DOI: 10.33994/kndise.2025.70.28
УДК 004.62; 006.3/.8; 343.9

Порядок збирання цифрових доказів

Тарас Івасишин
Кандидат біологічних наук, доцент, доцент кафедри кримінального процесу та криміналістики Навчально-наукового гуманітарного інституту Національної академії Служби безпеки України
ORCID: 0009-0007-6604-0362, e-mail: itavitaastra@gmail.com

Олександр Пірог
Кандидат технічних наук, головний судовий експерт експертного сектору Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України в Управлінні Служби безпеки України в Житомирській обл.
ORCID: 0009-0001-6111-9676

Стаття присвячена актуальним питанням збирання цифрових доказів у межах закону, відповідно до вимог захисту персональних даних і конфіденційності. Порядок збирання цифрових доказів надзвичайно важливий, оскільки від нього залежить їхня достовірність, допустимість у суді та можливість відтворення подій. Стрімкий розвиток цифрових технологій зумовив зростання кількості правопорушень у кіберпросторі, своєю чергою, це підвищило актуальність дослідження процесу збирання цифрових доказів. Розглянуто основні етапи цього процесу: від виявлення та фіксації доказів до їхнього документування, збереження та аналізування. Особливу увагу приділено важливості дотримання послідовності дій для забезпечення цілісності та автентичності доказів. Окреслено основні загрози, пов'язані з неналежним збором даних, серед яких ризик втрати, спотворення або підробки цифрових слідів. Проаналізовано міжнародні стандарти й найкращі практики цифрової криміналістики, що регламентують порядок поводження з електронними доказами. Вдосконалення підходів передбачає уніфікацію процесів відповідно до міжнародних стандартів, що полегшить розслідування транснаціональних злочинів. Акцентовано увагу на значенні міждисциплінарного підходу, який поєднує юридичні, технічні й організаційні аспекти, необхідні для забезпечення допустимості зібраних доказів у судовій практиці. Зазначено, що підвищена увага до захисту персональних даних і конфіденційності вимагає чіткого балансу між ефективністю збирання доказів та дотриманням прав користувачів.

Ключові слова: *цифрові докази; збирання цифрових доказів; процедура збирання; методи фіксації; документування доказів; міжнародні стандарти.*

Постановка проблеми. Сьогодні дедалі більше пристроїв підключені до глобальної мережі інтернет (комп'ютери, смартфони, IoT-пристрої тощо), що значно розширює кількість джерел цифрових доказів. Технологічний прогрес також додає нові типи даних (хмарні сервіси, криптовалюти), які потрібно враховувати під час розслідувань. Кіберзлочини стають дедалі складнішими. Шифрування даних, використання анонімних мереж, зловживання хмарними сервісами та інші методи вимагають вдосконалених підходів до збирання доказів, які б дали змогу виявляти та аналізувати такі злочини. Закони, що регулюють збирання цифрових доказів, різняться в різних країнах і регіонах. Вдосконалення підходів передбачає уніфікацію процесів відповідно до міжнародних стандартів, що полегшить розслідування транснаціональних злочинів. Підвищена увага до захисту персональних даних і конфіденційності вимагає чіткого балансу між ефективністю збирання доказів і дотриманням прав користувачів. Кількість кібератак постійно зростає, а злочини, пов'язані з соціальними мережами, фейковими новинами, маніпуляцією громадською думкою стають дедалі поширенішими. Вдосконалення підходів до збирання цифрових доказів є актуальним у світлі швидких технологічних змін, зростання загроз у кіберпросторі та необхідності дотримання правових і етичних норм.

Аналіз останніх досліджень і публікацій. Поміж останніх досліджень, присвячених проблематиці збирання цифрових доказів, слід відзначити роботу *P. Lewulis* [1], у якій автор аналізує недоліки чинного кримінального законодавства Польщі щодо збирання цифрових доказів з онлайн-джерел. Також варто згадати роботу *J.-R. Sun, M.-L. Shih* та *M.-Sh. Hwang* [2], в якій досліджено методи криміналістичного аналізу цифрових доказів та особливості проведення кіберкримінальних розслідувань.

