

Секція право	
УДК 343.14:004.056	
Дата першого надходження статті до видання	2026-03-12
Дата прийняття статті до друку після рецензування	2026-04-16
Дата публікації/оприлюднення	2026-04-19

Правове регулювання використання електронних (цифрових) доказів у кримінальному процесі

Предместніков Олег Гарійович

доктор юридичних наук, професор,
заслужений юрист України, завідувач кафедри права,
Мелітопольський державний педагогічний університет імені Богдана Хмельницького,
м.Запоріжжя, Україна

e-mail: predmestnikov@ukr.net

<http://orcid.org/0000-0001-8196-647X>

Татарнікова Тетяна Олександрівна

кандидат юридичних наук, заступник начальника
Центру судових і спеціальних експертиз,
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України, Київ, Україна

e-mail: t-tatarnikova@ukr.net

<https://orcid.org/0000-0002-5470-8288>

Семенюк-Прибатень Анна Вікторівна

кандидат юридичних наук, доцент кафедри археології,
спеціальних історичних та правознавчих дисциплін,
Кам'янець-Подільський національний університет імені Івана Огієнка,
Кам'янець-Подільський, Україна

e-mail: semanya31@ukr.net

<https://orcid.org/0000-0003-0520-5083>

Анотація. В статті здійснено комплексний аналіз правового регулювання використання електронних (цифрових) доказів у кримінальному процесі України, зумовленого стрімким розвитком цифровізації суспільства. Обґрунтовано актуальність дослідження, пов'язану із зростанням кількості кримінальних правопорушень, використанням інформаційних технологій, а також підвищенням ролі цифрових даних як джерела доказової інформації. Встановлено, що чинне кримінальне процесуальне законодавство не містить чіткого визначення поняття «електронні (цифрові) докази». Через це виникає їх неоднорідне тлумачення у правозастосовчій практиці, ускладнюючи формування єдиного підходу до їх оцінки.

Досліджено правову природу електронних (цифрових) доказів, їх характерні ознаки та місце в системі процесуальних джерел доказів. Визначено їх подвійну природу, що поєднує матеріальний носій та нематеріальний інформаційний зміст. Особливу увагу приділено проблемам збирання, фіксації, зберігання та дослідження електронних (цифрових) доказів, зокрема в частині забезпечення автентифікації, цілісності та допустимості. Проведено аналіз судової практики та наукових підходів до визначення

статусу електронних (цифрових) доказів. Окреслено основні проблеми, що виникають в процесі діяльності правоохоронних органів та суду.

Відсутність впроваджених в Україні уніфікованих стандартів роботи з електронними (цифровими) доказами, недостатня врегульованість процедур їх отримання й обробки, недосконалість механізмів міжнародного співробітництва впливають на ефективне розслідування кримінальних правопорушень. В рамках цього визначено необхідність впровадження принципу «ланцюга збереження доказів», використання сучасних технічних та криптографічних методів з метою забезпечення достовірності цифрової інформації та вдосконалення нормативно-правової бази.

На основі отриманих результатів дослідження запропоновано вдосконалити кримінально-процесуальне законодавство України, зокрема в частині визначення поняття електронних (цифрових) доказів, закріпити процедуру їх обробки та розширення процесуальних можливостей суб'єктів кримінального провадження. Практичне значення отриманих результатів полягає в можливості їх використання в правозастосовній діяльності та нормотворчому процесі з метою підвищення ефективності використання електронних (цифрових) доказів.

Ключові слова: електронні (цифрові) докази, кримінальний процес, ланцюг збереження доказів, судова практика, цифровізація, суб'єкти кримінального провадження, слідчий, дізнавач.

Legal regulation of the use of electronic (digital) evidence in criminal proceedings

Predmestnikov Oleh Gariyovych

Doctor of Law, Professor, Honored Lawyer of Ukraine,
Head of the Department of Law,
Bogdan Khmelnytsky Melitopol State Pedagogical University,
Zaporizhia, Ukraine

e-mail: predmestnikov@ukr.net

<http://orcid.org/0000-0001-8196-647X>

Tatarnikova Tetiana Oleksandrivna

PhD in Sciences of Law,
Deputy Head of the Center of Forensic and Special Expertises
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the
Security Service of Ukraine, Kyiv, Ukraine

e-mail: t-tatarnikova@ukr.net

<https://orcid.org/0000-0002-5470-8288>

Semeniuk-Prybaten Anna Viktorivna

Candidate of Law, Associate Professor of the Department of Archaeology,
Special Historical and Legal Disciplines
Ivan Ogienko National University of Kamyanets-Podilsky

e-mail: semanya31@ukr.net

<https://orcid.org/0000-0003-0520-5083>

Abstract. The article provides a comprehensive analysis of the legal regulation of the use of electronic (digital) evidence in the criminal process of Ukraine, due to the rapid development of the digitalization of society. The relevance of the study is substantiated, associated with the growth in the number of criminal offenses, the use of information technologies, as well as the

increasing role of digital data as a source of evidentiary information. It is established that the current criminal procedural legislation of Ukraine does not contain a clear definition of the concept of "electronic (digital) evidence". This leads to their heterogeneous interpretation in law enforcement practice, complicating the formation of a unified approach to their assessment.

The legal nature of electronic (digital) evidence, their characteristic features and place in the system of procedural sources of evidence are studied. Their dual nature, combining a material carrier and intangible information content, is determined. Special attention is paid to the problems of collecting, recording, storing and studying electronic (digital) evidence, in particular in terms of ensuring authentication, integrity and admissibility. An analysis of judicial practice and scientific approaches to determining the status of electronic (digital) evidence is conducted. The main problems that arise in the process of law enforcement agencies and the court are outlined.

The lack of unified standards for working with electronic (digital) evidence, insufficient regulation of the procedures for their receipt and processing, and the imperfection of international cooperation mechanisms affect the effective investigation of criminal offenses. Within this framework, the need to implement the principle of "chain of evidence preservation", the use of modern technical and cryptographic methods in order to ensure the reliability of digital information and improve the regulatory framework has been identified.

