Вплив цифровізації судочинства на якість доказування та стандарти допустимості електронних доказів

Яніна Волосна[1]

Опубліковано	Секція	УДК
30.01.2026	Право	347.94:004

DOI: https://doi.org/10.5281/zenodo.18504691

Анотація. Цифровізація судочинства суттєво трансформує процес доказування та значно впливає на якість і стандарти допустимості електронних доказів у цивільному, господарському та кримінальному процесах. Воєнний стан посилює таку динаміку та створює низку викликів: втрату паперових архівів, обмеження доступу до оригіналів, значне зростання обсягу цифрових даних, пов'язаних з воєнними злочинами та збитками. Ці обставини вимагають удосконалення правових механізмів підтвердження автентичності, цілісності та надійності електронних даних.

Удосконалення стандартів допустимості електронних доказів також набуває особливого практичного значення у зв'язку з необхідністю забезпечення притягнення до відповідальності в контексті післявоєнної відбудови. Цифрові докази стануть основою для міжнародних та національних судових процесів щодо репарацій і компенсацій. Обґрунтованою є необхідність гармонізації національного законодавства з міжнародними стандартами задля забезпечення правової визначеності та захисту прав учасників процесу.

Ключові слова: достовірність відомостей, цифрові сліди, воєнний злочин, військова агресія, відновлення правосуддя.

The impact of digitalization of legal proceedings on the quality of evidence and standards of admissibility of electronic evidence

Annotation. The ongoing digitization of justice in Ukraine represents a profound structural shift, significantly transforming the evidentiary process and fundamentally impacting the quality and standards for the admissibility of electronic evidence across civil, commercial, and criminal proceedings. This technological transformation is being drastically accelerated and complicated by the full-scale military aggression and the resulting martial law, which introduces a unique set of critical challenges.

These challenges include, but are not limited to, the mass loss or destruction of paper archives and physical documents, severe restrictions on access to original evidence and physical locations, and a exponential surge in the volume of digital data directly related to

[1] керівник адвокатського бюро «Яніни Волосної», ORCID: https://orcid.org/0009-0007-3829-5309.

documented war crimes and calculation of material and non-material damages. This unprecedented situation necessitates an immediate and significant overhaul of the legal and technical frameworks used to confirm the authenticity, integrity (non-mutability), and overall reliability of electronic data. In the absence of traditional physical controls, the reliance on advanced cryptographic methods, such as cryptographic hashing and the use of Qualified Electronic Time Stamps (QETS), becomes not just preferable, but mandatory for maintaining the chain of custody and legal validity of evidence.

The refinement and rigorous application of these admissibility standards for electronic evidence acquire particular practical significance in the immediate and long-term context of post-war accountability and national reconstruction. Digital evidence, including satellite imagery, data from social media, messaging apps, drone footage, and electronic register extracts, is set to form the cornerstone of evidence for all future international and national judicial processes concerning reparations, compensation claims, and the prosecution of individuals responsible for grave international crimes.

A key element of this necessary legal evolution is the imperative to harmonize national procedural legislation with established international standards and best practices governing the handling of electronic evidence, particularly those adopted by bodies such as the UNCITRAL (Model Law on Electronic Commerce) and the practice of the European Court of Human Rights. Such harmonization is crucial not only to ensure legal certainty and predictable judicial outcomes for participants but also to guarantee that Ukrainian-collected evidence remains admissible and credible in international legal forums and mechanisms created to adjudicate war-related claims. By robustly establishing high standards for data preservation and verification, Ukraine can effectively leverage digitization to rebuild its judicial integrity, protect the rights of its citizens, and secure justice in the recovery era. The efficacy of the entire national recovery effort hinges on the ability of the judicial system to reliably process and utilize these digital traces of war and damage.

Keywords: evidentiary reliability, digital forensics, war crimes prosecution, military aggression, transitional justice.

