Цифрова доказова база: електронні документи, інформація з гаджетів та blockchain як нові інструменти судового процесу

Лазько Гюльназ Заурівна[1], Бедратий Юрій Вячеславович[2], Завальнюк Ігор Вікторович[3]

Опубліковано	Секція	УДК
25.10.2025	Право	347.9:004.7

DOI: https://doi.org/10.5281/zenodo.17444536

Анотація. Стаття репрезентує інтегровану модель цифрової доказової бази, у межах якої електронні документи, дані з персональних гаджетів і блокчейн-записи розглядаються як узгоджена система джерел, процедур і критеріїв доказування. Теоретичною основою слугує поєднання класичних вимог належності, допустимості, достовірності та достатності з криміналістичними засадами надійності, ланцюга зберігання та відтворюваності. Показано, що у цифровому середовищі функцію «оригіналу» виконують перевірювані атрибути цілісності й походження (криптографічні хеші, мітки часу, кваліфіковані електронні підписи), а також документований ланцюг операцій із доказом. Сформульовано типологію ризиків: втрата метаданих, невидимі модифікації при «оживленні» пристрою, неповнота мережевого контексту, псевдонімність учасників блокчейну. Запропоновано узгоджені техніко-процесуальні запобіжники: створення форензичних образів із застосуванням модулю блокування запису, подвійне хешування на ключових етапах, протоколювання середовища збору (версії ПЗ, часові параметри, мережеві ідентифікатори), використання нотаріальних або кваліфікованих протоколів огляду веб-ресурсів, поєднання сліду у ланцюзі блоків із журнальними даними провайдерів. Розкрито роль судового контролю: безпосереднє дослідження електронних об’єктів, перевірка автентичності та ідентифікації джерела, своєчасне залучення експертів для складних артефактів. У межах єдиного каркаса обґрунтовано критерії прийнятності доказів з урахуванням специфіки адміністративного процесу та потреб криміналістичної практики: ідентифікація суб’єкта/пристрою/ключа, підтверджена цілісність, відтворюваність методики та прозора історія поводження з даними. Сформовано практичні рекомендації для

[1] Лазько Гюльназ Заурівна, кандидат юридичних наук, доцент, помічник-консультант народного депутата України, Верховна Рада України, ORCID: https://orcid.org/0000-0002-9671-8951.
[2] Бедратий Юрій Вячеславович, кандидат юридичних наук, доцент кафедри правових природоохоронних дисциплін, Національний університет водного господарства та природокористування, ORCID: https://orcid.org/0000-0001-9230-0438
[3] Завальнюк Ігор Вікторович, доктор юридичних наук, суддя Одеського окружного адміністративного суду, професор кафедри державно-правових дисциплін, Міжнародний гуманітарний університет, ORCID: https://orcid.org/0000-0002-6387-0199

учасників процесу та судів щодо збирання, збереження, автентифікації й презентації цифрових доказів, здатних витримати одночасно технічну й процесуальну перевірку.

Ключові слова: електронні докази; адміністративне судочинство; криміналістика; електронний документ; дані мобільних пристроїв; блокчейн; допустимість; автентичність; хеш-функції; ланцюг зберігання.

Digital evidence base: electronic documents, gadget information and blockchain as new litigation tools

Annotation. The article presents an integrated model of the digital evidence base in which electronic documents, data from personal gadgets, and blockchain records are treated as a coherent system of sources, procedures, and evidentiary criteria. The framework aligns classical requirements of relevance, admissibility, credibility, and sufficiency with forensic principles of soundness, chain of custody, and repeatability. In digital environments, the role of the "original" is performed by verifiable attributes of integrity and provenance (cryptographic hashes, trusted timestamps, qualified e-signatures) together with a documented operational history. A risk typology is outlined: loss of metadata, invisible modifications caused by device activation, omission of network context, and the pseudonymity of blockchain participants. Harmonised technical-procedural safeguards are specified: creation of forensic images using write-blockers, dual hashing at pivotal stages, rigorous logging of the acquisition environment (software versions, timing parameters, network identifiers), notarised or qualified protocols for web captures, and fusion of on-chain traces with providers' audit logs. The role of judicial control is articulated: direct examination of electronic artefacts, verification of authenticity and source attribution, and timely appointment of experts for complex datasets. Within a single conceptual scaffold, criteria of evidentiary acceptability are justified with regard to administrative proceedings and forensic practice: subject/device/key identification, demonstrated integrity, methodological reproducibility, and a transparent chain of custody. Practical guidance is formulated for litigants and courts on the collection, preservation, authentication, and persuasive presentation of digital evidence capable of withstanding both technical scrutiny and procedural review.

Keywords: electronic evidence; administrative proceedings; forensics; electronic document; mobile device data; blockchain; admissibility; authenticity; hash functions; chain of custody.

