УДК 343.359.3:343.985(477) **DOI:** https://doi.org/10.32631/v.2025.3.12

Костянтин Валерійович Караман,
доктор філософії за спеціальністю «Політологія»,
Ізмаїльський міськрайонний суд Одеської області (суддя);
https://orcid.org/0000-0003-2965-9661,
e-mail: karamankostantin@gmail.com

ВИЯВЛЕННЯ ЦИФРОВИХ СЛІДІВ: ОСОБЛИВОСТІ Й АЛГОРИТМ

У статті обґрунтовано, що цифрові сліди дедалі більше змінюють криміналістику, перетворюючись на ключовий ресурс доказування в умовах цифрової доби. Вони можуть зберігатися в різних технічних середовищах – від фізичних носіїв і системних журналів до хмарних сервісів, мережевих платформ та розумних пристроїв. Специфіка таких слідів вимагає застосування спеціалізованих методів їх виявлення, фіксації та перевірки автентичності, зокрема з використанням геш-функцій і метаданих. Водночас відсутність належного процесуального регламенту зумовлює потребу гармонізації законодавства з міжнародними стандартами та розроблення уніфікованої методології, яка гарантуватиме допустимість цифрових доказів у суді.

Ключові слова: досудове розслідування, докази, цифровий слід, електронний доказ, фіксація доказів.

Оригінальна стаття

Постановка проблеми

Стрімка цифровізація суспільних процесів породжує нові виклики для кримінального судочинства, зокрема у сфері виявлення та дослідження слідів злочинної діяльності. Якщо традиційні матеріальні сліди мають відносно сталу форму та фізичну прив'язку, то цифрові сліди злочинної діяльності вирізняються нематеріальною природою, високою динамічністю та вразливістю до змін. Вони можуть бути миттєво знищені, модифіковані чи підроблені, що суттєво ускладнює процес їх виявлення та подальше використання як доказів. Така специфіка актуалізує потребу у створенні чітких науково обґрунтованих алгоритмів пошуку, фіксації та перевірки цифрових слідів у кримінальному провадженні.

Водночас національна правова система досі не містить комплексного визначення цифрового або електронного доказу, його ознак і меж процесуального використання. Унаслідок цього слідчі, прокурори та суди часто стикаються із проблемою визнання таких доказів недопустимими через порушення порядку їх вилучення чи обробки. Недостатня регламентація ускладнює роботу не лише органів досудового розслідування, а й адвокатів, які змушені відстоювати інтереси

клієнтів в умовах відсутності чітких стандартів доказування в цифровій сфері.

Особливого значення набуває розроблення алгоритмів виявлення цифрових слідів, які б ураховували їхні технічні особливості й одночасно відповідали вимогам процесуального закону. Це передбачає інтеграцію спеціальних знань цифрової криміналістики у практику кримінального процесу, а також вироблення тактичних прийомів взаємодії між правниками та ІТ-фахівцями.

Крім того, на сучасному етапі розвитку українського законодавства важливим є врахування міжнародних зобов'язань, зокрема положень Будапештської конвенції про кіберзлочинність і стандартів Європейського Союзу, які вимагають гармонізації підходів до роботи з електронними доказами. Це потребує створення єдиної концепції цифрових доказів, яка відповідатиме як внутрішнім правовим реаліям, так і міжнародним вимогам.

Таким чином, проблема виявлення цифрових слідів виходить за межі суто технічного питання і перетворюється на комплексне завдання, що потребує системного вирішення із застосуванням міждисциплінарного підходу на межі криміналістики, кримінального процесу, інформаційних технологій і кібербезпеки. Її актуальність зумовлена необхідністю підвищення ефективності розслідування злочинів, забезпечення допустимості цифрових доказів у суді та формування надійних механізмів захисту прав людини в умовах цифрової епохи.

Стан дослідження проблеми

Питання виявлення та дослідження цифрових слідів, а також особливості збирання і процесуального використання електронних доказів стали предметом уваги таких дослідників, як А.-М. Ю. Ангеленюк, П. Є. Антонюк, М. В. Гуцалюк, І. Г. Каланча, А. В. Коваленко, А. В. Ратнова, О. В. Сіренко, С. С. Чернявський, Ю. Ю. Орлов, а також інших науковців [1–9].

