

Базиляк Ірина Олегівна,

здобувач вищої освіти навчально-наукового експертно-криміналістичного інституту Національної академії внутрішніх справ

Науковий керівник:

доцент кафедри кримінального процесу Національної академії внутрішніх справ, кандидат юридичних наук, доцент

Зайка Сергій Олегович

ОСОБЛИВОСТІ ЗБИРАННЯ, ОЦІНКИ ТА ВИЗНАННЯ ДОПУСТИМИМИ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Стрімкий розвиток цифрових технологій суттєво змінив механізми вчинення кримінальних правопорушень та методи їх розслідування. Сьогодні значна частина доказової бази існує в електронній формі.

Попри те, що Кримінальний процесуальний кодекс України (далі – КПК України) безпосередньо не виокремлює електронні докази як самостійний вид, цифрова інформація активно слугує джерелом доказування у формі документів, про що зазначено в ч. 1 ст. 99 КПК України [1]. До них належать матеріали фотозйомки, звуко- та відеозапису, інші носії інформації, зокрема комп'ютерні дані.

Головною особливістю таких даних є нематеріальна природа – вони потребують спеціальних технічних засобів для отримання й дослідження. Електронні докази мають специфічні властивості: їх можна швидко змінити, видалити або скопіювати без втрати якості, що створює додаткові труднощі для забезпечення їх належності, допустимості та достовірності. Саме тому питання оцінки та процесуального визнання доказів набуває особливої актуальності у кримінальному процесі.

Збирання електронних доказів є складним процесом, що поєднує процесуальні й технічні аспекти. Відповідно до ст. 93 КПК України збирання доказів здійснюється стороною обвинувачення, стороною захисту та потерпілим у межах їх процесуальних повноважень. До основних способів отримання

електронних доказів уповноваженими суб'єктами можна віднести: проведення слідчих (розшукових) дій (обшук, огляд місця події, зняття показань технічних приладів і технічних засобів за ст. 245-1 КПК України), негласних слідчих (розшукових) дій (зняття інформації з комунікаційних мереж) та деякі заходи забезпечення кримінального провадження щодо комп'ютерних систем (тимчасовий доступ до речей та документів, тимчасове вилучення й арешт майна) [2].

Водночас сторона захисту та потерпілий беруть участь у формуванні цієї доказової бази шляхом витребування відомостей, отримання висновків експертів або ініціювання згаданих процесуальних дій перед слідчим чи прокурором.

Під час роботи з цифровими носіями важливо не допускати зміни інформації. Навіть автоматичне ввімкнення вилученого пристрою може призвести до зміни службових даних. Тому для фіксації цифрової інформації застосовуються: створення цифрових копій, програми для збереження метаданих, контроль цілісності інформації через криптографічні хеш-функції [3, с. 31]. Ці методи гарантують, що отримані дані не зазнали змін після вилучення.

Крім безпосереднього вилучення пристроїв, електронні докази можуть бути отримані від операторів мобільного зв'язку, інтернет-провайдерів, адміністраторів веб-платформ або з державних реєстрів.

Оцінку електронних доказів здійснюють відповідно до принципу внутрішнього переконання суду. Зокрема, аналізують такі критерії, як належність, допустимість, достовірність і достатність. Практичне застосування правил оцінки електронних доказів на предмет їх допустимості можна дослідити в окремих рішеннях Верховного Суду України.

Як зазначено в постанові об'єднаної палати Касаційного кримінального суду у складі Верховного суду від 29 березня 2021 року у справі № 554/5090/16-к, для виконання завдань кримінального провадження, з огляду на положення Закону України «Про електронні документи та електронний документообіг», допустимість електронного документа як доказу не можна заперечувати винятково на підставі того, що він має електронну форму (ч. 2 ст. 8). Відповідно до ст. 7 цього Закону у випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Один і той самий

електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення.

Постанова об'єднаної палати Касаційного кримінального суду у складі Верховного суду від 25 вересня 2023 року у справі № 208/2160/18, стосується звернення сторони захисту про те, що протоколи НС(Р)Д є недопустимими доказами, оскільки додатками до них є технічні носії інформації, про які не зазначено у протоколах НС(Р)Д, що вони є первинними носіями інформації, не спростовують правильності висновків судів попередніх інстанцій про допустимість цих доказів. Безпідставним є ототожнення електронного доказу як засобу доказування та матеріального носія такого документа. Для виконання завдань кримінального провадження допустимість електронного документа як доказу не можна заперечувати винятково на підставі того, що він має електронну форму.

Суддя Верховного Суду Наталія Марчук зауважила, що прокурор має обґрунтувати походження електронних доказів та інші процесуальні питання, які стосуються наданих ним електронних доказів. Це дозволить суду оцінити їх належність і допустимість. Поширеним доказом у кримінальних провадженнях нині є записи з камер відеоспостереження. У цьому випадку необхідно зосередити увагу на якості відеозапису, щоб його можна було використати для підтвердження винуватості обвинуваченої особи. Також вона акцентувала, що електронні докази, отримані з відкритих джерел, необхідно перевіряти на достовірність крізь призму Протоколу Берклі [4].

Для визнання електронних доказів допустимими необхідне дотримання таких умов:

1. Усі процесуальні дії, спрямовані на отримання доказів, мають здійснюватися відповідно до вимог кримінального процесуального законодавства.

2. Необхідно підтвердити відсутність змін у цифрових даних від моменту їх отримання до дослідження в суді.

3. У протоколах слідчих дій мають бути зафіксовані: спосіб вилучення, технічні характеристики носія, умови його зберігання й технічні засоби, якими здійснювалось копіювання

4. Сторона захисту повинна мати реальну можливість ознайомитися з доказами та перевірити їх автентичність.

У судовій практиці часто виникають спори щодо допустимості скріншотів, записів телефонних розмов, листування в месенджерах і матеріалів із соціальних мереж. Оскільки їх легко підробити за допомогою графічних редакторів, для підтвердження їх достовірності нерідко призначають комп'ютерно-технічні експертизи.

Електронні докази стали невід'ємною частиною сучасного кримінального провадження та значно розширили можливості для встановлення істини. Водночас їх використання супроводжується низкою викликів, пов'язаних зі збереженням цілісності інформації, підтвердженням її достовірності та дотриманням законності отримання. Ефективне використання електронних доказів потребує не лише належного нормативного регулювання, а й високого рівня професійної підготовки слідчих, прокурорів, адвокатів і суддів, здатних працювати з цифровими технологіями.

Список використаних джерел

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

2. «Диджиталізація» кримінального провадження: що нового? *GoLaw*: веб-сайт. URL: <https://golaw.ua/ua/insights/publication/didzhitalizacziya-kriminalnogo-provadžhennya-shho-novogo/>.

3. Розслідування несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України) : наук.-метод. рекомендації для слідчих підрозділів та підрозділів дізнання Нац. поліції України / кол. авт. ; за заг. ред. д-ра юрид. наук, проф. М. С. Цуцкірідзе – 1-й заст. гол. Нац. поліції України, нач. ГСУ, генерала поліції 3-го рангу. Дніпро : Дніпров. держ. ун-т внутр. справ, 2025. 104 с.

4. Суддя Верховного Суду розповіла про судову практику щодо оцінювання електронних доказів у кримінальному провадженні в рамках курсу HELP «Кіберзлочинність та електронні докази». Верховний Суд. веб-сайт. URL: <https://surl.lu/nwvdtz>.