Вступ

Динамічний розвиток сучасного суспільства, що проявляється через масштабну діджиталізацію комунікаційних каналів та трансформацію значної частки соціальних взаємодій у віртуальну площину, генерує для правових систем країни якісно нові завдання та проблеми. Цифровізація правових відносин змінила природу доказу: замість унікального паперового носія предметом судового дослідження стають електронні документи, сліди взаємодії з персональними пристроями та ончейн-записи, що живуть у мережевих екосистемах і зберігають «пам'ять» подій точніше за людську. Щоби така «пам'ять даних» набула переконливої юридичної форми, класичні критерії належності, допустимості, достовірності й достатності узгоджуються з криміналістичними принципами форензичної надійності, ланцюга зберігання та відтворюваності методики. Також формальне закріплення електронних доказів в адміністративному судочинстві не вирішило всіх питань, а навпаки, породило глибоку доктринальну дискусію щодо їхньої фундаментальної правової ідентичності. Функцію «оригіналу» в цифровому середовищі

виконують перевірювані атрибути походження та цілісності - криптографічні хеші, довірчі часові позначки, кваліфіковані електронні підписи - у супроводі чітко протоколізованого середовища збору й обробки. Водночас ключовими стають уважність до метаданих, акуратна робота з часовою синхронізацією та гібридна атрибуція, що поєднує ончейн-трасування з офчейн-ідентифікаційними джерелами.

Постановка проблеми. Стрімка цифровізація комунікацій, документообігу й платіжних сервісів призвела до того, що значущі для правосуддя факти первинно фіксуються у цифровій формі: електронні документи, листування в месенджерах, телеметрія мобільних пристроїв, журнали подій, записи у блокчейн-реєстрах. У цих умовах традиційні уявлення про «оригінал», «копію» та «автентичність» потребують переосмислення: множинність біт-ідентичних примірників є нормою; доказова «оригінальність» забезпечується атрибутами цілісності та походження (хеш-функції, мітки часу, кваліфіковані електронні підписи) і відтворюваним ланцюгом поводження з об'єктом. Водночас посилюються ризики: невидимі модифікації при доступі до носія, втрата метаданих, «сліпі зони» мережевого контексту, псевдонімність учасників у публічних реєстрах. Потреба полягає у створенні інтегрованої моделі, що поєднує процесуальні критерії належності, допустимості, достовірності та достатності доказів з криміналістичною методикою (forensic soundness, chain of custody, відтворюваність), аби цифрові артефакти витримували і технічну, і юридичну перевірку та залишалися переконливими для суду. В адміністративному процесі однією з найгостріших проблем є встановлення особи, яка створила або поширила певну електронну інформацію, адже анонімність або можливість використання псевдонімів в інтернет-просторі значно ускладнює процес доказування.

Мета статті - запропонувати інтегровану, науково вивірену і водночас практично зрозумілу модель цифрової доказової бази як системи джерел, процедур і критеріїв, придатної до незалежної перевірки в адміністративному судочинстві та криміналістичній практиці, і окреслити операційні принципи збирання, збереження, автентифікації та представлення електронних артефактів, що мінімізують ризики невидимих модифікацій і втрати сенсу та підвищують доказову спроможність у змагальному процесі.

Аналіз останніх досліджень і публікацій. Міжнародні орієнтири задають керівні підходи до електронних доказів у судових процесах. До прикладу у рішеннях Комітету Міністрів Ради Європи, у котрих наголошено на стандартизації збору, збереження, автентифікації та подання цифрових даних. У вітчизняному нормативно-правовому полі акцент зроблено на специфічних рисах електронних доказів. В працях В.В. Самонова з адміністративного права підкреслено нематеріальну природу об'єкта, вирішальну роль метаданих і потребу чітких процесуальних форм подання та дослідження випадків [13]. Питання допустимості розглядаються крізь призму статусу електронної копії, меж отримання «оригіналу», обов'язку своєчасного розкриття доказів іншій стороні та наслідків порушення цих вимог у праці В.А. Будкевич [3]. Дискусію про нерівномірність судової практики та необхідність імпорту елементів зарубіжних стандартів автентифікації підтримує аналіз еволюції використання електронних доказів у господарському й адміністративному судочинстві [4]. Практикоорієнтовані дослідження В.В. Романюк зосереджують увагу на верифікації джерел, повноті мережевого контексту та ролі експертної підтримки при роботі з великими масивами цифрових даних, зокрема у справах, пов'язаних із колаборaційною діяльністю [12].

