

3. Школьник І. О., Волохата К. О. Фінансова безпека держави: теоретичні засади та практичні аспекти в Україні // Економіка та держава. 2023. № 8. С. 12–18.

Амбруш Д. Л., здобувачка освіти,
Коваль О.М., к.ю.н., доц.
Київський національний університет
технологій та дизайну

ПРАВОВЕ РЕГУЛЮВАННЯ ДІПФЕЙКІВ: ВИКЛИКИ ДЛЯ СИСТЕМИ ДОКАЗІВ У ЦИФРОВУ ЕПОХУ

Розвиток цифрових технологій на межі першої та другої чвертей ХХІ століття ознаменувався якісним стрибком у сфері синтезування медіаконтенту, що призвело до виникнення феномену дїпфейків. Термін «дїпфейк» (DeepFake), що походить від поєднання понять «глибинне навчання» (Deep Learning) та «підробка» (Fake), відображає складний процес використання штучного інтелекту для створення надзвичайно реалістичних зображень, аудіо- та відеоматеріалів.

На відміну від традиційних методів маніпуляції медіа, таких як ретушування або монтаж, дїпфейки базуються на алгоритмах нейронних мереж, які аналізують тисячі одиниць вихідних даних (фотографій, зразків голосу) для побудови динамічної «цифрової маски». Ця маска накладається на відео іншої людини, при цьому штучний інтелект забезпечує повну синхронізацію міміки, рухів губ та жестів, що робить результат практично невідрізнимим від реальності для пересічного спостерігача [1].

Правова природа дїпфейків є дуалістичною. З одного боку, технологія має значний позитивний потенціал у креативних індустріях, зокрема в кінематографії для «оживлення» акторів, виправлення технічних дефектів зйомки або вдосконалення дубляжу [2]. У маркетингових стратегіях використання синтетичних образів відомих осіб дозволяє створювати персоналізований та інноваційний контент, як це було продемонстровано у кампаніях за участю Ліонеля Мессі.

З іншого боку, здатність перетворювати будь-яку особу на «віртуальну маріонетку», що говорить або робить те, чого не було насправді, відкриває безпрецедентні можливості для дезінформації, шахрайства та підризу національної безпеки [1].

Ця технологічна трансформація створює фундаментальні виклики для правової системи, оскільки традиційні уявлення про автентичність цифрового контенту виявляються застарілими. У цифрову епоху «бачити» більше не означає «вірити», що вимагає перегляду базових принципів доказового права та впровадження нових механізмів верифікації інформації. Ситуація ускладнюється тим, що технологічний розвиток значно випереджає темпи

законодавчого регулювання, залишаючи суддів та правоохоронців у стані неочевидності при оцінці синтетичних медіа [4].

Європейський Союз став першим глобальним гравцем, який спробував встановити комплексні правила гри у сфері штучного інтелекту через ухвалення Регламенту про штучний інтелект (AI Act). Цей документ, що набув чинності 1 серпня 2024 року, запроваджує ризик-орієнтований підхід до регулювання систем ШІ, де дипфейки займають особливе місце в категорії систем зі специфічним ризиком прозорості [4].

Визначення дипфейка в межах AI Act є ширшим за суто технічне: воно охоплює згенеровані або маніпульовані зображення, аудіо- чи відеоматеріали, які нагадують існуючих осіб, об'єкти, місця чи сутності та можуть помилково сприйматися людиною як автентичні. Включення до дефініції «об'єктів» та «entities» (юридичних осіб) свідчить про усвідомлення законодавцем ризиків не лише для приватних осіб, а й для бізнесу та державних інституцій [5].

Основною стратегією AI Act щодо дипфейків є не заборона, а забезпечення прозорості. Постачальники систем ШІ зобов'язані гарантувати, що їхня продукція має вбудовані технічні рішення (водяні знаки, метадані), які дозволяють ідентифікувати контент як штучно створений у машинно-зчитуваному форматі [5]. Своєю чергою, розгортувачі (користувачі) систем ШІ, які створюють дипфейки, повинні чітко розкривати факт маніпуляції при публікації контенту [4].

Україна, прагнучи до інтеграції в єдиний цифровий ринок ЄС, обрала стратегію поступової адаптації національного законодавства до вимог AI Act. Міністерство цифрової трансформації презентувало у червні 2024 року «Білу книгу» з регулювання штучного інтелекту, яка базується на принципі «bottom-up» [6]. Цей підхід передбачає першочергову підготовку бізнесу до майбутніх правил через «м'які» інструменти: секторальні рекомендації, кодекси поведінки та регуляторні пісочниці.

Кінцевою метою є ухвалення закону-аналога європейського Регламенту, що дозволить синхронізувати правовий режим та забезпечити конкурентоспроможність українських ІТ-компаній на міжнародній арені [6].

Незважаючи на відсутність спеціального закону про ШІ станом на 2024–2025 роки, багато положень європейського акта вже мають транскордонний вплив на українських розробників. Якщо український постачальник вводить в обіг системи ШІ в ЄС або результати роботи таких систем використовуються в Європі, він зобов'язаний дотримуватися вимог AI Act [4].

Це стосується і зобов'язань щодо прозорості моделей загального призначення, які часто стають базою для створення дипфейк-інструментів [4].

Внутрішня дискусія в Україні також зосереджена на захисті прав людини та національної безпеки. Комітет Верховної Ради з питань цифрової трансформації наголошує на необхідності гармонізації політики у сфері ШІ для захисту прав громадян від маніпуляцій [7].