На теренах України актуальні питання збирання цифрових доказів висвітлено в наукових працях В. Романюка та Т. Фоміної [3], які проаналізували специфіку цифрових доказів у кримінальних провадженнях, пов'язаних із колабораційною діяльністю; М. Гуцалюк і П. Антонюк [4] розглянули основні підходи до визначення цифрової інформації як процесуального доказу, що має критичне значення для кримінального судочинства. У дослідженні В. Романюка і С. Абламського проаналізовано питання відповідності цифрових доказів критеріям допустимості, що є важливим аспектом у забезпеченні

їх правової значущості та належності в судовому процесі [5]. Також питання сутності та порядку збирання електронних доказів розкриті в роботах Г. Авдєєвої, А. Коваленка, В. Мурадова, А. Ратнової, Д. Цехана та інших дослідників, які зробили вагомий внесок у розвиток цієї наукової проблематики.

Мета дослідження. З'ясування порядку збирання цифрових доказів відповідно до міжнародних стандартів.

Викладення основного матеріалу. У сучасному світі, де цифрові технології проникли в усі сфери життя, важливість належного збирання та збереження цифрових доказів важко переоцінити. Цифрові сліди стають ключовими доказами в розслідуванні різних видів правопорушень — від кіберзлочинів до економічних шахрайств та міжнародного тероризму. Однак процеси фіксування, аналізування й зберігання таких доказів потребує не лише технічної обізнаності, а й дотримання чітких процедур, покликаних гарантувати достовірність отриманої інформації та її допустимість у суді.

Збирання цифрових доказів є складним процесом, що містить кілька важливих етапів: ідентифікацію джерел даних, фіксування інформації, створення форензічних копій, документування ланцюга зберігання та аналіз отриманих матеріалів. Недотримання належної процедури може призвести до втрати даних, їхньої компрометації або невизнання доказів у судовому процесі.

В умовах зростання кількості злочинів у кіберпросторі та посилення гібридних загроз набуває особливого значення дослідження порядку збирання цифрових доказів. Ця стаття покликана висвітлити ключові етапи процесу, окреслити основні методи забезпечення цілісності даних, а також проаналізувати міжнародні стандарти та найкращі практики у сфері цифрової криміналістики.

Основними міжнародними стандартами, що регламентують збирання цифрових доказів, вважають *IETF RFC 3227* [6], *NIST SP 800-86* [7] та *ISO/IEC 27037* [8].

IETF RFC 3227 наголошує, що під час збирання доказів необхідно дотримувати політику безпеки та залучати відповідний персонал, включно з командами реагування на інциденти та представниками правоохоронних органів. Важливо створити докладну картину стану системи на момент збирання доказів (зокрема, конфігурацію, активні процеси та мережеві з'єднання). Усі дії мають бути ретельно документовані з позначенням дат і часу. Важливо враховувати різницю між локальним часом системи та універсальним координованим часом (*UTC*), зазначаючи часові пояси. Ретельна документація всіх дій і часових позначок важлива для можливого свідчення в суді через певний час. Під час збирання даних необхідно мінімізувати їх зміни,

уникаючи оновлення часу доступу до файлів або каталогів. Необхідно ізолювати систему від зовнішніх впливів, які можуть спричинити несанкціоновані зміни. Спочатку слід здійснювати процедуру збирання даних, а вже потім їх аналізування. Процедури збирання повинні бути перевірені на ефективність і можливість їх реалізації в кризових умовах. Важливо максимально автоматизувати ці процеси для забезпечення швидкості та точності. Кожен пристрій необхідно аналізувати відповідно до визначеного порядку збирання даних, починаючи з нестабільних і завершуючи стабільними. Для проведення криміналістичного аналізу необхідно створювати побітову копію носія даних, оскільки аналіз може змінювати час доступу до файлів.

Порядок збирання даних за ступенем стабільності:

— регістри, кеш;

— таблиці маршрутизації, таблиця процесів, пам'ять;

— тимчасові файлові системи;

— диск;

— віддалені журнали та моніторинг;

— фізична конфігурація та топологія мережі;

— архівовані носії.