Технічна сторона обробки даних мобільних пристроїв формують стандарти методично регламентованого дослідження цифрових об'єктів, які нормують створення образів, використання модулів блокування запису, ведення журналів середовища та контроль цілісності хешами на ключових етапах вилучення й аналізу [14]. Для блокчейн-сегмента відзначається поєднання незмінності реєстру з обмеженнями ідентифікації

суб’єктів транзакцій; пропонуються моделі зв’язування ончейн-трас із даними провайдерів (KYC/AML) та аудиторськими логами для забезпечення атрибуції [15]. Нормативну основу в Україні становлять процесуальні приписи щодо подання електронних доказів (оригінал/електронна копія з КЕП, можливість отримання, оцінка на загальних засадах) та галузеві акти про електронні документи і довірчі послуги, які надають юридичну силу електронному підпису та мітці часу [10, 11]. Як приклад, КАС України встановлює чіткі вимоги до подання електронних доказів – вони можуть подаватися до суду в оригіналі або у вигляді електронної копії, яка обов'язково має бути засвідчена електронним підписом. При цьому сторона, яка подає копію, зобов'язана зазначити про наявність у неї або в іншої особи оригіналу. Практичні роз’яснення судів і органів юстиції конкретизують робочі процедури: від недопустимості «сюрприз-доказів» до протоколів засвідчення вебконтенту й листувань.

Матеріали та методи. Аналітичну базу становили національні процесуальні та спеціальні акти (КАС України; закони про електронні документи та електронні довірчі послуги) [8; 10; 11], керівні підходи Ради Європи щодо електронних доказів [7], технічні настанови мобільної форензики NIST [14] і методичні орієнтири щодо блокчейну в доказуванні й атрибуції [15]. Застосовано комплекс методів: догматичний аналіз норм і дефініцій для виокремлення критеріїв належності, допустимості, достовірності та достатності електронних доказів; порівняльно-правовий підхід для зіставлення національних приписів із міжнародними стандартами [7; 8; 10; 11]; структурно-функціональний аналіз архітектури електронного доказу (метадані, атрибути цілісності, часові позначки).

Результати

Питання автентифікації та оцінювання електронних документів і комунікацій у сучасному процесуальному середовищі не зводиться до фіксації зовнішнього вигляду цифрового об’єкта. Доказова цінність матеріалу формується не «візуальністю» доказу, а можливістю перевірки його походження та незмінності у часі. У цьому сенсі електронний документ набуває статусу повноцінного доказу тоді, коли його атрибути цілісності та джерела можуть бути підтверджені незалежним суб’єктом за процедурою, зрозумілою суду. Нормативне визначення Кодексом адміністративного судочинства України кореспондує із такою парадигмою: подання в оригіналі або в електронній копії, засвідченій кваліфікованим електронним підписом, поєднане з можливістю отримання біт-ідентичного екземпляра, переносить акцент із матеріального носія на властивості, які перевіряються, цифрового джерела. Таким чином, «оригінальність» у цифровій площині функціонально ототожнюється з наявністю криптографічних ознак цілісності, довірчих часових позначок та належного протоколу обігу об’єкта від моменту виникнення до моменту дослідження [8, с. 99].

Міжнародні підходи підтверджують необхідність методичної уніфікації процедур. Керівні принципи Комітету Міністрів Ради Європи щодо електронних доказів пропонують розглядати допустимість як похідну від форензичної валідності методики збирання, зберігання та представлення цифрової інформації, а також підкреслюють важливість організаційної та компетентнісної спроможності судів до роботи з такими матеріалами [7, с. 3]. У практичному вимірі це означає, що зміст електронного листування, записів серверів або файлів на носіях слід супроводжувати машинночитаними атрибутами, які дозволяють перевірити процесуально релевантні параметри: ідентифікацію джерела, часову прив’язку та незмінність. Власне через це вимоги до електронного підпису і міток часу у законодавстві про електронні документи та довірчі послуги набувають не лише цивільно-правової, а й доказової ваги: вони забезпечують відтворювану, технічно нейтральну основу для визнання походження та цілісності файлів у суді [10, с 7; 11, с. 18].

Специфіка електронних комунікацій у тому, що їх семантичний зміст безпосередньо залежить від метаданих. Ідентичний текст повідомлення, позбавлений контексту виникнення, маршруту передавання та серверних часових параметрів, має іншу доказову силу, ніж еквівалентний за змістом, але забезпечений повними заголовками, ланцюжком відомостей про пересилання та незалежною часовою прив'язкою. Метадані у цьому разі не є «допоміжним додатком»: вони забезпечують можливість реконструювати порядок подій, перевірити кореляцію між локальним часом пристрою та серверними позначками, а також зняти сумніви щодо фрагментарності або вибірковості презентованого матеріалу. Така конструкція інтелектуальної «прозорості» відповідає класичній доктрині процесуальної достовірності, однак реалізується технічними засобами, що підлягають незалежній перевірці у межах судової процедури.

Дані мобільних пристроїв потребують підвищеної дисципліни збирання. Природа операційних систем та застосунків зумовлює чутливість доказових елементів до будь-якої взаємодії з пристроєм: змінюються часові індекси, оновлюються кеші, перезаписуються журнали. Унаслідок цього аналіз в «живому» режимі без попереднього створення форензичного образу приводить до невідновних змін у структурі даних та компрометує можливість незалежної верифікації. Рекомендації NIST щодо мобільної форензики систематизують мінімальні вимоги безпечної роботи: ізоляція пристрою від мережевого середовища, пріоритет створення образу (логічного або фізичного) з використанням засобів, що унеможливлюють запис на носій, двоетапний контроль контрольних сум на ключових фазах, а також суворе протоколювання середовища виконання і застосованих інструментів [14, с. 11]. Подібна методика виступає не стільки технічним «стандартом», скільки гарантією процесуальної нейтральності: незалежний експерт здатен відтворити той самий шлях і отримати той самий результат, а суд — зрозуміти, яким чином забезпечено незмінність.