Based on the results of the study, it is proposed to improve the criminal procedural legislation of Ukraine, in particular in terms of defining the concept of electronic (digital) evidence, to consolidate the procedure for their processing and expanding the procedural capabilities of subjects of criminal proceedings. The practical significance of the results obtained lies in the possibility of their use in law enforcement activities and the rule-making process in order to increase the efficiency of the use of digital evidence.

Keywords: electronic (digital) evidence, criminal process, chain of evidence preservation, judicial practice, digitalization, subjects of criminal proceedings, investigator.

Вступ

Актуальність проблеми. Розвиток інформаційних технологій, цифровізація суспільства та активне використання мережі Інтернет зумовлюють поширення росту кримінальних правопорушень, пов'язаних із використанням електронних пристроїв та цифрового середовища. В рамках цього електронні (цифрові) докази стають ключовим джерелом доказової інформації у кримінальному процесі. Окреслена проблема набуває особливої актуальності з огляду на те, що традиційні підходи до збирання, фіксації, зберігання та оцінювання доказів не завжди є придатними для роботи з цифровими даними. Властиві електронним (цифровим) доказам ознаки – нематеріальність, легкість копіювання, можливість швидкої зміни чи знищення – ускладнюють забезпечення їх достовірності та процесуальної допустимості.

Окрім того, актуальним залишається питання нормативно-правового врегулювання питань використання електронних (цифрових) доказів у кримінальному процесі, відсутність чітко визначених та уніфікованих процедур їх збирання, фіксації, зберігання та дослідження. Це призводить до виникнення практичних труднощів у діяльності правоохоронних органів та суду, а також до неоднозначного тлумачення процесуальних норм.

Зважаючи на це, важливо забезпечити баланс між ефективністю кримінального провадження й дотриманням основоположних прав і свобод людини, зокрема права на приватність, захист персональних даних, недоторканість приватного життя. Окрім того

існує потреба в комплексному науковому аналізі правового регулювання використання електронних (цифрових) доказів, розробки пропозицій з вдосконалення кримінального процесуального законодавства та формування єдиної правозастосовної практики в обраній сфері.

Аналіз останніх досліджень і публікацій. Проблематику використання електронних (цифрових) доказів у кримінальному процесі за останні роки активно досліджували як вітчизняні, так і зарубіжні науковці. Значний теоретичний та практичний внесок у цьому напрямі здійснили Б.М. Орловський, С.Р. Тагієв, О.Д. Квашук, В.Д. Мехеда, І. Каланча, А.-М.Ю. Ангеленюк та інші (науковці в своїх публікаціях використовували терміни «електронний доказ», «цифровий доказ»; у цій роботі авторами застосовується термін «електронні (цифрові) докази» як такий, що об'єднує обидва варіанти й не виокремлює жодного через відсутність його закріплення в кримінально-процесуальному законодавстві України).

В наукових працях Б.М. Орловського та С.Р. Тагієва увага зосереджується на визначенні правової природи цифрових доказів та їх місці в системі доказів у кримінальному процесі. Дослідники підкреслюють їх специфічність, зокрема нематеріальний характер та залежність від технічних засобів.

Науковці О.Д. Квашук та Р. Бондаренко звертають увагу на проблеми практичного застосування електронних доказів, зокрема в питаннях їх допустимості, належності та процесуального оформлення. Дослідники В.Д. Мехеда та І. Каланча визначають необхідність запровадження сучасних технічних і правових механізмів забезпечення автентичності та цілісності цифрових даних, зокрема концепції «ланцюга збереження доказів» (chain of custody).

Проблемні аспекти нормативного регулювання та визначення процесуального статусу електронних (цифрових) доказів розглядаються в працях А.-М.Ю. Ангеленюк, яка наголошує на відсутності чітких законодавчих положень щодо джерел їх отримання та порядку використання. Питання міжнародного досвіду та порівняльно-правового аналізу висвітлено в роботах Я.В. Неділька, Н.М. Сенченка та В.Ю. Чумаченка, де обґрунтовується необхідність гармонізації національного законодавства з європейськими стандартами.

Не зважаючи на значну кількість наукових праць, питання комплексного правового регулювання використання електронних (цифрових) доказів у кримінальному процесі залишається недостатньо дослідженим, зумовлюючи актуальність подальших наукових розробок у цій сфері.

Виділення невирішеної частини проблеми. Незважаючи на активний розвиток наукових досліджень у сфері кримінального процесу та цифровізації правосуддя, низка важливих аспектів правового регулювання використання електронних (цифрових) доказів є недостатньо врегульованою як на теоретичному, так і в практичному вимірі. Насамперед відсутнє чітке та уніфіковане визначення поняття «електронні (цифрові) докази» у кримінально-процесуальному законодавстві, що призводить до різного їх тлумачення у правозастосовчій практиці. Недостатньо врегульованим залишається питання процесуального порядку збирання, фіксації, вилучення, зберігання й дослідження доказів, оскільки це ускладнює забезпечення їх належності, допустимості й достовірності.

Окремою невирішеною проблемою є відсутність єдиних стандартів та методик роботи з електронними (цифровими) доказами, зокрема в частині забезпечення їх цілісності, а також документування процесу їх отримання. Це, в свою чергу, формує ризики втрати доказової сили таких даних в суді. Поміж з тим потребують подальшого наукового опрацювання питання використання спеціальних знань та технічних засобів під час роботи з електронними (цифровими) доказами, а також визначення чіткого процесуального статусу спеціалістів та експертів у цій сфері, їхніх повноважень та відповідальності. Не до кінця врегульованим залишається питання міжнародного співробітництва у сфері отримання електронних (цифрових) доказів, зокрема доступу до даних, які зберігаються на серверах за межами держави. Це ускладнює ефективність розслідування транснаціональних кримінальних правопорушень.

Таким чином, актуальним є забезпечення належного балансу між інтересами кримінального правосуддя та дотриманням основоположних прав і свобод людини. Наявність зазначених невирішених питань свідчить про необхідність подальшого комплексного дослідження проблем правового регулювання використання електронних (цифрових) доказів у кримінальному процесі, а також розробки науково обґрунтованих підходів до їх вирішення та вдосконалення законодавчих і практичних аспектів.

