e-ISSN 3083-6018

**SOCIAL DEVELOPMENT: Economic and Legal Issues**

https://www.eu-scientists.com/index.php/sdel


# Peculiarities of Proof in Criminal Proceedings Related to Cybercrime

Nataliia Luhina [1] ● Oleksandr Paliukh [2 *]

[1] *State Tax University (Ukraine). Associate Professor at the Department of Criminal Law and Procedure, PhD in Law, Associate Professor.*

[2] *State Tax University (Ukraine). Applicant for Higher Education of the First (Bachelor's) Level, PhD in Economics.*

*** *Corresponding Author,*** e-mail: palyuh_@ukr.net

**ARTICLE INFO**

***Research Article***

**DOI:** 10.70651/3083-6018/2025.4.27



**ABSTRACT**

The article deals with topical issues of evidence in criminal proceedings related to cybercrime. The authors focus on the peculiarities of digital evidence, its authenticity, recording, storage and use in court proceedings. The objective of this article is to formulate evidence-based recommendations for enhancing the proof process in criminal proceedings involving cybercrime. This entails examining current methods for handling digital evidence, exploring international practices, and proposing strategies for their integration into domestic criminal justice systems. The lack of clear procedures for collecting digital evidence, insufficient technical equipment of investigators, and the lack of sufficient practice of cooperation between public and private entities in the field of cybersecurity. observance of the rights of participants in the process. Analysis of international experience, in particular the provisions of the Budapest Convention and GDPR, which can be integrated into the national legislation of Ukraine, and the search for adequate ways to resolve existing contradictions in the field of cybercrime investigation. The use of modern technologies, such as blockchain, artificial intelligence and cloud services, to improve the efficiency of digital evidence management. The authors outline the prospects for improving the legal and regulatory framework and training of specialists to combat cybercrime. It is considered promising to create a specialised body which would be a single centre for processing digital evidence in order to ensure standardisation of procedures, increase the efficiency of investigations and promote harmonisation of national legislation with international standards. The study found that digital evidence, as a key element in criminal proceedings related to cybercrime, requires special approaches to its collection, storage and analysis.

**KEYWORDS**

cybercrime, digital evidence, proof, blockchain, GDPR, Budapest Convention.

e-ISSN 3083-6018

СОЦІАЛЬНИЙ РОЗВИТОК: економіко-правові проблеми

https://www.eu-scientists.com/index.php/sdel


# Особливості доказування у кримінальних провадженнях, пов'язаних з кіберзлочинністю

Наталія А. Лугіна [1] ● Олександр М. Палюх [2 *]

[1] *Державний податковий університет (Україна). Доцент кафедри кримінального права та процесу, канд. юрид. наук, доцент.*

[2] *Державний податковий університет (Україна). Здобувач вищої освіти першого (бакалаврського) рівня, канд. екон. наук.*

