


UDC 343.1:65.012.8+004

DOI: <https://doi.org/10.32631/pb.2021.3.01>


OLEKSANDR VOLODYMYROVYCH MANZHAI,

*Candidate of Law, Associate Professor,
Kharkiv National University of Internal Affairs,
Department for Combating Cybercrime;*
 <https://orcid.org/0000-0001-5435-5921>,
e-mail: sofist@ukr.net;

ANTON OLEKSANDROVYCH POTYLCHAK,

*Kharkiv National University of Internal Affairs,
Department of Investigative Activities and Crime Detection;*
 <https://orcid.org/0000-0002-0973-1120>,
e-mail: antonpotylchak@gmail.com;

IRYNA ANDRIIVNA MANZHAI,

*Kharkiv University,
Educational Department;*
 <https://orcid.org/0000-0003-2664-4472>,
e-mail: irinamanzhai@gmail.com

**PROCEDURAL ASPECTS OF HANDLING THE ELECTRONIC EVIDENCE:
THE UKRAINIAN CONTEXT**

The article analyzes the procedural aspects of the seizure, recording and analysis of electronic traces of the crime. Some statistical data on persons convicted under Art. 361-363-1 of the Criminal Code of Ukraine. The history of formation of the institute of electronic proofs is considered. The theoretical basis for understanding the essence of electronic evidence is outlined. It is noted the lack of regulation of the issue of working with electronic evidence in criminal proceedings. Some procedural aspects of electronic document review are revealed and some examples are given. The authors believe that the nature of electronic data, the mechanism of their formation allow us to consider them as a separate type of evidence, and the forms of their fixation defined in the current Ukrainian legislation are not perfect at present. It is proved that when working on the network, law enforcement agencies can record only the projection of the original electronic document as a separate case of electronic evidence, and such a projection can not be considered the original. The method of recording electronic evidence in the framework of covert investigative (search) action to remove information from electronic information systems is analyzed. Some bills aimed at normalizing the peculiarities of working with electronic traces of crimes in criminal proceedings are studied.

Key words: *electronic evidence, procedural aspects, forensic aspects, crime prevention, Ukraine.*

Original article

INTRODUCTION. Investigation of modern types of crime by the law enforcement authorities is often accompanied by the need to collect, process and analyze data electronically, which is directly related to the introduction of information technology in all spheres of human life. While working with such data, many issues occur in terms of verifying the integrity of the information, its authorship and the direct analysis of individual parameters of the form and the content of specific information. As a rule, these topical issues are the subject of research of ‘digital forensics’ – a branch relatively new in Ukraine but widely known abroad. Essentially, it is based on “*the use of scientifically proven methods of preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evi-*

dence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations” (Palmer et al., 2001).

Eoghan Casey (2019) emphasizes that the considerable prevalence of digital technologies requires formalization of digital forensics within forensic science, which needs to be adapted to new digital realities in order to avoid becoming obsolete. At the same time, the procedure of collecting has to conform to the general forensic principles for the strengthening of trust in digital evidence. Michael Losavio, Kathryn C. Seigfried-Spellar and John J. Sloan (2016), in turn, point out that although computer technologies provide significant advantages for criminal investigation, they may

cause new risks resulting from improper application of the digital forensics tools.

Eva A. Vincze (2016) notes that digital forensics is facing a number of serious challenges related to the variety of hardware and software, the dispersion of stored information (including the use of cloud technologies), the complex process of data extraction and analysis of the same from a wide range of devices in varying formats, cryptographic transformations by the offenders, and the complexity of training and skills development of the staff for law-enforcement agencies. David Bennett (2012) also mentions high data volatility in mobile devices.

In this context, there is yet another problem that is characteristic of the majority of countries and is still unresolved in Ukraine. It comes to legal norms and the organizational component of law-enforcement activity that do not keep up with the development of technologies. For example, the Cyberpolice has only been fully functional in Ukraine since 2015, and the relevant substantive laws (such as Section XVI of the Criminal Code) have been formally effective since 2001, whereas the danger of so-called ‘computer’ crimes to the public has not been particularly reconsidered, thereby letting the offenders avoid serious punishment. (fig. 1)¹.