Мета статті. Мета статті полягає в комплексному науковому аналізі правового регулювання використання електронних (цифрових) доказів у кримінальному процесі, виявлення існуючих проблем та прогалин у законодавстві та правозастосовній практиці, обґрунтування шляхів їх усунення з метою вдосконалення кримінального процесуального законодавства й підвищення ефективності використання електронних (цифрових) доказів у кримінальному провадженні.

Наукова новизна. Наукова новизна отриманих результатів полягає в дослідженні особливостей правового регулювання використання електронних (цифрових) доказів у кримінальному процесі та формуванні нових науково обґрунтованих підходів до вирішення існуючих проблем в обраній сфері. В роботі уточнено зміст поняття «електронні (цифрові) докази» та виокремлено їх головні ознаки як самостійного виду доказів у кримінальному провадженні. Поміж з тим визначено специфіку їх збирання, фіксації, зберігання та оцінки із врахуванням технічних характеристик цифрової інформації. Обґрунтовано необхідність запровадження єдиних стандартів і процедур роботи з електронними (цифровими) доказами, спрямованих на забезпечення їх цілісності, автентичності й допустимості. Запропоновано напрями вдосконалення кримінального процесуального законодавства в частині регулювання використання електронних (цифрових) доказів. Отримані результати розширюють наукові уявлення про правову природу електронних (цифрових) доказів і можуть використовуватися для використання у подальших наукових дослідженнях та правозастосовній діяльності.

Практичне значення. Отримані результати полягають у можливості їх використання з метою вдосконалення кримінального процесуального законодавства України у сфері регулювання використання електронних (цифрових) доказів, а також у підвищенні ефективності правозастосовної діяльності. Висновки та пропозиції, висловлені в роботі, можуть використовуватися у практичній діяльності правоохоронних органів, слідчих, прокурорів, суддів, спеціалістів і експертів під час

збирання, фіксації, дослідження та оцінки цифрових доказів, сприяючи забезпеченню їх належності, допустимості та достовірності.

Результати дослідження можуть застосовуватися у навчальному процесі під час викладання кримінального процесу, а також при підготовці методичних матеріалів, рекомендацій і роз'яснень у роботі з електронними (цифровими) доказами. Окрім того практичні результати є основою для подальших наукових розробок у сфері цифровізації кримінального судочинства.

Методологія

Методи дослідження. Методологічну основу дослідження складають загальнонаукові та спеціально-юридичні підходи до аналізу правового регулювання використання електронних (цифрових) доказів у кримінальному процесі. Дослідження сформовано на принципах об'єктивності, системності, комплексності та міждисциплінарності. Це дає змогу поєднати правовий і технічний аспекти досліджуваної проблеми. Головна увага приділена взаємозв'язку норм кримінального процесуального права з сучасними інформаційними технологіями.

В процесі дослідження використано такі методи:

- діалектичний метод використовується для аналізу розвитку правового регулювання електронних (цифрових) доказів;
- формально-юридичний – застосовується для тлумачення норм кримінального процесуального законодавства;
- порівняльно-правовий – лежить в основі зіставлення національного законодавства з міжнародними нормами;
- системно-структурний – визначає місце електронних (цифрових) доказів у системі доказів у кримінальному процесі;
- логіко-правовий метод – використовується для формулювання висновків;
- аналіз та синтез – застосовується для узагальнення наукових підходів та практичного досвіду.

Джерела даних. Джерельна база дослідження наповнена нормами кримінального процесуального законодавства України, міжнародно-правовими актами у сфері протидії кіберзлочинності, науковими працями вітчизняних та зарубіжних вчених, судовою практикою, аналітичними матеріалами правоохоронних органів.

Інструменти аналізу. Для досягнення поставленої мети застосовано інструменти правового аналізу, зокрема нормативно-правовий аналіз, порівняльний аналіз законодавства, судової практики, елементи техніко-правового аналізу електронних (цифрових) доказів. Використання зазначених інструментів дозволить дослідити особливості правового регулювання та виявити існуючі прогалини.

Обмеження дослідження. Дослідження має певні обмеження, зумовлені швидким розвитком інформаційних технологій. Через це окремі нормативні положення й практичні підходи можуть швидко деактуалізуватися. Обмеження пов'язані також із недостатньою кількістю узагальнення судової практики щодо застосування електронних (цифрових) доказів, відсутністю єдиних стандартів їх обробки. Робота, зосереджена переважно на правових аспектах проблеми, не завжди дає можливість в повній мірі врахувати технічні особливості функціонування електронних (цифрових) доказів.

Результати

Розвиток доказового права завжди супроводжувався пошуком ефективних способів збору та оцінки інформації у кримінальних справах. У часи середньовіччя свідчення та письмові документи були основним джерелом доказів. Сучасними методами доказування є електронне документування та цифрове зберігання інформації. Важливо наголосити, що з появою інформаційних технологій у другій половині ХХ століття кримінальний процес зазнав істотних змін. Відтоді комп'ютерні системи, електронна пошта, мобільні пристрої та мережеві сервіси стали не лише об'єктом злочинної діяльності, а й джерелом важливих доказів. Зважаючи на це, виникла потреба у розробці спеціалізованих правових норм, які б регулювали збір, обробку та використання електронних (цифрових) доказів, визначаючи їх допустимість та оцінку. На відміну від традиційних, електронні (цифрові) докази легко змінити. Окрім того, вони залежні від технічних умов, в яких зберігаються.

Як слушно зазначає Б.М. Орловський, стрімкий розвиток кримінально-процесуального законодавства про докази й доказове право в умовах цифровізації зумовлює потребу в чіткому визначенні їх сутності та місця в кримінальному процесі. Стаття 84 КПК України [1] називає доказами будь-які фактичні дані, здобуті законним шляхом, на підставі яких встановлюються обставини кримінального провадження. Перелік процесуальних джерел доказів, визначених статтею, не в повній мірі відображає специфіку електронної інформації. Головна теоретична проблема на даному етапі полягає у визначенні, до якої з існуючих категорій необхідно віднести цифрові докази із врахуванням їхньої гібридної природи.