Вступ

Цифровізація є стратегічною імперативою для України, трансформуючи державне управління та, зокрема, сферу правосуддя. Впровадження Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС) та функціонування "Електронного суду" не просто модернізують судовий процес, а й формують фундамент для нової парадигми електронного доказування. Законодавче закріплення електронного доказу в процесуальних кодексах (ЦПК, ГПК, КПК) стало ключовим кроком до визнання його юридичної сили нарівні з традиційними паперовими документами. Проте, повномасштабна військова агресія рф проти України кардинально змінила контекст цієї трансформації, надавши проблемі цифровізації критичного, геополітичного та гуманітарного виміру. Першочергово йдеться про *масштабну втрату доказової бази* (фізичне знищення архівів, судових установ та паперових матеріалів справ, що у багатьох випадках перетворює цифрову копію на єдине доступне джерело) інформації); *масове створення неформальних цифрових доказів* (війна генерує величезний обсяг цифрового контенту – фото/відеофіксація військових злочинів, свідчення в месенджерах (*Telegram, Viber*), дані геолокації, супутникові знімки та інформація з відкритих державних реєстрів); *правосуддя в умовах доступу "нуль"* (унеможливлення

фізичного збору доказів і проведення традиційних слідчих дій на окупованих територіях або в зоні активних бойових дій).

Актуальність дослідження полягає у нагальній потребі розробки та закріплення нових, адаптованих стандартів допустимості та якості електронних доказів. Відсутність чітких та уніфікованих правил щодо автентичності (хто створив), цілісності (чи не змінювався) та надійності (як зібрано) цифрових даних може призвести до негативних наслідків, а саме: підриву ефективності національного судочинства у справах про воєнні злочини, а також ускладнення притягнення до міжнародної відповідальності та забезпечення компенсаційних механізмів, які є критично важливими для майбутньої відбудови України.

Проблематика електронного доказування традиційно перебуває в центрі уваги як вітчизняної, так і міжнародної юридичної думки. У доктрині України такі науковці як М. Пашковський, О. Пчеліна, В. Романюк, А. Ангелюк, О. Солдатенко висвітлювали теоретичні основи, аналізуючи поняття, природу та місце електронного доказу в системі доказів (предмет, засіб доказування), а також актуальні проблеми, що виникають в окресленій сфері на сучасному етапі в Україні. Серед закордонних науковців, праці яких були присвячені тематиці цифрових доказів, необхідно виокремити B. Guttman, O. Marandici та інших дослідників. Крім теоретичних праць, на формування підходів до електронного доказування суттєво впливає міжнародне регулювання. Практика Європейського суду з прав людини (ЄСПЛ), а також міжнародні регуляторні акти (зокрема, Модельний закон ЮНСІТРАЛ про електронну торгівлю) встановили базові вимоги до електронного підпису та достовірності електронних документів у цивільному обороті, що формує загальний стандарт для національних систем.

Попри значну кількість наукових праць, присвячених електронному доказуванню, наявні дослідження недостатньо охоплюють практичні виклики кримінального провадження в умовах воєнного стану та подальшої повоєнної відбудови України. Ця прогалина є критичною, особливо для розслідування воєнних злочинів та документування завданих ними збитків, в яких електронні дані є ключовими. Зокрема, бракує комплексних наукових розвідок щодо специфіки забезпечення цілісності (*Integrity*) електронних доказів. Актуальним є питання, як юридично коректно фіксувати незмінність доказів, зібраних неформальним шляхом (знімки екрану, повідомлення в месенджерах, відео з особистих телефонів) у зоні бойових дій, де традиційні процедури фіксації (наприклад, слідчий огляд, вилучення) часто недоступні або неможливі. Ця проблема тісно пов'язана з питанням суб'єктів автентифікації. Необхідно визначити належний суб’єкт (судова експертиза, нотаріальне засвідчення, міжнародні комісії, фахівці в галузі комп'ютерної криміналістики), який може підтвердити автентичність цифрових доказів у ситуаціях, якщо традиційні суб'єкти доказування (слідчі, прокурори) не можуть діяти або не мають необхідних технічних можливостей. Невизначеність суб’єкта ставить під загрозу допустимість таких доказів у суді.