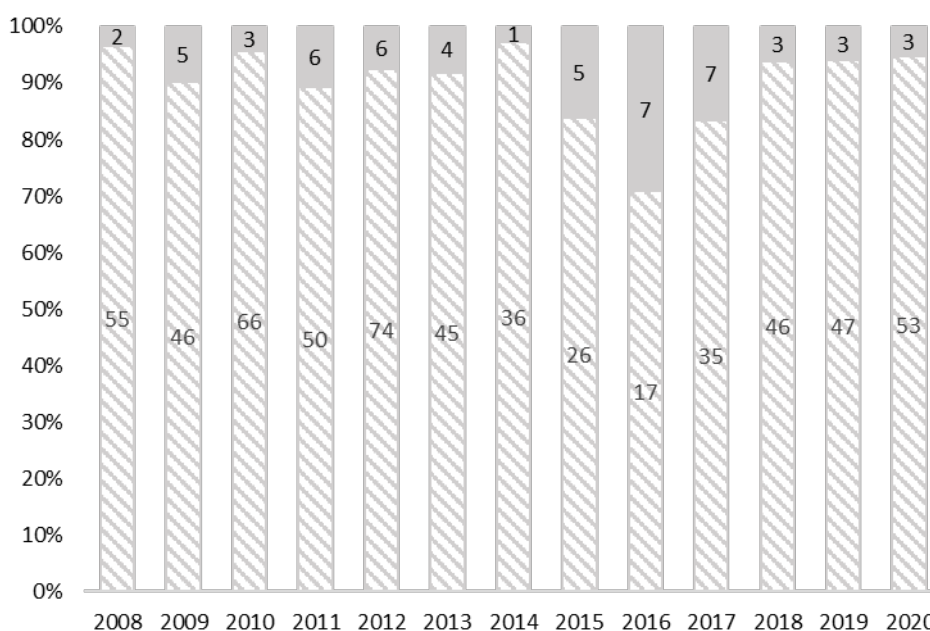


Figure 1. The ratio of sentenced individuals, who have been imposed the certain time imprisonment, to the general number of sentenced (art. 361–363-1 of the Criminal Code of Ukraine)

PURPOSE AND OBJECTIVES OF THE RESEARCH. This article serves to highlight the main procedural issues that occur during the seizure, registration and study of electronic traces of the crime and to suggest ways of addressing them.

METHODOLOGY. System analysis was used in the research of the internal structure of electronic evidence and the formation of the order of the processing of certain elements of electronic data. Historical method was used in the study of the development and modification of criminal procedures to the extent applicable to handling of electronic evidence. Comparative method was used during the study of organizational and criminalistic aspects pertinent to handling of the electronic evidence.

RESULTS AND DISCUSSION. Nowadays, there are two main aspects of the problem of how to handle the electronic evidence during the investigation. The first one is related to formalization of electronic evidence, the other one is how to handle their content.

The concept of ‘electronic evidence’ was established for the first time in Ukraine in 2017 and it covered the information in electronic (digital) form containing data about the circumstances that are essential to the case, especially electronic documents (including text documents, graphical images, plans, photographs, audio- and video recordings, etc.), Websites (pages), text, multimedia and voice messages, metadata, databases and other information in electronic form².

¹ Судова статистика // Судова влада України : офіц. сайт. URL: https://court.gov.ua/inshe/sudova_statystyka/ (accessed 13.07.2021).

² Про внесення змін до Господарського процесуального кодексу України, Цивільного

This game-changing step let resolve several issues concerning the use of evidentiary information in electronic form in civil, economic, and administrative processes. Certain court practices regulating the use of electronic evidence are in place already. In administrative proceedings, courts often rule on the importance of independent certification of electronic evidence¹, meaning the use of an electronic signature², or they just dismiss any digital data that are not properly formalized as evidence³. Unfortunately, the legislators have been mostly ignoring the criminal process where it pertains to regulation of the handling of electronic evidence, thereby causing certain complications in provision of evidence in the course of criminal proceedings to this day.

Among other things, it has to do with the procedural form of admission of the evidentiary information that is saved in electronic form. For example, a situation when a law enforcement officer needs to record information from a multimedia page on the Web. It would be a safe assumption that recording like this shall proceed within the framework of examination procedure set forth in Article 237 of the Criminal Procedure Code of Ukraine (CPC)⁴. However, examination of what, exactly?

процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів : Закон України від 03.10.2017 № 2147-VIII // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: <https://zakon.rada.gov.ua/laws/show/2147-19> (accessed: 13.07.2021).

¹ Ухвала Павлоградського міськрайонного суду Дніпропетровської обл. від 23.01.2019 : справа № 185/9599/18, провадження № 2-а/185/30/19 // Єдиний державний реєстр судових рішень. URL: <https://reyestr.court.gov.ua/Review/79377204> (accessed: 13.07.2021).

² Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (accessed: 13.07.2021).

