4 Avril, 2025;
Paris, République française

SECTION 7.
DROIT ET DROIT INTERNATIONAL

DOI 10.36074/logos-04.04.2025.015

ЦИФРОВІ ДОКАЗИ В СУДОВОМУ ПРОЦЕСІ: ПРОБЛЕМИ ДОПУСТИМОСТІ ТА АВТЕНТИЧНОСТІ

Горбань Маргарита Максимівна[1]

1. студентка 1 курсу
Харківський Національний Університет ім. В.Н. Каразіна, УКРАЇНА

Сучасна система правосуддя наразі перебуває посеред глибокої технологічної трансформації, яка змінює не лише процедурні аспекти, а й фундаментальні засади доказування. Цей процес вимагає переосмислення традиційних правових категорій у контексті стрімкого розвитку цифрових технологій, що створюють нові виклики для юридичної теорії та практики.

Актуальність цієї теми визначається тим, що інтеграція цифрових інструментів у судову систему України стала системною завдяки запровадженню Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС). Її функціональні модулі, зокрема "Електронний кабінет" і "Електронний суд", спрощують такі процеси, як онлайн-подача документів, дистанційна участь у засіданнях через відеоконференцзв'язок та автоматизований розподіл справ. Утім, ці інноваційні підходи виявили низку системних викликів, серед яких криза автентифікації, технологічна нерівність і невизначеність на законодавчому рівні.

Особливу увагу привертає зростання ваги цифрових доказів у кримінальній практиці. Так, у практиці Верховного Суду України дедалі частіше основними доказами стають відеозаписи з камер спостереження, які використовуються навіть за відсутності підписів понятих на протоколах обшуків. Це демонструє зміну акценту від формальних процедур до технічної достовірності електронних доказів.

Мета проведеного дослідження полягає в обґрунтуванні та розробці концепції "цифрової процесуальної гігієни" – системи правових та технічних гарантій автентичності електронних доказів. Основними завданнями визначено встановлення критеріїв допустимості нових видів доказів, аналіз ефективності механізму презумпції цілісності, чинного у практиці Верховного Суду України, а також розробку моделі "цифрового нотаріату" – автоматизованої системи фіксації доказів із застосуванням квантового шифрування.

Об'єктом дослідження виступає взаємодія технологічних інновацій з нормами процесуального права в межах функціонування ЄСІТС. Предметом є особливості електронних доказів як інформаційних об'єктів із динамічним набором параметрів, що охоплюють метадані, технічні характеристики та юридичні позначення.

Для досягнення зазначених цілей використано методологію, яка включає криптоаналіз, алгоритми машинного навчання та експертні опитування. Криптоаналіз застосовується для оцінки надійності хеш-функцій, машинне навчання допомагає прогнозувати можливі рішення судів на основі наявних даних, а експертні опитування дозволяють оцінити рівень готовності суддівського корпусу до роботи в умовах цифровізації. Комплексний підхід дає змогу ідентифікувати правові "сірі зони", в яких технологічні інновації випереджають розвиток нормативно-правової бази.

Цифрові свідчення являють собою новітній різновид доказової інформації, який кардинально відрізняється від звичних матеріальних носіїв даних. Вони існують у віртуальному просторі та здатні змінюватися під впливом технологічних, нормативних і суспільних факторів. Визначення цього явища вимагає поєднання правових та IT-концепцій. Відповідно до ст. 89 ЦПК України, цифрові свідчення — це дані, здобуті за допомогою інформаційно-телекомунікаційних систем. Але на практиці їх природа набагато складніша. Наприклад, дані з нейромереж або ті, що записані квантовими комп'ютерами, стирають межу між технічним артефактом та показами.