Хоча законодавець в статті 99 КПК України й намагався частково вирішити проблему визначення електронних носіїв як електронних (цифрових) доказів, однак відповідно до цієї статті документ може мати ознаки речового доказу, якщо він є незмінним. Саме цей підхід є одним із дискусійних в сучасному науковому просторі, оскільки головна характеристика цифрового світу є його мінливість та нематеріальність інформації як такої, на відміну від матеріального носія, на якому зберігається інформація.

Стаття 98 КПК [1] визначає речові докази матеріальними об'єктами, що зберегли в собі сліди правопорушення. Отже, якщо електронний носій використовується як знаряддя злочину чи містить сліди протиправних дій, він вважається речовим доказом. Більшість цінних електронних (цифрових) доказів, таких як дані з хмарних сховищ чи журнали віддалених серверів, є нематеріальною інформацією, яка вилучається шляхом копіювання, а не як оригінальний матеріальний об'єкт.

Вчений Б.М. Орловський зазначає, що на практиці цифрові докази мають подвійну правову природу: носій інформації, наприклад смартфон чи сервер, розглядається як речовий доказ у вигляді матеріального об'єкта, тоді як інформація, що зберігається на ньому, є різновидом документа – фактичними даними, зафіксованими електронними засобами [2, с. 138].

На думку науковця С.Р. Тагієва, використання електронних доказів у кримінальному судочинстві є звичною справою щодо переважної більшості категорій кримінальних справ. Електронними доказами виступають електронні записи, повідомлення, файли, інші дані, які зберігаються на електронних носіях. Нині будь-які обставини, що підлягають доказуванню, можуть бути у цифровій формі. Електронні докази охоплюють інформацію у цифровому вигляді, здатні встановлювати фактичні обставини кримінального провадження, що зберігаються на електронному носії чи існують незалежно від нього [3].

За роки незалежності України в КПК України законодавець не закріпив визначення поняття «електронний (цифровий) доказ» («цифровий доказ» або «електронний доказ»), задля з'ясування змісту досліджуваної правової категорії. В науці

кримінально-процесуального права міститься достатня кількість варіантів визначення цього поняття та пояснюється зміст його правової природи. Вчений В. Мурадов до електронних доказів відносить сукупність інформації, що міститься в електронному вигляді на будь-яких типах електронних носіїв і в електронних засобах [4, с. 314].

Вчений О.Д. Квашук зазначає, що вітчизняні суди зіштовхуються з низкою проблем, пов'язаних із допустимістю та оцінкою електронних доказів. Інколи суди відмовляються приймати докази через неналежне дотримання процесуальних вимог під час їх збору чи перевірки. Це ще раз наводить на думку вдосконалити правові норми та підвищити підготовку фахівців у цій сфері [5, с. 53].

Розвиток технічних засобів та поява нових нормативно-правових актів поступово змінює впровадження електронних (цифрових) доказів [6, с. 16]. Так у справі № 753/10840/19 від 13.07.2020 зроблено висновок, що повідомлення, надіслані за допомогою Viber та скріншоти з мобільних пристроїв є електронним (цифровим) доказом у справі про насильство. І хоча сторона відповідача наголошувала на тому, що такі повідомлення не є доказами, оскільки містить низку суттєвих характеристик, Касаційний цивільний суд не погодився із такими доводами і визнав скріншоти електронної переписки у застосунку Viber належними доказами психологічного насильства з боку відповідача [7].

У справі № 751/6069/19 Верховний Суд також висловив позитивну позицію, визнавши долучений до матеріалів провадження в якості речового доказу DVD-R-диск з відео-записом обставин подій. Тобто записаний на оптичний диск – носій інформації, електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документа [8].

В Україні інтеграція у кримінальний процес електронних (цифрових) доказів потребує вдосконалення нормативно-правової регламентації із врахуванням зарубіжного досвіду, де відповідна практика є більш розвиненою. До прикладу в США методи цифрової криміналістики успішно використовуються для збору й аналізу даних з мобільних телефонів та комп'ютерних пристроїв, дозволяючи ефективно боротися з кіберзлочинами [9, с. 47].

Національне законодавство Австрії, Болгарії, Чехії, Італії, Швеції та низки інших європейських країн не містить поняття «електронні (цифрові) докази». Подібна ситуація спостерігається і в законодавстві Португалії, де також не закріплено нормативного тлумачення терміну «електронний (цифровий) доказ». Водночас у науковій літературі використовується визначення, відповідно до якого електронний (цифровий) доказ розглядається як будь-яка інформація, що має доказове значення й зберігається на цифровому пристрої чи передається у цифровій формі [10, с. 169].

В Німеччині, Бельгії, Іспанії, Фінляндії, Франції, Ірландії, Люксембургу, Португалії та Румунії електронні (цифрові) докази рівнозначні з паперовими документами, що мають юридичне значення у судовому процесі [11, с. 286].

Стаття 16 КПК Латвії визначає електронними (цифровими) доказами у кримінальному провадженні факти у вигляді обробленої електронної інформації, яка зберігається чи передається автоматизованими пристроями чи системами обробки даних [12].

Міжнародна практика країн Європейського Союзу зазначає, що до електронних (цифрових) доказів у кримінальному провадженні суди застосовують низку критеріїв, які визначають їх достатність та допустимість:

- 1) законність отримання – передбачає, що докази повинні збиратися відповідно до законодавства, не порушуючи прав людини;
- 2) автентичність та цілісність – електронні (цифрові) докази повинні зберігатися в первісному вигляді, без жодних змін;

- 3) допустимість та належність передбачає, що доказ повинен стосуватися справи та підтверджувати чи спростовувати обставини, які розглядаються;
- 4) необхідно забезпечити документування кожного етапу роботи з електронними (цифровими) доказами;
- 5) технологічна нейтральність характеризується принципами застосування до всіх типів електронних (цифрових) доказів незалежно від платформи або технологій, яка використовувалася [13, с. 258-259].