Крім того, невирішеною залишається проблема техніко-правової імплементації. Це стосується практичного застосування національних та міжнародних стандартів (наприклад, ДСТУ 4145-2002 щодо кваліфікованих електронних підписів та печаток) для документування воєнних злочинів та майнових збитків. Без чітких протоколів використання цих стандартів існує ризик того, що цінні цифрові докази не будуть прийняті судом через недотримання процесуальних вимог щодо їхньої форми та надійності.

Мета проведеного дослідження полягає у комплексному аналізі впливу запровадженого в Україні воєнного стану та прискореної цифровізації на формування нових, посилених вимог до якості та стандартів допустимості електронних доказів, а також обґрунтуванні практичного значення їх удосконалення для забезпечення

правосуддя та юридичної основи для процесів відбудови України у повоєнний період. Відповідно до поставленої мети було сформульовано такі завдання дослідження: проаналізувати ключові правові та технічні виклики, що виникли у сфері електронного доказування внаслідок військової агресії (наприклад, проблема визнання доказів, зібраних відкритими джерелами, *OSINT*); дослідити та визначити найбільш ефективні правові та технічні механізми забезпечення цілісності та автентичності електронних доказів (зокрема, використання технології блокчейн для фіксації подій, сервіси електронного штампу часу (*Timestamping*), хешування даних); оцінити практичний вплив запропонованих стандартів на якість доказування у найбільш чутливих категоріях справ: про відшкодування збитків (як національних, так і міжнародних) та воєнні злочини; формулювати конкретні, науково обґрунтовані пропозиції щодо удосконалення національного процесуального законодавства та судової практики у сфері електронного доказування з урахуванням викликів воєнного часу.

Результати

Збройний конфлікт масово генерує значні обсяги електронного контенту, який, за своєю суттю та змістом, є неформальним доказом. До цієї категорії належать відеозаписи з особистих мобільних пристроїв, фотофіксація руйнувань, скріншоти комунікацій у месенджерах та матеріали, зібрані з відкритих джерел (*OSINT*) волонтерами та журналістами. Як зазначає М. Пашковський [1], обставини, які можуть бути доведені за допомогою таких доказів, передбачають головний факт і допоміжні факти (наприклад, місцезнаходження осіб, перевірка достовірності інших доказів), а інформація з відкритих джерел може слугувати приводом для внесення відомостей до ЄРДР. Одночасно з цим, наголошує науковець, існують ризики використання доказів з відкритих джерел, які пов'язані з особливостями цифрових доказів і надійністю самого джерела, в аспекті дотримання рекомендацій Протоколу Берклі для забезпечення їхньої належності та достовірності, особливо у провадженнях щодо злочинів проти нацбезпеки та воєнних злочинів.

Ця ключова онтологічна проблема полягає у відсутності процесуальної форми на етапі первинного збору, оскільки традиційне доказове право вимагає, щоб доказ був отриманий належним суб'єктом та оформлений у належній формі (йдеться про протокол). Останнє, зауважує О. Пчеліна [2], вимагає формулювання єдиного підходу та науково-практичних рекомендацій щодо криміналістичних особливостей і порядку огляду місця події під час досудового розслідування злочинів, пов’язаних зі збройною агресією проти України, на підготовчому, робочому та заключному етапах. Традиційне доказове право вимагає, щоб доказ був отриманий належним суб'єктом (слідчим, прокурором) і оформлений у належній формі (протокол). Якщо доказ збирається цивільною особою в умовах хаосу, він, по суті, не має юридичної історії (*Chain of Custody*), що гарантує його незмінність. Ця відсутність контрольованої історії прямо підриває фундаментальні критерії допустимості та надійності доказу. Без належної фіксації залишається відкритим питання про потенційну зміну, редагування або постфактум створення файлу. Як акцентує В. Романюк [3], попри те, що предмет доказування визначає перелік обставин, наявність або відсутність яких потрібно підтвердити за допомогою зібраних доказів у кримінальному провадженні (зокрема, щодо механізму злочину та відшкодування збитків), саме суворі стандарти доказування, які є імперативом у змагальному процесі, створюють значний ризик визнання цінного доказу недопустимим, особливо у справах про воєнні злочини.