³ Ухвала Харківського окружного адміністративного суду від 16.12.2019 : справа № 520/12545/19, провадження № 520/17656/19 // Єдиний державний реєстр судових рішень. URL: <https://reyestr.court.gov.ua/Review/86353191> (accessed: 13.07.2021); Рішення Путивльського районного суду Сумської обл. від 24.12.2019 : справа № 584/1572/19, провадження № 2-а/584/20/19 // Єдиний державний реєстр судових рішень. URL: <https://reyestr.court.gov.ua/Review/86648130> (accessed: 13.07.2021).

⁴ Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI // БД

Under applicable laws, the subject of examination may be represented by an area or things, items or documents. At the same time, physical evidence or area can hardly be considered as subjects of examination in this case, because physical evidence is a material object (Article 98 CPC). Some scholars tend to treat cyberspace as an area (Манжай, 2019) but it does not mean that the prosecutor's office or the court will think the same way. When it comes to the documents, the Criminal Procedure Code of Ukraine (Part 2 Article 99) indeed specifically mentions data storage devices, but it really refers to devices only. If we are talking about the computer network, what is the data storage device, exactly? One or several hard disks, which can be within any one or several foreign jurisdictions? Or can it be the electromagnetic field that is generated within the network?

The abovementioned issues once again indicate that the content and the procedure of examination of an electronic document are more complicated than examination of its classic analog. First and foremost, it can be explained by the need to follow a certain procedure of data recording and verification. In fact, the latter is mandatory under applicable administrative, commercial and civil codes.

The situation slightly improved in 2017 when legislators rephrased Part 4 Article 99 of the Criminal Procedure Code of Ukraine so that the copy of electronic information would be acknowledged as the original document. At the same time, the process of examination was deliberately complicated by requiring the mandatory involvement of a specialist. Along with this, the definition of the document was left unchanged and is worded through the prism of materiality. Electronic information cannot be perceived without additional processing by computer equipment. Dmytro M. Tsekhan (2013) points out that it has several features of intangible nature. In addition, it is not always possible to fully and structurally copy electronic information from remote servers even with the involvement of an expert. For example, a Website designed using various programming languages (PHP, Python, Java, PERL, Ruby, JavaScript, etc.) will look on the server side differently from the client side where it is displayed in HTML format.

So, the law enforcers can only record a *projection* of a web-page that simply cannot be treated as the original. Perhaps, this is exactly what

«Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/4651-17> (accessed: 13.07.2021).

the legislators meant using the term ‘image’ in Part 2 Article 99 of the Criminal Procedure Code (Yurii Orlov and Serhii Cherniavskiy (2017) suggested an expanded version of this term – ‘electronic image’). When it comes to the possibility of attaching printouts of electronic documents (Книжняк, 2017) to the inspection record, one needs to construe it only as a projection of the original electronic document, which, in this case, can be treated in the same manner as an item and its photograph.

Generally speaking, one should admit that an electronic document is only an isolated instance of electronic evidence (Алексєєва-Процюк, Брисковська, 2018) because electronic information can be much more complicated than data simply recorded in electronic form (like an article typed in a text editor or a Website). If it is, for example, a software product, it is capable of a certain sequence of actions which, in turn, are capable of constantly changing the current situation. This process can only be recorded in the dynamics. After all, will it be correct and logical to treat an artificial intelligence system as a document?

Taking all the foregoing into account, we believe no form of examination currently available is suitable for the recording of electronic evidence in a criminal procedure within this country in a sufficiently conclusive way, for the law enforcement officers have, in fact, to deal with a new subject matter with the form and content different from the classic evidence. In this context, the opinion of Anton V. Stolitni and Inha H. Kalancha appears to be vague. On the one hand, they say that the institution of ‘electronic evidence’ is artificial and, in fact, substitutes the electronic form of evidence documentation, while, on the other hand, they go on about prospects of expanding the sources of evidence through addition of the electronic evidence (Столїтній, Каланча, 2019).

In general evidence theory, one of the evidence classification criteria manifests itself through the evidence (personal and physical) formation mechanism. The principle of distinguishing each specific category of evidence in the current Criminal Procedure Code of Ukraine is more comprehensive. Consequently, the law outlines several sources of the most important evidence (Article 84 of The Criminal Procedure Code): testimony, physical evidence, documents and expert opinions. With all this in mind, electronic evidence quite possibly may comprise yet another element of the evidentiary system.

No amendments to the Criminal Procedure Code in connection with enforcement of the electronic evidence institution are actually mandatory, because legislators made provisions for yet

another way of the electronic evidence recording within the framework of undercover investigative process (detective work) involving the reading of information from electronic data systems in accordance with Part 2 Article 264 of the CPC¹. Despite certain scholars who are thoroughly skeptical about the possibility of the electronic evidence recording in accordance with the described procedure (Малахова, 2017), there are still precedents of procedural documenting of electronic information in this manner.

