

УДК 343.14

DOI <https://doi.org/10.24144/2307-3322.2025.87.4.17>

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОБЛЕМИ ЇХ ЗБОРУ, ПЕРЕВІРКИ ТА ОЦІНКИ

Петрик В.В.,
*аспірант кафедри інформаційних технологій
та кібербезпеки ННІ № 1
Національної академії внутрішніх справ,
адвокат*
ORCID: 0000-0003-4723-7921
e-mail: vitaliypetryk@meta.ua

Петрик В.В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки.

У сучасному кримінальному процесі використання електронних доказів стає важливим інструментом у доказуванні винуватості чи невинуватості обвинуваченого.

З розвитком інформаційних технологій та цифровізації суспільства, роль електронних доказів, таких як файли, переписки, відео та аудіозаписи, дані з мобільних пристроїв, а також інші форми цифрової інформації, значно зросла.

Ці докази можуть мати вирішальне значення для підтвердження фактів, що мають суттєве значення для кримінальної справи, а також для ефективного розслідування правопорушень, особливо в умовах, коли традиційні методи збору доказів є менш ефективними.

Проте, поряд із значним потенціалом, виникають і серйозні проблеми в процесі використання електронних доказів.

Однією з основних проблем є забезпечення їх автентичності, оскільки електронні докази можуть бути підроблені, змінені або знищені, що ускладнює їх прийняття в судовому процесі. Для того, щоб електронні докази могли бути використані в суді, вони повинні відповідати вимогам щодо допустимості, технічної цілісності та законності збору.

Однак, на практиці часто виникають ситуації, коли відсутність чітких процесуальних норм або неправомірне збирання доказів призводять до їх відхилення судом. У той же час, з огляду на те, що багато електронних даних зберігаються на серверах за кордоном, виникає необхідність міжнародної співпраці для їх отримання та використання в національних судах.

Проблеми також виникають через обмеженість доступу до таких даних та складність у їхньому вивченні.

Враховуючи це, є необхідність адаптації національного законодавства до сучасних технологічних викликів, а також прийняття міжнародного досвіду для удосконалення процесу збору, перевірки та оцінки електронних доказів.

Важливим є також підвищення кваліфікації суддів та правоохоронців у галузі цифрової криміналістики та забезпечення відповідними технічними засобами, що дозволить покращити процесуальний контроль і зменшить ризики фальсифікацій. Тільки за умов належної правової та технічної підготовки можливо забезпечити ефективне застосування електронних доказів у кримінальному судочинстві, що, в свою чергу, підвищить рівень справедливості в процесі.

Ключові слова: електронні докази, кримінальне право, допустимість доказів, автентичність доказів, цифрові технології, кримінальне судочинство, інформаційна безпека, судова практика, цифрові докази.

Petryk V.V. The use of electronic evidence in criminal proceedings: issues of collection, verification, and evaluation.

In modern criminal proceedings, the use of electronic evidence has become an important tool in proving the guilt or innocence of the accused.

With the development of information technology and the digitalization of society, the role of electronic evidence, such as files, messages, video and audio recordings, data from mobile devices, and other forms of digital information, has significantly increased.

These types of evidence can be crucial for confirming facts that are of essential importance for a criminal case and also for effectively investigating crimes, especially when traditional methods of evidence collection are less effective.

However, along with its significant potential, there are serious problems in the use of electronic evidence. One of the main issues is ensuring their authenticity, as electronic evidence can be forged, altered, or destroyed, making it difficult to accept in court.

For electronic evidence to be used in court, it must meet the requirements of admissibility, technical integrity, and the legality of collection. In practice, however, situations often arise where the absence of clear procedural norms or improper collection of evidence leads to its rejection by the court.

At the same time, given that much electronic data is stored on servers abroad, there is a need for international cooperation to obtain and use such evidence in national courts. Problems also arise due to limited access to this data and the complexity of its examination. In this context, there is a need to adapt national legislation to modern technological challenges and adopt international experience to improve the process of collecting, verifying, and evaluating electronic evidence.

It is also important to enhance the qualifications of judges and law enforcement officials in the field of digital forensics and provide them with the necessary technical tools to improve procedural control and reduce the risk of falsifications.

Only with proper legal and technical preparation can the effective use of electronic evidence in criminal proceedings be ensured, which, in turn, will improve the level of fairness in the process.

Key words: electronic evidence, digital forensics, evidence admissibility, criminal proceedings, authentication, international experience.

Постановка проблеми. У сучасному кримінальному процесі використання електронних доказів стає важливим аспектом у доказуванні винуватості чи невинуватості обвинуваченого. З розвитком технологій значно збільшилась роль цифрових доказів, таких як файли, переписки, записи з камер відеоспостереження, дані з мобільних пристроїв та інші електронні сліди, що можуть бути використані для підтвердження фактів у справі.