*** *Автор-кореспондент,*** e-mail: palyuh_@ukr.net

**СТАТТЯ**

***Дослідницька***

**DOI:** 10.70651/3083-6018/2025.4.27



**АНОТАЦІЯ**

У статті розглянуто актуальні питання доказування у кримінальних провадженнях, пов'язаних із кіберзлочинністю. Зосереджено увагу на особливостях цифрових доказів, їхній автентичності, фіксації, зберіганні та використанні у судових процесах. Метою статті є розробка науково обґрунтованих рекомендацій щодо вдосконалення процесу доказування у кримінальних провадженнях, пов'язаних з кіберзлочинністю. Це передбачає аналіз існуючих підходів до роботи з цифровими доказами, вивчення міжнародного досвіду та розробку пропозицій щодо їх імплементації у національне кримінальне провадження. Відсутність чітких процедур збирання цифрових доказів, недостатня технічна оснащеність слідчих, а також відсутність достатньої практики співпраці між державними та приватними структурами у сфері кібербезпеки. дотримання прав учасників процесу. Аналіз міжнородного досвіду, зокрема положення Будапештської конвенції та GDPR, які можуть бути інтегровані у національне законодавство України, пошук адекватних шляхів вирішення існуючих суперечностей у сфері розслідування кіберзлочинів. Використання сучасних технологій, таких як блокчейн, штучний інтелект та хмарні сервіси, для підвищення ефективності роботи з цифровими доказами. Окреслено перспективи вдосконалення нормативно-правового регулювання та підготовки фахівців для боротьби з кіберзлочинністю. Вбачається перспективним створити спеціалізований орган, який був би єдиним центром обробки цифрових доказів, з метою забезпечення стандартизації процедур, підвищення ефективності розслідування та сприяння гармонізації національного законодавства з міжнародними стандартами. У процесі дослідження встановлено, що цифрові докази, як ключовий елемент у кримінальних провадженнях, пов'язаних із кіберзлочинністю, потребують особливих підходів до їхнього збору, зберігання та аналізу.

**КЛЮЧОВІ СЛОВА**

кіберзлочинність, цифрові докази, доказування, блокчейн, GDPR, Будапештська конвенція.

## 1. Introduction

Changes in the criminal environment under the influence of digitalisation are prompting a rethinking of the methods of proof. Cybercrime is becoming not only a regional but also a global problem. Crimes committed in the virtual space have specifics that significantly complicate their investigation, as proof requires working with digital data that may be vulnerable to change or even destruction.

Particular attention should be paid to the problems of ensuring the integrity of evidence during its collection, recording and analysis. In addition, challenges are associated with the legal and regulatory framework for the use of digital evidence, which does not always correspond to modern technological realities. As a result, there is a need to harmonise the legislative and procedural aspects of evidence with the latest technologies and international experience.

## 2. Literature Review

The issue of proof in cybercrime has been the subject of many scientific studies. In particular, the works of D. Y. Nykyforchuk [6], devoted to the use of the results of operational and investigative activities in criminal proceedings, reveal the theoretical and practical aspects of their application. Also important are the studies of O. M. Bandurka and his co-authors [1], who emphasise the need for an integrated approach to operational and investigative comparative studies.

Particular attention is drawn to research in the field of ensuring the authenticity of digital evidence. The work of N. Savchuk [9] examines the main problems of cybercrime and methods of combating it, including the issue of preserving the integrity of digital data. The author also analyses international regulations, such as the General Data Protection Regulation (GDPR) [3], which regulate the protection of personal data in the context of working with digital evidence.

At the same time, a number of unresolved issues remain relevant. For example, the difficulty of identifying the source of data and its verification, as well as ensuring the continuity of the evidence chain in cases where data is transferred between different jurisdictions. As stated in the Budapest Convention [4], cross-border cooperation is a key element in the fight against cybercrime.

The research of O. A. Samoilenko [8] focuses on modern methods of investigating crimes in cyberspace, emphasising the importance of integrating technology into the process of proof. Also of interest are the works of S. R. Tahiev [10], which consider the procedures for temporary access to information held by telecommunications providers from the standpoint of observing the rights and freedoms of participants in criminal proceedings. In addition, this article is a continuation of a previous study by one of the co-authors on the problem of preventing criminal offenses related to the use of cryptocurrency [5].

As a result of the work carried out and the analysis of scientific sources, it is considered expedient to introduce adequate and effective methods of investigating cybercrime, to use the latest technologies, to centrally collect and record digital evidence with the introduction of modern methods.

## 3. Problem Statement

The purpose of the article is to develop scientifically based recommendations for improving the process of proof in criminal proceedings related to cybercrime. This includes analysing existing approaches to working with digital evidence, studying international experience and developing proposals for their implementation in national criminal proceedings.

The main objectives of the article are as follows:

- defining the features of digital evidence, its nature and requirements for preservation;
- analysis of the existing legal framework of Ukraine and its compliance with international standards;
- to consider the technological aspects of collection, recording and analysis of digital data;
- formulating recommendations for improving the legal framework and practical activities of law enforcement agencies.