Докази можуть бути легко знищені, тому слід уникати вимкнення системи до завершення збирання даних, а також не довіряти системним програмам. Під час збирання доказів необхідно поважати конфіденційність користувачів і дотримувати законодавство, уникаючи збирання надлишкових даних. Комп'ютерні докази повинні бути допустимими, достовірними, повними та надійними. Усі дії з доказами (зокрема, їх виявлення, використання та передавання) мають бути задокументовані. Слід забезпечити можливість виявлення несанкціонованого доступу до доказів. Інструменти, що використовують для збирання доказів, повинні бути надійними та перевіреними на предмет автентичності, із можливістю відтворення методик збирання доказів.

NIST SP 800-86 визначає основні ключові етапи процесу збирання цифрових доказів.

Збирання — визначення потенційних джерел даних (комп'ютери, сервери, мережеве обладнання, зовнішні носії тощо). Дані збирають відповідно до процедур, які забезпечують їх цілісність. Використовують інструменти для запобігання змінам оригінальних даних, дотримують принцип пріоритетності — спочатку збирають найбільш критичні та тимчасові дані (наприклад, дані оперативної пам'яті).

Відбирання — оброблення зібраних даних із використанням як автоматизованих, так і ручних методів для виділення релевантної

інформації. Під час цього етапу важливо зберігати оригінальність даних. Інструменти пошуку за ключовими словами та шаблонами зменшують обсяг даних, що потребують аналізу.

Аналізування — використання юридично обґрунтованих методик для інтерпретації та аналізування даних. Цей етап спрямований на отримання релевантної інформації, необхідної для подальших дій щодо підтримки слідства.

Звітування — документування результатів аналізу (зокрема, опис застосованих методик і рекомендації). Звіти мають бути юридично захищеними та зрозумілими.

Для ефективного збирання цифрових доказів організація повинна мати чіткі політики щодо ролей і відповідальності учасників процесу. Важливо використовувати методи хешування та дотримувати ланцюг зберігання доказів, щоб забезпечити їх автентичність та цілісність, запобігаючи звинувачень у фальсифікації.

Збирання даних із цифрових носіїв полягає в ідентифікації, збиранні та аналізуванні файлів, що зберігаються в різних файлових системах. Для забезпечення цілісності файлів використовують інструменти блокування запису, а їхню цілісність перевіряють за допомогою хешування. Збирання даних також може супроводжуватися технічними труднощами, пов'язаними з відновленням видалених файлів.

Дані з операційних систем поділяють на стабільні та нестабільні. Нестабільні дані (мережеві з'єднання або оперативна пам'ять) збирають першочергово, оскільки вони швидко змінюються або втрачаються після вимкнення системи. Стабільні дані зберігаються у файловій системі та містять конфігураційні файли, журнали, список користувачів тощо. Для збирання цих даних використовуються методи створення образів диска або копіювання окремих файлів.

Основними джерелами даних для аналізу мережевого трафіку є файрволи, маршрутизатори, пакетні сніфери та системи виявлення вторгнень. Дані мережевого трафіку можуть бути ускладнені через використання шифрування (наприклад, *IPsec, SSL*). Інструменти для аналізу трафіку дають можливість реконструювати події в мережі та виявляти підозрілі взаємодії. Для збирання таких даних можуть знадобитися згода користувачів або судовий дозвіл.

Застосунки зберігають цінну інформацію, зокрема конфігураційні файли, журнали подій, а також дані користувачів. Важливими джерелами доказів є електронна пошта, вебпереглядачі, чат-програми та програми обміну файлами. Дані застосунків можуть бути специфічними для користувача або мати унікальні конфігурації, що ускладнює їх аналіз.

Для всебічного аналізування інцидентів необхідно поєднувати дані з кількох джерел, таких як файли, операційні системи та мережевий трафік. Кореляція подій із різних джерел дає змогу ідентифікувати взаємозв'язки між системами, що є критичним для розслідування складних злочинів. Під час збирання таких даних важливо дотримувати процедури, що забезпечують їх цілісність і автентичність.

ISO/IEC 27037 надає чіткі рекомендації щодо загального порядку збирання цифрових доказів. Основні етапи процесу, що допомагають забезпечити збереження доказів і їх допустимість у суді, передбачають такий порядок.

Першим етапом є пошук та визначення потенційних цифрових доказів (зокрема, фізичних пристроїв, носіїв і логічних даних). Необхідно ретельно документувати всі потенційні джерела доказів, враховуючи як фізичні, так і віртуальні аспекти (наприклад, хмарні сервіси). Особливу увагу слід приділяти нестабільним даним (оперативна пам'ять і активні мережеві з'єднання), оскільки вони можуть бути втрачені після вимкнення системи.