Своєю чергою, А. Ангеленюк [4] наголошує, що через недостатність нормативно-правового регулювання та складну правову природу, неналежно оформлені електронні докази наражаються на ризик бути визнаними недопустимими судом. Саме тому, для мінімізації цих ризиків маніпуляцій та фальсифікації, які є невідчужуваними від

цифрової природи доказу, обґрунтовується необхідність законодавчого закріплення техніко-правового імперативу цілісності та автентичності, заснованого на криптографічних гарантіях. Ключовим технічним рішенням, яке надає неформальному доказу презумпцію незмінності, є криптографічне хешування, поєднане з кваліфікованим електронним штампом часу (*TSA*). Електронний файл трансформується унікальний, фіксований за розміром хеш-код (H) за допомогою детермінованої та односпрямованої функції. Навіть мінімальна зміна у вихідних даних призводить до кардинальної зміни H. Порівняння хеш-кодів є об'єктивним, технічно незаперечним доказом ідентичності файлів [5].

Сам хеш-код повинен бути засвідчений кваліфікованим електронним штампом часу від довірчого провайдера, що є відображенням міжнародного протоколу, в якому хешування (описане у наукових працях B. Guttman як метод перевірки цілісності) поєднується з незалежним часовим штампом, забезпечуючи юридично значущу прив'язку даних до конкретного моменту їхнього існування у незмінному стані [6]. Такий підхід розв'язує проблему мінливості цифрової інформації, оскільки кваліфікований електронний штамп часу надає доказовий слід автентичності (*audit trail*), який засвідчує, що хеш-код, а отже, і сам доказ, не був змінений після фіксації. Як відмічає О. Солдатенко [7], недосконалість чинних норм щодо порядку збирання та фіксації електронної інформації часто призводить до визнання її недопустимою. Це підтверджує тезу про те, що законодавче визнання Протоколу фіксації, який містить метадані, хеш-код доказу та КЕП/КЕПл відповідного суб'єкта, повинно стати достатнім первинним доказом цілісності, оскільки воно процесуально закріплює найкращі світові технічні практики, інтегруючи їх у національну систему допустимості доказів.

Для забезпечення незалежного та глобально верифікованого ланцюга зберігання (*Chain of Custody*), особливо для доказів, зібраних поза українською юрисдикцією, необхідно інтегрувати технологію блокчейн. Внесення хеш-коду доказу до розподіленого реєстру (блокчейну) робить факт фіксації незмінним і публічно підтвердженим. Блокчейн ефективно виключає можливість ретроактивних змін, слугуючи потужним непрямим доказом автентичності та надійності у міжнародних інстанціях, в яких незалежність джерела є критичною. O. Marandici [8] підкреслює важливість доказового права в міжнародних інстанціях, зокрема в МКС, та наголошує, що, попри гнучкість правил (вільну оцінку доказів), надійність та автентичність джерела є визначальними критеріями для допустимості доказів у міжнародному правосудді. Саме тому ланцюг зберігання (*Chain of Custody*) є найуразливішим етапом, оскільки будь-яке його порушення підриває довіру до легітимності доказу у суді. Отже, інтеграція технології блокчейн у процес фіксації та зберігання хеш-кодів є унікальним юридичним рішенням, що забезпечує глобально верифікований, незмінний слід, який знімає критичні питання щодо надійності джерела, які є центральними у доказовій практиці,