Наразі в міжнародній практиці відсутня універсальна міжнародна чи європейська правова база, яка б врегульовувала питання електронних (цифрових) доказів. Зазвичай держави керуються нормами національного законодавства під час збирання, використання та обміну такими доказами. Кримінальне законодавство багатьох країн сформовано задовго до розвитку інтернету та технологій, здатних створювати електронні (цифрові) докази. Зважаючи на це, частина держав адаптувала свою нормативно-правову базу до нових аспектів, в той час як інші продовжують застосовувати традиційні підходи, поширюючи їх і на цифрову сферу. Така неоднорідність зумовлює істотні відмінності національних правових систем і підходів, спрямованих на обробку міжнаціональних електронних (цифрових) доказів, ускладнюючи міжнародну співпрацю. Дослідження ООН у сфері кіберзлочинності, навіть у державах із подібними правовими традиціями доказування, можуть значно відрізнятися, формуючи додаткові перешкоди для ефективної міжнародної взаємодії у боротьбі зі злочинністю [14].

Вчена А.-М.Ю. Ангеленюк визначає низку проблемних питань, пов'язаних із використанням електронних (цифрових) доказів у кримінальному процесуальному праві України. Насамперед, це не розмежованість електронного (цифрового) доказу від інших джерел доказів. Низка дослідників відносять електронні (цифрові) докази до окремої самостійної групи. Судова практика також не є однорідною: з одного випадку суди визначають файли електронними (цифровими) доказами, а носії, де вони зберігаються – речовими доказами, в інших – електронні (цифрові) докази ототожнюються з електронними документами. Поняття електронного документа є більш вузьким, ніж електронного (цифрового) доказу, оскільки передбачає наявність обов'язкових реквізитів, характерних для документів. Своєю чергою електронні (цифрові) докази не завжди містять такі реквізити, однак в них наявна інформація, що має доказове значення. В рамках цього цілком доцільно виокремити носії електронної інформації як самостійні процесуальні джерела доказів.

Наступною причиною, яку вказує автор є невизначеність джерел отримання електронних (цифрових) доказів у кримінальному провадженні. Наразі кримінально-процесуальне законодавство України не містить чіткого визначення джерел отримання електронних (цифрових) доказів, тим самим створюючи правову невизначеність у цій сфері. Судова практика помалу заповнює цю прогалину, формуючи підходи до оцінки допустимості таких доказів залежно від способу їх отримання. Разом з тим, відсутність єдиного нормативного регулювання призводить до неоднакової правозастосовної практики. Зважаючи на це існує необхідність законодавчого регулювання джерел отримання електронних (цифрових) доказів у кримінальному провадженні. Доцільно доповнити КПК України окремою нормою, яка б чітко визначала перелік таких джерел.

Ще однією проблемою є недостатність нормативно-правового регулювання використання копії електронних (цифрових) доказів, оригінали яких втрачені. Положення статті 99 КПК України визначають можливість визнання копій як оригіналів за певних умов, однак на практиці виникають ситуації, коли реальне виконання цих вимог ускладнюється або зовсім не виконується. Зокрема це стосується електронних даних із обмеженим строком зберігання, які можуть бути втрачені до їх належного процесуального оформлення. В такому випадку постає нагальна потреба вдосконалення

законодавства шляхом розширення підстав допустимості копій електронних (цифрових) доказів. Доцільним є також визнання таких копій допустимими за умови відсутності ознак їх зміни та підтвердження відповідних відомостей іншими доказами.

Проблемним питанням на думку А.-М.Ю. Ангеленюк [15] є також обмеження можливостей дізнавача щодо використання електронних доказів. Для використання ресурсів інформаційно-телекомунікаційних систем досудового розслідування дізнавач повинен мати належні правові підстави, безпосередньо пов'язані із збиранням та дослідженням електронної інформації. Вітчизняне законодавство не в повній мірі враховує його повноваження у цій сфері, актуалізуючи потребу внесення змін до статті 99 КПК України [1] шляхом поширення положень щодо виготовлення копій та дублікатів документів також на дізнавача. Загалом, пропонується доповнити відповідну норму після слів «виготовлені слідчим» словом «дізнавачем».

Проблемним аспектом залишається також неорганізованість роботи інформаційно-телекомунікаційної системи досудового розслідування. Стаття 106-1 КПК України [1] визначає, що слідчий, дізнавач, прокурор, слідчий суддя, суд, захисник (за його згодою) використовують інформаційно-телекомунікаційну систему досудового розслідування під час реалізації своїх процесуальних повноважень, в той час як інші учасники кримінального провадження можуть користуватися нею за встановленими умовами та порядком. Порядок функціонування вказаної системи визначається відповідним положенням, затвердженим Офісом Генерального прокурора, органом досудового розслідування, органом, що регулює функціонування судової інформаційної системи. Відповідно до положень статті 106-1 КПК України [1], а також до вимог в частині інтеграції Єдиного реєстру досудових розслідувань із державними інформаційними системами та функціональних можливостей судових інформаційних систем, цілком очевидним є необхідність забезпечення ефективної взаємодії між відповідними цифровими платформами. В рамках цього планується вдосконалити організацію роботи інформаційно-телекомунікаційної системи досудового розслідування шляхом її системної інтеграції та належного нормативного врегулювання [15].

Вчений В.Д. Мехеда зазначає, що наразі вдосконалення правового регулювання електронних доказів у кримінальному процесі потребує чіткого визначення поняття «електронний доказ», а також нормативного закріплення процедур ідентифікації, забезпечення «ланцюга збереження» та верифікації цифрових даних. На думку науковця, доцільно також доповнити КПК України [1] окремою нормою, яка б встановлювала вимоги до електронної форми подання доказів, порядок їх автентифікації, можливість перевірки контрольних сум та залучення спеціалістів у сфері цифрової експертизи. Зазначені підходи вже імплементовані у кримінально-процесуальному законодавстві низки держав ЄС – в Німеччині, Франції, Польщі, де врегульовано алгоритм поводження з електронними доказами. Разом з тим обґрунтовується необхідність вдосконалення положень статті 246 КПК України [1] щодо негласних слідчих дій шляхом запровадження вимог окремого судового дозволу для кожної процесуальної дії чи епізоду, а також обов'язкового повного документування процесу збирання, збереження й передачі цифрових матеріалів [16].