Особливо гостро це питання стосується використання дідфейків як інформаційної зброї в умовах воєнного стану, що вимагає швидкої реакції правоохоронних органів та вдосконалення процесуальних механізмів збирання доказів [1].

Поява дідфейків створює екзистенційну загрозу для цілісності юридичного встановлення фактів. Традиційна система доказування в багатьох юрисдикціях, включаючи США та Україну, спирається на автентифікацію як «низький поріг» допуску матеріалів до розгляду [8].

Наприклад, згідно з правилом 901 Федеральних правил доказування США (FRE), прихильник доказу має лише надати достатньо відомостей, щоб суд міг дійти висновку, що предмет є тим, чим його називає сторона. Проліферація дідфейків робить цей стандарт небезпечно вразливим, оскільки фальсифіковані матеріали тепер можуть володіти всіма поверхневими ознаками автентичності [4].

Основним наслідком є підрив довіри до цифрових доказів загалом. Виникає ситуація, коли навіть справжні відео- чи аудіозаписи можуть бути поставлені під сумнів через голослівні твердження про їхнє ШІ-походження. Цей феномен, відомий як «дивіденд брехуна», дозволяє винним особам уникати відповідальності, просто вказуючи на існування технології дідфейк як на обґрунтований сумнів у достовірності доказів. Водночас існує ризик введення суду та присяжних в оману через високоякісні підробки, які людське око не здатне детектувати без спеціальних інструментів [5].

Висновки. Правова система повинна стати такою ж гнучкою та технологічною, як і інструменти, якими користуються зловмисники. Лише через поєднання суворих регуляторних вимог (AI Act), сучасних процесуальних правил та технічних засобів верифікації можливо зберегти цілісність правосуддя та довіру суспільства до системи доказів у цифрову епоху. Виклики, створені дідфейками, є не просто технічною проблемою, а перевіркою здатності права захищати об'єктивну істину в світі, де реальність стає предметом синтезу.

Література

1. Що таке дідфейк і як його розпізнати // Покровська сільська рада. – URL: <https://pokrovska-gromada.gov.ua/news/1706187747/> (дата звернення: 25.03.2026).

2. Способи захисту порушених прав при створенні та розповсюдженні дідфейків // Semantic Scholar. – URL: <https://pdfs.semanticscholar.org/899a/677dbca9c943ff64fed6cfbe209c73fe36.pdf> (дата звернення: 25.03.2026).

3. Adapting the Rules of Evidence for the Age of AI // Quinn Emanuel. – URL: <https://www.quinnemanuel.com/media/sa2jy0hl/client-note-adapting-the-rules-of-evidence-for-the-age-of-ai-05-11-25.pdf> (дата звернення: 25.03.2026).

4. В ЄС ухвалили перші у світі закони з регулювання штучного інтелекту // LIGA.net. – URL: <https://tech.liga.net/ua/technology/novosti/v-yes-ukhvalyly-pershi-v-sviti-zakony-z-rehuliyvannia-shtuchnoho-intelektu> (дата звернення: 25.03.2026).

5. EU AI Act unpacked #8: New rules on deepfakes // Freshfields Technology Quotient. – URL: <https://technologyquotient.freshfields.com/post/102jb19/eu-ai-act-unpacked-8-new-rules-on-deepfakes> (дата звернення: 25.03.2026).

6. Регулювання штучного інтелекту в Україні: презентуємо Білу книгу // Міністерство цифрової трансформації України. – URL: <https://thedigital.gov.ua/news/technologies/regulyvannya-shtuchnoho-intelektu-v-ukraini-prezentuemo-bilu-knigu> (дата звернення: 25.03.2026).

7. Правове регулювання штучного інтелекту. Яким шляхом рухатись // Комітет Верховної Ради України з питань цифрової трансформації. – URL: https://www.rada.gov.ua/news/news_kom/239849.html (дата звернення: 25.03.2026).

8. Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases // University of Chicago Legal Forum. – URL: <https://legal-forum.uchicago.edu/print-archive/deepfakes-court-how-judges-can-proactively-manage-alleged-ai-generated-material> (дата звернення: 25.03.2026).

Дем'яненко А. Ю., здобувач освіти
Київський національний університет
технологій та дизайну
Демченко Іван Сергійович, к.ю.н., доц.
Національний медичний
університет ім. О.Богомольця

ДОСТУПНІСТЬ ЛІКАРСЬКИХ ЗАСОБІВ ЯК СКЛАДНИК ПРАВА НА ОХОРОНУ ЗДОРОВ'Я: ПРАВОВИЙ ВИМІР У ПЕРІОД СУСПІЛЬНИХ ТРАНСФОРМАЦІЙ

Доступність лікарських засобів розглядається як складова конституційно закріпленого права на охорону здоров'я та медичну допомогу (стаття 49 Конституції України). Реалізація цього права неможлива без гарантованого доступу до безпечних, якісних та ефективних лікарських засобів. В період сучасних суспільних трансформацій, що зумовлені як глобальними (торгівельні санкції, тарифи, пандемії, тощо), так і внутрішніми чинниками (збройна агресія, трансформація національної системи охорони здоров'я), правовий вимір доступності лікарських засобів потребує уваги.

З урахуванням положень Закону України «Про державні фінансові гарантії медичного обслуговування населення» [1], держава гарантує повну оплату за рахунок коштів Державного бюджету України, у тому числі, відповідних лікарських засобів. Права та гарантії окремих категорій громадян