Класифікація цифрових доказів здійснюється за трьома основними критеріями: форматом, джерелом і юридичним значенням. За форматом вони можуть бути статичними (скріншоти, PDF-файли) або динамічними (стрімінгове відео, транзакції в блокчейні). За джерелом їх можна розподілити на призначені для користувача (смартфони, ноутбуки) та системні (серверні логи, метадані хмарних сховищ). За юридичним значенням вони можуть бути прямими (електронний договір із підписом) або непрямими (IP-адреса як підтвердження місця розташування).

Основні форми цифрових доказів охоплюють широкий спектр джерел інформації. До них належать електронні листи та файли, записи з камер відеоспостереження, дані з гаджетів, серверів і хмарних сервісів, а також лог-файли та метадані. Наприклад, у справі про корупцію у 2023 році листування в Telegram з використанням самознищення було відновлено з резервних копій на серверах провайдера. Верховний Суд України у 2024 році визнав допустимими записи з дронів у зоні АТО, навіть за відсутності сертифікації пристроїв. У цивільній справі про страхування смарт-годинник фіксував локацію та стан здоров'я позивача, що спростувало його твердження. Лог-

файли фінансових систем стали ключовим доказом у кримінальному провадженні проти хакерської групи.

Порівняння цифрових доказів із традиційними виявляє суттєві відмінності. Цифрові артефакти поєднують крихкість і надійність. Наприклад, паперовий документ можна фізично знищити, але електронний залишається в кеші браузера, резервних копіях або електронних листах. Відбитки пальців на зброї фізично прив'язуються до особи, в той час як Bitcoin-гаманець може належати багатьом анонімам. Підпис експерта на експертизі має графологічні характеристики, тоді як електронний підпис — це математична функція, яку можна зламати квантовим комп'ютером.

Цифрові свідчення володіють властивістю мультиплатформової цілісності. Наприклад, відеозапис із камери спостереження автоматично синхронізується з хмарним сховищем, породжуючи три типи доказів: вихідний файл (носій), метадані (час і геолокація), лог змін (історія редагувань). Така трирівнева структура робить їх одночасно вразливими для маніпуляцій та надійними завдяки технологіям типу blockchain-notarization.

Проте головна відмінність полягає в залежності від технологічного середовища. Суддя, який вивчає паперовий протокол, не потребує особливих знань, але для аналізу логів DDoS-атаки необхідні експерти з кібербезпеки, спеціалізоване програмне забезпечення та доступ до серверів. Це формує новий тип процесуальної нерівності: сторона, яка володіє технологічними ресурсами, здобуває перевагу в доказуванні.

Отже, цифрові свідчення не є простим «електронним аналогом» паперових документів. Вони формують нову реальність доказового права, де SHA-256 хеш файлу може мати більшу вагу, ніж підпис свідка, а алгоритм машинного навчання — визначати достовірність доказів. Ця трансформація вимагає перегляду не лише процесуальних кодексів, а й філософії правосуддя в цілому.

Доказовість цифрових свідчень у судових слуханнях продовжує бути одним із ключових дискусійних аспектів сучасного процесуального права. Українське законодавство визначає певні передумови для прийнятності доказів, проте нормативне окреслення самого поняття «цифровий доказ» у процесуальному праві ще далеке від досконалості. Це породжує чималі труднощі у практиці використання цифрових доказів, особливо коли йдеться про неприпустимість доказів, здобутих із порушенням законних процедур.

Вимоги законодавства до того, що може вважатися прийнятним доказом, викладені в Цивільному процесуальному кодексі України та Кримінальному процесуальному кодексі України. Відповідно до цих кодексів, докази мають бути здобуті законним способом та не порушувати права учасників судового

розгляду. Однак, у контексті цифрових доказів, встановлення того, що саме є «законним способом», нерідко стає предметом дебатів. Наприклад, питання допустимості відеозаписів з камер спостереження, встановлених без належної реєстрації, лишається відкритим для обговорення.

