УДК 343.98
DOI https://doi.org/10.32782/cuj-2026-1-2

Бондаренко Олена Григорівна
кандидат юридичних наук,
доцент кафедри кримінального права та процесу
Державний університет «Київський авіаційний інститут»
ORCID: 0000-0002-8270-5316

ЦИФРОВІ ДОКАЗИ В КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ: ПРОБЛЕМИ ДОПУСТИМОСТІ ТА ОЦІНКИ

У статті здійснено розгорнутий доктринальний та прикладний аналіз проблем становлення та застосування цифрових (електронних) доказів у кримінальному провадженні України, що зумовлено стрімкою цифровізацією суспільно-економічних процесів та радикальним зростанням кількості кіберзлочинів. Підкреслюється, що попри фундаментальні зміни у способах вчинення кримінальних правопорушень, чинний Кримінальний процесуальний кодекс України (КПК) усе ще містить фрагментарне й недостатньо адаптоване нормативне регулювання роботи з цифровою інформацією. Наявні правові норми здебільшого орієнтовані на моделі, притаманні традиційним матеріальним носіям доказової інформації, що формує ризики правової невизначеності та істотно ускладнює ефективне використання цифрових доказів у судовому процесі.

Основну увагу приділено розкриттю проблеми допустимості цифрових доказів, яка в українських реаліях найчастіше пов'язана не з їх змістом чи достовірністю, а з порушеннями процедур їх отримання, зберігання та фіксації, що суперечить вимогам ст. 86 КПК України. Практика слідчих органів засвідчує превалювання застарілих методів роботи, зокрема фізичного вилучення комп'ютерної техніки замість проведення професійного відтворення копій (forensic imaging) або створення криміналістичних образів. Такий підхід не лише не відповідає міжнародним стандартам, але й створює реальні ризики паралізації діяльності бізнесу, втрати критичної інформації, порушення прав власників та третіх осіб.

У статті детально досліджено найбільш проблемні колізійні питання застосування норм щодо обшуку, тимчасового доступу та виїмки цифрових даних, включаючи відсутність чітких вимог до протоколювання технічних параметрів вилучення, програмного забезпечення, носіїв та методів обробки даних. Особливе місце приділено аналізу проблеми забезпечення цілісності та незмінності цифрової інформації – ключової умови для визнання її судом належною та достовірною. Підкреслюється важливість застосування криптографічних методів контролю, зокрема хеш-функцій, які забезпечують простежуваність походження даних і підтримання безперервності ланцюга зберігання (Chain of Custody), що є загальноприйнятим міжнародним стандартом у сфері кіберфорензіки.

Окремо проаналізовано актуальні проблеми експертного дослідження цифрових доказів, включаючи недостатність спеціалізованої експертної інфраструктури, різний рівень кваліфікації фахівців, відсутність єдиних державних стандартів цифрово-криміналістичних процедур та практики застосування спеціалізованого програмного забезпечення. Наголошується, що саме експертний висновок часто є ключовою ланкою у доведенні автентичності та надійності електронних даних, однак без законодавчо врегульованих інструментів він може втратити належну доказову силу.

Ключові слова: *цифрові докази, електронні докази, допустимість доказів, оцінка доказів, Кримінальний процесуальний кодекс України (КПК), обшук, тимчасовий доступ, хеш-функція, Chain of Custody, Forensic Imaging.*

Bondarenko O. G. Digital Evidence in the Criminal Procedure of Ukraine: Problems of Admissibility and Evaluation

The article provides a comprehensive doctrinal and applied analysis of the challenges related to the development and application of digital (electronic) evidence in criminal proceedings in Ukraine, driven by the rapid digitalization of socio-economic processes and a radical increase in cybercrime. It is emphasized that despite the fundamental transformation in the ways criminal offenses are committed, the current Criminal Procedure Code of Ukraine (CPC) still contains fragmented and insufficiently adapted regulation of work with digital information. The existing

legal norms remain predominantly oriented toward models inherent to traditional material carriers of evidentiary information, creating risks of legal uncertainty and significantly complicating the effective use of digital evidence in judicial proceedings.

The main focus is placed on the issue of admissibility of digital evidence, which in the Ukrainian context is most often linked not to the content or reliability of information, but to violations of the procedures for its collection, storage, and documentation, contrary to the requirements of Article 86 of the CPC of Ukraine. Investigative practice demonstrates the prevalence of outdated methods – in particular, the physical seizure of computer equipment instead of professional duplication through forensic imaging or the creation of forensic data copies. Such an approach not only falls short of international standards but also creates real risks of paralyzing business operations, losing critical data, and violating the rights of owners and third parties.