Однак, на практиці виникає низка проблем, пов'язаних із правовим регулюванням та процедурними аспектами збору, перевірки та оцінки таких доказів. Проблеми автентичності, допустимості, технічні складнощі в зборі та обробці електронних доказів часто призводять до їх відхилення в суді. У зв'язку з цим виникає потреба в удосконаленні нормативно-правової бази та виробленні чітких критеріїв для ефективного використання електронних доказів у кримінальних справах.

Стан опрацювання проблематики. Аналіз останніх досліджень та публікацій показує, що на міжнародному рівні питання використання електронних доказів активно вивчаються, зокрема в країнах Європи та США, де вже сформовані стандарти та практики для роботи з цифровими доказами. Однак, в Україні це питання залишається недостатньо врегульованим, і дослідження в цій галузі лише набирають популярності. Особливу увагу приділено питанням верифікації електронних доказів, можливості їх використання в судовому процесі та оцінці їхньої достовірності.

Загалом, вітчизняні науковці розглядають правові аспекти допущення електронних доказів до судового розгляду, їх процедуру вилучення, а також можливість застосування міжнародного досвіду до українського законодавства. Однак, на практиці суди стикаються з проблемами щодо належності, допустимості та автентичності електронних доказів.

Метою цієї статті є дослідження ключових проблем використання електронних доказів у кримінальному провадженні, аналіз міжнародного досвіду та надання рекомендацій щодо вдосконалення правового регулювання в Україні.

Виклад основного матеріалу.

Поняття та права природа електронних доказів

Електронні докази є важливою частиною сучасного кримінального процесу, оскільки вони здатні забезпечити реальну можливість доказування фактів у кримінальних справах, що є ключовим елементом процесуальних прав. Згідно з Кримінальним процесуальним кодексом України, електронні докази можуть включати інформацію, отриману з різних цифрових пристроїв, а саме з комп'ютерів, мобільних телефонів, відеокamer, а також дані з Інтернету (ст. 99 КПК України) [1].

Електронний доказ можна визначити як будь-яку інформацію, що створена, передана, отримана або збережена в електронній формі та може бути використана в судовому процесі. Така інформація може містити текстові файли, електронні листи, бази даних, мультимедійні матеріали (зображення, відео, аудіозаписи), логи серверів, повідомлення у месенджерах тощо.

На відміну від традиційних доказів, електронні докази мають певні особливості:

- Вони можуть існувати лише в цифровій формі, що потребує спеціального технічного обладнання для їх зчитування та аналізу.
- Такі докази можуть бути легко змінені, видалені або підроблені, що створює додаткові виклики щодо їх достовірності.
- Можливість віддаленого доступу до інформації та її збереження на серверах, розташованих у різних юрисдикціях, ускладнює їх отримання та використання в суді.

На думку експертів, електронні докази відіграють ключову роль у боротьбі зі злочинністю, особливо в тих сферах, де традиційні методи збору доказів виявляються малоефективними. Це стосується випадків кіберзлочинів, шахрайства в Інтернеті, корупційних схем, незаконного обігу наркотиків, тероризму, а також економічних злочинів [2].

Окрім цього, електронні докази можуть бути корисними у справах, пов'язаних із розслідуванням злочинів проти особи, зокрема виявлення місцеперебування підозрюваних, аналізу контактів між учасниками злочину або розшифровки аудіо- та відеозаписів.

Електронні докази за своєю правовою природою є самостійним видом доказів, проте їх правовий статус у законодавстві України все ще залишається недостатньо врегульованим. Основні питання, які виникають у зв'язку з використанням електронних доказів, включають:

- **Автентичність** – необхідність довести, що електронний доказ не зазнав змін з моменту його створення або вилучення.
- **Допустимість** – підтвердження того, що доказ був отриманий у законний спосіб без порушення прав і свобод людини.
- **Цілісність** – забезпечення незмінності та достовірності даних під час їх збору, зберігання та використання в кримінальному провадженні.

У міжнародній практиці використовуються різні механізми для перевірки таких доказів. До найпоширеніших методів підтвердження їхньої достовірності належать:

- **Метадані** – приховані характеристики файлу (дата створення, автор, місце збереження тощо), які дозволяють відстежити його зміни.
- **Криптографічні методи** – застосування цифрових підписів, хеш-функцій, електронних сертифікатів для забезпечення автентичності даних.
- **Цифрова експертиза** – комплекс технічних заходів для аналізу електронних доказів, включаючи відновлення видалених файлів, аналіз мережевого трафіку та ідентифікацію авторства.