Труднощі з нормативним закріпленням поняття «цифровий доказ» у процесуальному праві кореняться у відсутності чіткого визначення цього терміну в законодавстві. Хоча українське законодавство визнає цифрові докази як окремий різновид доказів, відсутність детальної регламентації їх збору, зберігання та використання створює правову невизначеність. Це призводить до того, що суди нерідко мають розбіжності у прийнятті таких доказів. Наприклад, чи може електронний лист, позбавлений підпису, вважатися допустимим доказом, залишається спірним питанням.

Проблема недопустимості доказів, отриманих з порушенням правових норм, стає особливо гострою стосовно цифрових доказів. Наприклад, якщо дані були отримані в результаті хакерських атак або без дозволу власника інформації, вони можуть бути визнані неприйнятними. Верховний Суд України у своїх рішеннях акцентує увагу на важливості дотримання юридичних процедур при отриманні цифрових доказів, однак практика свідчить, що це не завжди можливо. Зокрема, у справах про кіберзлочини часто виникають питання щодо легітимності отримання доказів із серверів закордонних компаній.

Судова практика щодо визнання цифрових доказів неприйнятними демонструє розбіжності в підходах різних судових інстанцій. В окремих випадках суди визнають неприпустимими відеозаписи з камер спостереження, якщо вони були встановлені без відповідної реєстрації або згоди власника території. В інших випадках суди можуть визнати такі докази допустимими, якщо вони мають суттєве значення для справи та були здобуті без порушення прав учасників процесу. Такі розбіжності підкреслюють необхідність більш чіткої регламентації допустимості цифрових доказів у законодавстві України.

Отже, питання допустимості цифрових доказів залишається одним із найбільш проблемних в сучасному правосудді. Вирішення цієї проблеми вимагає як внесення змін до законодавства, так і розвитку судової практики щодо застосування цифрових доказів у процесі розгляду справ.

Автентичність цифрових свідчень є ключовим аспектом їх застосування у юридичних справах. Це поняття комбінує в собі як технічні, так і правові аспекти, бо воно визначає достовірність і незмінність цифрової інформації. Автентичність цифрового доказу означає, що він є справжнім і не підлягав змінам чи підробкам, повністю відповідаючи фактичним обставинам справи.

Технічний та юридичний аспекти автентичності тісно переплетені. З юридичної точки зору, автентичність встановлюється як відповідність доказу його первинному вигляду, тобто відсутність змін чи маніпуляцій. У технічному плані це досягається завдяки використанню спеціалізованого обладнання та методик, що забезпечують збереження цілісності інформації. Наприклад, електронні цифрові підписи використовуються для підтвердження джерела документа і його незмінності в процесі передачі та зберігання.

Методи перевірки автентичності охоплюють сучасні технологічні рішення. До них належать електронні цифрові підписи, хеш-функції та комп'ютерна криміналістика. Електронні цифрові підписи використовують криптографічний механізм для підтвердження авторства і незмінності документа. Хеш-функції перетворюють дані у унікальний код, який допомагає виявити будь-які зміни у даних. Комп'ютерна криміналістика включає спеціалізований аналіз цифрових доказів, такий як відновлення видаленої інформації, аналіз метаданих та дослідження історії змін файлів.

Проблема фальсифікації цифрових доказів стає дедалі гострішою через прогрес технологій. Найсерйозніші загрози включають технології створення штучних відео та аудіозаписів, редагування метаданих та втручання у системи зберігання даних. Такі загрози вимагають підвищеної уваги до безпеки цифрових доказів та застосування передових методів їх захисту.

Роль експертів у встановленні автентичності цифрової інформації є надзвичайно важливою. Експерти з кібербезпеки та цифрової криміналістики мають бути залучені для проведення спеціалізованих аналізів, що дозволяють встановити достовірність цифрових доказів. Їх висновки можуть мати визначальний вплив на результати судових розглядів, особливо у випадках, коли автентичність інформації під сумнівом. Крім того, міжнародні настанови підкреслюють необхідність навчання суддів і слідчих у роботі з цифровими доказами задля забезпечення їх автентичності та цілісності.