With this in mind, the article aims at addressing specific problems of proof in criminal proceedings related to cybercrime and providing practical recommendations for overcoming them.

## 4. Methods and Materials

The study employs a multifaceted approach to investigate proof processes in cybercrime-related criminal proceedings. A systematic analysis was used to examine the characteristics of digital evidence, focusing on its authenticity, collection, storage, and application in court. Legal documents, including the Budapest Convention on Cybercrime and Ukraine's Criminal Procedure Code, were analyzed through a comparative method to assess compliance with international standards like GDPR and ISO/IEC 27037:2012, which outline protocols for digital evidence handling.

Qualitative methods, such as content analysis of academic sources (Nykyforchuk, Bandurka, Savchuk), provided insights into challenges like data integrity and cross-border cooperation. Practical case studies, including the use of blockchain and AI in evidence management, were explored to evaluate technological applications in investigations. Statistical data from the Cyberpolice of Ukraine (2018) and materials from Diia's cyber hygiene course were used to assess technical and procedural gaps. Additionally, international practices, such as the EU's eDiscovery and U.S. data protection frameworks, were reviewed to propose actionable improvements. This combination of legal, technological, and empirical analysis forms the foundation for developing recommendations to enhance proof processes in Ukraine's cybercrime investigations.

## 5. Results and Discussion

Cybercrime, as a phenomenon of modern society, is rapidly gaining momentum, becoming one of the most significant threats to the security of states, businesses and individuals. With the development of information technology, the digital space is becoming a platform for committing crimes that have no physical boundaries and can cause damage on a global scale. In this context, ensuring effective evidence in criminal proceedings related to cybercrime is a critical task for law enforcement agencies.

The peculiarity of cybercrime is its technological nature. Crimes committed in the digital environment have specific features: lack of physical evidence, difficulty in identifying sources of information, risk of loss or modification of digital data. Digital traces, such as emails, log files, user activity records, etc., form the bulk of the evidence in such cases. At the same time, their collection, processing and storage require specialised knowledge and skills, as well as appropriate legal regulation.

Ukraine, as part of the international community, is actively adapting its legislation to international standards in the field of combating cybercrime. In particular, considerable attention is paid to the implementation of the provisions of the Budapest Convention on Cybercrime, which is the fundamental international document in this area [3]. However, despite the progress in harmonising national legislation, a number of issues remain that complicate effective investigation and evidence in cybercrime cases. These include the lack of clear procedures for collecting digital evidence, insufficient technical equipment of investigators, and the lack of sufficient cooperation between public and private entities in the field of cybersecurity.

In addition, the international nature of cybercrime often necessitates interstate cooperation, which makes it difficult to ensure the continuity of the evidence chain. In many cases, digital evidence is stored on servers located outside the country, which requires the use of international legal assistance mechanisms. This, in turn, requires not only knowledge of the specifics of working with international organisations such as Europol, Interpol or the International Criminal Court, but also the availability of appropriate tools and resources to ensure prompt access to information.

An additional challenge is the issue of preserving the integrity and authenticity of digital evidence. Any alteration or interference with the data may result in the loss of its evidentiary value. At the same time, in the case of cybercrime, such changes may be caused by both deliberate actions of criminals and shortcomings in the procedures for collecting or storing evidence. In particular, the insufficient level of professional training of investigators and experts working with digital data can lead to significant errors in the course of an investigation [1].

In today's environment, the fight against cybercrime is impossible without the integration of the latest technologies into the investigation process. The use of specialised data analysis software,

automated monitoring systems and encryption tools is not only a technical but also an organisational challenge for law enforcement agencies. At the same time, the effectiveness of such tools depends on the appropriate legal framework, which should create conditions for their legal and transparent use in the process of evidence.