Попри наявність значної кількості праць у цій сфері, повна й офіційна легалізація електронних доказів як самостійного засобу доказування у кримінальному провадженні в Україні досі не відбулася. Ця обставина зумовлює нагальну потребу в подальших теоретичних і прикладних дослідженнях, спрямованих на розроблення цілісної концепції процесуального статусу та практичного використання електронних доказів.

Мета і завдання дослідження

Метою статті є визначення особливостей та апробованих алгоритмів виявлення цифрових слідів. Для її досягнення було поставлено такі *завдання*: 1) визначити технічні аспекти виявлення цифрових

слідів та їх фіксації; 2) розробити уніфікований алгоритм виявлення цифрових слідів задля подальшої їх фіксації з метою використання в доказуванні.

Наукова новизна дослідження

Обґрунтовано, що цифрові сліди дедалі більше трансформують криміналістику, стаючи ключовим ресурсом доказування в цифрову добу. Вони зберігаються в різних технічних середовищах – від фізичних носіїв і системних журналів до хмарних сервісів, мережевих платформ та розумних пристроїв. Їхня специфіка зумовлює потребу у спеціалізованих методах виявлення, фіксації та перевірки автентичності, зокрема через використання геш-функцій і метаданих. Запропоновано алгоритм діяльності сторони обвинувачення під час роботи із цифровими слідами на етапах їх виявлення та фіксації. Наголошено, що відсутність належного процесуального регламенту потребує гармонізації законодавства з міжнародними стандартами та розроблення уніфікованої методології, що гарантуватиме допустимість цифрових доказів у суді.

Виклад основного матеріалу

Цифрові сліди дедалі відчутніше змінюють концептуальні орієнтири криміналістичної науки та практики, ініціюючи перехід до нової моделі доказування, адаптованої до умов інформаційно-комунікаційного середовища. Їхня юридична та криміналістична значущість полягає у здатності відтворювати ключові характеристики кримінальної події та поведінки її суб'єктів, водночас вимагаючи використання спеціалізованих методик виявлення, фіксації та процесуальної оцінки.

Сучасні проблеми в цій сфері охоплюють як прогалини правового регулювання, так і техніко-криміналістичні обмеження. Це зумовлює необхідність докорінного реформування процесуального законодавства, його гармонізації з міжнародними правовими стандартами та впровадження інноваційних інструментів криміналістичної тактики і методики.

Ключовим напрямом у цьому контексті слід вважати інтеграцію цифрових слідів у систему криміналістичної характеристики злочинів. Це має забезпечити підвищення ефективності досудового розслідування, формування повноцінної доказової бази та гарантування дотримання прав і законних інтересів усіх учасників кримінального провадження. У цьому контексті створення сучасної методології виявлення, аналізу та використання цифрових слідів постає не лише науково-теоретичним завданням, а й нагальною практичною вимогою доби цифрової трансформації правової системи.

Таким чином, сучасне розуміння криміналістичної значущості цифрових слідів ґрунтується на інтегрованому, міждисциплінарному і технологічно орієнтованому підході, у межах якого цифрові сліди

постають стратегічним ресурсом доказування. За умови дотримання національних процесуальних норм і міжнародно-правових зобов'язань вони набувають статусу повноцінних доказів, що дозволяє поєднувати ефективність кримінального переслідування з дотриманням загальних засад кримінального провадження.

Цифрові сліди зберігаються в різних технічних середовищах і на різних рівнях інформаційних систем, що зумовлює їхній багатовимірний характер. Основні місця зберігання можна умовно поділити на кілька груп.

1. Фізичні носії інформації:

– жорсткі диски (HDD), твердотільні накопичувачі (SSD), флеш-пам'ять (USB-накопичувачі, карти пам'яті SD, microSD тощо) – містять операційні системи, файли користувача, тимчасові дані та видалені записи, які можуть бути відновлені;

– оптичні носії (CD, DVD, Blu-ray) – хоч і використовуються рідше, але можуть зберігати резервні копії та архіви;

– мобільні пристрої (смартфони, планшети) – накопичують повідомлення, історію дзвінків, геолокаційні дані, фото, відео, журнали застосунків.

