DOI https://doi.org/10.30525/978-9934-26-686-7-5

ОСОБЛИВОСТІ ФІКСАЦІЇ ЦИФРОВИХ СЛІДІВ ПІД ЧАС ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Дзюрбель А. Д.

ВСТУП

Сучасний етап розвитку світової цивілізації характеризується тотальною трансформацією соціальних комунікацій, що зумовлена стрімким впровадженням інформаційних технологій у всі сфери людської життєдіяльності. Цей процес неминуче супроводжується якісною зміною структури злочинності: від класичних «матеріальних» правопорушень до кіберзлочинів та злочинів, де цифрові пристрої виступають знаряддям або об'єктом посягання. У цьому контексті перед криміналістичною наукою постає фундаментальне завдання – розробка теоретичних засад та практичних інструментів роботи з новим типом відображення реальності, а саме з цифровими (електронними) слідами[1].

Сучасні кримінальні правопорушення все частіше вчиняються у кіберпросторі або супроводжуються утворенням специфічних цифрових відображень, які за своєю природою суттєво відрізняються від традиційних матеріальних слідів[2]. Це ставить перед криміналістичною наукою виклик щодо переосмислення базових теоретичних положень та розробки нових методичних рекомендацій для суб'єктів досудового розслідування.

Актуальність теми зумовлена тим, що цифрові сліди сьогодні присутні майже в кожному кримінальному провадженні – від корупційних злочинів та шахрайства до воєнних злочинів та актів агресії. За оцінками Центру дослідження комп'ютерних злочинів, у 2025 році збитки від кіберзлочинності перевищать 12 трильйонів доларів США. Глобальний характер кіберризиків вимагає створення спільних дієвих міжнародних рамок для забезпечення стандартів кібербезпеки та захисту даних[3]. Також слід врахувати, що в умовах широкомасштабного вторгнення Російської Федерації в Україну цифрові докази стали основним інструментом документування звірств російських військових (відео з камер спостереження, записи з БПЛА, супутникові знімки та пости в соцмережах російських військових, тощо). У зв'язку з наведеним, перед правоохоронними органами постає питання про документування цих злочинів з врахуванням вимог національних та міжнародних правових

[1] Коломійцев С.О. Сутність та класифікація цифрових слідів кримінального правопорушення. *Вісник пенітенціарної асоціації України. 2025.* № 2 (32). С. 196-205.

[2] Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка,* № 4 (100), 2022. С. 226-236.

[3] Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний університет імені Юрія Федьковича. 27.02.2025. URL:https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist.

інституцій. Ключовою основою такої діяльності в умовах нашого сьогодення є цифрові технології і, зокрема цифрові докази[4].

Проте в юридичній доктрині України досі триває дискусія щодо термінологічної єдності, класифікаційних критеріїв та процесуального статусу таких об'єктів[5]. Більше того, динамічний розвиток технологій анти-криміналістики (шифрування, анонімізація, видалення даних) потребує від правоохоронних органів постійного оновлення технічного інструментарію та тактичних прийомів.

У контексті кримінального судочинства це зумовлює виникнення нових викликів перед теорією криміналістики та процесуальним правом, оскільки традиційні методи збирання та дослідження матеріальних доказів виявляються недостатніми для роботи з об'єктами нематеріальної природи. Поняття «цифровий слід» стає центральним елементом сучасної доказової бази. Це вимагає глибокого переосмислення правової природи таких слідів, удосконалення національного законодавства та гармонізації вітчизняної слідчо-судової практики з міжнародними стандартами.

Метою цієї статті є комплексний аналіз поняття, класифікації та криміналістичної характеристики цифрових слідів, дослідження проблемних аспектів їхнього використання у практичній діяльності та вивчення тенденцій сучасної судової практики для формування науково обґрунтованих пропозицій щодо вдосконалення механізмів збирання та дослідження цифрових доказів.

Питання цифрових (електронних) слідів досліджувалися багатьма вітчизняними та закордонними науковцями. Значний внесок у розвиток цифрової криміналістики зробили Г.К. Авдєєва, М.В. Капустіна, А.В. Коваленко, І.А. Колеснікова, О.І. Крицька, К.В. Латиш, В.Ю. Шепітько, І.З. Якименко та інші[6].

У працях вітчизняних науковців не досягнуто єдності в думках та поглядах у питанні визначення цифрових слідів, їх класифікації, місця та ролі у науці криміналістика та інших питаннях пов'язаних з зазначеним видом слідів. Враховуючи наведене, у статті проаналізуємо ряд проблемних та спірних питань щодо цифрових доказів та запропонуємо окремі шляхи їх вирішення.

1. Поняття, класифікація та криміналістична характеристика цифрових слідів у сучасній криміналістиці

Теоретичне осмислення сутності цифрових слідів потребує відходу від традиційної (матеріалістичної) трасологічної парадигми, де слід сприймається як фізичне відображення форми одного предмета на поверхні іншого. Саме тому, виникнення цифрових технологій змусило дослідників вийти за межі

[4] Цифрові докази війни: як технології допомагають Україні фіксувати злочини Росії. Українські правозахисники та юристи розповіли про нові методи збору доказів воєнних злочинів РФ, які витримують перевірку міжнародних судів URL: https://www.polskieradio.pl/398/7857.

[5] Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету. Серія Право.* Випуск 85: частина 4. С. 71-75.

[6] Там само.

традиційної трасології. Цифровий слід не є матеріальним об'єктом у звичному розумінні (як відбиток пальця чи сліди протектора), оскільки він існує у формі двійкового коду, записаного на фізичний носій за допомогою електромагнітних або оптичних сигналів.[7]

У науковій літературі тривалий час тривала дискусія щодо термінології. С. Хижняк пропонує використовувати термін «віртуальні сліди», розуміючи під ними будь-які зміни комп'ютерної інформації, пов'язані з подією злочину[7]. Проте інші дослідники слушно зауважують, що семантика слова «віртуальний» передбачає щось уявне або таке, що існує лише в уяві, тоді як цифрові дані є об'єктивною реальністю, яка, попри невидимість для людського ока без спеціальних пристроїв, має чітку матеріальну основу у вигляді стану напівпровідників або намагнічених ділянок диска[8]. Отже, найбільш обґрунтованим є термін «цифрові сліди», який підкреслює форму існування інформації (discrete/digital) та її нерозривний зв'язок з технологіями обробки даних[9].

Криміналістична характеристика цифрових слідів визначається їхніми специфічними властивостями, які докорінно відрізняють їх від традиційних матеріальних об'єктів. По-перше, це відсутність безпосереднього візуального сприйняття – для виявлення та фіксації цифрової інформації необхідне складне програмне та апаратне забезпечення. По-друге, це висока вразливість та нестабільність: інформація в оперативній пам'яті (RAM) зникає при відключенні живлення, а дані на накопичувачах можуть бути миттєво видалені або змінені шляхом дистанційного доступу. По-третє, цифрові сліди мають здатність до ідентичного копіювання без втрати первинних властивостей, що породжує проблему автентичності та розмежування оригіналу і копії в правовому полі.