Digital evidence forms an important part of the evidence base in criminal proceedings related to cybercrime. Unlike traditional evidence, such as witness statements or physical objects, digital evidence is intangible and can exist in the form of emails, log files, databases, screenshots or records of social media activity. This evidence has several key characteristics that make it both important and challenging to use.

### *5.1. Specifics of Recording and Storing Digital Evidence*

An important task for investigators is to confirm that the collected data has not been altered or falsified during its receipt, transmission or storage. According to a study by D. Y. Nykyforchuk [6], it is necessary to use specialised data encryption methods and electronic signatures that guarantee the integrity of information. In addition, international experience shows that the use of hash functions to verify data is an effective tool to ensure its authenticity [8].

Another challenge is the difficulty of identifying the source of the data. For example, in the case of investigating crimes involving the use of anonymous networks or VPNs, investigators face the need to work with fragmented evidence that may not contain direct information about the perpetrator. As noted by O. M. Bandurka and his co-authors [1], in such cases, it is important to apply a comprehensive approach, including metadata analysis, investigative experiments and cooperation with Internet service providers.

Another aspect is the regulation of the use of digital evidence in the legal field. In Ukraine, the adoption of the Criminal Procedure Code was an important step towards the legalisation of digital data as evidence in criminal proceedings [2]. However, according to O. Samoilenko, there is a problem of insufficient implementation of international standards, which complicates cooperation with foreign jurisdictions [8].

Recording digital evidence is an important stage of its use in criminal proceedings. This process includes collecting information, documenting it and storing it for further analysis. The main requirements for recording are to ensure the accuracy, completeness and integrity of the data. According to ISO/IEC 27037:2012 standards, effective recording is possible only with the use of specialised software that allows for automatic documentation of the investigator's actions and ensures the chain of custody of evidence [8].

Practice shows that verification of evidence is an equally important step. Verification includes checking the authenticity and accuracy of the data obtained. As noted by Savchuk [9], this stage is critical, as errors in verification can lead to the inadmissibility of evidence in court. In this context, blockchain technologies play an important role, allowing to create an unchanging register of actions with evidence and guarantee their authenticity [9].

At the same time, international practice has standards for the preservation of digital evidence, such as ISO/IEC 27037:2012, which defines methods for collecting, storing and analysing digital evidence. The implementation of these standards in Ukrainian legislation could significantly increase the level of trust in such evidence in courts [8].

### *5.2. Ukraine's Experience in Harmonising Legislation with International Norms in the Field of Cybercrime*

The legal aspects of evidence in criminal proceedings related to cybercrime cover a wide range of issues, including the admissibility of digital evidence in court, the regulation of its collection and analysis, and the observance of the rights of participants in the process. In this context, it is important to analyse the Budapest Convention, which establishes the basic principles of working with digital evidence at the international level [4].

Ukrainian legislation in this area is gradually adapting to the requirements of international law. However, as noted by D. Y. Nykyforchuk [6], there is a need to create specialised units in law enforcement agencies that would deal exclusively with the investigation of cybercrime and work with digital evidence.

The importance of protecting the rights of the accused in the process of collecting digital evidence should be emphasised. For example, the use of information obtained without proper authorisation may be considered a violation of the right to privacy guaranteed by Article 8 of the European Convention on Human Rights [7].

The practical use of digital evidence requires appropriate technical equipment for law enforcement agencies. As stated in ISO/IEC 27037:2012 [8], without the use of modern software, investigating cybercrime becomes almost impossible. It is also important to train investigators to work with these tools, which includes both technical training and familiarisation with the legal aspects of their use.

In today's environment, investigating cybercrime is impossible without the use of specialised technological tools. For example, EnCase, FTK, and X-Ways Forensics provide the ability to automate data search processes and generate reports for use in court [8].

### *5.3. International Experience in Investigating Cybercrime Cases*

The experience of the international community shows that the effective fight against cybercrime is possible only through close cooperation between countries. One of the key international documents in this area is the Budapest Convention, which sets standards for the handling of digital evidence, including the collection, transmission and use of information in legal proceedings [4]. The implementation of the principles of this convention allows countries to coordinate their actions in cases of investigating cross-border crimes.