In fact, this way of recording is logically more correct than the one within the framework of a modern procedure of handling the electronic evidence as documents. However, under the current laws², the information about the fact or methods of the undercover investigation (detective work) is classified as ‘confidential’ and, therefore, the unclassified procedure is artificially made confidential.

In turn, this can lead to other problems concerning the declassification of relevant information or submission of the findings of undercover investigation (detective work) to the court. In fact, the problem of evidentiary value of the procedural documents comprising the basis for the conduct of undercover investigation and withheld from the counsel for the defense on the pre-trial investigation stage in accordance with Article 290 of the Criminal Procedure Code was solved only in autumn of 2019³.

CONCLUSIONS. So how does one proceed today to properly record that kind of electronic evidence? It should be noted that the practice goes both ways described hereinabove, although

¹ Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : затв. Наказом Ген. прокуратури України, МВС України, СБ України, Адміністрації Держ. прикордонної служби України, М-ва фінансів України, М-ва юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5 // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/v0114900-12> (accessed: 13.07.2021).

² Звід відомостей, що становлять державну таємницю : затв. Наказом СБ України від 12.08.2005 № 440 // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/z0902-05> (accessed: 13.07.2021). Repealed.

³ Постанова Великої Палати Верховного Суду від 16.10.2019 : справа № 640/6847/15-к // Єдиний державний реєстр судових рішень. URL: <https://reyestr.court.gov.ua/Review/85174578> (accessed: 13.07.2021).

the relevant records are most frequently made as part of the examination procedure but the trick is to omit the object of examination from the title of the report.

For the time being, the Law Enforcement Committee with the Verkhovna Rada of Ukraine has drafted a motion with a number of amendments and modifications to the Criminal Code of Ukraine, Criminal Procedure Code of Ukraine, the Code of Administrative Offenses of Ukraine and to the Laws of Ukraine 'On Investigative Activities' and 'On Telecommunications' in the form of a draft bill 'On Amendments and Modifications to Certain Legislative Acts Related to Implementa-

tion of the Convention on Cybercrime Provisions and Enhancement of the Efficient Combating of Cybercrime'. The intention of this draft bill is to unequivocally stipulate that the actions envisaged by Part 2 Article 264 of the Criminal Code of Ukraine are investigative rather than undercover investigative (detective work). If this draft bill is passed, one will be able to proceed with the recording of electronic in a way that is more logical. So far, we have no idea whether or when this draft bill will be passed at all. Moreover, the idea of introduction of the category of electronic evidence to the Criminal Procedural Code found no support during the drafting of the bill.

REFERENCES

1. A Road Map for Digital Forensic Research (August 7–8, 2001) / G. Palmer et al. New York, 2001. 49 p. URL: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf (дата звернення: 13.07.2021).
2. Casey E. Interrelations Between Digital Investigation and Forensic Science. *Digital Investigation*. 2019. Vol. 28. DOI: <https://doi.org/10.1016/j.diin.2019.03.008>.
3. Casey E. Trust in Digital Evidence. *Digital Investigation*. 2019. Vol. 31. DOI: <https://doi.org/10.1016/j.fsidi.2019.200898>.
4. Losavio M., Seigfried-Spellar K. C., Sloan J. J. Why Digital Forensics is Not a Profession and How It Can Become One. *Criminal Justice Studies*. 2016. Vol. 2. Pp. 143–162. DOI: <https://doi.org/10.1080/1478601x.2016.1170281>.
5. Vincze E. A. Challenges in Digital Forensics. *Police Practice and Research*. 2016. Vol. 17. Pp. 183–194. DOI: <https://doi.org/10.1080/15614263.2015.1128163>.
6. Bennett D. The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations. *Information Security Journal: A Global Perspective*. 2012. Vol. 21, Iss. 3. Pp. 159–168. DOI: <https://doi.org/10.1080/19393555.2011.654317>.
7. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2019. № 4 (31). С. 215–219.
8. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2013. № 5. С. 256–260.
9. Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1 (13). С. 12–22.
10. Книжняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони*. 2017. № 4 (58). С. 80–85.
11. Алексеева-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. № 2. С. 247–253.
12. Столітній А. В., Каланча І. Г. Формування інституту електронний доказів у кримінальному процесі України. *Проблеми законності*. 2019. Вип. 146. С. 179–191.
13. Малахова О. В. До питання огляду сторонами кримінального провадження змісту інтернет-сторінок. *Вісник кримінального судочинства*. 2017. № 2. С. 64–69.

