Перевірка автентичності електронних доказів в адміністративному судочинстві

Володимир Горбалінський

доктор юридичних наук, суддя, голова суду, Дніпропетровський окружний адміністративний суд,
м. Дніпро, Україна, ORCID: https://orcid.org/0000-0002-6203-6151, e-mail: gorbalinskiy@gmail.com

Розглянуто підходи до перевірки автентичності електронних доказів в адміністративному судочинстві й окреслено основні ризики їх недостовірності. Виокремлено критерії походження, цілісності та контексту електронних даних, а також практичні способи їх підтвердження через належну форму подання, метадані, електронний підпис, часові позначки й експертну перевірку. Сформульовано орієнтири оцінки електронних доказів за умов заперечення їх справжності.

Ключові слова: *електронні докази; автентичність; адміністративне судочинство; електронний підпис; метадані; цілісність даних; допустимість доказів.*

Verification of the Authenticity of Electronic Evidence in Administrative Proceedings

Volodymyr Horbalinskyi

Approaches to verifying the authenticity of electronic evidence in administrative proceedings are examined, and the main risks of its unreliability are outlined. Criteria of origin, integrity, and context of electronic data are identified, as well as practical methods of confirmation through proper submission form, metadata, electronic signatures, time stamps, and expert examination. Guidelines for evaluating electronic evidence where its genuineness is contested are formulated.

Keywords: *electronic evidence; authenticity; administrative proceedings; electronic signature; metadata; data integrity; admissibility of evidence.*

Перевірка автентичності електронних доказів в адміністративному судочинстві є однією з основних практичних проблем сучасного доказування, оскільки цифрова інформація легко копіюється, редагується та виривається з контексту, а суд водночас має ухвалити рішення на підставі доказів, яким можна довіряти. У цьому сенсі автентичність електронного доказу слід розуміти як підтвердженість його походження, цілісності та зв'язку з юридично значущими обставинами, тобто здатність суду відтворити відповідь на три базові питання: що саме є доказом, звідки він отриманий і чи не змінювався він після створення або вилучення.

Нормативна рамка адміністративного процесу виходить з того, що електронні докази охоплюють широкий спектр цифрових даних, від електронних документів і фото чи відео до вебсторінок, повідомлень, метаданих та баз даних, а подаються вони або в оригіналі, або в електронній копії, засвідченій електронним підписом, при цьому паперова копія електронного доказу не ототожнюється з письмовим доказом і має допоміжний характер. Саме тому перевірка автентичності в адміністративній справі починається не з оцінки змісту, а з процесуально коректної форми подання та ідентифікації оригіналу, носія і способу отримання [1].

Практично доцільно виділяти три групи ризиків автентичності. Перша група, ризики походження, коли сторона не може переконливо показати, хто створив файл або повідомлення, з якого облікового запису, на якому пристрої чи в якій системі. Друга група, ризики цілісності, коли незрозуміло, чи не змінювався файл, скриншот або запис після створення, чи не монтувалося відео, чи не редагувалися метадані. Третя група, ризики контексту, коли доказ вирвано з загального ланцюга подій, наприклад подається фрагмент переписки без попередніх повідомлень, або скриншот вебсторінки без відомостей про дату і час фіксації та без підтвердження URL-адреси. Усі три групи ризиків зазвичай проявляються в суді через типові заперечення опонента, це не мій акаунт, це змонтовано, це вирвано з контексту, це копія невідомого походження, і тому сторона, яка подає електронний доказ, має одразу будувати процесуальну відповідь на кожне з таких заперечень.

Окремий практичний блок стосується електронних документів як найбільш

формалізованого виду електронних доказів. Якщо електронний документ створений і використовується в межах електронного документообігу, питання автентичності значною мірою вирішується через реквізити, ідентифікацію автора, структуру документа, можливість перевірки підпису та логіку зберігання. Тобто для суду важливо, щоб документ був поданий разом із даними, які дозволяють перевірити його як документ, а не як картинку з текстом. У цьому контексті коректна стратегія сторони полягає в тому, щоб надавати не лише візуальне відображення, а й файл у форматі, який зберігає технічні властивості, а також пояснювати, в якій системі він створений, як циркулював і де зберігався [2].

Для доказів, де основним є підтвердження автора і незмінності, центральне значення мають електронні довірчі механізми, насамперед електронний підпис і часові позначки, які дозволяють підтвердити, хто саме підписав документ і що з моменту накладення підпису вміст не змінювався без втрати валідації. Практична цінність таких інструментів для адміністративної справи полягає в тому, що вони переводять дискусію з рівня припущень на рівень технічної перевірки, суд може перевірити підпис, а опонент змушений доводити конкретні дефекти, а не просто заперечувати достовірність. Для сторони це означає, що подання електронних доказів у вигляді електронних копій, засвідчених підписом, і додавання технічних файлів перевірки підпису суттєво підвищують переконливість доказу [3].

Найскладнішими з погляду автентичності є скриншоти, повідомлення з месенджерів, контент із соціальних мереж і вебсторінок, тому що вони часто подаються як зображення або текстова роздруківка без метаданих. Практично коректний підхід полягає в тому, щоб фіксувати такі докази з максимальною відтворюваністю: зазначати точний URL, дату і час фіксації, надавати повні ланцюги повідомлень, а не окремі фрагменти, додавати технічні дані, якщо вони доступні, наприклад експорти чатів, заголовки електронної пошти, журнали подій, а також пояснювати спосіб отримання, хто саме здійснив фіксацію і на якому носії зберігається оригінал. Якщо доказ є принципово спірним, оптимальним інструментом стає комп'ютерно-технічна експертиза, яка перевіряє не зміст як правову оцінку, а саме технічні параметри, метадані, ознаки редагування та відповідність файлів заявленому походженню. У підходах Верховного Суду акцентується, що оцінка електронних доказів має спиратися на критерії допустимості та на концепцію цілісності електронних даних, яка передбачає необхідність предметного спростування, а не суто декларативного заперечення [4].

У висновках слід підкреслити, що перевірка автентичності електронних доказів в адміністративному судочинстві є не одноразовою технічною дією, а елементом доказової стратегії, який має бути закладений ще на стадії підготовки матеріалів до суду. Чим раніше сторона забезпечує ідентифікацію походження, підтвердження цілісності та відтворюваність контексту, тим менше простору залишається для процесуальних спорів про допустимість і тим більше уваги суд переходить приділяти змісту і релевантності доказу. Водночас саме практика електронних доказів показує, що успіх залежить не від кількості цифрових файлів у справі, а від здатності сторони пояснити суду їх джерело, шлях збереження та технічні гарантії незмінності, а також від готовності підтвердити ці елементи або через довірчі послуги, або через експертну перевірку.

Перелік джерел посилання

1. Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text (дата звернення: 28.01.2026).
2. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 28.01.2026).
3. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 28.01.2026).
4. Суддя Верховного Суду проаналізувала критерії допустимості й належності електронних доказів та презумпцію їх цілісності / Верховний Суд : офіц. вебсайт. 06.02.2025. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1751385/ (дата звернення: 28.01.2026).