The article provides an in-depth examination of the most problematic conflicts arising from the application of rules governing searches, temporary access, and seizure of digital data, including the absence of clear requirements for documenting technical parameters of data extraction, software tools, storage media, and methods of data processing. Particular attention is devoted to the issue of ensuring the integrity and immutability of digital information – a key condition for its recognition by the court as relevant and reliable. The article underscores the importance of cryptographic control tools, including hash functions, which ensure traceability of data origin and maintain the continuity of the chain of custody – a universally recognized international standard in the field of cyber forensics.

Additionally, the article analyzes pressing challenges associated with forensic examination of digital evidence, including the insufficient development of specialized expert infrastructure, differences in the level of professional competence, and the lack of unified state standards for digital forensic procedures and the use of specialized software. It is emphasized that an expert conclusion often serves as the crucial element in proving the authenticity and reliability of electronic data; however, without legally regulated instruments, it may lose its probative value.

Key words: *digital evidence, electronic evidence, admissibility of evidence, evaluation of evidence, Criminal Procedure Code of Ukraine (CPC), search, temporary access, hash function, Chain of Custody, Forensic Imaging.*

Вступ. Сучасний кримінальний процес дедалі більше трансформується у процес доказування цифрових слідів. Майже кожне кримінальне правопорушення – від шахрайства до державної зради – залишає інформаційний відбиток у пам'яті мобільних пристроїв, хмарних сервісах, телекомунікаційних мережах або інших цифрових системах. Це означає, що електронна інформація поступово перетворюється на один із ключових елементів доказової бази як на стадії досудового розслідування, так і під час судового розгляду.

Разом із тим цифрові докази характеризуються нематеріальним характером, волатильністю та латентністю. Ці властивості вступають у суперечність із традиційними процесуальними підходами до доказування, закладеними у кримінальному процесуальному законодавстві України. Чинний КПК України оперує насамперед категоріями «документ» та «речовий доказ» (ст. 99), що створює методологічну невідповідність при кваліфікації електронної інформації як доказу [1]. На практиці виникають цілком конкретні запитання: яким доказом є сервер або інший цифровий носій? Чи слід розглядати його як річ, яку необхідно фізично вилучити й зберігати в камері схову, чи як джерело інформації, з якого треба належним чином скопіювати дані, забезпечивши їх автентичність та цілісність? Відсутність чітко врегульованого порядку збирання, фіксації та дослідження електронних доказів спричиняє істотні труднощі з їх використанням у кримінальному провадженні. Швидка еволюція ІТ-технологій випереджає оновлення процесуальної доктрини, і, попри значну кількість наукових публікацій, питання правової природи та процесуального режиму електронних доказів залишається невирішеним [2, с. 246]. У підсумку формальні недоліки здатні нівелювати навіть фактичну доведеність вини особи.

Матеріали та методи. Методологічну основу даної статті становить сукупність загальнонаукових і спеціально-юридичних методів пізнання, що зумовлено комплексним характером проблематики цифрових доказів у кримінальному провадженні. Ключовим у дослідженні є формально-юридичний метод, за допомогою якого проаналізовано положення Кримінального процесуального кодексу України, що регулюють допустимість доказів, порядок отримання, фіксації та оцінки цифрової (електронної) інформації. Це дало змогу виявити прогалини та суперечності правового

регулювання, зумовлені орієнтацією процесуальних норм на традиційні матеріальні носії доказової інформації.

Для з'ясування місця цифрових доказів у системі кримінального доказування застосовано системно-структурний метод, який дозволив розглянути електронні дані як елемент цілісного процесу доказування та встановити взаємозв'язок між етапами їх отримання, збереження та оцінки. Також використано порівняльно-правовий метод, у межах якого проаналізовано сучасні підходи до роботи з цифровими доказами, зокрема застосування forensic imaging, забезпечення цілісності електронної інформації та дотримання безперервності ланцюга зберігання доказів (Chain of Custody).

Важливе місце у дослідженні посідає аналіз правозастосовної практики, що ґрунтується на узагальненні матеріалів кримінальних проваджень та судових рішень, у яких оцінювалася допустимість цифрових доказів. Це дозволило виявити типові процесуальні порушення, пов'язані з їх вилученням, фіксацією та експертним дослідженням.