Received the editorial office: 16.07.2021

МАНЖАЙ А. В., ПОТЫЛЬЧАК А. А., МАНЖАЙ И. А. ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ РАБОТЫ С ЭЛЕКТРОННЫМИ ДОКАЗАТЕЛЬСТВАМИ

Проведен анализ процессуальных аспектов изъятия, фиксации и анализа электронных следов совершения преступления. Проанализированы отдельные статистические данные в отношении лиц, осужденных по статьям 361–363-1 Уголовного кодекса Украины. Рассмотрена история становления института электронных доказательств. Определены теоретические основы понимания сущности электронных доказательств. Отмечена недостаточная урегулированность вопроса работы с электронными доказательствами в уголовном процессе. Раскрыты отдельные процессуальные аспекты осмотра электронного документа и приведены несколько примеров. Указано, что природа электронных данных, механизм формирования позволяют рассматривать их как отдельный вид

доказательств, а определенные действующим украинским законодательством формы их фиксации в настоящее время не являются совершенными. Доказано, что во время работы в сети правоохранительные органы могут зафиксировать только проекцию оригинального электронного документа как отдельного случая электронных доказательств, при этом такую проекцию нельзя считать оригиналом. Проанализирован способ фиксации электронных доказательств в рамках негласного следственного (розыскного) действия по снятию информации с электронных информационных систем. Изучены отдельные законопроекты, направленные на урегулирование особенностей работы с электронными следами преступлений в уголовном процессе.

Ключевые слова: *электронные доказательства, процессуальные аспекты, криминалистические аспекты, противодействие преступности, Украина.*

МАНЖАЙ О. В., ПОТИЛЬЧАК А. О., МАНЖАЙ І. А. ПРОЦЕСУАЛЬНІ АСПЕКТИ РОБОТИ З ЕЛЕКТРОННИМИ ДОКАЗАМИ

Проведено аналіз процесуальних аспектів вилучення, фіксації та аналізу електронних слідів учинення злочину. Проаналізовано окремі статистичні дані стосовно осіб, засуджених за статтями 361–363-1 Кримінального кодексу України. Розглянуто історію становлення інституту електронних доказів. Акцентовано увагу на тому, що нині існує два основних аспекти поводження з електронними доказами під час розслідування. Перший аспект стосується формалізації електронних доказів, другий – роботи з їх змістом. За допомогою методу системного аналізу вивчено внутрішню структуру електронних доказів та формування порядку опрацювання окремих елементів електронних даних. Окреслено теоретичне підґрунтя для розуміння сутності електронних доказів. Наголошено на недостатній урегульованості питання роботи з електронними доказами у кримінальному процесі. Констатовано, що електронний документ – це лише окремий випадок електронних доказів. Розкрито окремі процесуальні аспекти огляду електронного документа та наведено декілька прикладів. Доведено позицію, що жодна форма огляду на сьогодні не може бути застосована достатньо переконливо у кримінальному процесі України для фіксації електронних доказів, адже правоохоронцям насправді доводиться мати справу з новою сутністю, яка має відмінні від класичних доказів зміст і форму. Зазначено, що природа електронних даних, механізм формування дозволяють розглядати їх як окремий вид доказів, а визначені в чинному українському законодавстві форми їх фіксації нині не є досконалыми. Доведено, що під час роботи в мережі правоохоронні органи можуть зафіксувати лише проекцію оригінального електронного документа як окремого випадка електронних доказів, при цьому таку проекцію не можна вважати оригіналом. Проаналізовано спосіб фіксації електронних доказів під час проведення негласної слідчої (розшукової) дії зі зняття інформації з електронних інформаційних систем. Вивчено окремі законопроекты, спрямовані на унормування особливостей роботи з електронними слідами злочинів у кримінальному процесі. Наведено авторську позицію щодо загального порядку фіксації окремих видів електронних доказів у сучасних умовах.

Ключові слова: *електронні докази, процесуальні аспекти, криміналістичні аспекти, протидія злочинності, Україна.*

Цитування (ДСТУ 8302:2015): Manzhai O. V., Potylchak A. O., Manzhai I. A. Procedural Aspects of Handling the Electronic Evidence: the Ukrainian Context. *Law and Safety*. 2021. No. 3 (82). Pp. 13–18. DOI: <https://doi.org/10.32631/pb.2021.3.01>.

Citation (APA): Manzhai, O. V., Potylchak, A. O., & Manzhai, I. A. (2021). Procedural Aspects of Handling the Electronic Evidence: the Ukrainian Context. *Law and Safety*, 3(82), 13–18. <https://doi.org/10.32631/pb.2021.3.01>.