Мурзо Є. О. Аналіз відкритих джерел інформації під час досудового розслідування: правові основи та шляхи вдосконалення законодавчого регулювання / *Охорона та захист прав людини : студент. колект. моногр*. 2017. С. 60—90.

Shkolnikov, V. I., Murzo, Y. O. (2017). Analysis of open sources of information during pre-trial investigation: legal foundations and ways to improve legislative regulation. *Protection and protection of human rights :* student collective monograph. Pp. 60—90 [in Ukrainian].

11. Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : колект. моногр. Львів : ЛьвДУВС, 2022. 204 с. URL: http://surl.li/qdtqvt (дата звернення: 31.01.2024).

Gutnyk, A. V., Khytra, A. Ya. (2022). Criminal procedural and forensic basics of using electronic documents in evidence : a collective monograph. URL: http://surl.li/qdtqvt (access date: 31.01.2024) [in Ukrainian].

12. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651–VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 31.01.2024).

Criminal Procedure Code of Ukraine dated 13.04.2012 № 4651–VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (access date: 31.01.2024) [in Ukrainian].

13. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 31.01.2024).

About electronic documents and electronic document flow : Law of Ukraine (2003, May). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (access date: 31.01.2024) [in Ukrainian].

14. Алєксєєва-Процюк Д. О. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247—253.

Alekseeva-Protsyuk, D. O. (2018). Electronic evidence in criminal proceedings: concepts, signs and problematic aspects of application. *Scientific bulletin of public and private law*. Iss. 2. Pp. 247—253 [in Ukrainian].

15. Про функціонування системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі : постанова Кабінету Міністрів України від 10.11.2017 № 833. URL: https://zakon.rada.gov.ua/laws/show/833-2017-п#Text (дата звернення: 31.01.2024).

On the functioning of the system for recording administrative offenses in the field of ensuring road traffic safety in automatic mode: Resolution of the Cabinet of Ministers of Ukraine from 10.11.2017 № 833. URL: https://zakon.rada.gov.ua/laws/show/833-2017-п#Text (access date: 31.01.2024) [in Ukrainian].

16. Світличний В. А. Цифрова криміналістика особливості, можливості та перспективи. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану* : тези доп. Міжнар. наук.-практ. конф. Харків : ХНУВС, 2022. С. 371—375. Svitlichnyi, V. A. (2022). Digital forensics, features, possibilities and perspectives. *Modern trends in the development of criminology and the criminal process in the conditions of martial law.* Pp. 371—375 [in Ukrainian].

17. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 31.01.2024). Criminal Code of Ukraine dated 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (access date: 31.01.2024). [in Ukrainian].

18. Murzo, Ye., Halchenko, V. (2023). Electronic evidence as a means of proof during the pillage investigation. *Scientific Journal of the National Academy of Internal Affairs*. № 28(3). Pp. 48—57. DOI: 10.56215/naia-herald/3.2023.48.

19. Wang, B., Liu, Y. (2019). Collection and judgment of electronic data evidence in criminal cases: From the perspective of investigation and evidence collection by public security organs. *Journal of Forensic Science and Medicine*. № 5(4). Pp. 187—194. DOI: 10.4103/jfsm.jfsm_26_19.

20. Marcello, D. (2015). Evidence gathering in the realm of the European investigation order: From national rules to global principles. *New Journal of European Criminal Law.* № 6 (2). Pp. 179—194. DOI: 10.1177/203228441500600203.

21. Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: Mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*. № 29 (2). Pp. 118—153. DOI: 10.1093/ijlit/eaab001.

22. Chan, G., Magotiaux, S. (2021). Digital evidence. B. H. Greenspan, & V. Rondinelli (Eds.). Toronto : Emond Publishing. 310 p.

23. Lewulis, P. (2021). Digital forensic standards and digital evidence in Polish criminal proceedings. An updated definition of digital evidence in forensic science. *International Journal of Electronic Security and Digital Forensics.* № 13 (4). Art. No. 403. DOI: 10.1504/IJESDF.2021.10034988.

24. Kancauskiene, J. (2019). Computer forensics and electronic evidence in criminal legal proceedings: Lithuania's experience. *Digital Evidence and Electronic Signature Law Review*. № 16. Pp. 11—24.

25. Lasaka, M. (2023). Ius constituendum of electronic evidence arrangement in criminal procedure law. *Journal of Legality*. № 16 (2). Pp. 154—166.

Електронний документ як об'єкт судової експертизи під час розслідування мародерства

Є. Мурзо, В. Гальченко

Враховуючи рівень розвитку інформаційних комп'ютеризованих систем досить актуальним є інститут електронних доказів. Наведене у дослідженні опитування серед працівників Національної поліції

підтверджує, що процес збирання та аналізу інформації в електронному форматі супроводжується значними труднощами, зокрема в контексті призначення експертизи. Зазначене підкреслює актуальність дослідження. Автори аналізують важливість електронних документів під час розслідування мародерства. У роботі розглянуто стан наукової розробленості питань електронного документа, його ознак, належності та допустимості у кримінальному судочинстві. Стаття має на меті визначити особливості дослідження електронних документів у рамках судових експертиз під час розслідування мародерства. Проведено аналіз юридичного статусу електронних документів для визначення їх правової природи. До того жвизначено різновиди судових експертиз, які є рекомендованими для проведення у ході розслідування випадків мародерства. Відзначено, що проблематика даної теми полягає в особливостях збереження слідів при мародерстві, ідентифікації осіб, винних у ньому, та недостатньому використанні технічних засобів. Умови воєнного стану додатково ускладнюють процес збору та фіксації доказів, роблячи їх здобуття важливим викликом для правоохоронних органів. Такі обставини обумовлюють потребу у розробці та впровадженні спеціалізованих методів та технік цифрової криміналістики для ефективного вирішення вищезгаданих проблем у сфері розслідування мародерства в умовах воєнного стану. Основна увага приділяється аспектам зберігання та обробки електронних документів, а також їх передачі під час судової експертизи. Автори вивчають технологічні інструменти, які можуть бути використані для забезпечення цілісності та автентичності електронних доказів. Окрема увага приділяється методам виявлення можливих підробок електронних документів, що стає надзвичайно важливим у сучасному цифровому середовищі. Дослідження може бути корисним для практикуючих юристів, судових експертів та правоохоронних органів, які залучені до розслідування випадків мародерства. Результати дослідження можуть допомогти оптимізувати процеси судової експертизи, покращити якість доказів та підвищити загальний рівень ефективності судових розслідувань у цій сфері завдяки застосуванню передових технологічних засобів.

Ключові слова: докази; форензіка; судова експертиза; допустимість; кримінальне провадження; мародерство.

⇒ Murzo, Ye. O., Galchenko V. S. (2024). Electronic document as an object of forensic examination during the investigation of marauding. *Криміналістика і судова експертиза.* Вип. 69. С. 258—269. DOI: 10.33994/kndise.2024.69.24.