For example, in the United States, law enforcement agencies widely apply the principles of eDiscovery, which include procedures for collecting, processing and transmitting digital evidence in civil and criminal cases. This helps to ensure transparency in the exchange of evidence between the parties and guarantees the rights of all participants in court proceedings. The use of such approaches helps to increase the efficiency of investigation and trial of cases involving digital evidence [8].

European Union. In the EU, special attention is paid to the protection of personal data when working with digital evidence. The GDPR sets out clear rules for the processing of personal information, including in criminal investigations. This allows for a balance between the need to obtain evidence to investigate crimes and ensuring the right to privacy guaranteed to participants in the process [3].

Ukraine. In Ukraine, legislation in the field of digital evidence is actively developing, but still has certain gaps that need to be addressed. The adoption of the Criminal Procedure Code of Ukraine has defined the basic principles of working with digital evidence, but the issues of cross-border cooperation remain insufficiently regulated. In particular, the lack of clear provisions on the transfer of evidence abroad creates difficulties in international cooperation [2].

A practical step towards solving these problems was the creation of cybercrime units within the structure of the National Police of Ukraine. However, as noted by D. Y. Nykyforchuk [6], these units often face a lack of technical equipment and insufficient professional training of personnel. In addition, the lack of a unified methodology for working with digital evidence can cause errors in its collection and analysis, which negatively affects the outcome of criminal proceedings [10].

An additional aspect that requires attention is the issue of standardisation of procedures for working with digital evidence. According to international practice, the introduction of uniform protocols for the collection, storage and analysis of digital data is a key factor in improving the efficiency of investigations.

At the same time, it remains important to develop mechanisms for preserving digital evidence during its transfer between different investigative bodies or international partners. For this purpose, modern technologies such as blockchain can be used, which guarantee the immutability of data and transparency of the chain of their transfer. As noted by D. Y. Nykyforchuk [6], such technologies can minimise the risks of loss or distortion of evidence.

Particular attention should be paid to the issues of interaction with private companies, which often hold important data. For example, large IT companies, such as Google or Meta, possess information that may be critical to the investigation of cybercrime. As EU practice shows, engaging such companies in cooperation is possible subject to clear legal regulation that takes into account both the interests of the investigation and the need to respect privacy rights [3].

Another challenge is to ensure proper education and technical training of law enforcement personnel. The use of modern software products, such as EnCase, FTK or X-Ways Forensics, requires

not only basic technical knowledge, but also a deep understanding of the legal aspects of their use. Unfortunately, as noted by O. Samoilenko [9], the lack of such knowledge often causes ineffective work of investigators in cases related to cybercrime.

It is equally important to improve international cooperation in combating cybercrime. The Budapest Convention [4] provides for the establishment of mechanisms for the prompt exchange of information between participating countries, but in practice such cooperation often faces bureaucratic obstacles and technical difficulties. As noted in the research of S. R. Tahiev [10], to eliminate these problems, it is necessary to adapt Ukrainian legislation to the requirements of international standards and create specialised platforms for data exchange.

These steps will not only improve the process of investigating cybercrime, but also ensure that the rights of participants in the process are respected, which is an important aspect of justice in the modern digital environment.

## 6. Conclusions

In this context, it is promising to create single digital evidence processing centre, which will ensure standardisation of procedures, increase the efficiency of investigations and promote the harmonisation of national legislation with international standards.

The study found that digital evidence, as a key element in criminal proceedings related to cybercrime, requires special approaches to its collection, storage and analysis. The peculiarities of such evidence necessitate their adaptation to modern legal and technological conditions. Ensuring the authenticity and integrity of the data is essential, which is the basis for its admissibility in court.

The study underlined the urgency of addressing the problems associated with identifying data sources, improving national legislation and raising the level of technical training of law enforcement agencies.