Судова практика в Україні та за її межами, що стосується цифрових доказів, є об'єктом особливої уваги, адже вона ілюструє актуальні тренди розвитку правової системи в умовах цифровізації. Вивчення вітчизняної та закордонної практики дозволяє ідентифікувати найбільш ефективні методи використання цифрових доказів у судочинстві та напрацювати рекомендації для вдосконалення українського законодавства.

Аналіз досвіду національних судів щодо використання цифрових доказів демонструє, що Верховний Суд України активно опікується питаннями прийнятності та достовірності цифрових доказів. Наприклад, у справах про державну зраду та воєнні злочини електронні докази відіграли ключову роль. Верховний Суд наголошує на необхідності дотримання процедур збору та

зберігання цифрових даних, а також використання електронних цифрових підписів для підтвердження автентичності документів. Проте, практика показує, що відсутність чітких законодавчих вимог щодо цифрових доказів іноді створює складнощі в їх використанні. Скажімо, питання допустимості відеозаписів з камер спостереження, встановлених без відповідної реєстрації, залишається відкритим.

Порівняльний аналіз підходів до цифрових доказів у США, ЄС та Великобританії виявляє значні відмінності в регулюванні цифрових доказів. Наприклад, у США широко використовується концепція "доказової цілісності", що передбачає забезпечення цілісності та достовірності цифрових даних на етапі їх збору та зберігання. Це реалізується за допомогою спеціальних стандартів і протоколів, які регламентують роботу з цифровими доказами. В ЄС діє директива про захист даних, яка встановлює високі стандарти захисту особистої інформації, що впливає на використання цифрових доказів у судових процесах. У Великій Британії застосовується принцип "доказової прийнятності", який передбачає оцінку доказів на основі їхньої надійності та значущості для справи.

В Сполучених Штатах також широко поширена концепція "електронного розкриття", яка передбачає обов'язкову передачу всіх електронних документів стороною, яка ними володіє, для забезпечення прозорості та справедливості процесу. У Європейському Союзі особливу увагу приділяють захисту прав людини при використанні цифрових доказів, зокрема у справах, що стосуються особистої інформації. У Великій Британії суди мають право вимагати від учасників процесу надання будь-яких цифрових даних, які можуть бути важливими для справи, що забезпечує ефективність процесу.

З міжнародної практики Україна може винести декілька важливих уроків:

1. Чітке законодавче регулювання: розвиток законодавчої бази щодо цифрових доказів, що чітко визначало б їх допустимість та процедури використання. Це може передбачати створення окремого розділу у процесуальних кодексах, повністю присвяченого цифровим доказам.

2. Стандартизація процедур: впровадження стандартизованих процедур збору, зберігання та захисту цифрових доказів, як це практикується в США. Це може включати розробку спеціальних протоколів для роботи з різними видами цифрових даних.

3. Підтримка міжнародного співробітництва: активізація міжнародного співробітництва у питаннях обміну досвідом та стандартами в сфері цифрових доказів, особливо з країнами ЄС. Це може передбачати участь України в міжнародних організаціях, які займаються питаннями цифрових доказів.

4. Підвищення кваліфікації суддів та слідчих: організація регулярних тренінгів для суддів та слідчих щодо роботи з цифровими доказами, подібно

до того, як це відбувається у Великій Британії та США. Це може включати навчання з питань цифрової криміналістики та захисту інформації.

Отже, аналіз вітчизняної та зарубіжної практики дозволяє Україні розвивати власну систему використання цифрових доказів, базуючись на передовому міжнародному досвіді та законодавчих рішеннях. Це сприятиме створенню більш ефективної та справедливої системи правосуддя, що відповідає вимогам сучасної цифрової епохи.

