

Резворович К. Р.,*доктор юридичних наук, доцент,
завідувач кафедри цивільно-правових дисциплін
Дніпровського державного університету внутрішніх справ
ORCID: <https://orcid.org/0000-0003-3500-6763>***Лисюк Я. О.,***курсант факультету підготовки фахівців
для органів досудового розслідування Національної поліції України
Дніпровського державного університету внутрішніх справ
ORCID: <https://orcid.org/0009-0002-5285-1221>*

ФАЛЬШИВІ ДОКАЗИ В ЦИВІЛЬНОМУ ПРОЦЕСІ: БОРІТЬБА З DEERFAKE ТА ІНФОРМАЦІЙНИМИ МАНІПУЛЯЦІЯМИ

Анотація. Сучасний розвиток цифрових технологій, зокрема штучного інтелекту, створив нові виклики для судочинства. Одним із найбільш загрозливих явищ у цивільному процесі є поява та використання фальшивих доказів, створених за допомогою технології «deepfake» або інших методів цифрової маніпуляції інформацією. Такі докази можуть істотно впливати на результат розгляду справи, підтримуючи принципи змагальності, об'єктивності та справедливості судового процесу. У статті розглядаються правові, етичні та технічні аспекти проблеми визнання, виявлення та протидії фальсифікованим доказам у цивільному процесі України. Аналізується чинне законодавство, практика судів, а також міжнародний досвід щодо допустимості цифрових доказів і відповідальності за їх підроблення.

Окрему увагу приділено питанню експертизи цифрових матеріалів, ролі судових експертів у встановленні автентичності відео, фото та аудіозаписів, а також необхідності підвищення цифрової компетентності суддів і адвокатів. Запропоновано напрями удосконалення процесуального законодавства, зокрема запровадження спеціальної процедури перевірки достовірності електронних доказів, створення національного центру цифрової експертизи та розроблення етичних стандартів використання штучного інтелекту у судовій сфері. Розв'язання проблеми фальшивих доказів вимагає комплексного підходу, що поєднує правові, технічні та освітні інструменти, спрямовані на зміцнення довіри до судової системи в умовах цифрової трансформації.

Ключові слова: цивільний процес, фальшиві докази, deepfake, цифрові технології, інформаційна безпека, судова експертиза, електронні докази.

Постановка проблеми. З поширенням цифрових технологій судовий процес зіткнувся з новими викликами достовірності доказів. Фото-, відео- та аудіозаписи, які раніше сприймалися як надійні джерела доказів, нині можуть бути створені або змінені за допомогою штучного інтелекту. Технологія «deepfake» дозволяє генерувати зображення чи голоси, практично не відрізняючи їх від реальних. У цивільних справах, де доказування часто базується на електронних документах, таких як листування, записи чи відео, виникає ризик маніпулювання фактами.

Проблема ускладнюється відсутністю чітких процедур перевірки цифрових доказів у Цивільному процесуальному кодексі України (далі – ЦПК України) та обмеженою технічною компетентністю учасників процесу. Необхідність вироблення ефективних правових і технічних механізмів боротьби з фальшивими доказами є ключовою умовою забезпечення справедливого судочинства.

Предметом дослідження є правові, етичні та технічні механізми виявлення, визнання недопустимими та протидії фальшивим доказам (зокрема, створеним за допомогою «deepfake» та інших методів цифрової маніпуляції) у цивільному процесі України.

Об'єктом дослідження є цивільний процес України в умовах цифрової трансформації, зокрема відносини, що виникають при поданні, дослідженні та оцінці електронних доказів (відео-, аудіо-, фотофіксація, цифрові документи), які можуть бути об'єктом маніпуляції за допомогою «deepfake» або інших інформаційних технологій.

Аналіз останніх джерел та публікацій. У наукових працях останніх років відзначається зміщення акценту з традиційних питань допустимості доказів на комплексне вивчення загроз цифрових фальсифікацій та необхідність формування адаптивних правових механізмів.

Тематика електронних доказів та цифрових маніпуляцій ґрунтовно розкривається у працях Резворович К.Р., Юніної М.П., Юніна О.С., Круглової О.О. та Ділігула А.С., які підкреслюють проблеми процесуального статусу електронних доказів та недосконалість механізмів перевірки їх достовірності у цивільному судочинстві.