Вимоги до електронних доказів у справах про відшкодування збитків та відбудову повинні бути адаптовані із зосередженням на Кваліфікованій електронній печатці (КЕПл). Масове документування збитків та руйнувань через державні реєстри при цьому повинно супроводжуватися засвідченням таких масивів даних як КЕПл відповідного державного органу (наприклад, місцевої адміністрації). Це надає даним юридичну презумпцію достовірності, мінімізуючи необхідність індивідуальної судової перевірки кожного документа та забезпечуючи оперативність подання доказів у компенсаційних механізмах. Крім того, критично важливо реформувати судову комп'ютерно-технічну експертизу (СКТЕ), уніфікувавши методики аналізу метаданих, геолокації та верифікації контенту відповідно до міжнародних стандартів цифрової криміналістики (*forensics*). Таким чином, можна провести порівняння традиційного та техніко-правового підходу до електронного доказу (Табл. 1).

Таблиця 1

Порівняння традиційного та техніко-правового підходу до електронного доказу

Критерій	Традиційний процесуальний доказ	Неформальний цифровий доказ (без фіксації)	Техніко-правовий доказ (з криптографією)
Критерій допустимості	Належна форма (протокол) та суб'єкт.	Відсутність юридичної історії.	Технічна цілісність (хеш-код) та час (TSA).
Chain of Custody	Забезпечується процесуальними діями слідчого/прокурора.	Фактично відсутній або не підтверджений.	Забезпечується криптографічними механізмами, блокчейном.
Ризик маніпуляцій	Низький, за умови дотримання процедури.	Високий, легко оспорюється захистом.	Мінімальний, технічно верифікований і незаперечний.
Механізм надійності	Презумпція достовірності (законна форма).	Вимагає складної судової експертизи автентичності.	Презумпція незмінності (хеш + TSA/блокчейн).
Значення для суду	Високе.	Низьке, високий ризик недопустимості.	Презумпція незмінності (хеш + TSA/блокчейн).

Імплементація викладених техніко-правових стандартів вимагає внесення прямих норм до процесуальних кодексів (ЦПК, ГПК, КПК) та інших підзаконних актів України. Йдеться про:

- пряме визнання криптографічних методів. Законодавче визнання хешування та електронного штампу часу як достатніх методів підтвердження цілісності електронного доказу;
- розширення суб'єктів засвідчення. Розширення переліку суб'єктів, які можуть засвідчувати цілісність (включно зі спеціалізованими державними або акредитованими міжнародними організаціями);
- імператив КЕПл. Встановлення вимог до використання КЕПл для масового засвідчення державних реєстрів пошкодженого майна.

Перераховані кроки є необхідним фундаментом для забезпечення правової стійкості України в умовах військової агресії та успішної реалізації процесів її повоєнної відбудови та міжнародного правосуддя.

Висновки

Військова агресія проти України виступила каталізатором незворотної трансформації доказового права. Виявлено, що традиційна процесуальна форма збору доказів виявилася неадекватною для фіксації масового, неформального цифрового контенту, генерованого цивільними особами та *OSINT*-джерелами у зоні конфлікту. Головний виклик полягає у доведенні цілісності (незмінності) та автентичності таких доказів, що є критичним для їхньої допустимості як у національних, так і в міжнародних судах. Дослідженням обґрунтовано, що гарантування надійності електронного доказу має бути перенесено з суб'єктивної сфери експертної оцінки до об'єктивної техніко-правової фіксації. Ключовими інструментами для цього є:

- криптографічне хешування та електронний штамп часу (Timestamping). Забезпечують технічно незаперечну фіксацію стану та часу існування доказу, що є необхідною умовою для презумпції цілісності;
- технологія Блокчейн. Пропонується як децентралізований механізм для забезпечення незмінного ланцюга зберігання (Chain of Custody), що критично важливо для міжнародної легітимізації доказів воєнних злочинів.

Удосконалення стандартів електронного доказування має стратегічне значення для процесів відбудови. Забезпечення високої якості та юридичної сили електронних реєстрів збитків, засвідчених кваліфікованою електронною печаткою (КЕПл), є основою для успішного використання компенсаційних механізмів та подання позовів проти держави-агресора.