Емпіричну та інформаційну базу дослідження становлять матеріали кримінальних проваджень, судова практика, наукові праці вітчизняних і зарубіжних авторів, а також міжнародні рекомендації та стандарти у сфері цифрової криміналістики.

Метою статті є дослідження проблем застосування цифрових доказів у кримінальному процесі України з точки зору їх допустимості та оцінки, а також обґрунтування напрямів удосконалення процесуальних механізмів роботи з електронною інформацією.

Результати. Цифрові сліди, на відміну від класичних речових доказів, не мають сталої фізичної форми, можуть бути легко змінені, перезаписані або видалені. Це безпосередньо впливає на їх автентичність, а отже – і на допустимість як доказів. Будь-яке порушення процедури фіксації, копіювання чи зберігання електронних даних створює підстави для їхнього відхилення судом як недопустимих відповідно до ст. 87 КПК України. Таким чином, навіть об'єктивно значущі електронні відомості нерідко визнаються недопустимими, а органи досудового розслідування опиняються в ситуації процесуальних «пасток», яких не існувало у класичній парадигмі речових доказів.

У національному контексті України зазначена проблематика набуває особливої гостроти. Повномасштабна збройна агресія РФ призвела не лише до зростання кількості «традиційних» кримінальних правопорушень, а й до масштабного сплеску кіберзлочинності, атак на об'єкти критичної інфраструктури, незаконного втручання в інформаційні системи органів державної влади, фінансових установ, ЗМІ. Додатковим виміром є системне використання російською стороною технологій дезінформації, у тому числі deepfake-контенту, спрямованого на дискредитацію українських військових, посадових осіб та інституцій. Ця технологія дозволяє створювати гіперреалістичні зображення, відео та аудіозаписи, відмежувати які від справжніх без спеціальних знань і технічних засобів украй складно, що робить її надзвичайно ефективним інструментом маніпуляції громадською думкою. Здатність deepfake-контенту імітувати реальність ставить під сумнів традиційну довіру до візуальних та аудіодоказів, які раніше сприймалися як найбільш переконливі [3, с. 112]. В умовах гібридної війни цифрові докази стають ключовим інструментом не лише для розслідування воєнних злочинів та злочинів проти основ національної безпеки, а й для документування інформаційно-психологічних операцій противника.

Водночас реалії воєнного стану – окупація частини територій, пошкодження серверів та телекомунікаційної інфраструктури, обмежений фізичний доступ слідчих до місць зберігання даних, масове переміщення населення – істотно ускладнюють належне вилучення, збереження та верифікацію цифрових слідів. Це посилює ризики втрати, модифікації або компрометації електронної інформації та безпосередньо впливає на питання допустимості таких доказів у кримінальному провадженні.

Основною причиною «руйнування» цифрових доказів у суді часто виступає не їх сумнівна достовірність, а грубе порушення процесуальної форми. Судова практика демонструє, що грубі порушення процедури отримання цифрових доказів призводять до їх

автоматичного виключення з доказової бази, навіть за наявності очевидних ознак винуватості особи. Так, в ухвалі з ідентифікатором № 116888878 від 09.02.2024 суд відмовився враховувати результати втручання в приватне спілкування, оскільки сторона обвинувачення не дотрималася встановленої КПК України процедури отримання відповідного дозволу [4]. Суд наголосив, що дані, здобуті внаслідок негласних слідчих (розшукових) дій без належного судового контролю, є недопустимими, оскільки отримані з порушенням конституційних гарантій та права на повагу до приватного життя.

Подібний підхід простежується й у рішенні № 118206960 від 08.04.2024 (справа № 908/1264/18), де суд визнав недопустимими документи електронного листування, мотивуючи це неможливістю достовірно ідентифікувати відправника, відсутністю кваліфікованого електронного підпису та недотриманням встановлених сторонами правил електронного документообігу. Суд зауважив, що електронні копії повідомлень без належного підтвердження їх автентичності не відповідають критеріям допустимого доказу і не забезпечують достатнього захисту від фальсифікації [5]. Зазначені рішення наочно демонструють: технічні вади, відсутність первинних метаданих, неналежна процесуальна фіксація та порушення ланцюга зберігання даних (chain of custody) є типовими підставами для визнання цифрових доказів нікчемними. Судова практика формує до сторони обвинувачення чітку вимогу: кожен цифровий доказ має супроводжуватися належним техніко-криміналістичним підтвердженням його автентичності та незмінності.