Особливого значення набуває правильна інтерпретація часу. Розсинхронізація локальних налаштувань пристрою, параметрів часової зони та відомостей серверів призводить до хибних висновків щодо послідовності подій. Тому у поважній (можливо замінити на правовій) процедурі завжди присутнє зіставлення локального і серверного часу, а також фіксація умов, за яких проводилося копіювання або експорт даних. Такі деталі мають значення і для адміністративного процесу, де час вчинення дій суб'єкта владних повноважень та час одержання повідомлення або відповіді можуть формувати матеріальну частину предмета доказування [1, с. 214].

Аудіовізуальні матеріали, попри інтуїтивну «наочність», позначені (можливо – вирізняються) ризиками невидимих модифікацій. Перекодування, зміна контейнера, обтинання вмісту або повторні збереження залишають слід у технічних атрибутах, але не завжди візуально виявляються. У доказовому плані належним є збереження первинної структури файлів і контейнерів, копіювання з первинного носія з обчисленням контрольних сум, документування моделі пристрою, версії прошивки та налаштувань, а також фіксація часової конфігурації системи відеоспостереження або диктофона. Такий підхід дозволяє суду здійснювати безпосереднє дослідження із можливістю технічної перевірки — саме те, що відповідає природі принципу безпосередності та вимогам достовірності [4, с. 9].

Окремий блок дослідження пов'язаний із блокчейн-технологією. Розподілений реєстр забезпечує незмінність та публічну перевірюваність транзакційного журналу, однак не розв'язує питання ідентифікації особи. У доказовому сенсі реєстр є надійним джерелом фактів існування і часу подій, але юридичний зв'язок між адресою та конкретним суб'єктом встановлюється поза ланцюгом блоків. У цьому полягає сенс гібридної моделі, за якої ончейн-відомості поєднуються з офчейн-даними провайдерів послуг віртуальних активів, кастодіанів або бірж: профілі ідентифікації (KYC), журнали доступу, договори обслуговування та білінг мережевих з'єднань формують необхідний

місток для атрибуції події людині або організації. Саме така модель пропонується у міжнародних дослідженнях, де незмінність реєстру трактується як елемент забезпечення цілісності, тоді як ідентифікація суб'єктів досягається через регульовані офчейн-процедури [15, с. 11–16]. Поза тим, технологія використовується як допоміжний механізм фіксації часу та цілісності інших електронних доказів: оприлюднення хешів у блокчейні створює верифіковану часову прив'язку, що у тривалих спорах дозволяє доводити існування конкретної біт-послідовності на певну дату. Зрозуміло, така фіксація не підміняє кваліфікованих довірчих послуг, проте підсилює їх там, де задіяно багато незалежних сторін і важливо усунути залежність від одного зберігача.

Синтез процесуальних критеріїв і криміналістичних процедур набуває практичного виміру у вигляді стандартизованих пакетів перевірки. Для електронних листів переконливість забезпечується наданням повних заголовків, які відображають маршрутизацію та результати доменної автентифікації, і супроводжувальними контрольними сумами на контейнері експорту. Для історій повідомлень у месенджерах ключовим є повний експорт у машиночитаному форматі, що зберігає ідентифікатори діалогів і часові параметри, а також незалежна фіксація часу на архіві. Для аудіовізуальних файлів істотною є відсутність повторного кодування та безперервність ланцюга зберігання, включно з фіксацією налаштувань пристрою. Для блокчейн-записів достатність досягається через поєднання ончейн-верифікації з офчейн-підтвердженням контролю адреси у відповідний період. Усі ці категорії підпорядковуються загальному принципу відтворюваності: незалежний учасник повинен мати змогу перевірити той самий артефакт, використавши описану методику та отримавши тотожні контрольні величини [2].

Істотною проблемою залишається низький рівень компетентності у сфері електронного доказування, притаманний як учасникам судових справ, так і частині суддівського корпусу. Це є наслідком новизни цифрових технологій у порівнянні з глибоко укоріненою практикою використання паперових носіїв. На відміну від традиційних документів, робота з якими зазвичай не викликає труднощів, електронні докази систематично потребують залучення спеціалізованих знань на всіх етапах – від збору до дослідження.

Узагальнюючи зазначене, доцільно представити стислий інструментарій перевірок. Він не підміняє процедури і не виконує роль «жорсткого стандарту», однак надає спільну мову для професійної комунікації між судом, учасниками процесу та експертами.