2. Системні середовища комп'ютера, зокрема:

– операційні системи – зберігають журнали подій (*event logs*), тимчасові файли, кеш браузерів, історію входів і виходів у систему;

– прикладне програмне забезпечення – бази даних, електронні таблиці, текстові документи, мультимедійні файли, електронна пошта;

– тимчасові файли та резервні копії – створюються автоматично в процесі роботи програм і можуть зберігати дані навіть після видалення основного документа.

3. Мережеві середовища:

– інтернет-провайдери – фіксують журнали з'єднань, IP-адреси, інформацію про трафік користувачів;

– сервери та маршрутизатори – зберігають журнали активності, налаштування та сліди передавання даних;

– електронна пошта, соціальні мережі, месенджери – містять дані про переписку, історію дзвінків, передані файли, метадані.

4. Хмарні сховища та віддалені сервери:

– хмарні сервіси (Google Drive, iCloud, Dropbox та ін.) – зберігають файли, резервні копії мобільних пристроїв, історію редагувань документів;

– віртуальні сервери та віртуальні машини – містять цифрові сліди у формі логів і образів дисків.

5. Спеціалізовані пристрої та системи:

– системи відеоспостереження (CCTV, IP-камери) – зберігають відеозаписи подій, метадані про час і місце зйомки;

– розумні пристрої – смартгодинники, фітнес-трекери, автомобільні системи (GPS-навігатори, бортові комп'ютери), які фіксують рух, стан здоров'я та геолокацію;

– маршрутизатори, концентратори, комутатори – зберігають цифрові сліди мережевої активності [10, с. 8–9].

Найбільш типовим у слідчій практиці є виявлення та збереження цифрових слідів у вигляді комп'ютерних даних. До них висуваються ті самі вимоги, що й до інших цифрових доказів. Водночас їхня специфіка обумовлена бінарною природою (послідовність нулів та одиниць), що робить унесені зміни практично непомітними для людського ока. Тому процедури ідентифікації комп'ютерних даних у кримінальному провадженні повинні забезпечувати підтвердження їхньої цілісності та незмінності з істотно вищим рівнем достовірності, ніж це можливо при використанні традиційних методів виявлення цифрових слідів.

З огляду на відсутність у Кримінальному процесуальному кодексі України (далі – КПК України) та підзаконних актах чіткого регламенту таких технічних процедур доцільним, як слушно зазначають учені, є звернення до положень ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» (ISO/IEC 27037: 2012, IDT). У ньому містяться методичні рекомендації для носіїв спеціальних знань, залучених як спеціалістів (у розумінні ст. 71 КПК України) з метою виявлення, вилучення та збереження цифрових слідів, що можуть мати доказове значення. Крім того, положення цього ДСТУ спрямовані на уніфікацію процедур оброблення електронних доказів і забезпечення можливості їхнього належного обміну між різними юрисдикціями [11].

Зауважимо, що в ДСТУ ISO/IEC 27037:2017 застосовується термін «ідентифікація» (на відміну від усталеного у вітчизняній криміналістиці поняття «вилучення»), під яким розуміють процес пошуку, розпізнавання та документування потенційних цифрових доказів. Це поняття необхідно відрізняти від «ідентифікації» у значенні п. 3 ч. 3 ст. 104 КПК України, де воно використовується здебільшого як спосіб підтвердження незмінності та цілісності комп'ютерних даних. На цьому етапі ключову роль відіграє застосування геш-функцій, обчислення та документування відповідних геш-значень, які виступають універсальним засобом перевірки автентичності цифрових об'єктів.

Геш-функція є алгоритмом, який перетворює вхідні дані довільної довжини в послідовність фіксованої довжини (дайджест). Обчислене геш-значення є унікальним для кожного набору даних, а збіг гешів свідчить про їхню ідентичність на бітовому рівні. Це дозволяє виявити навіть мінімальні зміни у файлі чи повідомленні. Практичне застосування геш-функцій охоплює перевірку цілісності даних, зберігання та верифікацію паролів, створення цифрових підписів.