На підставі отриманих наукових результатів, для удосконалення національного процесуального законодавства та судової практики, пропонується наступне:

1. Необхідно внести зміни до процесуальних кодексів (ЦПК, ГПК, КПК) та Закону України «Про електронні довірчі послуги», які б прямо визнавали криптографічне хешування та використання кваліфікованого електронного штампу часу як достатній і пріоритетний спосіб підтвердження цілісності електронного доказу, зібраного поза традиційними слідчими діями. Такий протокол фіксації має мати преюдиційний характер щодо факту незмінності даних.
2. Розширення та регламентація суб'єктів фіксації. Необхідно законодавчо розширити перелік суб'єктів, уповноважених проводити фіксацію електронних доказів з гарантуванням їхньої цілісності. Це включає не лише нотаріусів, а й, за умов воєнного стану, акредитовані державні органи (наприклад, спеціалізовані відділи Міністерства цифрової трансформації України) або міжнародні неурядові організації, що діють відповідно до українського законодавства, шляхом використання ними КЕПл для засвідчення протоколів фіксації хеш-кодів.
3. Реформування судової експертизи. Необхідна стандартизація та уніфікація методик проведення судової комп'ютерно-технічної експертизи (СКТЕ). Методики повинні бути орієнтовані на верифікацію метаданих, аналіз контенту з соціальних мереж та месенджерів, а також на ідентифікацію ознак застосування технологій штучного інтелекту (наприклад, Deepfake). Це дозволить експертам швидко та ефективно працювати з неформальними доказами, використовуючи міжнародні стандарти цифрової криміналістики (Digital Forensics).

Перспективи подальших наукових розвідок полягають у детальному аналізі практичного впровадження блокчейн-технологій для створення єдиного, захищеного, децентралізованого реєстру доказів воєнних злочинів та розробці модельних процесуальних норм щодо допустимості доказів, отриманих в порядку міжнародно-правової допомоги (наприклад, з міжнародних баз даних OSINT), які мають ключове значення для притягнення агресора до відповідальності.

Список використаних джерел

1. Пашковський М. Обставини, що мають значення для кримінального провадження, та належність цифрових доказів з відкритих джерел. *Наукові перспективи*. 2024. № 10(52). DOI: 10.52058/2708-7530-2024-10(52)-984-998
2. Пчеліна О., Фоміна Т. Особливості проведення огляду місця події під час досудового розслідування злочинів, пов’язаних зі збройною агресією проти

України. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2024. № 2. С. 251–259. DOI: 10.31733/2078-3566-2023-2-251-259

3. Anheleniuk A. M. The use of electronic evidence in the criminal procedural law of Ukraine (problematic issues). *Uzhhorod National University Herald. Series: Law*. 2023. Vol. 2, № 79. P. 214–218. DOI: 10.24144/2307-3322.2023.79.2.32

4. Романюк В. Предмет доказування у кримінальних провадженнях щодо економічних злочинів. *Наукові перспективи*. 2023. № 2(32). DOI: 10.52058/2708-7530-2023-2(32)-413-422

5. Applied and methodical aspects of using hash functions for information security / Y. Zhdanova et al. *Cybersecurity: education, science, technique*. 2020. Vol. 4, № 8. P. 85–96. DOI: 10.28925/2663-4023.2020.8.8596

6. A model checking-based framework for testing security properties of protocols under development / J. Yao et al. *Computer Networks*. 2025. Vol. 265. P. 111259. DOI: 10.1016/j.comnet.2025.111259

7. Солдатенко О., Яровий О. Проблема допустимості електронних доказів у кримінальному провадженні. *Актуальні питання у сучасній науці*. 2025. № 9(39). DOI: 10.52058/2786-6300-2025-9(39)-768-778

8. Transnational gathering of electronic evidences: challenges and perspectives in the European Union / O. Marandici et al. *The Journal of the National Institute of Justice*. 2022. No. 3(62). P. 54–60. DOI: 10.52277/1857-2405.2022.3(62).08