Науковий аналіз дозволяє виділити кілька ключових підходів до визначення поняття цифрові сліди:

1. *Технічний підхід:* Цифровий слід як стан комп'ютерної системи або послідовність бітів на носії[10].

2. *Інформаційний підхід:* Як криміналістично значуща інформація про подію злочину, зафіксована в цифровій формі[11].

3. *Діяльнісний підхід:* Як відображення активності особи у віртуальному просторі (логи, транзакції, повідомлення)[12].

---

[7] Хижняк Є.С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права.* 2017. Вип.79. С. 159-166.

[8] Колеснікова І.А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний електронний журнал*. 2023. № 10. С. 472-475.

[9] Коломійцев С.О. Сутність та класифікація цифрових слідів кримінального правопорушення. *Вісник пенітенціарної асоціації України*. *2025.* № 2 (32). С. 196-205.

[10] Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304-307.

[11] Крицька І. О. «Доріжка цифрових слідів»: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні / І. О. Крицька // Цифрові трансформації України 2020: виклики та реалії: зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за матеріалами круглого столу, 18 вересня 2020 р. Харків: НДІ ПЗІР НАПрН України, 2020. С. 92-97.

Враховуючи наведене, на наш погляд, найбільш адаптованим до сучасних умов є визначення запропоноване Демидовою Є.Є., згідно з яким *цифровий слід* – це дані, що залишаються у цифровому просторі в результаті використання цифрових пристроїв, технологій та інформаційних мереж, які містять відомості про обставини вчинення кримінального правопорушення[13]. Важливо також розмежовувати поняття «цифровий слід» та «джерело цифрового сліду» (наприклад, смартфон або сервер). Слід – це інформація, тоді як пристрій – це лише її матеріальний носій.

Досліджуючи поняття цифрових слідів, слід зазначити, що їм притаманні певні ключові особливості, а саме:

1. *Цифрова (бінарна) форма існування.* Інформація представлена у вигляді нулів та одиниць. Це обумовлює можливість ідеального копіювання: криміналістичний образ (image) носія є бінарно ідентичним оригіналу, що дозволяє проводити дослідження без ризику модифікації первинних даних.
2. *Волатильність (летючість).* Значна частина цифрових слідів існує лише під час роботи пристрою. Дані в оперативній пам'яті (RAM), активні мережеві з'єднання та тимчасові системні процеси зникають при вимкненні живлення. Це вимагає тактики «живого аналізу» (live forensics) перед фізичним вилученням техніки.
3. *Прихованість та залежність від засобів візуалізації.* На відміну від традиційних слідів, цифрові сліди неможливо сприйняти безпосередньо органами чуття людини. Вони потребують «перекладача» – програмно-апаратного комплексу (Cellebrite, EnCase), який декодує бінарний код у зрозумілий текст, зображення чи відео.
4. *Схильність до швидкої модифікації та знищення.* Цифрові сліди можуть бути змінені або видалені дистанційно. Функції «віддаленого стирання» у смартфонах або автоматичне очищення логів у серверах створюють ризик незворотної втрати доказів.
5. *Трансмежовість (екстериторіальність).* Механізм утворення сліду може розпочатися в одній країні (пристрій зловмисника), а завершитися в іншій (сервер провайдера), що створює складні проблеми юрисдикції та міжнародної співпраці.

Формування цифрового сліду є результатом взаємодії користувача з операційною системою або прикладним програмним забезпеченням. Будь-яка операція залишає артефакти:

- *Тимчасові мітки (Timestamps):* MAC-дати (Modified, Accessed, Created), які фіксують час будь-якої дії з файлом.
- *Лог-файли (Logs):* Системні журнали, що реєструють події (вхід у систему, підключення до Wi-Fi, встановлення програм).

---

[12] Лазебний А.М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип.1 (10) С. 226-233.

[13] Демидова Є.Є. *Цифрові сліди кримінального правопорушення: поняття та особливості. Науковий вісник Ужгородського Національного Університету. Серія Право.* Випуск 85: частина 4. С. 71-75.

- *Метадані:* Інформація «про інформацію», прихована всередині файлів (EXIF-дані фотографій з координатами GPS, авторство документів Word).

Для ефективної побудови методики виявлення та фіксації слідів критично важливою є їхня наукова класифікація. Авдєєва Г.К. та Стороженко С.В. пропонують диференціювати електронні сліди за об'єктом, що їх утворює, способом доступу та правомірністю входу до системи[14]. Гринько Л.П. вважає, що електронні сліди потрібно поділяти на ті, які містяться в мережі Інтернет та ті, що знаходяться на електронних носіях[15]. В свою чергу Колодіна А.С. та Федорова Т.С. виділяють активні та пасивні цифрові сліди, а також виокремлюють такі їх різновид як контент та метадані[16]. На наш погляд, найбільш розгорнуту систему критеріїв пропонує А. В. Коваленко, розділяючи сліди на групи за ознаками слідоутворюючого об'єкта, характеристиками самих даних та особливостями носія[17].

За ознаками носія (слідоприймаючого об'єкта) сліди поділяються на локальні та віддалені. Локальні сліди знаходяться безпосередньо в межах місця події на персональних пристроях (смартфони, ноутбуки, флеш-накопичувачі). Віддалені сліди можуть перебувати як у межах національної юрисдикції (сервери вітчизняних провайдерів), так і поза її межами (хмарні сервіси Google, Apple, Microsoft, сервери месенджерів Telegram або WhatsApp). Цей поділ безпосередньо впливає на тактику слідчої дії: якщо для вилучення локальних слідів достатньо проведення огляду або обшуку, то робота з віддаленими слідами вимагає застосування процедур тимчасового доступу до речей і документів або використання механізмів Будапештської конвенції про кіберзлочинність[18].

Додатково слід виокремити класифікацію за способом сприйняття та форматуванням даних. Цифрові сліди існують у формі текстових документів, графічних зображень, відео- та звукозаписів, лог-файлів (журналів реєстрації подій), метаданих (EXIF-дані фотографій, історія редагування документів) та баз даних. Метадані часто мають вищу криміналістичну цінність, ніж сам зміст файлу, оскільки вони фіксують час створення, координати GPS та ідентифікатори пристрою, що дозволяє встановити об'єктивну картину події незалежно від показань підозрюваного.

Особливу категорію складають сліди, що перебувають у захищеному стані. Розвиток технологій шифрування (наприклад, File-Based Encryption в Android

---

[14] Авдєєва Г.К., Стороженко С.В. Електронні сліди: поняття і види. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2017. № 1(77). С. 168-175.

[15] Гринько Л.П. «Слідова картина» шахрайств, вчинених через мережу Інтернет. *Полтавський правовий часопис*. 2022. № 3. С. 16-27.

[16] Колодіна А.С., Федотова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Київський правовий часопис*. Випуск 1. С. 176-180.

[17] Коваленко А.В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності.* 2023. Випуск 161. С. 202-214.