Збирання стосується вилучення фізичних носіїв або інших пристроїв, які містять потенційні докази. Залежно від обставин пристрої можуть бути зібрані в увімкненому або вимкненому стані. Важливо зберігати оригінальні дані, уникати їх змін або псування. Необхідно використовувати захищене пакування для запобігання фізичному пошкодженню та спотворенню даних під час транспортування, для чого створюють копію потенційних цифрових доказів (наприклад, зображення жорсткого диска). Усі дії та методи отримання даних повинні бути докладно задокументовані. Необхідно застосовувати перевірені методи для мінімізації змін в оригінальних даних і гарантувати цілісність доказів через верифікацію (наприклад, хешування).

Забезпечення цілісності та автентичності цифрових доказів є критично важливим. Необхідно запобігати пошкодженню або зміні даних, зокрема метаданих (часових позначок). Потрібно використовувати належні умови для зберігання цифрових носіїв (контроль вологості, захист від магнітних полів тощо) та документувати всі дії, пов'язані з обробленням доказів. Ланцюжок збереження доказів має бути чітко задокументований із моменту збирання доказів до їх представлення їх у суді. Документація повинна містити унікальний ідентифікатор доказу, дати та дані осіб, які мали до нього доступ.

Першочергово необхідно збирати найменливіші дані. Якщо існує загроза втрати даних через вимкнення пристрою, слід зосередитися на збиранні даних, які можуть бути втрачені першими (наприклад, вміст оперативної пам'яті).

Усі три проаналізовані документи описують процес збирання цифрових доказів, проте кожен підхід акцентує увагу на різних аспектах і методах, що дає змогу краще зрозуміти повний процес.

ISO/IEC 27037 зосереджений на етапах від пошуку до зберігання даних, акцентуючи увагу на необхідності документування кожного кроку, забезпеченні цілісності та ланцюга зберігання доказів. *NIST SP 800-86* чітко структурує процес на чотири етапи (збирання, відбирання, аналізування та звітування), виокремлюючи важливість інструментів для оброблення даних і методів пошуку, що полегшують виокремлення релевантних доказів. *RFC 3227* приділяє більше уваги деталям процедури збирання, зокрема документуванню часу й мінімізації змін у даних, із акцентом на порядку збирання даних за їх ступенем стабільності. *ISO/IEC 27037* підкреслює важливість збирання найбільш нестабільних даних (зокрема, оперативної пам'яті й активних мережевих з'єднань), що може бути втрачено після вимкнення системи. *NIST SP 800-86* також звертає увагу на першочергове збирання нестабільних даних, наголошуючи на важливості дотримання процедур для забезпечення їх цілісності. *IETF RFC 3227* додає докладну схему порядку збирання даних (від регістрів і кешу до архівних носіїв), а також застерігає від вимкнення системи до завершення збирання, що відповідає рекомендаціям щодо роботи з нестабільними даними.

ISO/IEC 27037 акцентує увагу на збереженні оригінальних даних, перевірці їх цілісності через хешування та створення копій для подальшого аналізу. *NIST SP 800-86* описує інструменти блокування запису та методи хешування для перевірки цілісності файлів, а також відзначає важливість створення образів дисків і роботу з копіями. *IETF RFC 3227* приділяє увагу побітовій копії носіїв та забезпеченню того, щоб інструменти для збирання доказів були надійними й могли бути перевірені іншими експертами.

ISO/IEC 27037 і *IETF RFC 3227* приділяють особливу увагу документації кожного кроку з фіксуванням часу, унікальних ідентифікаторів доказів та учасників процесу. *IETF RFC 3227* наголошує на необхідності враховувати різницю між локальним часом і *UTC*. *NIST SP 800-86* менш докладно описує документування, але наголошує на необхідності створення юридично обґрунтованих звітів після аналізу.

Усі три документи відзначають важливість дотримання вимог законодавства і процедур, щоб уникнути фальсифікації доказів. Однак *IETF RFC 3227* акцентує на конфіденційності користувачів та уникненні надмірного збирання даних.