Сучасна судова система України постала перед потребою оновлення процесуального законодавства задля гарантування ефективного застосування цифрових доказів у судових розглядах. Цифровізація правосуддя вимагає не тільки технічних удосконалень, але й глибинних змін у законодавстві та практиці використання цифрових технологій. Виникає потреба у створенні правової бази, котра б чітко регулювала питання прийнятності та справжності цифрових доказів, забезпечуючи їх безпеку та недоторканність під час збору, зберігання та використання.

Необхідність оновлення процесуального законодавства вбачається у формуванні чітких та зрозумілих норм, котрі стосуються цифрових доказів. Потрібно розробити окремий розділ у процесуальних кодексах, котрий був би присвячений виключно цифровим доказам, визначаючи процедури їх збору, зберігання та застосування. Це допоможе уникнути розбіжностей у судовій практиці та гарантувати справедливість процесу. Приміром, законодавство повинно чітко визначати, які саме дані можна вважати цифровими доказами, як вони мають бути зібрані та збережені, а також які заходи необхідно вжити для їх захисту від несанкціонованого доступу.

Розробка єдиних стандартів збору, зберігання та перевірки цифрових доказів є одним з ключових напрямків покращення правового регулювання. Такі стандарти мають охоплювати вимоги до технічної інфраструктури, процедур захисту інформації та вимог до кваліфікації фахівців, котрі працюють з цифровими доказами. Це сприятиме збереженню цілісності та достовірності цифрових даних під час їх збору та зберігання, а також підвищить довіру до судової системи. Наприклад, стандарти можуть передбачати обов'язкове використання електронних цифрових підписів для підтвердження справжності документів та застосування блокчейн-технологій для реєстрації та зберігання судових рішень.

Підвищення цифрової грамотності суддів, адвокатів, прокурорів є важливим аспектом успішного впровадження цифрових технологій у правосуддя. Необхідно організувати регулярні тренінги та курси підвищення кваліфікації для фахівців юридичної сфери щодо роботи з цифровими доказами, цифрової форензики та захисту інформації. Це дозволить їм

ефективно застосовувати нові технології та розуміти особливості цифрових доказів. Наприклад, навчання повинно охоплювати питання використання спеціалізованого програмного забезпечення для аналізу цифрових даних, розуміння принципів криптографічного захисту інформації та застосування блокчейн-технологій у судовому процесі.

Роль цифрової судової інфраструктури у вдосконаленні правового регулювання є визначальною. Електронний суд та єдиний реєстр судових рішень здатні значно підвищити ефективність процесу та прозорість судової системи. Цифрові платформи надають учасникам процесу можливість подавати документи онлайн, отримувати повістки та брати участь у засіданнях через відеоконференцзв'язок. Крім того, застосування блокчейн-технологій для реєстрації та зберігання судових рішень може забезпечити їх недоторканність та недоступність для несанкціонованого доступу. Це сприятиме підвищенню довіри громадян до судової системи та зробить процес більш прозорим і ефективним.

Отже, вдосконалення правового регулювання цифрових доказів потребує комплексного підходу, котрий включає законодавчі зміни, розвиток технічної інфраструктури та підвищення кваліфікації фахівців юридичної сфери. Це допоможе створити сучасну та ефективну систему правосуддя, яка відповідає вимогам цифрової епохи та забезпечує справедливість і прозорість процесу.

У процесі дослідження було виявлено ряд критичних питань, пов'язаних з прийнятністю та достовірністю цифрових доказів у теперішній судовій системі України. Цифровізація юстиції породжує нові виклики як для законодавчого поля, так і для судової практики, вимагаючи модернізації правового інструментарію задля ефективного застосування цифрових доказів. Основними проблемними факторами є відсутність чіткого законодавчого регулювання щодо цифрових доказів, ризики спотворення інформації та недостатній рівень кваліфікації фахівців юридичної галузі щодо роботи з цифровими свідченнями.