Значний внесок зроблено також Кондрат'євою Л.А., котра аналізує труднощі оцінки електронних доказів у період підвищених інформаційних ризиків під час воєнного стану, вказуючи на потребу у спеціалізованій цифровій експертизі.

Актуальні аспекти цифрової безпеки та її правового забезпечення розкриті у новітніх працях Kulchitskyi T., Rezvorovych K., Povalena M., Dutchak S. та Kramar R., які аналізують трансформацію правового регулювання в умовах стрімкої цифровізації та наголошують на необхідності адаптації законодавства до

нових технологічних загроз. Дослідники акцентують увагу на потребі створення цілісної системи правових гарантій цифрової безпеки, яка охоплюватиме виявлення цифрових фальсифікацій, регулювання використання штучного інтелекту, а також вдосконалення експертних процедур. Їхні висновки підкреслюють, що без оновлення законодавства суд не може ефективно реагувати на загрозу фальшивих доказів.

Варто також відзначити роботи Ткаченка О., Ільєнка А., Улічева О., Мелешка Є. та Смірнова О., які присвячені аналізу інформаційних впливів у соціальних мережах – саме у тих середовищах, де активно поширюється фальсифікований контент та deepfake-матеріали. Автори доводять, що соціальні платформи є ключовими каналами маніпулятивного впливу, а отже, у судових спорах зростає частка доказів, отриманих із цих джерел. Вони підкреслюють небезпеку неконтрольованого поширення синтетичних зображень, аудіо- та відеофайлів, які в подальшому можуть використовуватися як докази у цивільних справах. Це потребує від судової системи здатності оперативно ідентифікувати такі ризики та застосовувати інструменти перевірки автентичності.

На міжнародному рівні технічні аспекти цифрових фальсифікацій ґрунтовно досліджені такими відомими вченими, як Hany Farid та Luisa Verdoliva, які розробляють алгоритми детекції deepfake-контенту та цифрових маніпуляцій. У роботах Yisroel Mirsky, Wenke Lee та інших розглядається природа створення штучно згенерованих медіа та методи їх виявлення за допомогою цифрової криміналістики та штучного інтелекту.

Виклад основного матеріалу. Цивільне судочинство є одним із основних механізмів захисту прав і свобод громадян. Його ефективність безпосередньо залежить від достовірності доказів, які подають сторони під час розгляду справи.

Відповідно до статті 76 Цивільного процесуального кодексу України, доказами є будь-які дані, на підставі яких суд встановлює наявність або відсутність обставин (фактів), що обґрунтовують вимоги і заперечення учасників справи, та інших обставин, які мають значення для вирішення справи [1].

Слід зазначити, що на думку Kulchytskyi T., Rezvorovych K., Povalena M., Dutchak S. і Kramar R., цифрові трансформації створюють принципово новий формат ризиків для судового процесу, що вимагає адаптації законодавства й оновлення інструментів доказування [3].

На думку Ткаченка О., Ільєнка А., Улічева О., Мелешка Є. та Смірнова О., соціальні мережі є головним середовищем поширення фальсифікованих фото-, відео- та аудіоматеріалів, які згодом можуть стати доказами у цивільних справах, що суттєво ускладнює їхню судову оцінку [7].

У добу цифровізації та стрімкого розвитку штучного інтелекту з'явилася нова загроза об'єктивності судового процесу – використання фальшивих доказів, створених за допомогою технології «deepfake» та інших інструментів цифрової маніпуляції. Ця проблема не лише підриває принципи справедливості та верховенства права, а й ставить під сумнів довіру до всієї судової системи.

Технологія «deepfake» – це інструмент, який використовує алгоритми глибокого навчання для створення реалістичних, але повністю змінених або вигаданих зображень, відео чи аудіозаписів [4, с. 11].

Фальшивість доказів може встановлюватись різними шляхами, наприклад, шляхом допиту свідків, співставленням з іншими

доказами. Наприклад, свідок може повідомити суду, що він бачив, як підроблювався документ, або документ, який має містити голографічний захист, не містить його. У таких випадках суд без ускладнень може встановити, що доказ є фальшивим.