Синтез підходів до збирання цифрових доказів на основі розглянутих трьох документів можна представити як комплексний процес,

що містить кілька важливих етапів і принципів, спрямованих на забезпечення збереження, цілісності та допустимості доказів у суді.

Першим етапом є пошук і визначення джерел цифрових доказів. Це можуть бути фізичні пристрої (комп'ютери, сервери, зовнішні носії), логічні дані (файлові системи, конфігураційні файли, журнали) та нестабільні дані (оперативна пам'ять, мережеві з'єднання). Важливо ретельно задокументувати всі джерела даних, враховуючи фізичні та віртуальні аспекти (хмарні сервіси).

Спочатку необхідно зібрати найбільш нестабільні дані з оперативної пам'яті, регістрів, кешу й активних мережевих з'єднань, адже вони швидко зникають після вимкнення системи, тому важливо їх задокументувати та вилучити перед переходом до стабільніших джерел. Після збирання нестабільних даних фокус переходить на стабільні джерела (файлові системи, журнали подій, архівні носії тощо).

Дані необхідно збирати у такий спосіб, щоб уникнути будь-яких змін в оригінальних файлах. Для цього використовуються інструменти блокування запису, що запобігають внесенню змін на носії. Створення копій (зокрема, побітових образів дисків) є обов'язковим для подальшого аналізу. Для верифікації цілісності доказів застосовують методи хешування, що дають змогу підтвердити, що дані не були змінені в процесі збирання та аналізування.

Усі дії, пов'язані з процесом збирання доказів, мають бути докладно задокументовані із зазначенням часу кожної дії (з урахуванням різниці між локальним часом системи та універсальним координованим часом), ідентифікацією кожного доказу, а також осіб, які мали доступ до даних. Підтримання ланцюга зберігання доказів є критично важливим для забезпечення їх допустимості в суді.

Для забезпечення точності та швидкості процесу слід використовувати автоматизовані інструменти, які допомагають відбирати релевантні дані за допомогою пошуку за ключовими словами або шаблонами, що мінімізує обсяг даних, які потребують подальшого аналізу. Процеси збирання повинні бути перевіреними.

Після завершення збирання даних їх опрацьовують та аналізують. Цей етап передбачає застосування юридично обґрунтованих методик для інтерпретації даних, а також створення звітів. Інструменти для аналізування мережевого трафіку, файлових систем і конфігурацій дають можливість ідентифікувати підозрілі взаємодії або інциденти.

Висновки. Отже, збирати дані необхідно з урахуванням законодавства та конфіденційності користувачів. Слід уникати збирання надлишкових або нерелевантних даних, щоб не порушити права

осіб, чиї дані аналізують. Докази повинні бути допустимими, достовірними, повними та надійними для їх використання в суді. Усі дії з доказами мають бути прозорими та піддаватися перевірці. Щоб уникнути несанкціонованих змін або втручання необхідно ізолювати систему від зовнішніх впливів. Також слід контролювати доступ до доказів і використовувати надійні інструменти для збирання, які можуть перевірити незалежні експерти.

Синтезований підхід до збирання цифрових доказів містить докладний процес ідентифікації потенційних джерел, пріоритетного збирання нестабільних даних, збереження цілісності та документування дій. Автоматизація та ефективність процесу, дотримання правових та етичних норм, а також ретельна перевірка й контроль доступу до доказів є ключовими елементами успішного збирання та аналізування цифрових доказів.

Тому збирання цифрових доказів — це складний і багатоетапний процес, який вимагає дотримання чітких процедур для забезпечення достовірності та допустимості зібраних даних. Від правильності виконання кожного етапу (від фіксування доказів до документування ланцюга їх зберігання) залежить не лише успішність розслідування, а й законність використання цифрових слідів у судовому процесі.

Дотримання принципів цілісності, автентичності та відтворюваності є наріжними каменями цифрової криміналістики. Застосування міжнародних стандартів і найкращих практик дає змогу мінімізувати ризики втрати або спотворення даних, а також створює умови для об'єктивного й неупередженого аналізування цифрових доказів. У сучасних умовах, коли кіберзлочинність набуває дедалі складніших форм, розвиток методів збирання цифрових доказів та їхня інтеграція у правові процеси є важливим кроком до зміцнення інформаційної безпеки та справедливості правосуддя.