Таблиця 1. **Матриця перевірок автентичності та цілісності для типових цифрових доказів.**

Клас доказу	**Ключові атрибути автентифікації**	**Перевірка цілісності та часу**	**Елементи історії (Chain of Custody)**	**Мінімально достатня форма подання**
Електронні листи	Повні заголовки листів із даними маршрутизації та доменної автентифікації	Контрольні суми на контейнері експорту; довірча мітка часу	Опис інструмента, версії ПЗ, часу експорту; фіксація місця зберігання	Електронна копія з КЕП або оригінал; готовність надати біт-ідентичний екземпляр
Повідомлення в месенджерах	Повний машиночитаний експорт із ідентифікаторами	Хеш архіву; мітка часу; за можливості	Опис середовища експорту, інструментів і	Архів експорту, засвідчений належним чином; за

	діалогів і часовими параметрами	підписаний контейнер	доступів; місце зберігання	потреби форензичний образ пристрою
Відео- та аудіофайли	Збереження первинного контейнера і кодека, фіксація налаштувань пристрою	Контрольні суми оригінальних файлів; збереження без перекодування	Протокол копіювання з носія; позначення відповідальних осіб та часових меж	Електронні копії з контрольними сумами і можливістю відтворення у суді
Блокчейн-записи	Ідентифікація транзакції (tx hash, блок, адреси, час підтвердження)	Верифікація через незалежний клієнт; хеші/мітки часу на витягах	Опис мережевого середовища; зшивання з офчейн-ідентифікаторами	Витяг із реєстру у поєднанні з відповідями провайдерів (KYC/AML)

Джерело: Складено авторами на основі джерел [7, 8, 14, 15,]

Запропонована матриця виконує роль операційного інструментарію, у якому процесуальні критерії належності, допустимості, достовірності та достатності електронних доказів отримують предметний зміст через технічні та методичні гарантії достовірності. Відсутність хоча б одного елемента не завжди означає недопустимість, але означає зниження рівня переконливості та потребу в компенсаторних засобах перевірки, насамперед у судово-технічній експертизі. Натомість повнота атрибутів і прозорість історії поводження з об'єктом зменшують процесуальні ризики, роблять артефакт інтелектуально доступним для судового сприйняття і полегшують здійснення безпосереднього дослідження [12, с. 93].

У підсумку електронний доказ постає як конструкція, у якій технічна відтворюваність і процесуальна форма не протистоять одна одній, а є взаємозалежними компонентами. Саме через таку інтеграцію досягається баланс між вимогами технологічної доброчесності і процесуальної забезпеченості, що дозволяє одночасно зберігати точність і забезпечувати зрозумілість для судової системи. Такий підхід не надає абсолютності жодному окремому інструменту: і електронний підпис, і мітка часу, і контрольні суми, і створення протоколів середовища мають значення лише як частини цілісного методу, придатного для незалежної перевірки за правилами змагальності. У науковому вимірі це означає переорієнтацію з формально-носієвої концепції доказу на концепцію процедурно-підтверджуваної автентичності, де логіка доказування будується на можливості ретельної реконструкції шляху даних і критичної оцінки кожного етапу їхнього існування [2].

Подальший розвиток цифрової доказової бази потребує від права тонкої сенситивності до природи даних і від криміналістики - усвідомлення процесуальної логіки судового контролю. Ці два шляхи не конкурують, а визначають спосіб, у який електронний доказ може набувати статусу переконливого. Відмова від носієвої унікальності на користь перевірюваної цілісності та відтворюваної доказової бази не зменшує рівень захисту сторін, а, навпаки, робить його більш рівномірним: незалежно від того, чи йдеться про файл, журнал сервера, чат або запис у блокчейні, критерії прийнятності формуються з позицій можливості незалежної верифікації. У цій логіці «оригінал» у цифровому сенсі не «річ», а функція надійного підтвердження незмінності та походження, яке може бути повторене іншою стороною або експертом за описаною методикою. Саме тому визнання електронних доказів у нормативних актах, що

регулюють адміністративний процес, і в актах про електронний документ та довірчі послуги істотно підсилює процесуальну інфраструктуру правосуддя: мітки часу, кваліфікований підпис ідентифікують джерело та утримують відтворювану «пам'ять» об'єкта, що критично для подальшої оцінки судом [8, с 5; 11, с. 18].

Коли цифровий доказ входить до (можливо – є частиною) матеріалів справи, суд стикається з подвійним завданням. По-перше, необхідно з'ясувати, чи відповідає артефакт процесуальним вимогам належності та допустимості. По-друге, потрібно оцінити його достовірність і достатність як окремо, так і у світлі всієї сукупності матеріалів. Зміщення акценту з носія на атрибути цілісності не означає зниження стандартів: перевірюваність хешів, часових позначок і підписів надає більш прозорі критерії оцінювання, ніж у традиційних письмових доказах, де процес відтворення «шляху документа» часто має латентні ділянки. У цьому сенсі судова оцінка в цифрових (можливо – електронних доказів у) справах поступово набуває ознак методологічної дисципліни: замість інтуїтивного порівняння копій відбувається контроль процедурних та криптографічних індикаторів, що в ідеалі описуються в поданні сторони простими для відтворення кроками [2].