У міжнародній та національній практиці використовуються різні алгоритми гешування, зокрема MD5, SHA-1, SHA-256, а також національний стандарт ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування», що базується на криптографічній функції «Купина». Визначальною характеристикою криптографічних геш-функцій є відсутність колізій, що гарантує унікальність обчислених значень і забезпечує можливість використання цих функцій як інструмента криміналістичної ідентифікації [12]. Таким чином, розрахунок і фіксація геш-значень у протоколах процесуальних дій має розглядатися як ключовий спосіб фіксації комп'ютерних даних у розумінні вимог п. 3 ч. 3 ст. 104 КПК України. Це забезпечує підтвердження їхньої цілісності на всіх етапах кримінального провадження та створює надійні гарантії допустимості електронних доказів у суді.

Апробованим нині методом збирання електронних доказів є фіксація даних, отриманих за результатами проведеної розвідки з відкритих джерел (далі – OSINT), яка у кримінальному провадженні має здійснюватися з дотриманням вимог кримінального процесуального законодавства України та міжнародних стандартів у сфері поводження із цифровими доказами. Виходячи зі змісту ст. 99 КПК України, результати OSINT доцільно кваліфікувати як документи, що підлягають фіксації у протоколах процесуальних дій із долученням відповідних носіїв інформації. Найчастіше така діяльність реалізується в межах проведення огляду (ст. 237 КПК України), що зумовлює необхідність відображення отриманих матеріалів у протоколі та забезпечення їх цілісності шляхом додатків (зокрема фото-, відеозаписів, скриншотів, електронних файлів).

Особливої уваги потребує застосування технічних інструментів для підтвердження автентичності зібраних даних, зокрема шляхом фіксації метаданих і геш-значень. Такий підхід узгоджується з положеннями міжнародних документів, зокрема Протоколу Берклі. Водночас необхідно наголосити, що на сьогодні відсутній нормативно-правовий акт, який би комплексно визначав процесуальні засади збирання та легалізації електронних доказів у кримінальному провадженні [13; 14].

У цьому контексті результати OSINT можуть визнаватися належними доказами лише за умови правильної процесуальної фіксації, що забезпечує їх допустимість у суді. Вирішальним є те, що фіксація має відбуватися у формі, яка дозволяє перевірити цілісність і незмінність даних, а також підтвердити їх походження з відкритих джерел. Нерідко для цього і під час досудового розслідування, і під час судового розгляду залучається спеціаліст.

В умовах стрімкої цифровізації суспільних процесів електронні докази посідають дедалі важливіше місце у кримінальному провадженні. Їхня правова та криміналістична цінність визначається здатністю відображати механізм злочинної діяльності, сліди окремих

актів протиправної поведінки або навіть цілі технології злочинної діяльності. Водночас ця особливість зумовлює потребу у впровадженні специфічних процедур їх виявлення та фіксації.

На підставі проведеного аналізу можна виокремити кілька ключових особливостей виявлення цифрових слідів. По-перше, їхня природа суттєво відрізняється від традиційних матеріальних об'єктів: вони існують у формі бінарних даних, які не мають чіткої прив'язки до фізичного носія та можуть бути легко змінені або знищені. Це зумовлює необхідність застосування спеціалізованих технічних засобів та алгоритмів для їх виявлення. По-друге, автентичність і достовірність цифрових доказів забезпечується через процедури, які фіксують їхню цілісність (зокрема, використання геш-функцій і документування метаданих). По-третє, цифрові сліди характеризуються мобільністю і глобальністю: вони можуть походити з відкритих джерел у мережі «Інтернет» (зокрема результатів OSINT), що потребує додаткових процесуальних гарантій для їхньої легалізації та подальшого використання в суді.

Отже, можемо окреслити певний алгоритм виявлення цифрових слідів, який узгоджується з вимогами криміналістичної тактики та положеннями міжнародних стандартів, зокрема ДСТУ ISO/IEC 27037:2017.