У криміналістиці для забезпечення цілісності (автентичності) цифрових доказів використовується хешування – математична функція, яка генерує унікальний «відбиток» (наприклад, SHA-256) для певного масиву даних. Якщо хеш-сума, зафіксована під час вилучення, збігається з хеш-сумою на етапі експертизи, цілісність даних вважається підтвердженою. Проте в більшості протоколів обшуку чи огляду електронних носіїв в Україні відсутні будь-які посилання на хеш-значення, що дозволяє стороні захисту обґрунтовано ставити під сумнів, чи не була інформація змінена після вилучення. Показовим є й поширене використання у практиці «скріншотів» як основної форми фіксації електронної інформації. В українському законодавстві термін «скріншот» відсутній, однак він активно використовується на практиці для позначення зображення екрана, збереженого у вигляді графічного файлу. Подальший друк такого зображення не створює нового доказу, а лише відтворює фрагмент електронного документа, доступний користувачеві на момент фіксації. Тому роздруківка скріншота не може самостійно визнаватися допустимим доказом без підтвердження цілісності й походження відповідних даних з первинного носія [6, с. 93].

Окремий пласт проблем пов'язаний із територіальною недосяжністю значної частини цифрових доказів. У багатьох кримінальних провадженнях дані зберігаються на серверах іноземних провайдерів або в хмарних інфраструктурах транснаціональних компаній, що об'єктивно виводить їх за межі прямої юрисдикції українських органів досудового розслідування. Як слушно зазначає І. С. Нуруллаєв, класичні інструменти міжнародного співробітництва (MLA-запити, судові доручення) виявляються надто повільними в умовах кіберзлочинності: цифрові дані можуть бути змінені або знищені за лічені години, тоді як виконання запиту про міжнародну правову допомогу триває від кількох місяців до року [7, с. 151]. Це створює реальну загрозу втрати релевантної інформації ще до того, як держава фактично отримає до неї доступ.

Саме для подолання зазначених ризиків у Будапештській конвенції про кіберзлочинність (Конвенція Ради Європи ETS № 185), до якої приєдналася й Україна, запроваджено інститут термінового збереження комп'ютерних даних (expedited preservation). Відповідно до ст. 29 Конвенції компетентний орган держави-учасниці може невідкладно звернутися до іноземного провайдера з вимогою зберегти наявні комп'ютерні дані на визначений строк (як правило, до 90 днів) до надходження формалізованого запиту про міжнародну правову допомогу. Такий підхід дозволяє «заморозити» потенційно важливу інформацію, мінімізуючи

ризик її видалення або модифікації, і лише після цього реалізовувати повноцінну процедуру вилучення та передачі відповідно до вимог національного й міжнародного права [8].

Практичну значущість механізму expedited preservation підкреслюють і міжнародні інституції. У посібнику Ради Європи "Electronic evidence: a basic guide for judges, prosecutors and lawyers" наголошується, що у справах про кіберзлочини час є критичним фактором: провайдери законно видаляють журнали доступу, резервні копії та інші дані через обмежені строки зберігання, а отже оперативні запити на збереження розглядаються як ключова гарантія ефективного розслідування. Аналогічний підхід відображено й у документах ЄС, присвячених «життєвому циклу» електронних доказів, де підкреслюється необхідність поєднання швидких тимчасових заходів (preservation) із подальшим формалізованим доступом до інформації [9].

Українська практика поступово рухається в цьому ж напрямку, однак залишається фрагментарною. В окремих провадженнях кіберполіція та інші органи досудового розслідування застосовують механізми термінового збереження даних і пряму взаємодію з іноземними провайдерами, спираючись на положення Будапештської конвенції та двосторонніх угод. Водночас відсутність детальної регламентації таких процедур у КПК України, а також залежність від корпоративної політики приватних компаній зумовлюють нерівномірність практики: в одних справах цифрові дані вдається зберегти й використати, в інших – вони безповоротно втрачаються через затягування процесу або пасивність провайдера.

На цьому тлі особливої ваги набуває не лише питання доступу до цифрових даних, а й форми їх фіксації та подальшого використання як доказів у кримінальному провадженні. Міжнародні стандарти цифрової криміналістики виходять із того, що належним об'єктом дослідження є не стільки фізичний носій (сервер, жорсткий диск, смартфон), скільки його криміналістичний образ (forensic image) – повна побітова копія даних, створена із застосуванням засобів захисту від запису (write-block) та верифікована за допомогою хеш-функцій. Цей підхід детально описаний у спеціальній літературі з цифрової криміналістики, зокрема в роботах Е. Кейсі та інших дослідників, присвячених форензійному знімкуванню і використанню write-block-пристроїв [10].