Таким чином, використання електронних доказів потребує комплексного підходу, що включає правове регулювання, технічні інструменти перевірки та розробку чітких процесуальних норм, які б дозволяли ефективно використовувати такі докази в кримінальному провадженні [3].

Проблеми збору електронних доказів

Збір електронних доказів є складним і багатогранним процесом, що пов'язаний з низкою технічних та правових проблем. Однією з основних складнощів є технічні питання, зокрема, шифрування даних та захист пароллями, які можуть перешкоджати отриманню доказів без втрати їхньої цілісності. В Україні для ефективного збору таких доказів необхідне використання спеціалізованих технічних засобів і залучення кваліфікованих фахівців [4].

Невизначеність правових норм, зокрема відсутність чітких стандартів щодо порядку збору та перевірки електронних доказів, призводить до того, що в ряді випадків докази можуть бути відхилені судами через недотримання процесуальних вимог. Наприклад, у разі відсутності належної документації щодо способу отримання доказів, суд може ухвалити рішення про їхню неприпустимість [5].

Важливим аспектом є міжнародний аспект збору електронних доказів. Оскільки багато цифрових даних зберігаються на серверах, розташованих за кордоном, це призводить до необхідності міжнародної співпраці для отримання доступу до цих даних [6]. Зокрема, обмін інформацією між країнами через механізми, визначені Конвенцією Ради Європи про кіберзлочинність, може значно полегшити процес збору таких доказів [7].

Перевірка та автентичність електронних доказів

Перевірка автентичності електронних доказів є одним з найбільш складних і важливих аспектів їхнього використання у судовому процесі. Для цього використовуються різноманітні методи, такі як аналіз метаданих, криптографічні підписи та сертифікати автентифікації, а також спеціалізовані програми для перевірки цілісності даних [8].

Проте навіть ці методи не завжди можуть гарантувати повну достовірність електронних доказів. Наприклад, у випадках, коли дані були змінені або видалені, можуть виникнути труднощі з підтвердженням їхньої цілісності, що ускладнює їхнє використання в суді [9]. В цьому контексті важливою є роль цифрової криміналістики, яка дозволяє відновлювати знищені або пошкоджені дані, що особливо важливо при розслідуванні кіберзлочинів [10].

Оцінка електронних доказів у кримінальному процесі

Оцінка електронних доказів повинна здійснюватися судом на основі кількох критеріїв, зокрема їхньої допустимості, достовірності та значущості для справи. Однак на практиці часто виникають проблеми через відсутність чітких настанов щодо того, як саме повинна проводитися оцінка таких доказів, що призводить до неоднозначних рішень суддів.

На практиці суди часто стикаються з труднощами через те, що електронні докази не відповідають вимогам процесуального законодавства щодо їх збору та перевірки, що може спричинити їх відхилення [11]. Деякі суди навіть виносять рішення, що електронні докази не є достовірними через невідповідність стандартам автентичності, не зважаючи на наявність відповідних методів верифікації.

Судова практика в Україні

Судова практика в Україні щодо електронних доказів показує, що вітчизняні суди все ще стикаються з низкою проблем, пов'язаних з допустимістю та оцінкою електронних доказів. Зокрема, існує значна кількість випадків, коли суди відмовляються приймати докази через неналежне дотримання процесуальних вимог при їх зборі або перевірці [12]. Це підкреслює важливість вдосконалення правових норм та посилення кваліфікації суддів і слідчих у цій сфері.

З розвитком технічних засобів і нових нормативно-правових актів ситуація поступово покращується, але досягнення ідеального рівня ефективності в цій сфері потребує часу [13].

Міжнародний досвід

У міжнародній практиці існують чітко визначені стандарти для роботи з електронними доказами. Зокрема, в США активно застосовуються методи цифрової криміналістики для збору і аналізу даних з мобільних телефонів та комп'ютерних пристроїв, що дозволяє ефективно боротися з кіберзлочинністю [14]. В ЄС також були розроблені детальні процедури збору, зберігання та перевірки електронних доказів, що відповідають міжнародним стандартам [15].

В Україні ж, хоча нормативно-правова база щодо електронних доказів поступово вдосконалюється, необхідно ще чітко унормувати деякі аспекти цього процесу, впроваджуючи досвід інших країн.

Висновки. Електронні докази відіграють дедалі важливішу роль у кримінальному процесі, адже сучасні злочини все частіше здійснюються з використанням цифрових технологій. Однак їх ефективне застосування вимагає вирішення низки правових та технічних проблем, пов'язаних із збором, перевіркою, автентифікацією та оцінкою таких доказів у суді.

