



Судова експертиза в умовах цифрової трансформації кримінального процесу

Світлана Афанасенко

кандидат юридичних наук, доцент, судовий експерт відділу науково-методичного та інформаційно-аналітичного забезпечення експертної діяльності, Одеський науково-дослідний інститут судових експертиз Міністерства юстиції України, м. Одеса, Україна, ORCID: <https://orcid.org/0009-0008-3017-1683>, e-mail: afanasenosvitlana@gmail.com

Розглянуто виклики, що постають перед судовою експертизою в умовах цифровізації кримінального процесу. Проаналізовано нові типи експертиз, роль експерта як суб'єкта доказування та необхідність міждисциплінарного підходу.

Ключові слова: *судова експертиза; цифрові докази; криміналістика; доказування.*

Forensic Examination in the Context of the Digital Transformation of Criminal Proceedings

Svitlana Afanasenko

The paper explores the challenges faced by forensic examination amid the digitalization of criminal proceedings. It analyzes new types of expertise, the expert's role in evidence evaluation, and the need for an interdisciplinary approach.

Keywords: *forensic examination; digital evidence; criminalistics; evidence.*

Цифровізація суспільства призвела до появи нових форм злочинності, зокрема кіберзлочинів, що потребують спеціальних знань для їх розслідування. Традиційні методи експертизи не завжди ефективні у разі, коли доказова інформація міститься на цифрових носіях, у хмарних сервісах або зашифрованих каналах зв'язку. Водночас законодавство часто не встигає за технологічними змінами, що створює прогалини у правовому регулюванні.

Судова експертиза має адаптуватися до нових умов, зберігаючи свої наукову обґрунтованість, об'єктивність і процесуальну незалежність. Особливої уваги потребує питання кваліфікації експертів, які мали набути знання цифрових технологій [1].

У зв'язку з цифровізацією кримінального процесу традиційна класи-

фікація судових експертиз потребує перегляду. З'являються нові напрями, які раніше не мали окремого статусу:

- комп'ютерно-технічна експертиза — аналіз апаратного забезпечення, носіїв інформації, слідів утручання в системи;
- інформаційно-телекомунікаційна експертиза — дослідження даних, переданих через мережі, включно з VoIP, VPN, хмарними сервісами;
- кіберлінгвістична експертиза — поєднання лінгвістичного аналізу з цифровим контекстом, наприклад, виявлення маніпулятивних технік у соцмережах;
- експертиза цифрових слідів поведінки — аналізування дій користувача в онлайн-середовищі (кліки, переходи, пошукові



запити), що може свідчити про наміри або мотиви.

Ці напрями потребують не лише технічної компетентності, а й розуміння правових меж допустимості таких доказів [2].

Цифрові докази мають низку особливостей:

- волатильність: дані можуть бути змінені або знищені без слідів;
- масштабність: обсяг інформації, що підлягає аналізу, може сягати терабайтів;
- міжнародність: дані часто зберігаються на серверах за межами юрисдикції.

Це потребує нових методик фіксування, збереження та аналізу цифрових слідів. Наприклад, застосування блокчейн-технологій для фіксування часу доступу до файлів або застосування хеш-функцій для підтвердження автентичності.

Застосування штучного інтелекту в експертній практиці відкриває нові обрії, але й породжує ризики:

- непрозорість алгоритмів: експерт може не мати доступу до логіки роботи програмного забезпечення;
- відсутність емоційного контексту: автоматизовані системи не здатні враховувати психологічні нюанси;
- ризик упередженості: алгоритми можуть відтворювати упередження, закладені в навчальних даних.

Саме тому важливо зберігати баланс між технічними можливостями та експертним оцінюванням.

Аналіз рішень судів першої та апеляційної інстанцій за останні два роки свідчить про:

- зростання кількості справ, де цифрова експертиза є ключовим доказом;
- труднощі в оцінюванні достовірності цифрових висновків під час судового засідання;
- відсутність єдиних стандартів (це призводить до неоднозначного трактування результатів експертизи).

У США, Великій Британії та країнах ЄС уже діють стандарти цифрової експертизи, зокрема:

- ISO/IEC 27037:2012 — рекомендації щодо ідентифікації, збору та збереження цифрових доказів [3];
- ACPO Good Practice Guide for Digital Evidence (UK) — практичні настанови для слідчих та експертів.

Україна має потенціал для адаптації цих стандартів, ураховуючи національні особливості правозастосування.

Важливою складовою розвитку цифрової експертизи є підготовка кадрів. Пропонуємо:

- упровадження міждисциплінарних магістерських програм (право + IT + криміналістика);
- сертифікацію експертів за міжнародними стандартами;
- створення національного реєстру цифрових експертів.

Судова експертиза має адаптуватися до цифрових викликів, зберігаючи наукову обґрунтованість та процесуальну незалежність.



Необхідно оновити нормативну базу, зокрема щодо допустимості та автентичності цифрових доказів. Варто розробити стандарти для нових видів експертиз з урахуванням міжнародного досвіду. Потрібна систем-

на підготовка експертів із міждисциплінарною компетенцією (право, ІТ, психологія). Міждисциплінарний підхід має стати нормою в експертній практиці, особливо у справах, що стосуються кіберзлочинів.

Перелік джерел посилання

1. Дуфенюк О. М. Цифрова криміналістика у системі криміналістичних знань. *Цифровізація кримінального провадження: стан та перспективи* : мат-ли наук.-практ. кругл. столу (Харків, 19.09.2024). Харків, 2024. URL: <https://surl.lu/xbdiug> (дата звернення: 16.09.2025).
2. Демидова Є. Є., Домашенко О. М., Колеснікова І. А., Латиш К. В. Судовий експерт як суб'єкт судово-експертної діяльності: правовий статус. *Юридичний науковий електронний журнал*. 2022. № 5. С. 549—553. DOI: 10.32782/2524-0374/2022-5/132 (дата звернення: 16.09.2025).
3. ISO/IEC 27037:2012(E). Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva, 2012. 48 p. URL: <https://amnfzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf> (дата звернення: 16.09.2025).