Вчена І. Каланча наголошує, що ефективність використання електронних доказів у кримінальному провадженні зумовлена наявністю надійних механізмів забезпечення їх цілісності та автентичності. Ключовим елементом цього процесу є концепція chain of custody (ланцюг збереження доказів). Зазначена концепція охоплює низку технічних та процесуальних засобів, спрямованих на ідентифікацію, збирання, отримання, збереження. Дослідження, аналіз та подання доказів. Застосування зазначеної концепції здатне мінімізувати ризики несанкціонованого втручання, зміни чи підміни електронної інформації, при цьому забезпечуючи її належну доказову силу.

Процесуальні норми КПК України, зокрема протоколювання, фіксація та ідентифікація, здатні забезпечити лише базовий рівень захисту електронних (цифрових) доказів. Разом з тим, відсутність чітко визначених технічних процедур, зокрема хешування чи побітове копіювання, а також єдиних правил роботи з цифровими даними знижує їх надійність, при цьому створюючи ризики втрати або зміни інформації. Міжнародний стандарт ISO/IEC 27037:2012 (національний стандарт ДСТУ ISO/IEC 27037:2017), особливості якого описує вчена, пропонує чіткі правила виявлення, збирання й збереження електронних (цифрових) доказів, однак в Україні вони не впроваджені в достатній мірі. Цьому в першу чергу заважають особливості кримінального процесу. В рамках цього дослідника пропонує розробити чіткі стандарти для слідчих, прокурорів та експертів, які б врегульовували всі етапи роботи з електронними (цифровими) доказами. Важливо також на законодавчому рівні закріпити принцип «ланцюга збереження доказів», з метою відстеження всіх дій з доказами, як гарантії їх незмінності. Впровадження подібних підходів сприятиме підвищенню достовірності електронних (цифрових) доказів і покращенню захисту прав учасників кримінального провадження [17].

Незважаючи на низку проблемних питань використання електронних (цифрових) доказів у кримінальному процесі, визначених різними дослідниками, цілком закономірно виокремити ще одне не менш важливе питання – недостатня урегульованість питань автентифікації електронних (цифрових) доказів, збереження їх цілісності під час обігу в межах кримінального провадження. Вітчизняне законодавство не містить уніфікованих вимог, що стосуються технічних та процесуальних стандартів підтвердження достовірності цифрових даних, ускладнюючи їх належну оцінку судом. На практиці це призводить до залежності допустимості електронних (цифрових) доказів від способу їх отримання й рівня технічного оформлення, а не від єдиних правових критеріїв. Зважаючи на це, актуалізується необхідність законодавчого закріплення чітких механізмів ідентифікації, перевірки й фіксації цілісності електронних (цифрових) доказів з використанням сучасних криптографічних та інформаційних технологій.

Разом з тим важливо продовжувати впроваджувати раніше запропоновані інновації, зокрема розробку стандартних операційних процедур роботи з електронними (цифровими) доказами, інтеграція міжнародних стандартів у національне законодавство, а також нормативне закріплення принципу «ланцюга збереження доказів». Комплексна реалізація цих підходів сприятиме підвищенню ефективності використання електронних (цифрових) доказів, забезпеченню їх достовірності та зміцненню процесуальних гарантій у кримінальному провадженні.

Обговорення

Інтерпретація результатів. Одержані результати свідчать про те, що сучасний стан правового регулювання використання електронних (цифрових) доказів у кримінальному процесі України визначається фрагментарністю та наявністю істотних прогалин. Встановлено, що відсутність чіткого визначення в кримінальному процесуальному законодавстві поняття «електронний (цифровий) доказ» («електронний доказ» або «цифровий доказ»), складнощі, пов'язані із його співвідношенням з іншими процесуальними джерелами доказів ускладнюють формування єдиної правозастосовної практики. Доведено, що головними проблемами наразі залишаються неврегульованість джерел отримання електронних (цифрових) доказів, недостатність нормативного забезпечення їх автентифікації й цілісності, а також обмеженість процесуальних можливостей окремих об'єктів кримінального провадження.

Результати дослідження підтверджують, що ефективність використання електронних (цифрових) доказів залежить від впровадження комплексу технічних та процесуальних механізмів, зокрема принципу «ланцюга збереження доказів», стандартів ідентифікації та перевірки цифрових даних. Разом з тим доведено необхідність системної інтеграції інформаційно-телекомунікаційних систем та адаптації міжнародних стандартів до національного законодавства.

Порівняння з іншими дослідженнями. Отримані результати узгоджені із науковими підходами, викладеними в наукових працях Б.М. Орловського, С.Р. Тагієва, О.Д. Квашук, А.-М. Ю. Ангеленюк, В.Д. Мехеди та І. Каланчі. Згадані науковці зосереджували увагу на проблемних аспектах правового визначення електронних (цифрових) доказів, їх допустимості й оцінки у кримінальному процесі. У висновках наукових напрацювань підтверджено існування подвійної правової природи електронних (цифрових) доказів та відсутність єдиного підходу до їх класифікації

На відміну від зазначених наукових праць в даному дослідженні більш комплексно обґрунтовано необхідність поєднання правових і технічних механізмів забезпечення автентичності та цілісності електронних (цифрових) доказів, в тому числі через впровадження криптографічних методів і стандартів цифрової криміналістики. Разом з тим, розширено підхід до аналізу проблеми шляхом врахування організаційних аспектів функціонування інформаційно-телекомунікаційних систем та їх взаємодії з іншими державними реєстрами.