[18] Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний університет імені Юрія Федьковича. 27.02.2025. URL: https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist.

або Data Protection в iOS) призводить до того, що вилучений носій без знання ключа або пароля перетворюється на «нечитабельну» сукупність даних[19]. Це актуалізує проблему правомірності вилучення паролів та біометричних даних під час слідчих дій, а також необхідність залучення фахівців, здатних використовувати спеціалізовані методи обходу засобів захисту (brute-force, розшифрування за допомогою апаратних ключів)[18]. Розуміння цієї класифікаційної структури є обов'язковою умовою для забезпечення допустимості доказів, оскільки неправильне визначення типу сліду призводить до вибору невідповідної процедури його фіксації.

Незважаючи на стрімкий розвиток технологій, Кримінальний процесуальний кодекс України станом на 2025–2026 роки не містить окремої норми, яка б прямо визначала поняття «електронний доказ» або «цифровий слід». Стаття 84 КПК України (Далі КПК) встановлює вичерпний перелік процесуальних джерел доказів: показання, речові докази, документи та висновки експертів. У цій структурі електронна інформація традиційно відноситься до категорії документів. КПК оперує поняттям «документи», до яких відносить і комп'ютерні дані (ст. 99). Відповідно до зазначеної статті КПК, до документів належать матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації, у тому числі електронні[20].

Таке нормативне регулювання породжує низку проблем у правозастосовчій діяльності. По-перше, електронна інформація за своїми властивостями часто ближча до речових доказів, оскільки вона є слідовим відображенням злочинної діяльності в пам'яті пристрою, а не просто засобом фіксації думок чи фактів, як класичний документ. По-друге, відсутність чіткої диференціації ускладнює процес збирання та перевірки таких доказів. На відміну від цивільного, господарського та адміністративного судочинства, де статус електронних доказів закріплений в окремих статтях ще з 2017 року, кримінальний процес залишається надмірно консервативним[21].

Підсумовуючи наведене, ми повністю поділяємо точку зору наукової спільноти щодо внесення змін до КПК України, зокрема до статей 84 та 99, для виокремлення електронних доказів як самостійного виду. Це зумовлено специфікою їх природи: вони існують лише в цифровій формі, потребують спеціального обладнання для зчитування та професійного аналізу, а також мають надзвичайну вразливість до маніпуляцій.

---

[19] Курман О.В. Особливості та проблеми виявлення й фіксації цифрових слідів під час огляду мобільних засобів зв'язку. *Електронне наукове видання «Аналітично-порівняльне правознавство».* Випуск № 04, 2025, частина 3. С. 238-242.

[20] Науково-практичний коментар Кримінального процесуального кодексу України – науково-методична робота. Станом на 14 квітня 2024 року / За заг. ред. Стратонова В.М. Київ: Видавничий дім «Професіонал», 2024. 1208 с.; Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

[21] Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів : Закон України від 3 жовт. 2017 р. No 2147-VIII. URL: https://zakon.rada.gov.ua/laws/show/2147-19.

2. Процесуальний порядок отримання та міжнародні стандарти ідентифікації та збереження електронних доказів

У сучасній юридичній науці триває дискусія щодо співвідношення термінів «електронні докази» та «цифрові докази». Хоча стаття 99 КПК України використовує термін «електронні документи» та їхні дублікати, практика та доктрина дедалі частіше схиляються до ширшого поняття – цифрових доказів. Правова природа таких доказів визначається як будь-яка інформація, створена, передана, отримана або збережена в електронній формі, яка має значення для кримінального провадження[22].

Ключовою особливістю цифрових доказів є їхня бінарна форма існування, що робить їх невидимими для людського ока без спеціального інтерфейсу. Це створює ситуацію, коли доказом є не сам фізичний носій (флеш-драйв чи сервер), а саме логічна послідовність даних, зафіксована на ньому.

Відмінність цифрових доказів від традиційних полягає в тому, що вони є надзвичайно крихкими. Якщо для пошкодження паперового документа потрібен фізичний вплив, то для зміни цифрового файлу достатньо відкрити його без використання спеціальних засобів блокування запису (write-blockers), що автоматично змінює метадані (час останнього доступу). Саме тому процесуальний порядок їх збирання має бути значно суворішим, ніж для матеріальних об’єктів.

Згідно з чинним законодавством України, збирання цифрових доказів здійснюється шляхом проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій (НСРД) та через запити до володільців інформації. Основним інструментарієм є огляд, обшук та тимчасовий доступ.

Огляд комп’ютерних даних. Стаття 237 КПК регламентує проведення огляду, який у контексті цифровізації найчастіше стосується інформації з відкритих джерел (вебсайтів, соцмереж) або вмісту гаджетів. Процедура огляду вимагає відображення інформації в протоколі у формі, придатній для сприйняття: через скриншоти, відеозапис процесу навігації по сайту або виготовлення паперових копій[23]. Важливо, що при огляді даних із мережі Інтернет слідчі мають дотримуватися стандартів Протоколу Берклі, щоб забезпечити допустимість матеріалів у міжнародних інстанціях, що особливо актуально при документування воєнних злочинів[24].

Слід також відмітити, що процедура огляду комп’ютерних даних (ч. 2 ст. 237 КПК) потребує особливої уваги. Слідчий має право проводити огляд не лише

---

[22] Петрик В.В. Використання електронних доказів у кримінальних провадженнях: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського Національного Університету.* 2025. Серія Право. Випуск 87: частина 4. С. 119-123.

[23] Маркіна А.В. Способи збирання стороною обвинувачення електронних доказів у кримінальних провадженнях щодо воєнних злочинів. *Право.ua.* 2025 № 4. С. 104-112.

[24] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf

фізичних носіїв, а й безпосередньо інформації. При цьому, згідно з позицією Верховного Суду та науковими рекомендаціями, вилучення електронної інформації має бути зафіксоване в протоколі, а носій – визнаний речовим доказом[25]. Проте існує колізія: чи можна вилучати інформацію шляхом копіювання без вилучення самого пристрою? Сучасна практика схиляється до того, що копіювання (imaging) є допустимим засобом фіксації, якщо воно здійснюється за участю спеціаліста та з використанням засобів, що гарантують ідентичність копії та оригіналу[26]. Це дозволяє не паралізувати роботу підприємств вилученням серверів, одночасно забезпечуючи інтереси слідства.

Тимчасовий доступ та виїмка. Механізм тимчасового доступу до речей і документів (ст. 159 КПК) є критично важливим для отримання даних від провайдерів. Проте закон встановлює обмеження: якщо доступ надається до електронних інформаційних систем, він здійснюється виключно шляхом зняття копії інформації без вилучення самих систем (комп'ютерів, серверів), якщо інше не вказано в ухвалі[27]. Це положення спрямоване на захист інтересів бізнесу та забезпечення безперервності роботи критичної інфраструктури.