Важким у вирішенні питання про фальшивість доказів є те, що тут виникає необхідність встановлення того, що документ не відображає дійсності, наприклад, підпис у документі чи почерк не належать відповідній особі або печатка є підробною. Визначення цього потребує спеціальних знань, а тому вимагає призначення експертизи, що займає певний час. До того ж сторони можуть і не заявити клопотання про її проведення.

Відтак, «deepfake» – це методика синтезу зображення людини, яка базується на штучному інтелекті. Використовують для поєднання і накладення одних зображень та відео на інші зображення або відеоролики.

У початкових етапах розвитку ця технологія мала переважно розважальне або експериментальне значення, однак сьогодні вона активно використовується для маніпулювання інформацією, створення дезінформації та навіть підроблення доказів у судових справах.

У цивільному процесі такі фальсифікації можуть мати серйозні наслідки. Наприклад, змонтоване відео може створити ілюзію певних дій, яких насправді не було, а підроблений аудіозапис – імітувати розмову між сторонами. За відсутності належної експертизи суд може сприйняти такі матеріали як достовірні, що призведе до ухвалення неправомірного рішення. Таким чином, «deepfake» не просто порушує правила процесу, а й руйнує довіру до самої ідеї доказовості в суді [5, с. 10].

Основна складність боротьби з фальшивими доказами полягає у високому рівні технологічності таких підробок. Сучасні deepfake-алгоритми здатні настільки точно відтворювати міміку, інтонації та особливості голосу людини, що навіть досвідчені експерти не завжди можуть одразу визначити підробку [6, с. 8]. У більшості випадків виявлення таких фальсифікацій потребує залучення спеціалістів із цифрової криміналістики, використання штучного інтелекту для зворотного аналізу даних та порівняння з оригінальними джерелами інформації.

Проблемою є також відсутність чітко врегульованої процедури перевірки автентичності цифрових доказів у ЦПК України. Суддя часто не має необхідних інструментів і компетенцій для самостійної оцінки технічних характеристик електронних доказів. Це створює ситуацію, коли рішення щодо достовірності доказу може ґрунтуватися не на об'єктивних критеріях, а на припущеннях чи формальних ознаках [2, с. 91].

У світовій практиці питання боротьби з «deepfake» активно обговорюється як на правовому, так і на технічному рівнях. У США, наприклад, у кількох штатах ухвалені закони, які прямо забороняють створення та розповсюдження «deepfake», якщо вони використовуються для введення в оману або завдання шкоди. У Європейському Союзі питання достовірності цифрових доказів регулюється в межах Загального регламенту із захисту даних (GDPR) та директив щодо електронних доказів, що передбачають створення спеціалізованих експертних лабораторій для перевірки автентичності цифрових матеріалів.

У США, наприклад, у кількох штатах ухвалені закони, які прямо забороняють створення та розповсюдження «deepfake», якщо вони використовуються для введення в оману або завдання шкоди. Зокрема, станом на 2025 рік, закони проти «deepfake» набули чинності у Вашингтоні та Пенсильванії, де передбачено

цивільну відповідальність за несанкціоноване використання зображень осіб у фальсифікованих матеріалах, з штрафами до 10 000 доларів США за порушення.

Загалом, 45 штатів США ввели законодавство щодо сексуально експліцитних «deepfake», включаючи кримінальну відповідальність за їх створення та поширення (наприклад, у Каліфорнії – до 1 року ув'язнення за Act 35 від липня 2025 року). На федеральному рівні ключовим є «Take It Down Act» (ухвалений у червні 2025 року), який криміналізує публікацію неконсенсусних інтимних зображень, включаючи «deepfake», та зобов'язує онлайн-платформи (як-от Meta чи X) впроваджувати механізми швидкого видалення такого контенту за скаргою жертви, з штрафами до 150 000 доларів за ігнорування. Крім того, у контексті виборів 27 штатів (включаючи Техас і Вірджінію) заборонили «deepfake» у політичній рекламі без чіткого маркування, з акцентом на захист демократії від маніпуляцій. Ці норми часто інтегруються з правом на публічність (right of publicity), дозволяючи жертвам позоватися за моральну шкоду.