Порівняння зазначених стандартів із українською практикою виявляє істотний розрив: у протоколах обшуку та огляду здебільшого детально описується лише фізичний носій (марка, модель, серійний номер), тоді як процедура створення копії, застосування write-block-засобів чи фіксація хеш-значень або відсутні, або згадуються формально. Це суттєво ускладнює доведення автентичності цифрових доказів та дає стороні захисту підстави ставити під сумнів їх допустимість. На цьому тлі імплементація forensic-підходів (криміналістичного знімкування, хеш-контролю, детального протоколювання ланцюга зберігання даних) та їх нормативне закріплення у КПК України видається не просто технічними рекомендаціями, а необхідною умовою забезпечення належної доказової сили цифрових слідів у кримінальному провадженні.

Висновки. Проведене дослідження підтверджує, що цифрові докази стають одним із провідних інструментів доказування у кримінальному провадженні України, особливо в умовах цифрової трансформації та гібридної війни. Водночас чинна модель кримінального процесу залишається недостатньо адаптованою до їхньої специфіки, що призводить до численних випадків визнання електронних доказів недопустимими – насамперед через порушення процедури їх отримання, зберігання та фіксації. Для забезпечення реальної доказової сили цифрових слідів необхідним є надання їм чіткої процесуальної природи в КПК України, із визначенням правил їх віднесення, збору та фіксації. Упровадження міжнародних стандартів криміналістичного знімкування (forensic imaging), обов'язкової фіксації хеш-сум і ведення повного ланцюга зберігання даних (chain of custody) є ключовою передумовою підвищення їх автентичності та надійності. Важливою складовою є також уніфікація технічних підходів шляхом розроблення єдиних національних методичних

стандартів роботи з електронною інформацією. Посилення експертного потенціалу – розвиток цифрово-криміналістичних лабораторій, підготовка фахівців, використання сертифікованого програмного забезпечення – має стати окремим напрямом державної політики. Крім того, у зв'язку з транскордонним характером цифрових даних слід забезпечити ефективні механізми оперативного доступу до інформації, що зберігається в іноземних хмарних сервісах, спираючись на інструменти Будапештської конвенції. Лише системне реформування законодавчої та практичної бази кримінального процесу здатне гарантувати належність, достовірність і допустимість цифрових доказів, забезпечуючи реальну ефективність кримінального переслідування в сучасних умовах.

Література

1. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-VI. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

2. Перцова-Тодорова Л. «Електронний доказ» під час обшуку. *Підприємництво, господарство і право.* 2020. №6. С. 243–247. DOI: https://doi.org/10.32849/2663-5313/2020.6.41

3. Усова П. П**.** Deepfake-контент у просторі сучасної політики: проблематика фабрикації реальності. *Вісник Сковородинівської академії молодих учених : зб. наук. пр. Харк. нац. пед. ун-т ім. Г. С. Сковороди*, 2025. Вип. № 2. С. 110–126. URL: https://dspace.hnpu.edu.ua/bitstreams/a1fb5e93-eba5-4cef-b3d1-5306f69d5fe0/download

4. Ухвала Красилівського районного суду Хмельницької області у справі № 1-кп/677/1/24 від 09.02.2024 р. *Єдиний державний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/121283501

5. Рішення Богуславського районного суду Київської області № 118206960 від 08.04.2024 р**.** *Єдиний державний реєстр судових рішень*. URL: https://reyestr.court.gov.ua/Review/118206960

6. Ратнова А. В. Використання роздруківки та скріншоту інтернет-сторінки під час доказування у кримінальному провадженні. *Кримінальне процесуальне та криміналістичне забезпечення досудового розслідування* : матеріали науково-практичного семінару (25 жовт. 2019 р.) / упор. Р. М. Шехавцов. Львів : ЛьвДУВС. 2019. С. 92–95. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3747/1/ratnova_d.pdf

7. Нуруллаєв І. С. Особливості конвенційного механізму міжнародного співробітництва в боротьбі зі злочинністю в Європейському Союзі (на прикладі протидії кіберзлочинності). *Юридичний бюлетень.* 2019. Вип. 10. с. 148–155. DOI https://doi.org/10.32850/2414-4207.2019-10.20

