

Список використаних джерел

1. Кримінальний процесуальний кодекс України : затв. Законом України від 13 квіт. 2012 р. № 4651-VI. *Верховна Рада України*: [сайт]. URL: <https://zakon.rada.gov.ua/laws/show/4651-1775>
2. Михайленко В.В. Реалізація засади верховенства права у кримінальному провадженні : дис. ... канд. юрид. наук : 12.00.09. Київ, 2019. 281 с.
3. Юдківська Г. Принцип пропорційності в системі захисту прав людини. *Слово Національної школи суддів України*. 2015. № 4 (13). С. 118-123.
4. Огляд практики Європейського суду з прав людини у справах проти інших держав за період 01.01.2023 – 01.04.2023. *«Бюлетень: Верховенство права. Права людини»*. 2023 № 1 С. 22–45

Власова Ганна Петрівна,

завідувач кафедри публічного права
факультету права та міжнародних
відносин Київського столичного
університету імені Бориса Грінченка,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України

ЕЛЕКТРОННІ ЦИФРОВІ ДОКАЗИ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ

Електронні цифрові докази стали важливим компонентом у сучасних розслідуваннях кримінальних проваджень, особливо у зв'язку зі зростанням кіберзлочинності та використанням інформаційних технологій. Такі докази можуть включати будь-яку інформацію, що зберігається або передається електронними засобами, яка має юридичну силу у розслідуванні справ.

Відповідно до ст. 84 Кримінального процесуального кодексу України (КПК) України доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. Згідно ст. 98 КПК України речовими доказами є матеріальні об'єкти, які були знаряддям вчинення кримінального правопорушення, зберегли

на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, в тому числі предмети, що були об'єктом кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом. Відповідно до ст. 99 КПК України документи є речовими доказами, якщо вони містять відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. До документів можуть належати: матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні), а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії. У деяких випадках, а саме тоді, коли документ незмінний, він може мати одночасно ознаки і документа, і речового доказу. [2]. Оскільки на законодавчому рівні поняття не розрізняються і пропонуємо їх використовувати саме у розумінні поняття «електронні цифрові докази», не розділяючи ці поняття та ототожнюючи їх. [1, С.5]

До основних характеристик електронних цифрових доказів ми пропонуємо виділити належить: нематеріальна природа (електронні докази не мають фізичної форми, що ускладнює їх ідентифікацію, вилучення та збереження); легкість зміни (електронні дані можуть бути легко змінені або знищені, що вимагає дотримання суворих процедур для забезпечення їх цілісності та достовірності); метадані (інформація про те, коли та ким були створені, змінені чи переглянуті дані, що може бути вирішальним для визначення обставин події).

Аналізуючи наукову літературу можна визначити наступні типи електронних цифрових доказів:

1. Електронні листи та повідомлення: Використовуються для встановлення комунікацій між підозрюваними або іншими сторонами.

2. Дані з мобільних пристроїв: Містять інформацію про дзвінки, SMS, геолокацію та використання мобільних додатків.

3. Дані з комп'ютерів та серверів: Можуть включати файли, журнали дій користувачів, документи, бази даних тощо.

4. Інтернет-дані: Веб-сторінки, історія браузера, активність у соціальних мережах.

5. Відеоспостереження: Дані з камер, які можуть бути збережені на електронних носіях або в хмарних сервісах.

Щодо використання електронних доказів у кримінальних провадженнях пр розслідуванні кримінальних праворушень слід виділити ряд важливих етапів, таких як:

- збір та вилучення - для забезпечення допустимості доказів необхідно дотримуватись процедур, що передбачають законне отримання та документування доказів;

- збереження - важливо забезпечити цілісність доказів за допомогою спеціальних технологій, таких як хешування, яке дозволяє перевірити, що дані не були змінені;

- аналіз - фахівці з цифрової криміналістики проводять аналіз електронних доказів, щоб відновити видалені файли, розшифрувати зашифровані дані та встановити послідовність дій;

- представлення електронних цифрових доказів у суді - експерти з цифрової криміналістики зазвичай виступають свідками для пояснення технічних аспектів отриманих доказів.

Цілком погоджуємося із авторам, що у кримінальному процесі докази мають відповідати двом вимогам, які висуваються до його змісту та форми, – належності (ст. 85 КПК України) і допустимості (ст. 86 КПК України). Закономірно, що такі ознаки повинен мати й електронний доказ, що може забезпечуватися коректністю фіксації та подальшою незмінністю комп'ютерних даних [1, с. 6]. Але поруч із цією тезою ми маємо акцентувати увагу на тих проблемах та викликах, які постають перед усіма учасниками процесу. Перш за все це **захист приватності**, де використання електронних доказів може порушувати права на приватність, тому необхідно забезпечити баланс між інтересами слідства і захистом прав громадян. **Зміна технологій**, пов'язана із швидким розвитком технологій, що створює нові труднощі для слідчих у питаннях виявлення та аналізу електронних доказів. **Правове закріплення**, пов'язано з тим, що законодавство щодо цифрових доказів потребує постійного оновлення для адаптації до нових викликів.

Таким чином, електронні цифрові докази є невід'ємною частиною сучасних розслідувань і відіграють важливу роль у встановленні істини та доведенні вини чи невинуватості у кримінальних провадженнях. Їх характеристика, нормативно-правове закріплення, постійна зміна технологій, технічні трансформаційні процеси заходяться у постійному видозміненому стані, що потребує особливої уваги та дослідження як на науковому, так і практичному рівні.

Список використаних джерел

1. Використання електронних (цифрових) доказів у кримінальних провадженнях [Текст] : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

2. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI: станом на 1 листоп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.

Воляннюк Олександр Дмитрович,
старший викладач кафедри спеціальної фізичної підготовки Національної академії внутрішніх справ, кандидат юридичних наук;

Воляннюк Катерина Олександрівна,
заступник директора Київського центру первинної професійної підготовки «Академія поліції» навчально-наукового інституту № 1, кандидат юридичних наук

ОРГАНІЗАЦІЯ ДІЙ ПОЛІЦЕЙСЬКИХ ПІСЛЯ ПРИБУТТЯ НА МІСЦЕ ПОДІЇ

Організація дій поліцейських під час прибуття на місце події є важливим етапом виконання службових обов'язків та забезпечення безпеки громадян. Нижче наведено перелік перших дій, які повинні бути здійснені поліцейськими при прибутті на місце події:

Забезпечення безпеки: Прибувши на місце події, поліцейський повинен забезпечити безпеку для себе, своїх колег та громадян. Поліцейський повинен оцінити ризики, визначити можливі загрози та діяти відповідно до цього.

Виклик необхідних служб: При необхідності, поліцейський повинен негайно викликати на місце події необхідні служби, такі як медичну допомогу, пожежну частину, аварійно-рятувальну службу та інші [1, с. 74].

Збір інформації: Поліцейський повинен зібрати якомога більше інформації про подію, щоб діяти відповідно до неї. Поліцейський повинен дізнатися про місце та час події, кількість постраждалих, наявність зброї, причини події та інші важливі деталі.