1. Виявлення потенційних цифрових об'єктів. Передбачає пошук і розпізнавання даних, що можуть мати доказове значення, з обов'язковим документуванням джерела їх виявлення. У разі відсутності у слідчого чи детектива спеціальних знань такі дії мають виконуватися за участю спеціаліста, який не лише забезпечує технічну підтримку, а й консультує сторону обвинувачення щодо особливостей подальшого дослідження даних, зокрема під час експертного аналізу.

2. Фіксація виявленої інформації. Здійснюється шляхом складання протоколу процесуальної дії з усіма необхідними додатками. Доцільно забезпечити фото- та відеофіксацію, виготовлення скриншотів кожної дії, а також долучення електронного носія з копіями виявлених даних, які було виявлено на попередньому етапі.

3. Забезпечення автентичності та незмінності. Реалізується через обчислення та фіксацію геш-значень, збереження метаданих та інших параметрів, що підтверджують цілісність об'єкта. На цьому етапі важливо вжити заходів, які унеможливлюють зміну, пошкодження або знищення даних.

4. Збереження і передача даних. Відбувається з дотриманням правил ланцюга збереження доказів (*chain of custody*), що гарантує прозорість усіх етапів роботи з потенційним джерелом доказу.

5. Процесуальне оформлення. Полягає в інтеграції результатів у систему доказування шляхом віднесення їх до категорії «документи» (ст. 99 КПК України). За необхідності здійснюється додатковий огляд матеріалів із подальшим їх долученням до кримінального провадження

на підставі відповідного процесуального рішення (постанови про залучення як доказу та приєднання до матеріалів кримінального провадження).

Таким чином, цифрові сліди можуть бути ефективно інтегровані у кримінальне провадження лише за умови дотримання чітко визначених процедур виявлення, фіксації та перевірки їхньої автентичності. Запровадження цього алгоритму створює підґрунтя для формування уніфікованої методології роботи з електронними доказами, що відповідатиме міжнародним стандартам і забезпечуватиме їхню допустимість у судовій практиці.

Висновки

Цифрові сліди становлять якісно нову категорію об'єктів криміналістичного дослідження, що зумовлює необхідність перегляду традиційних підходів до доказування. Їхня криміналістична значущість полягає у здатності відображати ключові елементи злочинної діяльності та поведінки її суб'єктів, тоді як особливості природи (бінарність, мобільність, глобальність) визначають специфіку виявлення, фіксації та процесуальної легалізації таких слідів.

Цифрові сліди можуть зберігатися в різних середовищах і відображатися на різноманітних носіях – від фізичних накопичувачів і системних ресурсів комп'ютера до мережевих платформ, хмарних сервісів і спеціалізованих розумних пристроїв. Така розосередженість потребує використання комплексних методів виявлення та застосування спеціальних знань, що забезпечує повноту та достовірність отриманих результатів, їхню якість, а отже, у подальшому визначатиме допустимість.

Ключовим елементом гарантування автентичності та допустимості цифрових слідів у кримінальному провадженні є застосування технічних інструментів перевірки їхньої цілісності, зокрема геш-функцій і документування метаданих. Водночас необхідно дотримуватися принципу ланцюга збереження доказів і впровадження міжнародних стандартів (наприклад, ДСТУ ISO/IEC 27037:2017) як базових орієнтирів.

Важливе значення має впровадження алгоритму роботи із цифровими слідами, що охоплює виявлення, процесуальну фіксацію, забезпечення автентичності, належне збереження та інтеграцію в систему доказування. Лише за таких умов електронні дані можуть бути визнані повноцінними доказами в суді.

Узагальнюючи, можна стверджувати, що ефективне використання цифрових слідів у кримінальному провадженні можливе за умови:

1) оновлення процесуального законодавства та його гармонізації з міжнародними стандартами;

2) розроблення уніфікованої криміналістичної методології роботи з електронними доказами;

3) системної інтеграції цифрових слідів у криміналістичну характеристику злочинів та включення відповідних рекомендацій до методичних матеріалів з розслідування кримінальних правопорушень.