У Європейському Союзі питання достовірності цифрових доказів регулюється в межах Загального регламенту із захисту даних (GDPR), що передбачають створення спеціалізованих експертних лабораторій для перевірки автентичності цифрових матеріалів. Зокрема, Регламент eIDAS 2.0 (оновлений у 2024 році та чинний з 2025) [8] встановлює стандарти для електронних підписів і сертифікації цифрових доказів, вимагаючи від постачальників послуг (як-от нотаріусів чи судових експертів) використання кваліфікованих інструментів для верифікації автентичності, включаючи блокчейн-технології для фіксації метаданих.

Щодо «deepfake», ключовим є EU AI Act [10] (вступив у силу в серпні 2024, з поетапним застосуванням з лютого 2025), який класифікує «deepfake» як системи AI з обмеженим ризиком (limited risk), зобов'язуючи розробників і користувачів маркувати синтетичний контент (наприклад, водяними знаками або метатегами) та впроваджувати інструменти детекції, з штрафами до 35 млн євро або 7% глобального обороту за порушення.

Україна лише розпочинає формування правових механізмів у цій сфері. Окремі норми щодо електронних доказів уже закріплені в ЦПК України, проте вони не враховують виклики, пов'язані з розвитком штучного інтелекту. Необхідно доповнити законодавство спеціальними положеннями, які б визначали поняття цифрової фальсифікації, порядок її виявлення та наслідки для сторін, які свідомо подають фейкові матеріали до суду.

Одним із ключових інструментів у боротьбі з фальшивими доказами є судова експертиза цифрових матеріалів. Експерти з комп'ютерної техніки, аудіо- та відеоаналізу можуть встановити ознаки монтажу, визначити джерело походження файлу, час його створення та можливі зміни. Проте для ефективної роботи таких експертів необхідна державна підтримка, розвиток лабораторій і впровадження сучасних технологій аналізу даних [9].

Крім того, варто підвищувати рівень цифрової грамотності суддів, адвокатів і прокурорів. У сучасних умовах суддя повинен не лише знати норми процесуального права, а й розуміти основні принципи функціонування цифрових технологій. Це дозволить більш критично оцінювати подані електронні матеріали, своєчасно призначати експертизи та запобігати використанню фальшивих доказів.

Поширення «deepfake» має не лише правові, а й глибокі етичні наслідки. Фальсифікація доказів підриває не лише справедливість конкретної справи, а й репутацію судової системи

в цілому. Громадяни втрачають віру в те, що суд може відрізнити правду від маніпуляції. Тому боротьба з інформаційними підробками має відбуватися не лише через санкції, а й через формування культури цифрової відповідальності та професійної етики учасників процесу.

Варто також запроваджувати просвітницькі програми, спрямовані на підвищення обізнаності суспільства щодо небезпеки фальшивих цифрових матеріалів. Це сприятиме формуванню правової свідомості та відповідальному використанню технологій.

Проблема фальшивих доказів у цивільному процесі є складним і багатовимірним явищем, що потребує комплексного підходу. Технології «deepfake» відкривають нові горизонти для маніпуляцій, але водночас стимулюють удосконалення судової системи та законодавства. Для ефективної протидії необхідно:

- а) внести до законодавства положення про цифрову фальсифікацію та відповідальність за подання підроблених електронних доказів;
- б) створити національний центр цифрової експертизи для перевірки автентичності матеріалів;
- в) розробити стандарти зберігання, подання та перевірки електронних доказів;
- г) впровадити системне навчання суддів та юристів з питань цифрової безпеки;
- ґ) підвищувати цифрову грамотність суспільства в цілому.

Лише поєднання правових, технологічних і освітніх заходів дозволить мінімізувати ризики інформаційних маніпуляцій і забезпечити головне – справедливість судового процесу, заснованого на істині, а не на ілюзії.

Висновки. Фальсифікація доказів із використанням технологій «deepfake» становить серйозну загрозу для цивільного процесу. Система правосуддя має адаптуватися до цифрової реальності шляхом: удосконалення процесуального законодавства щодо перевірки достовірності електронних доказів; впровадження судово-технічної експертизи цифрових матеріалів як обов'язкового етапу при сумнівах у їх автентичності; створення спеціалізованих державних лабораторій цифрової експертизи; підвищення цифрової грамотності суддів, адвокатів і експертів; формування етичних стандартів використання штучного інтелекту у правовій сфері.