Форензична методика, орієнтована на мінімальне втручання і повноцінне журналювання, пропонує суду довіроздатний «наратив» артефакта. Якщо на етапі збирання дотримано ізоляції пристрою, створення форензичного образу, застосовано модуль блокування запису, проведено подвійне хешування та протоколювання середовища, то у залі суду відпадає потреба у здогадах щодо того, чи не були дані змінені ненавмисно в процесі аналізу. У свою чергу, коректно сформований пакет електронних комунікацій із повними заголовками, машинночитаними атрибутами та довірчою міткою часу долає типові сумніви щодо походження й хронології подій. Така процедура не є тільки технічною вимогою, це, у свою чергу, гуманізований стандарт прозорості, який робить цифровий доказ доступним для розуміння без спеціальної освіти, бо кожне твердження підкріплене параметрами, що підлягають перевірці в умовах змагальності судового процесу [14, с. 29].

Важливо, що універсальність цифрових атрибутів не знеособлює контекст доказу. Електронна «сила» не замінює процесуальну логіку предмета доказування, а тільки додає їй інструментальної точності. В адміністративних спорах, де часто необхідно відтворити комунікацію з органом влади або стан офіційного вебресурсу на певний момент, цифрові індикатори дозволяють не лише зафіксувати дату й час події, а й довести стабільність вмісту. У цьому сенсі Єдина судова інформаційно-телекомунікаційна система забезпечує механізми як подання, дослідження та оцінки електронних доказів у судовому процесі, але й гарантує збереження цілісності електронних доказів через застосування криптографічних методів захисту та електронного цифрового підпису. Особливостями застосування електронних доказів в ЄСІТС є автоматична фіксація часу та обставин їх подання, можливість перевірки автентичності та цілісності інформації, а також забезпечення доступу всіх учасників процесу до електронних матеріалів справи.

У криміналістичному аспекті та сама структура індикаторів забезпечує контроль за тим, як дані потрапили до справи: чи не відбулося непомітне втручання під час експорту або копіювання, чи збережено первинні контейнери і чи може незалежний експерт відтворити процедуру. Концептуально це означає зближення «допустимості» та «форензичної валідності», про яке послідовно нагадують міжнародні орієнтири щодо електронних доказів у судовому процесі [7, с.8].

Особливу увагу слід звернути на визначення часу у доказовому процесі. У цифровому середовищі час перестає бути суто календарною категорією, він перетворюється на мережеву властивість систем і сервісів. Внутрішній час пристрою, серверні часові позначки, мітки довірчих служб і блокчейн-підтвердження - це різні

етапи хронології, яка повинна відтворюватись і які можуть розбігатися. Криміналістичне оцінювання таких матеріалів потребує чіткої артикуляції шару, до якого належить кожна позначка, і пояснення технічних механізмів синхронізації. Там, де хронологічні зміни неминучі, їх не варто трактувати як дефект доказу правильніше розглядати як параметр, який підлягає калібруванню через зіставлення з референтними подіями або зовнішніми журналами. Цей підхід розвантажує процес від риторичних спорів і переводить питання часу в площину технічної інтерпретації. Нормативна конструкція довірчих міток і кваліфікованого підпису дає для цього достатньо опор: верифікація підпису і прив'язка до довірчого часу дозволяють узгодити локальні й серверні дані у спосіб, прийнятний для суду [11, с.18].

Не менш показовою є взаємодія цифрової доказової бази з приватністю та інформаційною безпекою. Правоохоронні органи, що вирішують питання про витребування або огляд електронних матеріалів, вимушено балансують між повнотою доказу й мінімізацією доступу до несуттєвих персональних даних. Форензична практика виробила з цього приводу поміркований стандарт: технічні інструменти дозволяють створювати звужені вивантаження, застосовувати хеш-фільтри, маскувати поля, що не стосуються предмета доказування, і водночас зберігати відтворюваність процедури. Такий підхід не компрометує ідею змагальності; він підсилює її, адже надає опоненту можливість перевірки методики без доступу до надлишкової інформації. У підсумку досягається баланс між доказовою релевантністю та етичними межами обробки даних, що відповідає як завданням адміністративного судочинства, так і криміналістичним вимогам точності [12, с. 94].

