Кусень В.
студентка юридичного факультету
Західноукраїнського національного університету.
Науковий керівник: доктор юридичних наук, доцент,
професор кафедри теорії права та конституціоналізму
Західноукраїнського національного університету
Колесніков А. П.

ЦИФРОВІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ: ПРОБЛЕМИ ЗБОРУ ТА ОЦІНКИ

Конституція України гарантує кожному право на справедливий судовий розгляд та захист прав і свобод людини [1]. У сучасних умовах цифровізації суспільства значна частина інформації існує в електронній формі, а тому дедалі більшого значення у кримінальному провадженні набувають цифрові докази. Розвиток інформаційних технологій призвів до того, що електронні повідомлення, дані мобільних пристроїв, записи камер відеоспостереження, інформація із соціальних мереж та хмарних сервісів стали важливими джерелами доказової інформації. Водночас використання таких даних породжує низку правових і технічних проблем, пов'язаних зі збором, збереженням та оцінкою цифрових доказів.

Цифрові докази являють собою інформацію, що зберігається або передається в електронній формі та може бути використана для встановлення обставин кримінального правопорушення. Особливістю таких доказів є їхня нематеріальна природа, можливість швидкого копіювання, зміни або знищення без видимих слідів. На відміну від традиційних речових доказів, цифрова інформація потребує спеціальних методів вилучення та дослідження. За даними міжнародних досліджень у сфері цифрової криміналістики, понад 90 % кримінальних проваджень у розвинених державах сьогодні містять хоча б один вид електронних доказів [2].

В Україні правове регулювання використання цифрових доказів здійснюється насамперед положеннями Кримінального процесуального кодексу України. Відповідно до ст. 99 КПК України, документи можуть існувати в електронній формі та використовуватися як джерело доказів [3]. Разом із тим на практиці виникають труднощі щодо визначення належності та допустимості таких доказів. Однією з головних проблем є забезпечення цілісності цифрової інформації після її вилучення. Будь-яке втручання в електронний носій може призвести до зміни метаданих або втрати частини інформації, що ставить під сумнів достовірність отриманих відомостей.

Особливої актуальності набуває питання збирання цифрових доказів із мобільних телефонів, комп'ютерів та хмарних сховищ. Значна частина даних може знаходитися на серверах, розташованих за

межами України, що потребує використання механізмів міжнародної правової допомоги. Крім того, поширення наскрізного шифрування у месенджерах ускладнює доступ правоохоронних органів до інформації навіть за наявності судового дозволу. Науковці відзначають необхідність удосконалення процесуальних механізмів отримання цифрових доказів та їх гармонізації з міжнародними стандартами цифрової криміналістики [4].

Не менш важливою є проблема оцінки цифрових доказів судом. Електронна інформація часто потребує спеціальних знань для її аналізу та інтерпретації. У зв'язку з цим суттєву роль відіграють експерти у сфері комп'ютерно-технічних досліджень. Водночас судова практика свідчить про випадки, коли сторони кримінального провадження по-різному трактують результати експертиз або ставлять під сумнів достовірність отриманих даних. Додатковою проблемою є використання матеріалів із соціальних мереж, де складно встановити справжнього автора повідомлення чи факт відсутності змін у публікації після її створення.

В умовах розвитку штучного інтелекту та технологій створення підробленого цифрового контенту (deepfake) проблема достовірності цифрових доказів набуває нового виміру. Сучасні технології дозволяють створювати відео-, аудіо- та фотоматеріали, які важко відрізнити від справжніх. Це вимагає впровадження нових методів цифрової експертизи та підвищення кваліфікації працівників правоохоронних органів і суддів. Відсутність ефективних механізмів виявлення цифрових підробок може створити ризики для забезпечення принципів законності та справедливості кримінального судочинства.

Отже, цифрові докази стали невід'ємним елементом сучасного кримінального процесу. Їх використання відкриває широкі можливості для встановлення істини у справі, проте водночас породжує низку правових, технічних та організаційних проблем. Для підвищення ефективності використання цифрових доказів необхідним є вдосконалення кримінального процесуального законодавства, запровадження єдиних стандартів цифрової криміналістики, розвиток міжнародного співробітництва та підвищення рівня професійної підготовки фахівців у сфері інформаційних технологій і права.

Список використаних джерел

1. Конституція України від 28 червня 1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17

3. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15

4. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 01 грудня 2022 року № 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/2801-20
5. Конвенція про кіберзлочинність (Будапештська конвенція) від 23 листопада 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_575
6. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 4th ed. London : Academic Press, 2020. 848 p.