Подальші дослідження в цій галузі сприятимуть вдосконаленню як технічних, так і правових аспектів роботи з цифровими слідами, що має ключове значення для протидії сучасним загрозам у цифровому просторі.

Перелік посилань **References**

1. Lewulis, P. (2022). Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law. *Crim Law Forum*. Vol. 33. DOI: 10.1007/s10609-021-09430-4 (access date: 24.03.2025).
2. Sun, J.-R., Shih, M.-L., Hwang, M.-Sh. (2015). A survey of digital evidences forensic and cybercrime investigation procedure. *International Journal of Network Security*. Vol. 17.

3. Романюк В., Фоміна Т. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність. *Вісник Кримінологічної асоціації України*. 2024. № 32 (2). С. 344—353. DOI: 10.32631/vca.2024.2.25 (дата звернення: 24.03.2025).

Romaniuk, V., Fomina, T. (2024). The Procedure for Collecting Electronic (Digital) Evidence in Criminal Proceedings on Collaboration Activities. *Bulletin of the Criminological Association of Ukraine*. Vol. 32 (2). DOI: 10.32631/vca.2024.2.25 (access date: 24.03.2025) [in Ukrainian].

4. Гуцалюк М. В., Антонюк П. Є. Щодо сутності електронної (цифрової) інформації як джерела доказів у кримінальному провадженні. *Криміналістичний вісник*. 2021. № 33 (1). С. 37—49. DOI: 10.37025/1992-4437/2020-33-1-37 (дата звернення: 24.03.2025).

Hutsaliuk, M. V., Antoniuk, P. Ye. (2021). On the Essence of Electronic (Digital) Information as a Source of Evidence in Criminal Proceedings. *Criminalistics Bulletin*. Vol. 33 (1). DOI: 10.37025/1992-4437/2020-33-1-37 (access date: 24.03.2025) [in Ukrainian].

5. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека*. 2024. № 2 (93). С. 140—150. DOI: 10.32631/pb.2024.2.13

Romaniuk, V. V., Ablamskyi, S. Ye. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law and Safety*. Vol. 2 (93). DOI: 10.32631/pb.2024.2.13 (access date: 24.03.2025) [in Ukrainian].

6. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. 2018. 31 с.

DSTU ISO/IEC 27037:2017 Information technology. Protection methods. Guidelines for the identification, collection, acquisition and preservation of digital evidence (2018) [in Ukrainian].

7. IETF RFC 3227 Guidelines for Evidence Collection and Archiving. URL: https://datatracker.ietf.org/doc/html/rfc3227 (access date: 24.03.2025).

8. NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response.

Procedure for collecting digital evidence

Taras Ivasyshyn, Oleksandr Pirog

The article is devoted to the topical issues of digital evidence collection within the law, in accordance with the requirements of personal data protection and confidentiality. The procedure for collecting digital evidence is extremely important, as it affects its reliability, admissibility in court and the ability to reproduce events. The rapid development of digital technologies has led to an increase in the number of offenses in cyberspace, and this, in turn, has increased the relevance of studying the process of digital evidence collection. The author examines the

main stages of this process: from identifying and recording evidence to documenting, preserving and analyzing it. Particular attention is paid to the importance of following the sequence of actions to ensure the integrity and authenticity of evidence. The main threats associated with improper data collection are outlined, including the risk of loss, distortion, or forgery of digital traces. International standards and best practices in digital forensics that regulate the handling of electronic evidence are analyzed. Improving approaches involves unifying processes in accordance with international standards, which will facilitate the investigation of transnational crimes. The author emphasizes the importance of an interdisciplinary approach that combines legal, technical and organizational aspects necessary to ensure the admissibility of collected evidence in court practice. It is noted that increased attention to the protection of personal data and confidentiality requires a clear balance between the efficiency of evidence collection and the observance of users' rights.

Keywords: *digital evidence; collection of digital evidence; collection procedure; methods of fixation; documentation of evidence; international standards.*

⇒ Івасишин, Т., Пірог, О. (2025). Порядок збирання цифрових доказів. *Криміналістика і судова експертиза*. Вип. 70. С. 371—381. DOI: 10.33994/kndise.2025.70.28.