Наукова новизна (розгорнуто). Новизна наукового дослідження полягає в комплексному поєднанні теоретичних та прикладних підходів до вдосконалення правового регулювання використання електронних (цифрових) доказів у кримінальному процесі України. В процесі дослідження уточнено зміст поняття «електронний (цифровий) доказ» із врахуванням його нематеріальної природи та інформаційного змісту. Крім того поглиблено наукові підходи до визначення місця електронних (цифрових) доказів в системі процесуальних джерел доказів, а також обґрунтовано доцільність їх виокремлення як самостійної категорії. Вперше здійснено обґрунтування необхідності законодавчого закріплення механізмів автентифікації, ідентифікації та забезпечення цілісності електронних (цифрових) доказів із застосуванням сучасних інформаційних та криптографічних технологій. Обґрунтовано необхідність впровадження типу «ланцюга збереження доказів» як ключового елемента забезпечення достовірної цифрової інформації, а також запропоновано напрями вдосконалення організації функціонування інформаційно-комунікаційних систем досудового розслідування шляхом інтеграції з іншими державними цифровими платформами. Загалом, дослідження формує новий комплексний підхід до вирішення проблем використання електронних (цифрових) доказів, поєднуючи правові, організаційні та технічні аспекти.

Практичне значення (розгорнуто). Практичне значення отриманих результатів полягає у можливості їх безпосереднього використання з метою вдосконалення кримінального процесуального законодавства України та підвищення ефективності правозастосовної діяльності. Запропоновані положення можуть використовуватися у нормотворчій діяльності з метою підготовки змін і доповнень до КПК України, зокрема в частині визначення електронних (цифрових) доказів, джерел їх отримання, правил

автентифікації та забезпечення цілісності. Разом з тим результати дослідження можуть використовуватися в практичній діяльності слідчих, дізнавачів, прокурорів, суддів, спеціалістів і експертів з метою вдосконалення процедур збирання, фіксації, дослідження та оцінки електронних (цифрових) доказів; при розробці стандартних операційних процедур і методичних рекомендацій щодо роботи з електронними (цифровими) доказами відповідно до міжнародних стандартів. У навчальному процесі результати дослідження можуть використовуватися в процесі викладання дисциплін з кримінального процесу, криміналістики та інформаційного права. У сфері міжнародної діяльності отримані результати сприятимуть гармонізації національного законодавства з європейськими стандартами у сфері застосування електронних (цифрових) доказів. Реалізація запропонованих підходів сприятиме підвищенню достовірності електронних (цифрових) доказів, забезпеченню їх належної процесуальної оцінки, а також зміцненню гарантій прав учасників кримінального провадження.

Висновки

Проведене дослідження встановило, що в умовах цифровізації суспільства електронні (цифрові) докази набувають важливого значення у кримінальному процесі, виступаючи важливим джерелом доказової інформації. Разом з тим, їх правова природа, особливості формування й використання зумовлюють необхідність переосмислення традиційних підходів до доказування.

В рамках статті підтверджено, що вітчизняне кримінально-процесуальне законодавство України не забезпечує належного та комплексного регулювання використання електронних (цифрових) доказів. Відсутність законодавчо закріпленого поняття «електронний (цифровий) доказ» («електронний доказ» або «цифровий доказ»), нечіткість у визначенні їх місця серед процесуальних джерел доказів, а також неврегульованість процедур їх збирання, фіксації, зберігання й дослідження зумовлюють неоднорідний підхід до правозастосовної практики. На основі цього обґрунтовано, що ключовими проблемами у сфері використання електронних (цифрових) доказів є відсутність єдиних стандартів і процедур їх обробки, недостатня урегульованість питань автентифікації та забезпечення цілісності цифрових даних; невизначеність джерел отримання таких доказів; обмеженість процесуальних можливостей окремих суб'єктів кримінального провадження; складність міжнародного співробітництва у сфері отримання електронних (цифрових) доказів.

Зважаючи на це, подальший розвиток правового регулювання використання електронних (цифрових) доказів має здійснюватися на основі комплексного підходу, який би поєднував правові, технічні та організаційні аспекти. Реалізація запропонованих у дослідженні положень сприятиме підвищенню ефективності кримінального провадження, забезпеченню належної доказової сили електронних (цифрових) доказів, а також дотриманню прав і свобод людини в умовах цифровізації.

Список використаних джерел

1. Кримінальний процесуальний кодекс України : зі змінами та доповненнями станом на 01.07.2025 (офіційний текст). Київ : Видавництво «Паливода А.В.», 2025. 552 с.
2. Орловський, Б. М. (2025). Кримінально-процесуальні аспекти використання цифрових доказів та електронних носіїв інформації. *Правова держава*, (60), 133–140. <https://doi.org/10.18524/2411-2054.2025.60.348090>

3. Тагієв, С. Р. (2025). Проблемні питання правового регулювання використання електронних доказів у кримінальному процесі. *Академічні візії*, (41). вилучено із <https://academy-vision.org/index.php/av/article/view/1742>
4. Мурадов В. Електронні докази: криміналістичний аспект використання. *Порівняльне правознавство*. 2013. No 3–2. С. 313–315.
5. Квашук О.Д. Використання електронних доказів у кримінальному провадженні. *Центральноукраїнський вісник права та публічного управління*. Випуск 2(10). 2025. С. 50-56. DOI <https://doi.org/10.32782/cuj-2025-2-5>
6. С. 16 Сидоренко М. Використання цифрових доказів у кримінальних справах: правові та технічні аспекти. *Юридичний вісник*. 2021. No 15 (3). С. 14–19.
7. Постанова Верховного Суду від 13 липня 2020. Справа No 753/10840/19. Провадження No 61-22727св19. URL: <https://reyestr.court.gov.ua/Review/90385050> (дата звернення: 02.06.2025)
8. Постанова Верховного Суду від 10 вересня 2020 р. Справа No 751/6069/19. Провадження No 51–1704км20. URL: <https://reyestr.court.gov.ua/Review/91722819> (дата звернення: 04.06.2025)
9. С. 47 Бондаренко Р. Проблеми процесуального оформлення електронних доказів. *Кримінальний процес*. 2020. No 11 (1). С. 45–50
10. С. 169. Ратнова А. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. докт. філософ. : 12.00.09. Львів, 2021. 248 с
11. С. 286. Fredesvinda I. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*. 2007. No. 1 (4). P. 285–289
12. *Criminal Procedure Law*. URL: <https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law.com> (дата звернення 03.02.2025).
13. С. 258-259. Неділько Я.В. Доктрина електронних доказів у кримінальному процесі: національні особливості та світові тенденції. *Правова держава*. Випуск 57. 2025. С. 254-262. <https://pd.onu.edu.ua/article/view/325402/317572>
14. Сенченко Н.М., Чумаченко В.Ю. Електронні докази у кримінальному провадженні: досвід реалізації у зарубіжних країнах. *Академічні візії*. Випуск 42. 2025. DOI: <https://doi.org/10.5281/zenodo.15395747>
15. Ангеленюк А.-М.Ю. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського Національного Університету*. Випуск 79:2. 2023. <https://visnyk-pravo.uzhnu.edu.ua/article/view/289572/283146>
16. Мехеда В.Д. Доказування у кримінальному процесі в умовах цифровізації: європейські стандарти та українські реалії. *Наукові записки*. Серія: право. Випуск 19. 2025. <https://pravo.cusu.edu.ua/index.php/pravo/article/view/649/674>
17. Каланча І. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світовій концепції chain of custody. *Відомості та перспективи*. Випуск 8(51). 2025. https://www.researchgate.net/publication/394998880_Kalanca_IG_Dokazi_so_maut_elektronnu_formu_v_kriminalnomu_procesi_Ukraini_identifikacia_ta_cilisnist_u_svitli_koncepcii_chain_of_custody_Veda_a_perspektivy_No_851_2025_C_206-230