The authors consider the feasibility of establishing single digital evidence processing centre in Ukraine, which would facilitate the centralised organisation of processing procedures, the introduction of the latest technologies and the training of specialists based on international standards. Particular attention is paid to the need to protect human rights when dealing with digital evidence, which involves the adaptation of relevant international norms to national legislation.

## References

1. Bandurka, O. M., Perepelytsia, M. M., Manzhai, O. V., et al. (2013). *Operatyvno-rozshukova komparatyvistyka: Monohrafiia* [Operational-search comparativistics: Monograph]. Kharkiv: Zolota mylia. (in Ukrainian)
2. Cyberpolice of Ukraine. (2018). *Pidsumky 2018 roku v tsyfrakh* [Results of 2018 in figures]. https://cyberpolice.gov.ua/results/2018 (in Ukrainian)
3. Diia. Osvita. (n.d.). *Osnovy kiberhihieny* [Cyber hygiene fundamentals]. https://osvita.diia.gov.ua/courses/cyber-hygiene (in Ukrainian)
4. Kabinet Ministriv Ukrainy. (2012). *Pravyla nadannia ta otrymannia telekomunikatsiinykh posluh, zatverdzheni postanovoiu № 295 vid 11 kvitnia 2012 r.: iz zminamy na 08.04.2013* [Rules for the provision and receipt of telecommunications services, approved by Resolution No. 295 of April 11, 2012, as amended on 08.04.2013]. https://zakon.rada.gov.ua/laws/show/295-2012-%D0%BF#Text (in Ukrainian)
5. Luhina, N. A., & Kybysh, I. V. (2022). *Zapobihannia kryminalnym pravoporushenniam, pov'iazanym iz vykorystanniam kryptovaliuty* [Prevention of criminal offenses related to the use of cryptocurrency]. *Analitychno-porivnialne pravoznavstvo – Analytical and Comparative Jurisprudence*, (4), 287–292. https://doi.org/10.24144/2788-6018.2022.04.52 (in Ukrainian)
6. Nykyforchuk, D. Y. (2010). Do pytannia vykorystannia rezultativ operatyvno-rozshukovoi diialnosti u kryminalnomu sudochynstvi [On the use of operational-search activity results in criminal proceedings]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)*, (22), 61–66. http://nbuv.gov.ua/UJRN/boz_2010_22_7 (in Ukrainian)
7. Sambor, M. A. (2013). *Nehlasni slidchi (rozshukovi) dii, poviazani iz zniattiam informatsii z transportnykh telekomunikatsiinykh merezh ta vstanovlenniam mistseznakhodzhennia radioelektronnoho zasobu* [Covert investigative (search) actions related to the interception of data from telecommunications networks and

tracking the location of a radio-electronic device]. *Visnyk Dnipropetrovskoho universytetu imeni Alfreda Nobelia. Seriia: Yurydychni nauky*, (1), 74–81. http://nbuv.gov.ua/UJRN/vdujn_2013_1_13 (in Ukrainian)

8. Samoilenko, O. A. (2020). *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostrori* [Fundamentals of methodology for investigating crimes committed in cyberspace] (A. F. Volobuiev, Ed.). Odesa: TES. https://doi.org/10.32837/11300.13264 (in Ukrainian)
9. Savchuk, N. V. (2009). *Kiberzlochynnist: zmist ta metody borotby* [Cybercrime: content and methods of combating]. *Teoretychni ta prykladni pytannia ekonomiky*, (19), 338–342. http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf (in Ukrainian)
10. Tahiiev, S. R. (2013). *Tymchasovyi dostup do informatsii, yaka znakhodytsia v operatoriv ta provideriv telekomunikatsii, u kryminalnomu provadzhenni* [Temporary access to information held by telecommunications operators and providers in criminal proceedings]. *Chasopys tsyvilnoho i kryminalnoho sudochynstva*, (4), 98–110. http://nbuv.gov.ua/UJRN/Chcks_2013_4_9 (in Ukrainian)