Блокчейн у цьому процесі виступає як подвійний інструмент: він уможливлює публічну перевірку незмінності транзакцій та одночасно слугує зовнішнім якорем для фіксації часу та цілісності інших електронних матеріалів. Обидві функції мають сенс тільки тоді, коли усвідомлюється їхня межа. Незмінність журналу не ототожнюється з ідентифікацією особи, тому правова атрибуція потребує офчейн-джерел, насамперед від постачальників послуг віртуальних активів. Там, де такий місток налаштований, блокчейн надає доказу параметри перевірюваності, які важко відтворити іншими засобами, - незалежність інфраструктури, довготривалу доступність журналу, мультиагентну перевірку. У частині timestamping реєстр працює як додатковий механізм фіксації, котрий не суперечить довірчим послугам, а доповнює їх, підвищуючи надійність у багатосторонніх відносинах та довгих циклах оскарження [15, с. 11].

Синтез процесуальної та криміналістичної перспективи дає можливість сформулювати універсальний критерій переконливості цифрових доказів: готовність до незалежної перевірки. Усе інше - лише реалізація цього критерію в конкретних середовищах даних. У комунікаціях такою реалізацією стають повні заголовки, експорти і часові прив'язки; у мобільних пристроях - образи, журнали й контрольні суми; в аудіовізуальних матеріалах - збереження первинних контейнерів і відмова від повторного кодування; у блокчейні - зв'язування ончейн-події з офчейн-ідентифікацією. Всі ці підстави не виключають необхідності експертизи, але зменшують її «обсяг невизначеності», бо на вхід експертного аналізу надходить структурований, відтворюваний масив. Правова оцінка, своєю чергою, спирається не на емоційне враження від «цифровості», а на можливість співставити контрольні параметри, реконструювати часову шкалу та зрозуміти шлях об'єкта від моменту виникнення до моменту дослідження [2].

Таке зближення методологій неминуче змінює й судову комунікацію. Письмові пояснення та висновки починають містити не тільки правові доводи, а й короткі описові схеми технічної процедури, зрозумілі нефахівцю, - які інструменти застосовано, які контрольні величини отримано, яким чином забезпечено ланцюг зберігання. Наукова чесність тут поєднується з прагматичною ясністю, що підвищує якість змагальності:

опонент працює із зрозумілими параметрами, суддя - із відтворюваною картиною подій, експерт - із даними, які допускають повторення експерименту. У сукупності це створює середовище, де цифрові докази не потребують «особливого ставлення», а органічно вбудовуються у процесуальні фільтри, встановлені для будь-якого виду доказів.

Водночас, механізми фіксації, документування та верифікації цифрових доказів досі залишаються поза межами належної правової регламентації. Відсутній єдиний, послідовний протокол роботи з такими доказовими засобами на всіх стадіях - від моменту їх виявлення і закріплення до представлення та оцінки судом. Законодавець не встановив однозначних параметрів для диференціації понять "оригінал" і "копія" стосовно електронних доказів, що породжує численні дискусії та конфлікти в правозастосовній практиці. Актуальним завданням є створення докладнішої, доступнішої та стандартизованої процесуальної основи для операцій з цифровими доказами. Результатом такого реформування повинно стати подолання розбіжностей у судовій діяльності та гарантування неухильного виконання законодавчих приписів, що сприятиме підвищенню якості судочинства. Належне науково-теоретичне обґрунтування інноваційних доказових стандартів є критичною умовою для вичерпного використання їх нормативного потенціалу та посилення захисту суб'єктивних прав учасників адміністративного процесу.

У горизонті розвитку слід очікувати подальшої інституціоналізації технічних стандартів у процесуальних нормах. Мова не про жорстку «кодифікацію інструментів», а про встановлення мінімальних процедурних маркерів, що сигналізують суду про достатню відтворюваність: фіксація часу та джерела, контрольні суми, опис середовища одержання, доступність біт-ідентичних екземплярів. Подібні підходи вже проступають у рекомендаціях і керівних засадах, зорієнтованих на адаптацію судових систем до цифрової реальності, і корелюють із національними нормами про електронні документи та довірчі послуги. Імовірно, правозастосування дедалі активніше покладатиметься на поєднання процесуальних рамок із галузевими технічними настановами, подібними до мобільної форензики, де навіть базові протоколи вже сьогодні забезпечують судову відтворюваність і зменшують простір для спекуляцій [14, p. 29–36].

У підсумковому висновку цифрова доказова база постає не як сукупність нових «видів доказів», а як спосіб мислення про доказовість у середовищі, де дані з’являються, переміщуються і засвідчуються інакше, ніж на папері. Вона вимагає одночасно точності та емпатії: точності - у дотриманні процедур, що роблять цифровий об’єкт відтворюваним, і емпатії - у формулюванні пояснень, які дозволяють суду зрозуміти технічні дії без спеціальних знань. Право і криміналістика зустрічаються в цій точці не як опоненти, а як співавтори методології: перше встановлює мету і критерії, друга - надає інструменти і верифікаційні механізми. Там, де ця співпраця реалізована, електронний доказ перестає бути об’єктом підозри і стає повноцінним учасником процесуальної розмови; там, де її бракує, цифровість підміняє доказовість, а наукова мова втрачає силу переконання.