8. Конвенція про кіберзлочинність (Будапешт, 23 листопада 2001 року) : ратифікована Законом України від 7 вересня 2005 р. № 2824-IV. *Офіційний вісник України*. 2006. № 32. Ст. 1970. URL: https://rm.coe.int/1680081561

9. Electronic Evidence: A Basic Guide for Judges, Prosecutors and Lawyers. Strasbourg: Council of Europe, 2013. URL: https://rm.coe.int/16803028af

10. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Academic Press, 2011. 840 p. URL: https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf

References

1. Verkhovna Rada Ukrainy. (2012). Kryminalnyi protsesualnyi kodeks Ukrainy [Criminal Procedure Code of Ukraine] (Law No. 4651-VI, April 13, 2012). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text [in Ukrainian].

2. Pertsova-Todorova, L. (2020). Elektronni dokazy pid chas provedennia obshuku [Electronic evidence during a search]. *Pidpryiemnytstvo, hospodarstvo i pravo – Entrepreneurship, Economy and Law,* 6, 243–247. Retrieved from https://doi.org/10.32849/2663-5313/2020.6.41 [in Ukrainian].

3. Usova, P. P. (2025). Deepfake-kontent u suchasnomu politychnomu prostori: problemy fabrikatsii realnosti [Deepfake content in contemporary political space: Issues of reality fabrication]. *Visnyk Skovorodynivskoi Akademii Molodykh Uchenykh – Bulletin of Skovorodynivska Academy of Young Scientists,* 2, 110–126. Retrieved from https://dspace.hnpu.edu.ua/bitstreams/a1fb5e93-eba5-4cef-b3d1-5306f69d5fe0/download [in Ukrainian].

4. Krasylivskyi raionnyi sud Khmelnytskoi oblasti. (2024, February 9). Uhvala u spravi No. 1-kp/677/1/24 [Ruling in case No. 1-kp/677/1/24]. *Yedynyi derzhavnyi reiestr sudovykh rishen – Unified State Register of Court Decisions*. Retrieved from https://reyestr.court.gov.ua/Review/121283501 [in Ukrainian].

5. Bohuslavskyi raionnyi sud Kyivskoi oblasti. (2024, April 8). Rishennia No. 118206960 [Decision No. 118206960]. *Yedynyi derzhavnyi reiestr sudovykh rishen – Unified State Register of Court Decisions*. Retrieved from https://reyestr.court.gov.ua/Review/118206960 [in Ukrainian].

6. Ratnova, A. V. (2019). Vykorystannia rozdrukivok ta skrinshotiv web-storinok u kryminalnomu provadzhenni [Use of printouts and screenshots of web pages in criminal proceedings]. In R. M. Shekhavtsov (Ed.), Kryminalno-protsesualne ta kryminalistychne zabezpechennia dosudovoho rozsliduvannia – Criminal procedural and forensic support of pre-trial investigation (pp. 92–95). Lviv : Lviv State University of Internal Affairs. Retrieved from https://dspace.lvduvs.edu.ua/bitstream/1234567890/3747/1/ratnova_d.pdf [in Ukrainian].

7. Nurullaiev, I. S. (2019). Osoblyvosti tradytsiinoho mekhanizmu mizhnarodnoho spivrobitnytstva u borotbi zi zlochynnistiu v Yevropeiskomu Soiuzi (na prykladi protydii kiberzlochynnosti) [Features of the conventional mechanism of international cooperation in combating crime in the European Union (on the example of countering cybercrime)]. *Yurydychnyi visnyk – Legal Bulletin*, 10, 148–155. https://doi.org/10.32850/2414-4207.2019-10.20 [in Ukrainian].

8. Council of Europe. (2001). Convention on Cybercrime (Budapest, November 23, 2001). rm.coe.int. Retrieved from https://rm.coe.int/1680081561 [in English].

9. Council of Europe. (2013). Electronic evidence: A basic guide for judges, prosecutors and lawyers. Strasbourg : Council of Europe. Retrieved from https://rm.coe.int/16803028af [in English].

10. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Amsterdam : Academic Press. Retrieved from https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf [in English].

Дата першого надходження статті до видання: 08.01.2026
Дата прийняття статті до друку після рецензування: 11.03.2026
Дата публікації (оприлюднення) статті: 20.04.2026