Обшук та вилучення носіїв. Обшук (ст. 234 КПК) застосовується у випадках, коли є підстави вважати, що цифрова техніка містить сліди злочину і власник не надасть їх добровільно. Головною проблемою під час обшуку є вилучення всієї техніки замість копіювання конкретних файлів. Судова практика поступово схиляється до того, що вилучення фізичних носіїв є виправданим лише у разі потреби проведення комплексної комп'ютерно-технічної експертизи або коли є ризик видалення даних за допомогою віддаленого доступу[28].

Негласні слідчі (розшукові) дії. НСРД (ст. 263, 264 КПК) проводяться за ухвалою слідчого судді виключно щодо тяжких та особливо тяжких злочинів. Отримання електронних доказів під час НСРД вимагає специфічного підходу до фіксації «цифрового сліду», який включає не лише сам файл, а й умови його створення та передачі. Проблема отримання доказів за ст. 263 КПК полягає в тому, що сучасні оператори зв'язку використовують складні протоколи передачі даних. Процедура передбачає доступ до каналів зв'язку в режимі реального часу. Судова практика Верховного Суду 2024 року вказує, що інформація про спеціальні технічні засоби, які використовуються для такої НСРД, є державною таємницею, і її нерозголошення в суді є обґрунтованим[29].

---

[25] Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Трибуна молодого вченого.* 2021. № 6. С. 273-278.

[26] Кохановський В.Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2019. № 1(31). С. 13-19.

[27] Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. № 8. С. 336-339.

[28] Маркіна А.В. Способи збирання стороною обвинувачення електронних доказів у кримінальних провадженнях щодо воєнних злочинів. *Право.ua.* 2025 № 4. С. 104-112.

[29] Телизіна Я. Оцінка доказів, отриманих в результаті проведення НСРД: частина 2. URL:https://advokatpost.com/pro-otsinku-dokaziv-otrymanykh-u-rezultati-provedennia-nsrd-prokuror-iana-talyzina.

Основною проблемою при знятті інформації з електронних інформаційних систем (ст.264 КПК) є доступ до зашифрованих даних месенджерів (Telegram, WhatsApp)[30]. Оскільки інформація зазвичай захищена наскрізним шифруванням, перехоплення трафіку (ст. 263) часто є малоефективним. Натомість НСРД за ст. 264 КПК дозволяє отримати доступ безпосередньо до пристрою або серверної частини системи. Проблеми виникають при використанні віддаленого доступу до хмарних сховищ (Google Drive, iCloud). Юридична невизначеність щодо юрисдикції даних, які фізично знаходяться на серверах у США або ЄС, створює перешкоди для легітимізації таких доказів в українських судах[31].

Суттєвим недоліком в роботі з цифровими слідами загалом є те, що КПК не містить детальних інструкцій щодо того, як саме технічно їх фіксувати, щоб вони не втратили допустимості. Це призводить до того, що слідчі часто обмежуються скріншотами, які без належного засвідчення метаданих легко піддаються сумніву в суді[32].

Проблема «фейків» та легкості маніпулювання цифровими даними вимагає від правоохоронців використання спеціальних криптографічних засобів під час оформлення доказів. Ключовим поняттям тут є хешування – створення унікального цифрового «відбитка» файлу за допомогою алгоритмів.

У протоколі слідчої дії обов'язково мають бути зазначені хеш-суми всіх скопійованих файлів. Це дозволяє в суді через будь-який проміжок часу перевірити, чи не вносилися зміни у доказ. Якщо хеш-сума файлу в суді не збігається з тією, що вказана в протоколі, доказ вважається недостовірним. Верховний Суд у своїх постановах (наприклад, від 29 березня 2021 року у справі № 554/5090/16-к) підкреслює, що допустимість електронного документа залежить від можливості перевірки його цілісності та автентичності[33].

Ланцюг збереження доказів (Chain of Custody) у вітчизняній практиці. Забезпечення цілісності електронного доказу від моменту його виявлення до подання суду є ключовим завданням процесуального порядку. У міжнародній практиці та стандартах цифрової криміналістики це реалізується через «ланцюг збереження» (chain of custody)[34].

Ланцюг збереження – це документально зафіксований шлях доказу, що включає:

1. Ідентифікацію джерела (URL, фізичний пристрій, IMEI, MAC-адреса).

---

[30] Кірчев В.О. Новітні засоби доказування пропозиції, обіцянки або надання неправомірної вигоди службовій особі. *Європейський правничий часопис.* 2025. Випуск 6,7. С. 216-223.

[31] Петрик В.В. Використання електронних доказів у кримінальних провадженнях: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського Національного Університету.* 2025. Серія Право. Випуск 87: частина 4. С. 119-123.

[32] Колісник О.В., Король С.С. Електронні докази:критерії їх оцінки. *Юридичний науковий електронний журнал.* 2024. № 4. С. 158-160.

[33] Постанова від 29.03.2021 № 554/5090/16-к Верховний Суд. Касаційний кримінальний суд. URL:https://verdictum.ligazakon.net/document/96074938.

[34] Погорецький М.А. Використання даних ENCROCHAT у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий журнал.* 2025. Випуск № 8. С. 223-229.

2. Фіксацію стану в момент виявлення через розрахунок хеш-суми (MD5, SHA-1, SHA-256). Хеш-сума є «цифровим відбитком» файла; будь-яка зміна навіть одного біта в даних змінить це значення

3. Опис інструментів збирання (назва та версія програмного забезпечення, наприклад, FTK Imager, EnCase)[35].

4. Документування кожної передачі доказу між особами (слідчий – експерт – суд) із зазначенням часу та способу транспортування (сейф-пакет, зашифрований канал) [36].

В українському процесуальному законодавстві термін «chain of custody» прямо не вживається, хоча його елементи присутні у вимогах до протоколювання слідчих дій (ст. 104 КПК). Проте на практиці суди все частіше звертають увагу на цей стандарт. Відсутність у протоколі огляду інформації про хеш-суму вилученого файла або про використання пристроїв блокування запису (write-blockers) дає підстави захисту висувати версію про можливість штучного створення або модифікації доказів правоохоронцями.

Іншими словами, концепція ланцюжка зберігання передбачає хронологічне документування всіх етапів життя доказу: від моменту виявлення на місці події до представлення в суді. Це включає фіксацію:

- Хто мав доступ до доказу?
- Коли і де він зберігався?
- Які інструменти використовувалися для аналізу?
- Чи забезпечено захист від зовнішнього (електромагнітного) впливу.

Будь-яка прогалина в цьому ланцюжку (наприклад, якщо жорсткий диск зберігався в незапечатаному вигляді в кабінеті слідчого) є підставою для визнання доказу недопустимим, оскільки створюється «обґрунтований сумнів» щодо його незмінності[37].

Процесуальне дослідження цифрової інформації здебільшого реалізується через залучення експертів. Комп'ютерно-технічна експертиза (КТЕ) проводиться відповідно до Інструкції Мін'юсту № 53/5 та має на меті відповіді на питання про наявність певних файлів, відновлення видаленої переписки, виявлення слідів злому або стороннього втручання[38].

Метадані (дані про дані) часто є більш важливими, ніж основний контент. Наприклад, файл фотографії містить метадані EXIF, де вказано модель

[35] Погорецький М.А. Криптовалюта як об'єкт, предмет та засіб вчинення злочину: проблеми виявлення, документування і доказування в досудовому та судовому провадженнях. *Держава і регіони. Серія:Право.* 2025. № 3(88). С. 70-90.

[36] Погорецький М.А. Використання даних ENCROCHAT у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий журнал.* 2025. Випуск № 8. С. 223-229.

[37] Стефанів Н. Суддя ВС проаналізувала критерії допустимості й достовірності електронних доказів у кримінальному процесі. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1751385.

[38] Наказ Міністерства юстиції України № 53/5 від 08.10.1998 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень». URL: https://https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

телефону, точний час зйомки та GPS-координати. Експертиза дозволяє встановити, чи був файл створений саме на тому пристрої, який вилучено у підозрюваного. Проте слід враховувати, що багато месенджерів (Viber, Telegram) при пересиланні файлів автоматично стирають метадані, що вимагає використання складніших методів відновлення з пам'яті самого пристрою[39].

Сучасні розслідування оперують терабайтами даних. У таких умовах ручний аналіз неможливий. Новітні тенденції в криміналістиці передбачають використання ШІ для автоматичного пошуку аномалій, ідентифікації об'єктів на тисячах годин відеозаписів та встановлення зв'язків між фігурантами через аналіз «великих даних» (Big Data)[40]. Впровадження таких інструментів потребує створення відповідної нормативної бази, щоб результати роботи алгоритмів могли бути визнані допустимими доказами.

Злочинність у цифрову епоху не визнає державних кордонів. Часто жертва знаходиться у Львові, злочинець – в Берліні, а дані зберігаються на сервері в Каліфорнії. Це робить міжнародне співробітництво життєво необхідним.

Будапештська конвенція та Другий додатковий протокол. На міжнародному рівні основним документом, що визначає стандарти роботи з цифровими даними, є Конвенція про кіберзлочинність (Будапештська конвенція). Вона встановлює обов'язок держав-учасниць запровадити механізми термінового збереження комп'ютерних даних (стаття 16) та часткового розкриття даних про рух інформації (стаття 17)[41]. Це критично важливо для випадків, коли дані можуть бути видалені провайдером автоматично або за запитом користувача. Конвенція передбачає оперативне забезпечення збереженості даних, які можуть бути змінені або втрачені в процесі розслідування. В Україні ці положення частково імплементовані через процедуру тимчасового доступу до речей і документів, проте механізм «термінового збереження» (data preservation order) без судового рішення на короткий строк (до 90 днів за Конвенцією) все ще потребує вдосконалення в національному законодавстві.

Також важливим кроком стало прийняття Другого додаткового протоколу (2022), який запровадив механізми прямої взаємодії правоохоронців із сервіс-провайдерами (Google, Meta) без традиційних і повільних запитів про міжнародну правову допомогу[42]. Це дозволяє в екстрених випадках (наприклад, загроза життю) отримати дані протягом годин, а не місяців.

---

[39] Карпець Ю.В. Цифрові докази та комп»ютерно-технічні експертизи у кримінальних провадженнях про військові злочини. *Юридичний науковий електронний журнал.* 2025. № 11. С. 226-230.

[40] Орещук В. Докази, отримані за допомогою штучного інтелекту, та їх використання в суді. URL:https:// www.hsa.org.ua/blog/dokazi-otrimani-za-dopomogoiu-stucnogo-intelektu-ta-yix-vikoristannia-v-sudi.

[41] Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний університет імені Юрія Федьковича. 27.02.2025. URL: https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist.

[42] ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text.

*Новий Регламент ЄС e-Evidence (2023).*Європейський Союз запровадив революційні зміни, прийнявши Регламент (EU) 2023/1543[43]. Основні нововведення включають:

- *European Production Order (EPOC):* Наказ, що зобов'язує провайдера надати дані протягом 10 днів (або 8 годин у термінових випадках) безпосередньо органу іншої країни ЄС.
- *European Preservation Order (EPOC-PR):* Наказ про негайне заморожування даних, щоб вони не були видалені до моменту отримання основного запиту.

Цей Регламент ігнорує територіальний принцип: провайдер зобов'язаний надати дані, навіть якщо вони зберігаються за межами ЄС, якщо компанія пропонує послуги на європейському ринку. За невиконання передбачено штрафи до 2% від світового обороту компанії.

Технічна процедура фіксації має базуватися на принципах, викладених у міжнародному стандарті ISO/IEC 27037:2012 «Настанови щодо ідентифікації, збирання, отримання та збереження електронних доказів», який в Україні діє як ДСТУ EN ISO/IEC 27037:2022[44]. Стандарт визначає чотири ключові процеси, виконання яких гарантує надійність доказів. А саме: ідентифікацію, збирання, здобуття та збереження.

Фундаментальним принципом за ISO/IEC 27037 є мінімізація оброблення первісних цифрових пристроїв. Будь-які дії, що призводять до зміни стану пристрою (наприклад, увімкнення смартфона для перегляду повідомлень без спеціального обладнання), повинні бути детально описані та обґрунтовані в протоколі. Якщо слідчий самостійно оглядає телефон, він фактично змінює метадані файлів (час останнього доступу), що може бути використано захистом для тверджень про фальсифікацію. Тому стандарт вимагає документування кожного кроку, щоб незалежний експерт міг відтворити дії слідчого та прийти до того ж результату.

Важливою є роль суб'єктів виявлення та вилучення. Крім слідчих, до процесу залучаються інспектори-криміналісти, фахівці Департаменту кіберполіції та експерти Експертної служби МВС. Стандартизація їхньої діяльності через впровадження ДСТУ ISO/IEC 27037 дозволяє уніфікувати вимоги до їхньої кваліфікації та методів роботи, що є критичним для забезпечення допустимості результатів їхньої праці у судовому засіданні.

[43] The E-Evidence Regulation (eER) entered into force on 18 August 2023. After a three-year transition period, it will become binding from 18 August 2026. The Regulation regulates direct cross-border access to electronic evidence by law enforcement authorities of the Member States. URL:https:// www.bfdi.bund.de/EN/Fachthemen/Inhalte/Polizei-Strafjustiz/E-Evidence.html

[44] ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

3. Техніко-криміналістичне та тактичне забезпечення вилучення цифрової інформації

Технічне забезпечення фіксації цифрових слідів пройшло еволюцію від простого копіювання файлів до використання складних програмно-апаратних комплексів (ПАК), що працюють на рівні мікросхем та прошивок. Провідним інструментом у світовій та вітчизняній практиці є комплекс UFED (Universal Forensic Extraction Device), який дозволяє здійснювати фізичне та логічне вилучення даних з тисяч моделей мобільних пристроїв. Функціонал таких комплексів включає можливість обходу блокувань екрана, вилучення видалених повідомлень з месенджерів (Viber, Telegram, WhatsApp), відновлення історії браузерів та геолокаційних даних[45].

Однак ефективність ПАК постійно обмежується вдосконаленням систем безпеки виробниками смартфонів. Вихід нових версій iOS та Android з посиленим шифруванням та протоколами Secure Enclave створює ситуації, коли навіть найсучасніше обладнання не може «пробити» захист[46]. У таких випадках тактика слідчої дії повинна трансформуватися від технічного зламу до використання тактичних прийомів, наприклад, проведення огляду пристрою, поки він знаходиться в розблокованому стані безпосередньо під час затримання («live forensics»)[47].

Для забезпечення незмінності даних під час підключення носія до комп'ютера слідчого обов'язковим є використання блокуваторів запису (Forensic Write Blockers). Ці пристрої на апаратному рівні блокують будь-які команди запису, що надходять від операційної системи до накопичувача, дозволяючи лише читання даних.

Тактичні особливості проведення слідчих дій (огляду, обшуку) за наявності цифрових слідів вимагають суворої послідовності дій. На підготовчому етапі слідчий повинен передбачити наявність засобів ізоляції пристроїв від мережі (клітки Фарадея або авіарежим), щоб запобігти дистанційному видаленню даних (Remote Wipe)[48]. На робочому етапі огляду місця події фіксація повинна відбуватися за принципом «від найбільш летких даних до найменш летких»[49]. Це означає, що спочатку фіксується вміст оперативної пам'яті (RAM) та відкриті вікна програм, і лише після цього пристрій може бути вимкнений для вилучення.

---

[45] Климчук М.П., Кунтій А.І. Виявлення та вилучення слідів кримінальних правопорушень , учинених із використанням засобів стільникового зв'язку. *Соціально-правові студії.* 2020. Випуск 3(9). С. 111-118.

[46] Курман О.В. Особливості та проблеми виявлення й фіксації цифрових слідів під час огляду мобільних засобів зв'язку. *Електронне наукове видання «Аналітично-порівняльне правознавство». Випуск № 04,* 2025, частина 3. С. 238-242.

[47] Караман К.В. Вилучення цифрових слідів під час реалізації ухвали на отримання тимчасового доступу до відомостей, що становлять охоронювану законом таємницю. *Вісник кримінологічної асоціації України* № 36(3). С. 257-267.

[48] Там само.

[49] Коваленко А.В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності.* 2023. Випуск 161. С. 202-214.

Процес фіксації у протоколі має бути максимально деталізованим. Недостатньо просто вказати «вилучено мобільний телефон». Необхідно зафіксувати:

1. Точну модель та серійний номер (IMEI) пристрою.
2. Стан пристрою на момент виявлення (увімкнений/вимкнений, підключений до мережі).
3. Наявність та тип засобів блокування (пароль, графічний ключ, FaceID).
4. Метод вилучення (фізичне вилучення пристрою або копіювання інформації на місці).
5. Алгоритм та значення хеш-суми для кожного вилученого масиву даних або фізичного образу носія.

Хеш-сума (hash value) є математичним результатом обробки даних, який є унікальним для кожного набору інформації. Порівняння хеш-сум, розрахованих слідчим під час вилучення та експертом під час дослідження, є головним доказом того, що інформація не була підроблена. Будь-яка зміна хоча б одного біта інформації призведе до повної зміни значення хеш-суми, що робить цей інструмент надійним запобіжником проти маніпуляцій.

Особливим тактичним прийомом є використання Big Data та OSINT (Open Source Intelligence) під час проведення НСРД. Фіксація даних з відкритих джерел (соціальні мережі, форуми) потребує негайної фіксації шляхом створення знімків екрана (скріншотів) та збереження копій вебсторінок, оскільки автори можуть видалити публікації після усвідомлення уваги правоохоронних органів[50]. При цьому важливо фіксувати не лише візуальне відображення, а й HTTP-заголовки та вихідний код сторінки, що дозволяє верифікувати джерело походження інформації[51].

Слід також зазначити, що в умовах триваючої війни з російським агресором цифрові сліди фактично стали ключовим інструментом фіксації їх звірств.

Тут критично важливою є верифікація за допомогою геолокації та аналізу метаданих, щоб довести, що відео було знято саме в Бучі та саме у березні 2022 року. Для цього українські органи активно співпрацюють з Міжнародним кримінальним судом (МКС) та використовують стандарти Протоколу Берклі, які вимагають збереження «цифрового негатива» – первинного файлу без жодних модифікацій[52].

---

[50] Климчук М.П., Кунтій А.І. Виявлення та вилучення слідів кримінальних правопорушень , учинених із використанням засобів стільникового зв'язку. *Соціально-правові студії.* 2020. Випуск 3(9). С. 111-118.

[51] Главюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету*. 2025. Випуск 91: частина 4. С. 251-259.

[52] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник./ неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/ wp-content/uploads/ 2022/03/Berkeley-ProtocolUkrainian.pdf

4. Типові помилки та проблеми фіксації цифрових слідів у судовій практиці: шляхи вдосконалення

Аналіз судово-слідчої практики свідчить про те, що цифрові сліди часто стають об'єктом жорсткої критики з боку захисту, що призводить до визнання їх недопустимими доказами. Основним каменем спотикання є недотримання встановленої законом процесуальної форми та технічних регламентів[53]. Типові помилки слідчих можна згрупувати за кількома напрямами.

Перша група помилок стосується порушення порядку вилучення. Часто слідчі вилучають комп'ютерну техніку без отримання спеціального дозволу слідчого судді, передбаченого ст. 234-236 КПК, або вилучають «все підряд» без обґрунтування зв'язку пристроїв з предметом доказування[54]. Суди, керуючись доктриною «плодів отруєного дерева», визнають такі докази недопустимими, навіть якщо на них міститься пряме підтвердження вини[55].

Друга група – це технічні помилки при фіксації. Відсутність у протоколі відомостей про розрахунок хеш-сум є однією з найпоширеніших проблем[56]. Без хеш-суми неможливо довести, що файл, який досліджує експерт через два місяці після обшуку, є тим самим файлом, що був знайдений у підозрюваного. Також критичною помилкою є огляд пристрою без залучення спеціаліста, що призводить до випадкової зміни системних файлів або дати доступу, що стає підставою для сумнівів у цілісності даних.

Третя група – помилки у забезпеченні ланцюга зберігання (Chain of Custody). Якщо у матеріалах справи відсутня інформація про те, як доказ транспортувався, де зберігався (наприклад, відсутність сейф-пакетів або їх пошкодження), суд не може бути впевнений, що до носія не мали доступу сторонні особи[57].

Сучасна судова практика Верховного Суду демонструє поступове формування стандартів оцінки електронних доказів. У постанові ККС ВС від 7 грудня 2023 року у справі № 420/15422/22 було акцентовано увагу на тому, що електронне листування є належним доказом, якщо можна встановити його

---

[53] Юр»єв Д.С., Мірошніченко А.О., Забудський О.П. Електронні докази в кримінальному провадженні: практика застосування. *UNIVERSUM*/ 2026. № 28. С. 101-104.

[54] Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Трибуна молодого вченого.* 2021. № 6. С. 273-278.

[55] Використання цифрової інформації в розслідуванні кримінальних правопо рушень: матеріали міжнар. наук.-практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Со коленко. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. 104 с. DOI: https://doi.org/10.31359/978-966-998-460-9. Techniques and standards for Preservation of Data.

[56] Techniques and standards for Preservation of Data. Digital Forensics 2023-2024. Topic 4. С. 27-38. URL:https://www.uomustansiriyah.edu.iq/media/lectures/6/6_2024_05_10!06_53_48_AM.pdf

[57] Юр»єв Д.С., Мірошніченко А.О., Забудський О.П. Електронні докази в кримінальному провадженні: практика застосування. *UNIVERSUM*/ 2026. № 28. С. 101-104.

походження та автентичність[58]. Суди починають приймати скріншоти месенджерів як докази, але лише за умови, що вони підкріплені оглядом самого пристрою або даними від провайдера. Проте залишається проблема автентичності: у справах про кібершахрайство зловмисники часто використовують спуфінг (підміну номера або імені), що вимагає від суду глибшого аналізу технічних логів, а не лише візуального змісту повідомлень[59].

Для подолання цих проблем та гармонізації українського законодавства з міжнародними стандартами пропонуються такі кроки:

1. Законодавче закріплення поняття «електронний доказ» та «цифровий слід» у КПК України, а також встановлення чіткої процедури їх копіювання як альтернативи вилученню техніки.
2. Розробка та впровадження обов'язкових методичних рекомендацій для слідчих, заснованих на ДСТУ ISO/IEC 27037, щодо порядку ідентифікації та збереження цифрових даних.
3. Створення єдиної цифрової системи обліку речових доказів (e-Evidence), яка б автоматично фіксувала кожен етап «ланцюга зберігання» та інтегрувала значення хеш-сум у електронний протокол.
4. Підвищення рівня кваліфікації слідчих та суддів через спеціалізовані курси з цифрової криміналістики, оскільки нерозуміння різниці між файлом та носієм або між логічним та фізичним образом призводить до судових помилок.

Окремим викликом є використання результатів штучного інтелекту (ШІ) у доказуванні. Вже зафіксовані випадки спроб використання ChatGPT для обґрунтування юридичних позицій[60]. У майбутньому ШІ може використовуватися для аналізу гігабайтів лог-файлів, проте фіксація результатів такого аналізу потребуватиме нових законодавчих визначень та процесуальних гарантій.

ВИСНОВКИ

Фіксація цифрових слідів у сучасному кримінальному процесі є критично важливим етапом, від успішності якого залежить можливість розкриття переважної більшості злочинів. Цифрова трансформація вимагає від криміналістики відмови від застарілих підходів на користь динамічних методів, що базуються на міжнародних стандартах та передових технологіях. Дослідження показало, що цифровий слід є складним інформаційним об'єктом, який характеризується невидимістю, легкістю модифікації та транскордонністю, що обумовлює специфіку його правового режиму.

---

[58] Постанова ККС ВС від 7 грудня 2023 року у справі № 420/15422/22. URL: https://iplex.com.ua/doc.php?regnum=115484427; Судді ВС обговорили судову практику щодо електронних доказів і захист права на приватність при роботі з доказами в умовах застосування штучного інтелекту. URL:https://supreme.court.gov.ua/supreme/pokaznikidiyalnosti/navch_suddiv_praciv__aparativ_2021.

[59] Кохановський В.Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2019. № 1(31). С. 13-19.

[60] Огляд судової практики Верховного Суду щодо використання технології штучного інтелекту в судовому процесі (актуальна судова практика станом на 22.07.2025). URL:https://court.gov.ua/storage/portal/sud5023/Scintelekt.pdf.

Основними гарантіями допустимості цифрових доказів є суворе дотримання «ланцюга зберігання», використання апаратних засобів блокування запису та обов'язкова верифікація даних через хеш-функції. Імплементація стандартів ISO/IEC 27037 у вітчизняну практику дозволить мінімізувати суб'єктивний фактор та забезпечити належну якість збирання доказів. Водночас технічний прогрес у сфері шифрування та захисту даних вимагає постійного оновлення парку програмно-апаратних комплексів (як-от UFED) та посилення взаємодії між слідчими органами та підрозділами кіберполіції.

Подальше вдосконалення процесуального законодавства має йти шляхом деталізації процедур роботи з електронною інформацією, впровадження інституту термінового збереження даних та легалізації цифрових методів фіксації (копіювання образу диска). Лише комплексна синергія правових норм, технічних інструментів та фахової компетентності учасників кримінального провадження дозволить ефективно протидіяти викликам злочинності у цифрову епоху.

АНОТАЦІЯ

У статті проведено комплексне дослідження теоретичних та прикладних аспектів функціонування цифрових слідів у сучасній криміналістиці. Визначено понятійно-категоріальний апарат, проаналізовано співвідношення термінів «цифровий слід», «електронний доказ» та «віртуальне відображення». Особливу увагу приділено криміналістичній характеристиці таких слідів, їхнім специфічним властивостям, таким як волатильність, реплікованість та трансмежовість. На основі аналізу останніх досягнень техніко-криміналістичного забезпечення розкрито методику виявлення, фіксації та вилучення цифрової інформації з використанням спеціалізованих апаратно-програмних комплексів. Окремий розділ присвячено аналізу актуальних проблем практичної діяльності, зокрема подоланню шифрування та роботі з хмарними сховищами. Проаналізовано сучасну судову практику Верховного Суду України (2023–2025 рр.) щодо допустимості скріншотів, месенджерів та електронного листування як доказів у кримінальному провадженні. Сформульовано рекомендації щодо вдосконалення процесуального законодавства та імплементації міжнародних стандартів ISO/IEC 27037.

Ключові слова: цифрові сліди, цифрова криміналістика, електронні докази, криміналістична характеристика, судова практика, ланцюжок збереження доказів, Cellebrite UFED, хмарні технології, кіберзлочинність.

Література

1. Коломійцев С.О. Сутність та класифікація цифрових слідів кримінального правопорушення. *Вісник пенітенціарної асоціації України. 2025. №2 (32).* С. 196-205.

2. Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, № 4 (100), 2022.* С. 226-236.

3. Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний

університет імені Юрія Федьковича. 27.02.2025. URL:https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist.

4. Цифрові докази війни: як технології допомагають Україні фіксувати злочини Росії. Українські правозахисники та юристи розповіли про нові методи збору доказів воєнних злочинів РФ, які витримують перевірку міжнародних судів URL: https://www.polskieradio.pl/398/7857.

5. Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету. Серія Право. Випуск 85: частина 4.* С.71-75.

6. Хижняк Є.С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права.* 2017. Вип.79. С.159-166.