Узагальнення основних проблем допустимості та автентичності цифрових доказів демонструє, що неврегульованість на законодавчому рівні створює правову невизначеність. Судова практика часто зустрічається з неузгодженостями у визначенні прийнятності таких доказів, що потенційно може призвести до несправедливих судових рішень. Крім того, ризики фальсифікації інформації, зокрема використання технологій deepfake або редагування метаданих, потребують розробки спеціальних методів для їх виявлення та запобігання. Недостатній рівень підготовки фахівців юридичної сфери щодо роботи з цифровими доказами також становить серйозну

проблему, оскільки вони повинні вміти коректно застосовувати новітні технології та розуміти специфіку цифрових доказів.

Пропозиції щодо вдосконалення правового механізму передбачають розробку окремого законодавства щодо цифрових доказів, яке б чітко визначало їхню прийнятність та процедури використання. Необхідно створити єдині стандарти збору, зберігання та перевірки цифрових доказів, що забезпечувало б їхню цілісність та автентичність. Це може бути досягнуто шляхом впровадження спеціальних протоколів для роботи з різними типами цифрових даних та застосування блокчейн-технологій для реєстрації та зберігання судових рішень. Крім того, важливим є підвищення рівня цифрової обізнаності суддів, адвокатів та прокурорів через організацію регулярних тренінгів та курсів підвищення кваліфікації з питань роботи з цифровими доказами та захисту інформації.

Перспективи подальших досліджень у цій сфері виглядають багатообіцяючими та актуальними. Дослідження можуть бути спрямовані на аналіз міжнародного досвіду у сфері використання цифрових доказів та розробку рекомендацій для України щодо імплементації найкращих практик. Наприклад, можна дослідити досвід США щодо застосування концепції "електронного відкриття" або досвід ЄС щодо захисту даних під час використання цифрових доказів. Також перспективним є вивчення застосування блокчейн-технологій та інших інноваційних рішень для забезпечення безпеки та цілісності цифрових доказів. Дослідження в галузі цифрової криміналістики та захисту інформації можуть допомогти розробити ефективні методи виявлення спроб фальсифікації цифрових доказів та підвищити довіру до судової системи.

Таким чином, подальші дослідження в області цифрових доказів мають велике значення для розвитку сучасної судової системи України та забезпечення її відповідності вимогам цифрової епохи. Вони сприятимуть створенню більш ефективної та справедливої системи правосуддя, здатної успішно використовувати новітні технології для захисту прав громадян та забезпечення безпеки інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] Цивільний процесуальний кодекс України: Закон України від 18.03.2004 № 1618-IV // Відомості Верховної Ради України. – 2004. – № 40–41, № 42, № 43.
[2] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI // Відомості Верховної Ради України. – 2013. – № 9–10, № 11–12, № 13.
[3] Рішення Верховного Суду України у справах, що стосуються використання цифрових доказів. – [Електронний ресурс]. – Режим доступу: https://supreme.court.gov.ua – Дата звернення: 16.03.2025.

[4] Директива (ЄС) 2016/680 Європейського парламенту і Ради від 27 квітня 2016 р. щодо захисту фізичних осіб у зв'язку з обробкою персональних даних. – [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu– Дата звернення: 16.03.2025.
[5] Рекомендації Ради Європи щодо електронних доказів у кримінальному судочинстві. – [Електронний ресурс]. – Режим доступу: https://www.coe.int – Дата звернення: 16.03.2025.
[6] Наукові публікації з питань цифрових доказів // Національна академія правових наук України. – [Електронний ресурс]. – Режим доступу: https://nalasu.org.ua – Дата звернення: 16.03.2025.
[7] Міністерство юстиції України. Офіційний сайт. – [Електронний ресурс]. – Режим доступу: https://minjust.gov.ua – Дата звернення: 16.03.2025.
[8] Державна судова адміністрація України. Офіційний сайт. – [Електронний ресурс]. – Режим доступу: https://court.gov.ua – Дата звернення: 16.03.2025.