Комплексна реалізація цих заходів дозволить мінімізувати ризики інформаційних маніпуляцій, забезпечити захист прав учасників процесу та зміцнити довіру суспільства до судової системи.

Література:

1. Цивільний процесуальний кодекс України. *Відомості Верховної Ради України* (ВВР), 2004, № 40-41, 42, ст.492.
2. Кондрат'єва Л. А. Електронні докази в цивільному судочинстві в період воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 3. С. 90–93.
3. Кульчицький Т., Резворович К., Повалена М., Дутчак С. та Крамар Р. Правове регулювання кібербезпеки в контексті цифрової трансформації українського суспільства. 2024. ст. 443–460.
4. Цивільний процес : навч. посіб. кол. авт. Резворович К.Р., Юнін О.С., Юніна М.П. та ін. Дніпро. ДДУВС. 2023. 224 с.
5. Цивільне право : навч. практикум кол. авт. Резворович К.Р., Юніна М.П., Ділігул А.С. та ін. Дніпро. ДДУВС. 2022. 220 с.
6. Повноваження поліції щодо охорони цивільних прав та свобод : метод. рек. щодо організації та проведення квесту. кол.

авт. Резворович К.Р., Круглова О.О., Юніна М.П. та ін. Дніпро. Видавець Біла К.О. 2021. 16 с.

7. Ткаченко О., Ільєнко А., Улічев О., Мелешко Є., Галата Л. Сучасні дослідження інформаційних впливів у соціальних мережах. «Кібербезпека: освіта, наука, техніка», 2025. № 27, с. 120–140.
8. Take It Down Act. URL: <https://www.congress.gov/bill/119th-congress/senate-bill/146> (дата звернення – 07.11.2025).
9. EU AI Act. URL: <https://artificialintelligenceact.eu/> (дата звернення – 07.11.2025)
10. Регламент eIDAS 2.0. URL: [https://www.european-digital-identity-regulation.com/European_Digital_Identity_Regulation_Articles_\(Regulation_EU_2024_1183\).html](https://www.european-digital-identity-regulation.com/European_Digital_Identity_Regulation_Articles_(Regulation_EU_2024_1183).html) (дата звернення – 07.11.2025).

Rezvorovych K., Lysiuk Ya. False evidence in civil proceedings: fighting deepfakes and information manipulations

Summary. The modern development of digital technologies, in particular artificial intelligence, has created new challenges for the judiciary. One of the most threatening phenomena in civil proceedings is the emergence and use of false evidence created using «deepfake» technology or other methods of digital manipulation of information. Such evidence can significantly affect the outcome of the case, undermining the principles of adversarial, objectivity and fairness of the judicial process. The article examines the legal, ethical and technical aspects of the problem of recognition, detection and counteraction to falsified evidence in the civil process of Ukraine. The current legislation, court practice, as well as

international experience regarding the admissibility of digital evidence and liability for its forgery are analyzed.

Special attention is paid to the issue of examination of digital materials, the role of forensic experts in establishing the authenticity of videos, photos and audio recordings, as well as the need to improve the digital competence of judges and lawyers. Directions for improving procedural legislation are proposed, in particular, the introduction of a special procedure for verifying the authenticity of electronic evidence, the creation of a national center for digital expertise, and the development of ethical standards for the use of artificial intelligence in the judicial sphere. Solving the problem of false evidence requires a comprehensive approach that combines legal, technical, and educational tools aimed at strengthening trust in the judicial system in the context of digital transformation.

As a conclusion, it is noted that the falsification of evidence using «deepfake» technologies poses a serious threat to civil proceedings. The justice system must adapt to the digital reality by: improving procedural legislation on verifying the authenticity of electronic evidence; introducing forensic examination of digital materials as a mandatory stage in case of doubts about their authenticity; creating specialized state laboratories for digital expertise; increasing the digital literacy of judges, lawyers, and experts; forming ethical standards for the use of artificial intelligence in the legal sphere.

Key words: civil procedure, fake evidence, deepfake, digital technologies, information manipulation, forensic expertise, electronic evidence.



Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Дата першого надходження статті до видання: 10.06.2026

Дата прийняття статті до друку після рецензування: 08.07.2026

Дата публікації (оприлюднення) статті: 10.09.2026