References

1. Kryminalnyi protsesualnyi kodeks Ukrainy. (2025). *Criminal Procedure Code of Ukraine*. Kyiv: Vydavnytstvo "Palyvoda A.V."
2. Orlovskiy, B. M. (2025). Kryminalno-protsesualni aspekty vykorystannia tsyfrovyykh dokaziv ta elektronnykh nosiiv informatsii [Criminal procedural aspects of the use of digital

- evidence and electronic data carriers]. *Pravova derzhava*, (60), 133–140. <https://doi.org/10.18524/2411-2054.2025.60.348090>
3. Tahiev, S. R. (2025). Problemni pytannia pravovoho rehuliuвання vykorystannia elektronnykh dokaziv u kryminalnomu protsesi [Problematic issues of legal regulation of the use of electronic evidence in criminal proceedings]. *Akademichni vizii*, (41). <https://academy-vision.org/index.php/av/article/view/1742>
 4. Muradov, V. (2013). Elektronni dokazy: kryminalistychnyi aspekt vykorystannia [Electronic evidence: Forensic aspects of use]. *Porivnialne pravoznavstvo*, (3–2), 313–315.
 5. Kvashuk, O. D. (2025). Vykorystannia elektronnykh dokaziv u kryminalnomu provadzhenni [The use of electronic evidence in criminal proceedings]. *Tsentrlnoukrajnskyi visnyk prava ta publicnoho upravlinnia*, 2(10), 50–56. <https://doi.org/10.32782/cuj-2025-2-5>
 6. Sydorenko, M. (2021). Vykorystannia tsyfrovyykh dokaziv u kryminalnykh spravakh: pravovi ta tekhnichni aspekty [Use of digital evidence in criminal cases: Legal and technical aspects]. *Yurydychnyi visnyk*, 15(3), 14–19.
 7. Supreme Court. (2020, July 13). Postanova u spravi No. 753/10840/19 (provadzhennia No. 61-22727sv19) [Decision in case No. 753/10840/19]. <https://reyestr.court.gov.ua/Review/90385050>
 8. Supreme Court. (2020, September 10). Postanova u spravi No. 751/6069/19 (provadzhennia No. 51-1704km20) [Decision in case No. 751/6069/19]. <https://reyestr.court.gov.ua/Review/91722819>
 9. Bondarenko, R. (2020). Problemy protsesualnogo oformlennia elektronnykh dokaziv [Problems of procedural formalization of electronic evidence]. *Kryminalnyi protses*, 11(1), 45–50.
 10. Ratnova, A. (2021). Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni [Criminal procedural and forensic foundations of the use of electronic documents in evidence] (PhD dissertation). Lviv.
 11. Fredesvinda, I. (2007). The admissibility of electronic evidence in court (A.E.E.C.): Fighting against high-tech crime – Results of a European study. *Journal of Digital Forensic Practice*, 1(4), 285–289.
 12. Criminal Procedure Law. (n.d.). <https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law.com>
 13. Nedilko, Y. V. (2025). Doktryna elektronnykh dokaziv u kryminalnomu protsesi: natsionalni osoblyvosti ta svitovi tendentsii [The doctrine of electronic evidence in criminal procedure: National features and global trends]. *Pravova derzhava*, (57), 254–262. <https://pd.onu.edu.ua/article/view/325402/317572>
 14. Senchenko, N. M., & Chumachenko, V. Y. (2025). Elektronni dokazy u kryminalnomu provadzhenni: dosvid realizatsii u zarubizhnykh krainakh [Electronic evidence in criminal proceedings: Experience of implementation in foreign countries]. *Akademichni vizii*, (42). <https://doi.org/10.5281/zenodo.15395747>
 15. Anheliniuk, A.-M. Y. (2023). Vykorystannia elektronnykh dokaziv u kryminalnomu protsesualnomu pravi Ukrainy (problemni pytannia) [The use of electronic evidence in criminal procedural law of Ukraine (problematic issues)]. *Scientific Bulletin of Uzhhorod National University*, 79(2). <https://visnyk-pravo.uzhnu.edu.ua/article/view/289572/283146>
 16. Mekheda, V. D. (2025). Dokazuvannia u kryminalnomu protsesi v umovakh tsyfrovizatsii: yevropeyski standarty ta ukrainski realii [Evidence in criminal proceedings in the context of digitalization: European standards and Ukrainian realities]. *Naukovi zapysky. Serii: Pravo*, (19). <https://pravo.cusu.edu.ua/index.php/pravo/article/view/649/674>
 17. Kalancha, I. (2025). Dokazy, shcho maiut elektronnu formu v kryminalnomu protsesi Ukrainy: identyfikatsiia ta tsilisnist u svitovii kontseptsii chain of custody [Evidence in electronic form in the criminal process of Ukraine: Identification and integrity in the context of

the chain of custody concept]. *Vidomosti ta perspektyvy*, 8(51).
<https://www.researchgate.net/publication/394998880>