Висновки

Цифрова доказова база постає як цілісна система, у якій процесуальні критерії належності, допустимості, достовірності та достатності набувають предметного змісту через криміналістичні процедури і технічні гарантії. Електронні документи, дані з персональних гаджетів та записи у блокчейн-реєстрах не є ізольованими «видами доказів», їхня переконливість визначається здатністю забезпечити відтворюваність перевірки: ідентифікацію джерела, підтвердження цілісності, прозорий ланцюг поводження з об’єктом і зрозумілу часову прив’язку. У цифровій площині «оригінал» функціонально ототожнюється з біт-ідентичністю та перевірюваними атрибутами походження (контрольні хеші, довірчі мітки часу, кваліфіковані електронні підписи),

тоді як унікальність матеріального носія втрачає визначальне значення. Саме ця трансформація забезпечує інтелектуальну доступність електронного доказу для суду: замість риторики довіри пропонується механіка перевірки.

Інституційна готовність правосуддя до роботи з цифровими доказами потребує узгодження правових норм із технічними стандартами. Мінімальні маркери відтворюваності - фіксація часу та джерела, контрольні суми, опис застосованих інструментів, доступність біт-ідентичних екземплярів - мають перетворитися на звичні елементи процесуальної культури. Така «процедурна економія» не ускладнює провадження, а навпаки, зменшує обсяг експертної невизначеності та кількість спірних припущень. У підсумку цифрові матеріали природно проходять через ті самі фільтри, що й традиційні докази, але з вищою прозорістю внутрішньої будови. У контексті адміністративного судочинства зазначене має кінцевою метою повне та всебічне встановлення фактичних обставин справи з достатнім ступенем достовірності, що є необхідною передумовою для реалізації конституційного права на судовий захист та забезпечення верховенства права у сфері публічного адміністрування.

Список використаних джерел

1. Ангеленюк, А.-М. Ю. (2023). Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія Право*, (79, ч. 2), 214–218. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/10/34-1.pdf
2. Бекетова, Д. (2024). Електронні докази як засіб доказування в цивільному процесі України та інших держав. *Universum Iuris*. URL: https://archive.liga.science/index.php/universum/article/view/1530
3. Будкевич, В. А. (2022). Електронні докази в адміністративному судочинстві: окремі питання теорії та практики. *Адміністративне право і процес,* (2), 120–128. URL: https://jes.nuoua.od.ua/archive/2_2022/12.pdf
4. Гвасалія, А. В. (2021). Електронні докази як засоби доказування у господарському та адміністративному судочинстві. *Економіка. Фінанси. Право*, (12), 8–12. URL: https://elar.navs.edu.ua/items/669926af-6567-43f9-806d-2a0310e92998
5. European Parliament. (2022). Electronic signatures in the EU: Legal effect and admissibility under eIDAS (Briefing). URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739238/EPRS_ATA%282022%29739238_EN.pdf
6. Йосифович, Н.-Л. Д. (2025). Теорія і практика застосування електронних доказів у адміністративному судочинстві (дис. канд. юрид. наук). Львів. URL: https://www.lvduvs.edu.ua/documents_pdf/nauka/dorobok_zdobuvachiv/yosifovich_d.pdf
7. Council of Europe, Committee of Ministers. (2019). Guidelines on electronic evidence in civil and administrative proceedings: *Text and explanatory memorandum*. URL: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5
8. Верховна Рада України. (2005). Кодекс адміністративного судочинства України (Закон № 2747-IV, зі змінами), ст. 99. URL: https://zakon.rada.gov.ua/go/2747-15
9. Хмельницький окружний адміністративний суд. (2021, 13 травня). Електронні докази в адміністративному судочинстві (роз'яснення). URL: https://adm.km.court.gov.ua/sud2270/pres-centr/nov/1119353/
10. Верховна Рада України. (2003). Про електронні документи та електронний документообіг (Закон № 851-IV, зі змінами). URL: https://zakon.rada.gov.ua/go/851-15

11. Верховна Рада України. (2017). Про електронну ідентифікацію та електронні довірчі послуги (Закон № 2155-VIII, зі змінами). URL: https://zakon.rada.gov.ua/go/2155-19
12. Романюк, В. В. (2024). Електронні докази під час розслідування колабораційної діяльності: проблеми збирання та оцінки. *Вісник Харківського національного університету внутрішніх справ,* (3), 90–98. URL: https://vca.univd.edu.ua/index.php/vca/article/download/261/261/275
13. Самонова, В. В. (2021). Ознаки електронних доказів в адміністративному судочинстві. Правова позиція, 3(32), 38–43. URL: https://legalposition.umsf.in.ua/archive/2021/3/7.pdf, URL: https://doi.org/10.32836/2521-6473.2021-3.7
14. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101, Rev. 1). *National Institute of Standards and Technology*. URL: https://doi.org/10.6028/NIST.SP.800-101r1
15. United Nations Economic Commission for Europe. (2019). White paper on blockchain in trade facilitation. URL: https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf