

Сошенко Богдан Олексійович,
аспірант кафедри кримінального процесу
та криміналістики Навчально-наукового
інституту права Київського національного
університету імені Тараса Шевченка

ДОКУМЕНТУВАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ ТА ПРОЦЕСУАЛЬНА ФОРМА ЇЇ ЗАКРІПЛЕННЯ

Сучасний кримінальний процес дедалі частіше має справу не лише з традиційними матеріальними слідами кримінального правопорушення, а й із цифровою інформацією, що виникає, зберігається, передається та змінюється у комп'ютерних системах, мобільних пристроях, мережах зв'язку, хмарних сервісах, месенджерах, соціальних мережах, електронних платформах і відкритих цифрових джерелах. У зв'язку з цим документування цифрової інформації стає однією з ключових проблем кримінального процесуального доказування, оскільки саме від належного процесуального закріплення такої інформації залежить її подальша доказова придатність, можливість судової перевірки, допустимість і використання під час ухвалення процесуальних рішень.

Актуальність цієї проблематики зумовлена тим, що цифрова інформація має специфічну природу. Вона не завжди прив'язана до одного матеріального носія, може швидко копіюватися, змінюватися, переміщуватися, видалятися або втрачати частину своїх технічних характеристик. На відміну від традиційного речового доказу, цифровий об'єкт часто має доказове значення не лише через свій зміст, а й через метадані, технічне середовище створення, спосіб збереження, час формування, електронні ідентифікатори, геш-значення, журнали доступу, електронні підписи, часові мітки та інші технічні ознаки. Саме тому просте долучення до матеріалів кримінального провадження скріншота, роздруківки, копії файлу або електронного носія не може автоматично свідчити про належне документування цифрової інформації.

У криміналістичному аспекті ще в дослідженнях А. С. Білоусова обґрунтовувалося, що об'єкти комп'ютерних злочинів мають специфічні властивості, які потребують особливого підходу до їх виявлення, фіксації та аналізу [1]. Надалі ця проблематика набула розвитку у працях, присвячених

електронним і цифровим доказам у кримінальному провадженні, зокрема у роботах А. В. Коваленка, О. Г. Козицької, О. П. Метелева, І. Г. Каланчі, А. А. Шищенко та М. А. Погорецького [2–5; 7–10]. Узагальнення цих наукових підходів дає підстави стверджувати, що цифрова інформація в кримінальному процесі повинна розглядатися не як суто технічний об'єкт, а як особлива форма доказово значущих відомостей, яка потребує поєднання процесуальних, криміналістичних і технічних способів закріплення.

Документування цифрової інформації доцільно визначати як урегульовану кримінальним процесуальним законом і забезпечену криміналістичними засобами діяльність уповноважених суб'єктів, спрямовану на виявлення, фіксацію, копіювання, вилучення, збереження, опис, перевірку та процесуальне оформлення цифрових даних, які мають або можуть мати значення для кримінального провадження. Його зміст не обмежується технічним збереженням файлу чи носія. Воно охоплює встановлення джерела походження цифрової інформації, фіксацію умов її існування, визначення способу доступу до неї, опис технічного середовища, забезпечення цілісності даних, документування дій осіб, які працювали з цифровим об'єктом, і створення можливості для подальшої перевірки автентичності та незмінності відповідної інформації.

У цьому контексті важливим є розмежування понять цифрової інформації, електронного документа, цифрового доказу та цифрової форми доказів. Електронний документ є лише одним із можливих способів існування цифрової інформації. Натомість цифрові дані можуть міститися у файлах, журналах подій, базах даних, мобільних застосунках, електронних повідомленнях, хмарних сервісах, системах відеоспостереження, логах серверів, платіжних системах або відкритих інтернет-джерелах. Як слушно зазначає М. А. Погорецький, розмежування цифрових доказів і цифрової форми доказів має істотне значення для кримінального процесуального доказування, оскільки дозволяє уникнути змішування змісту доказової інформації, її носія та процесуальної форми закріплення [9].

Проблема процесуальної форми закріплення цифрової інформації полягає в тому, що кримінальний процес традиційно оперує визначеними джерелами доказів, серед яких документи, речові докази, показання, висновки експертів. Цифрова інформація може бути представлена в межах різних процесуальних джерел. В одних випадках вона набуває форми

електронного документа; в інших – має значення як інформація, що міститься на матеріальному носії; у третіх – постає як результат технічної фіксації процесуальної дії; у четвертих – потребує експертного дослідження. Тому питання не зводиться лише до того, куди саме «віднести» цифрову інформацію. Важливо визначити, яким способом вона була одержана, хто її зафіксував, чи збережено її цілісність, чи можна перевірити її походження і чи відповідає спосіб її закріплення вимогам допустимості доказів.

У працях М. Є. Шумила та М. А. Погорецького доказування розглядається як складна пізнавальна і процесуальна діяльність, що передбачає не механічне накопичення відомостей, а їх належне процесуальне одержання, перевірку та оцінку [11]. Цей підхід має особливе значення для цифрової інформації, оскільки її доказова цінність безпосередньо залежить від процесуальної коректності її фіксації. Якщо цифрові дані були отримані з порушенням закону, без належного суб'єкта, без опису джерела, без забезпечення цілісності або без можливості перевірити їх походження, то навіть фактично важлива інформація може втратити доказове значення.

Процесуальна форма закріплення цифрової інформації повинна виконувати щонайменше чотири взаємопов'язані функції. По-перше, вона має легалізувати одержання цифрових даних, тобто підтвердити, що інформацію отримано уповноваженим суб'єктом у межах визначеної законом процедури. По-друге, вона повинна забезпечити ідентифікацію джерела цифрової інформації: пристрою, акаунта, сервера, вебресурсу, електронної адреси, інформаційної системи або іншого цифрового середовища. По-третє, процесуальна форма має гарантувати збереження технічних ознак цифрового об'єкта, зокрема метаданих, часових параметрів, геш-ідентифікаторів, ознак електронного підпису чи способу копіювання. По-четверте, вона повинна створити умови для подальшої судової перевірки: сторона захисту, прокурор і суд мають мати можливість оцінити не лише зміст цифрової інформації, а й спосіб її одержання, повноту, цілісність і незмінність.

У практичному вимірі документування цифрової інформації має починатися з правильного виявлення її джерела. Для кримінального провадження важливо не просто встановити факт існування певного файлу, повідомлення, зображення чи електронного листування, а з'ясувати, де саме ці дані виникли, кому належить відповідний пристрій або обліковий запис, у якому технічному середовищі інформація створювалася і чи збереглися її

первинні технічні характеристики. Якщо джерело не встановлено або встановлено формально, виникає ризик втрати зв'язку між цифровим об'єктом і обставинами кримінального правопорушення. Саме тому в науковій літературі наголошується, що цифрові докази повинні оцінюватися з урахуванням їх походження, способу одержання та технічної перевірюваності [2; 5; 10].

Наступним елементом є вибір належного способу фіксації. У різних ситуаціях він може бути неоднаковим. Іноді необхідним є вилучення матеріального носія; іноді – створення криміналістичної копії; іноді – фіксація інформації шляхом огляду вебсторінки або електронного листування; іноді – отримання даних від провайдера, адміністратора сервісу чи власника інформаційної системи. Водночас кожен із цих способів має бути не лише технічно доцільним, а й процесуально допустимим. Неправильний вибір способу фіксації може призвести до втрати метаданих, зміни змісту файлу, порушення цілісності цифрового об'єкта або неможливості довести його автентичність у суді.

Особливого значення набуває питання копіювання цифрової інформації. Звичайне копіювання файлу не завжди гарантує збереження його доказових властивостей, оскільки внаслідок такого копіювання можуть змінюватися атрибути створення, доступу або редагування, втрачатися метадані, порушуватися структура даних. Тому при роботі з цифровою інформацією важливо фіксувати не лише сам факт копіювання, а й його спосіб, технічні засоби, суб'єкта, час, умови, носії, контрольні значення та інші параметри. Саме ця обставина зумовлює необхідність активнішого використання спеціальних знань під час документування цифрової інформації. Позиція про те, що цифрові докази потребують одночасного правового і технічного підходу, послідовно простежується у працях І. Г. Каланчі та О. П. Метелева [2; 5].

Не менш важливим є збереження цілісності цифрової інформації після її виявлення та фіксації. У кримінальному провадженні має бути зрозуміло, хто, коли, за яких умов і з якою метою отримував доступ до цифрового об'єкта, чи змінювався він після первинної фіксації, чи створювалися копії, де вони зберігалися, хто відповідав за їх передання та дослідження. Без такого ланцюга збереження виникає ризик сумніву в автентичності цифрової інформації. Це особливо важливо у справах, де сторона захисту ставить питання про можливість

підміну файлу, монтаж зображення, зміну повідомлення, втрату контексту або вибіркове використання цифрових фрагментів.

Процесуальна форма закріплення цифрової інформації повинна також забезпечувати її контекстуальність. Цифровий доказ не може оцінюватися ізольовано від середовища, у якому він виник. Наприклад, електронне повідомлення має інше доказове значення, якщо відомо, з якого акаунта воно надіслане, кому адресоване, коли доставлене, чи змінювалося, чи є пов'язане листування, чи підтверджується воно журналами доступу або іншими даними. Аналогічно скріншот вебсторінки без фіксації адреси, часу доступу, технічних параметрів, способу збереження та можливості перевірки не може мати такої самої доказової сили, як належно оформлений огляд цифрового джерела.

У цьому аспекті особливе значення має допустимість цифрових доказів. Вона не може оцінюватися лише за формальною ознакою наявності цифрового файлу в матеріалах кримінального провадження. Допустимість цифрової інформації залежить від належного джерела, належного суб'єкта, належного способу одержання, належного процесуального оформлення і належного збереження. Саме така сукупність критеріїв надає можливість відмежувати цифрові дані, які можуть бути використані як доказ, від інформації, що має лише орієнтуюче, оперативне або допоміжне значення. На цьому наголошують і сучасні дослідження цифрових доказів, у яких підкреслюється значення автентичності, цілісності та процесуальної форми їх закріплення [3–5; 10].

Документування цифрової інформації має бути підпорядковане не лише завданням ефективного розслідування, а й вимогам верховенства права. У цифровому середовищі втручання у приватне життя особи може бути значно глибшим, ніж під час роботи з традиційними матеріальними об'єктами. Один мобільний пристрій, акаунт або хмарне сховище можуть містити великий масив приватної, професійної, фінансової, комунікаційної та іншої інформації, що не завжди має стосунок до предмета доказування. Тому процесуальна форма повинна не лише забезпечувати отримання доказово значущих даних, а й обмежувати надмірне втручання, гарантувати пропорційність, судовий контроль і можливість оспорування дій стороною захисту. У цьому контексті особливої ваги набуває концепція верховенства права у кримінальному процесуальному доказуванні, розроблена М. А. Погорецьким [8].

Важливим аспектом є також процесуальна доброчесність під час роботи з цифровою інформацією. Її зміст полягає не лише у формальному дотриманні вимог кримінального процесуального закону, а й у забезпеченні чесності, прозорості, повноти та перевірюваності всіх дій із цифровими даними. Процесуальна доброчесність передбачає недопущення маніпуляцій із файлами, вибіркового вилучення даних із контексту, приховування способу одержання інформації, підміни носіїв, штучного створення цифрових слідів або використання технічної складності цифрового середовища для обмеження прав сторони захисту. У цьому значенні документування цифрової інформації є не лише технічною процедурою, а й важливою гарантією справедливого кримінального провадження.

Науковий аналіз дає підстави стверджувати, що чинне кримінальне процесуальне регулювання ще не повною мірою відповідає складності цифрового доказування. Законодавство містить загальні норми про докази, документи, речові докази, тимчасовий доступ, огляд, обшук, вилучення та інші процесуальні дії, однак не завжди достатньо чітко регулює особливості цифрової інформації. Зокрема, потребують подальшого уточнення питання процесуального статусу цифрових доказів, правил копіювання цифрових даних, фіксації метаданих, використання геш-ідентифікаторів, документування ланцюга збереження, оформлення огляду відкритих цифрових джерел і залучення спеціаліста. Без такого уточнення правозастосовна практика й надалі буде стикатися з ризиками неоднакового підходу до допустимості цифрових доказів.

Водночас розв'язання цієї проблеми не повинно зводитися лише до механічного доповнення кримінального процесуального закону новими термінами. Необхідним є формування цілісної моделі цифрового доказування, у якій процесуальна форма, криміналістична тактика та технічні стандарти працюватимуть узгоджено. Така модель має виходити з того, що цифрова інформація потребує спеціального режиму поводження, але цей режим не може підміняти собою загальні засади кримінального провадження. Навпаки, цифрові технології мають використовуватися таким чином, щоб посилювати доказування, забезпечувати його точність і перевірюваність, але не послаблювати права людини, судовий контроль і стандарти допустимості.

Отже, документування цифрової інформації та процесуальна форма її закріплення є одними з центральних

питань сучасного кримінального процесуального доказування. Належне документування повинно охоплювати не лише збереження змісту цифрових даних, а й фіксацію їх джерела, технічного середовища, способу одержання, суб'єкта фіксації, параметрів копіювання, ознак цілісності та можливості подальшої перевірки. Процесуальна форма закріплення цифрової інформації має забезпечувати її допустимість, автентичність, незмінність, контекстуальність і судову перевірюваність. У підсумку цифрові докази можуть бути належно використані у кримінальному провадженні лише за умови поєднання трьох елементів: процесуальної законності, технічної коректності та процесуальної доброчесності.

Перспективними напрямками подальших наукових досліджень є розроблення чітких критеріїв допустимості цифрових доказів; визначення процесуальних правил фіксації метаданих і геш-значень; удосконалення порядку огляду цифрових джерел; формування стандартів криміналістичного копіювання; запровадження належної моделі ланцюга збереження цифрових доказів; підвищення цифрової компетентності слідчих, прокурорів, суддів, адвокатів і спеціалістів; а також гармонізація національної практики з європейськими стандартами електронного доказування. Саме це дозволить забезпечити ефективне, справедливе й правомірне використання цифрової інформації у кримінальному провадженні.

Список використаних джерел

1. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2008. 18 с.
2. Каланча І. Г. Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект : монографія. Київ : SBA Print, 2025a. 528 с.
3. Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2018. Вип. 4. С. 237–245.
4. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421. DOI: <https://doi.org/10.32782/2524-0374/2020-8/103>.
5. Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального*

судочинства. 2023. № 1–2. С. 42–53. DOI: <https://doi.org/10.17721/2413-5372.2023.1-2/42-53>.

6. Погорецький М. А. Доказування у кримінальному процесі: поняття, зміст, структура. *Актуальні проблеми доказування у кримінальному провадженні* : матеріали Всеукр. наук.-практ. інтернет-конференції (Одеса, 27 листопада 2013 р.) / відпов. за випуск Ю. П. Алєнін. Одеса : Юридична література, 2013. С. 17–21.

7. Погорецький М. А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів: проблемні питання. *Вісник кримінального судочинства*. 2023. № 3–4. С. 84–102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf.

8. Погорецький М. А. Верховенство права у кримінальному процесуальному доказуванні: методологія та практика застосування. *Вісник Національної академії правових наук України*. 2025а. Т. 32. № 3. С. 275–299. DOI: <https://doi.org/10.31359/19930909.2025.32.3.275>.

9. Погорецький М. А. Цифрові (електронні) докази та цифрова (електронна) форма доказів: розмежування понять і його значення для кримінального процесуального доказування. *Аналітично-порівняльне правознавство*. 2026. № 1. Ч. 3. С. 115–125. ISSN 2788-6018. DOI: <https://doi.org/10.24144/2788-6018.2026.01.3.18>.

10. Погорецький М. А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. *Аналітично-порівняльне правознавство*. 2025. Т. 3. № 4. С. 269–279. DOI: <https://doi.org/10.24144/2788-6018.2025.04.3.40>.

11. Шищенко А. А. Цифрові докази у кримінальному процесі: проблеми автентичності та допустимості. *Аналітично-порівняльне правознавство*. 2025. Т. 3. № 5. DOI: <https://doi.org/10.24144/2788-6018.2025.05.3.46>.

12. Шумило М. Є., Погорецький М. А. Докази і доказування. Кримінально-процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т. 1 / О. М. Бандурка, Є. М. Блажівський, Є. П. Бурдоль та ін. ; за заг. ред. В. Я. Тація та ін. Харків : Право, 2012. С. 247–308.