Таким чином, цифрові сліди набувають статусу стратегічного ресурсу сучасного доказування, здатного одночасно підвищити ефективність досудового розслідування та забезпечити баланс між результативністю кримінального переслідування і дотриманням прав людини.

Список бібліографічних посилань: 1. Ангеленюк А.-М. Ю. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Т. 2, № 79. С. 214–218. DOI: https://doi.org/10.24144/2307-3322.2023.79.2.32. **2.** Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2016. Вип. 36 (2). С. 123–125. **3.** Гуцалюк М. В., Антонюк П. Є. Щодо сутності електронної (цифрової) інформації як джерела доказів у кримінальному провадженні. *Криміналістичний вісник.* 2020. Т. 33, № 1. С. 37–49. DOI: https://doi.org/10.37025/1992-4437/2020-33-1-37. **4.** Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Т. 4, № 85. С. 71–75. DOI: https://doi.org/10.24144/2307-3322.2024.85.4.10. **5.** Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2018. № 4. С. 237–245. **6.** Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2022. № 4. С. 226–236. DOI: https://doi.org/10.33766/2524-0323.100.226-236. **7.** Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права.* 2022. № 1. С. 176–180. DOI: https://doi.org/10.32782/klj/2022.1.27. **8.** Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльне правознавство.* 2013. № 3–2. С. 313–315. **9.** Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ.* 2017. № 1. С. 12–24. **10.** Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін. ; за заг. ред. О. В. Корнейка. Вид. 2-ге, допов. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с. **11.** Каланча І. Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні // Сучасні виклики та актуальні проблеми судової реформи в Україні : матеріали VII Міжнар. наук.-практ. конф. (м. Чернівці, 27 жовт. 2023 р.) / редкол.: О. В. Щербанюк та ін.

Чернівці, 2023. С. 253–258. **12.** Каланча І. Г., Стемковський Д. Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. *Аналітично-порівняльне правознавство.* 2025. № 2. С. 1001–1008. DOI: https://doi.org/10.24144/2788-6018.2025.02.148. **13.** Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с. **14.** Радейко Р. І. Теоретико-правові засади фіксації OSINT-доказів із соціальних мереж: процесуальні вимоги та методологічні підходи (на прикладі справи № 990/232/24). *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* 2025. № 45. С. 110–116. DOI: https://doi.org/10.5281/zenodo.15648855.

Надійшла до редколегії 20.08.2025

Прийнята до опублікування 11.09.2025

Karaman K. V. Detecting Digital Traces: Features and Algorithm

The article argues that digital traces constitute a qualitatively new category of objects of forensic investigation, which requires a revision of traditional approaches to evidence. Their forensic significance is due to their ability to reflect key elements of criminal activity and the behaviour of its perpetrators, while their specific nature (binarity, mobility, globality) determines the specifics of their detection, recording and procedural legalisation.

It has been established that digital traces are stored in many environments – from physical media and computer system resources to network platforms, cloud services and specialised Internet of Things devices. Such dispersion requires the use of complex search methods and the involvement of specialised knowledge to ensure the completeness and reliability of the results obtained.

It has been proven that the key element in ensuring the authenticity and admissibility of digital traces in criminal proceedings is the use of technical tools to verify their integrity, in particular hash functions and metadata documentation. At the same time, emphasis is placed on the need to comply with the principle of the chain of custody of evidence and the implementation of international standards (in particular, DSTU ISO/IEC 27037:2017) as basic guidelines. Of particular importance is the implementation of an algorithm for working with digital traces, which covers their detection, procedural recording, authenticity assurance, preservation and proper inclusion in the evidence system. Only under such conditions can electronic data acquire the status of full-fledged evidence in court.

It is emphasised that the effective use of digital traces in criminal proceedings is possible under the following conditions: updating procedural legislation and harmonising it with international standards; developing a unified forensic methodology for working with electronic evidence; and systematically integrating digital traces into the forensic characterisation of crimes.

It is concluded that digital traces are a strategic resource of modern evidence, capable of increasing the effectiveness of pre-trial investigations and ensuring a balance between the effectiveness of criminal prosecution and respect for human rights.

Keywords: pre-trial investigation, evidence, digital trace, electronic evidence, evidence recording.