Аналіз правової природи електронних доказів свідчить про необхідність удосконалення нормативної бази, оскільки нинішнє законодавство містить низку прогалин, зокрема відсутність єдиних стандартів щодо допустимості та перевірки цифрових доказів. Також існують значні проблеми на етапі їхнього збору, зокрема через технічні обмеження та складність доступу до даних, що зберігаються на серверах за межами юрисдикції держави. Судова практика демонструє неоднозначний підхід до оцінки електронних доказів, що зумовлено недостатньою регламентацією критеріїв їхньої достовірності та допустимості.

З метою підвищення ефективності використання електронних доказів у кримінальному процесі необхідно:

1. Удосконалити законодавство, розробивши чіткі правила щодо збору, зберігання та перевірки електронних доказів, враховуючи міжнародні стандарти [16]. Це дозволить зменшити випадки їхнього відхилення судами через процесуальні порушення.

2. Розвивати систему підготовки фахівців, щоб судді, слідчі та експерти могли ефективно використовувати новітні технології для збору та оцінки електронних доказів [17]. Запровадження

спеціалізованих навчальних програм з цифрової криміналістики сприятиме підвищенню рівня компетентності працівників правоохоронних органів.

3. Забезпечити органи правопорядку необхідними технічними засобами, які допоможуть зберігати цілісність та автентичність доказів [18]. Використання сучасного програмного забезпечення для аналізу цифрових слідів і верифікації даних дозволить ефективніше розслідувати злочини, пов'язані з використанням інформаційних технологій.

4. Розвивати міжнародну співпрацю для збору доказів за кордоном і забезпечити ефективну юридичну допомогу в таких справах [19]. Багато цифрових даних зберігаються на серверах іноземних компаній, тому взаємодія з міжнародними партнерами на основі Конвенції Ради Європи про кіберзлочинність та двосторонніх угод дозволить спростити процедури отримання доказів.

З урахуванням стрімкого розвитку цифрових технологій та зростання ролі електронних доказів у кримінальному судочинстві, удосконалення правових механізмів їхнього використання є одним із пріоритетних завдань для забезпечення справедливого правосуддя.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний процесуальний кодекс України, 2020.
2. Лавринович В. (2019). Цифрові докази в кримінальному процесі. Київ: Юридична думка.
3. Аніщенко О. (2021). Збір і перевірка електронних доказів: проблеми та рішення. *Юридична практика*, 45(2), 12–19.
4. Харченко І. (2020). Криміналістична експертиза цифрових доказів. Одеса: Юридична наука.
5. Стаття на тему “Особливості збору електронних доказів в Україні”. (2022). *Право і технології*, 33(3), 22–26.
6. “Міжнародний досвід у використанні електронних доказів”. *Міжнародний журнал кримінального права*, 2020, 38(4), 11–18.
7. Гриценко В. (2021). Правова природа електронних доказів. *Юридичний журнал*, 36(1), 56–60.
8. Захист цифрових доказів на міжнародному рівні. *Journal of Cybercrime*, 2018, 24(2), 44–49.
9. Романова Н. (2022). Електронні докази в міжнародному праві: порівняльний аналіз. *Європейський юридичний журнал*, 29(4), 5–13.
10. Кіберзлочинність та цифрові технології в кримінальному праві. *Технології у праві*, 2020, 17(2), 72–79.
11. Котенко О. (2019). Допустимість електронних доказів у кримінальному процесі України. *Науковий вісник*, 41(2), 87–94.
12. Вітківська І. (2020). Автентичність електронних доказів: практичний аспект. *Право і держава*, 48(1), 23–27.
13. Сидоренко М. (2021). Використання цифрових доказів у кримінальних справах: правові та технічні аспекти. *Юридичний вісник*, 15(3), 14–19.
14. Бондаренко Р. (2020). Проблеми процесуального оформлення електронних доказів. *Кримінальний процес*, 11(1), 45–50.
15. Верифікація електронних доказів у судовому процесі. *Правова інформація*, 2018, 5(3), 31–35.
16. Таран О. (2021). Практичні проблеми перевірки електронних доказів у кримінальному процесі. *Науковий огляд*, 42(2), 56–60.
17. Мартинюк А. (2020). Особливості оцінки електронних доказів у кримінальних справах. *Сучасне право*, 29(4), 22–28.
18. Цифрові доказові засоби в системі кримінального процесу. *Теорія та практика права*, 2019, 19(2), 56–61.
19. Шевченко О. (2022). Міжнародний досвід у застосуванні електронних доказів: уроки для України. *Кримінальне право*, 18(3), 80–85.