7. Колеснікова І.А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний електронний журнал. 2023. №10.* С.472-475.

8. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право. 2019. №5.* С. 304-307.

9. Крицька І. О. «Доріжка цифрових слідів»: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні / І. О. Крицька // Цифрові трансформації України 2020: виклики та реалії: зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за матеріалами круглого столу, 18 вересня 2020 р. – Харків: НДІ ПЗІР НАПрН України, 2020. – С. 92-97.

10. Лазебний А.М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип. 1 (10) С.226-233.

11. Авдєєва Г.К., Стороженко С.В. Електронні сліди: поняття і види. *Вісник Луганського державного університету внутрішніх справ імені Е.О.Дідоренка.* 2017. №1(77). С.168-175.

12. Гринько Л.П. «Слідова картина» шахрайств, вчинених через мережу Інтернет. *Полтавський правовий часопис.* 2022. №3. С.16-27.

13. Колодіна А.С., Федотова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Київський правовий часопис.* Випуск 1. С.176-180.

14. Коваленко А.В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності. 2023. Випуск 161*. С.202-214.

15. Курман О.В. Особливості та проблеми виявлення й фіксації цифрових слідів під час огляду мобільних засобів зв'язку. *Електронне наукове видання «Аналітично-порівняльне правознавство». Випуск №04, 2025, частина 3.* С.238-242.

16. Науково-практичний коментар Кримінального процесуального кодексу України – науково-методична робота. Станом на 14 квітня 2024 року / За заг. ред. Стратонова В.М. – Київ: Видавничий дім «Професіонал», 2024. – 1208 с.; Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 №4651-VI. URL: https://zakon.rada.gov.ua/laws/ show/4651-17#Text.

17. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного

судочинства України та інших законодавчих актів : Закон України від 3 жовт. 2017 р. No 2147-VIII. URL: https://zakon.rada.gov.ua/laws/show/2147-19.

18. Петрик В.В. Використання електронних доказів у кримінальних провадженнях: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського Національного Університету. 2025. Серія Право. Випуск 87: частина 4.* С.119-123.

19. Маркіна А.В. Способи збирання стороною обвинувачення електронних доказів у кримінальних провадженнях щодо воєнних злочинів. *Право.ua. 2025 №4.* С.104-112.

20. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf.

21. Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Трибуна молодого вченого. 2021. №6.* С.273-278.

22. Кохановський В.Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник. 2019. №1(31).* С.13-19.

23. Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал. 2021. №8.* С.336-339.

24. Телизіна Я. Оцінка доказів, отриманих в результаті проведення НСРД: частина 2. URL:https://advokatpost.com/pro-otsinku-dokaziv-otrymanykh-u-rezultati-provedennia-nsrd-prokuror-iana-talyzina.

25. Кірчев В.О. Новітні засоби доказування пропозиції, обіцянки або надання неправомірної вигоди службовій особі. *Європейський правничий часопис. 2025. Випуск 6,7.* С.216-223.

26. Колісник О.В., Король С.С. Електронні докази:критерії їх оцінки. *Юридичний науковий електронний журнал. 2024. №4.* С.158-160.

27. Постанова від 29.03.2021 № 554/5090/16-к ВС. Касаційний кримінальний суд. URL:https://verdictum.ligazakon.net/document/96074938.

28. Погорецький М.А. Використання даних ENCROCHAT у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий журнал. 2025. Випуск №8.* С.223-229.

29. Погорецький М.А. Криптовалюта як об’єкт, предмет та засіб вчинення злочину: проблеми виявлення, документування і доказування в досудовому та судовому провадженнях. *Держава і регіони. Серія:Право.* 2025. №3(88). С. 70-90.

30. Стефанів Н. Суддя ВС проаналізувала критерії допустимості й достовірності електронних доказів у кримінальному процесі. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1751385.

31. Наказ Міністерства юстиції України №53/5 від 08.10.1998 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень». URL:https://https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

32. Карпець Ю.В. Цифрові докази та комп»ютерно-технічні експертизи у кримінальних провадженнях про військові злочини. *Юридичний науковий електронний журнал. 2025. №11.* С.226-230.

33. Орещук В. Докази, отримані за допомогою штучного інтелекту, та їх використання в суді. URL:https:// www.hsa.org.ua/blog/dokazi-otrimani-za-dopomogoiu-stucnogo-intelektu-ta-yix-vikoristannia-v-sudi.

34. ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL:https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text.

35. The E-Evidence Regulation (eER) entered into force on 18 August 2023. After a three-year transition period, it will become binding from 18 August 2026. The Regulation regulates direct cross-border access to electronic evidence by law enforcement authorities of the Member States. URL: https:// www.bfdi.bund.de/EN/Fachthemen/Inhalte/Polizei-Strafjustiz/E-Evidence.html.

36. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf.

37. Климчук М.П., Кунтій А.І. Виявлення та вилучення слідів кримінальних правопорушень , учинених із використанням засобів стільникового зв'язку. *Соціально-правові студії.* 2020. Випуск 3(9). С.111-118.

38. Караман К.В. Вилучення цифрових слідів під час реалізації ухвали на отримання тимчасового доступу до відомостей, що становлять охоронювану законом таємницю. *Вісник кримінологічної асоціації України №36(3).* С. 257-267.

39. Гловюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету.* 2025. Випуск 91: частина 4. С. 251-259.

40. Юр»єв Д.С., Мірошніченко А.О., Забудський О.П. Електронні докази в кримінальному провадженні: практика застосування. *UNIVERSUM/* 2026. № 28. С.101-104.

41. Використання цифрової інформації в розслідуванні кримінальних правопо рушень: матеріали міжнар. наук.-практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Со коленко. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. 104 с. DOI:

https://doi.org/10.31359/978-966-998-460-9. Techniques and standards for Preservation of Data.

42. Techniques and standards for Preservation of Data. Digital Forensics 2023-2024.Topic4. С. 27-38. URL: https://www.uomustansiriyah.edu.iq/media/lectures/6/6_2024_05_10!06_53_48_AM.pdf.

43. Постанова ККС ВС від 7 грудня 2023 року у справі № 420/15422/22. URL: https://iplex.com.ua/doc.php?regnum=115484427; Судді ВС обговорили судову практику щодо електронних доказів і захист права на приватність при роботі з доказами в умовах застосування штучного інтелекту. URL: https://supreme.court.gov.ua/supreme/pokazniki-diyalnosti/navch-_suddiv_praciv__aparativ_2021.

44. Огляд судової практики ВС щодо використання технології штучного інтелекту в судовому процесі (актуальна судова практика станом на 22.07.2025).URL:https://court.gov.ua/storage/portal/sud5023/Scintelekt.pdf.

Information about the author:
Dzyurbel Andriy Dariiovych,
Candidate of Legal Sciences,
Senior lecturer of the Department of Criminal Law and Procedure
West Ukrainian National University
11, Lvivska St., 11, Ternopil, 46009, Ukraine
https://orcid.org/0009-0000-1778-8699