УДК 347.78:004.8
DOI: https://doi.org/10.24144/2307-3322.2026.94.1.49

ЦИВІЛЬНО-ПРАВОВИЙ ЗАХИСТ ОСОБИСТИХ НЕМАЙНОВИХ ПРАВ У ЗВ'ЯЗКУ З ПОШИРЕННЯМ ДІПФЕЙКІВ

Парасюк М. В.,
кандидат юридичних наук, доцент,
доцент кафедри цивільного права та процесу
Інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»
ORCID: 0000-0001-8600-5264

Парасюк М. В. Цивільно-правовий захист особистих немайнових прав у зв'язку з поширенням діпфейків.

Статтю присвячено дослідженню особливостей використання об'єктів, згенерованих штучним інтелектом, із фокусом на діпфейках як новітньому явищі цифрового середовища. Обґрунтовано, що масове поширення таких технологій зумовлює виникнення нових викликів для цивільного права, зокрема у сфері захисту особистих немайнових прав особи. Встановлено, що створення та використання діпфейків може призводити до порушення права на честь, гідність, ділову репутацію, зображення та приватність, а також формувати підстави для виникнення деліктних зобов'язань.

Визначено цивільно-правову природу діпфейків як форми неправомірного використання особистих немайнових благ без згоди їх носія. Проаналізовано основні способи цивільно-правового захисту, зокрема спростування недостовірної інформації, припинення її поширення, видалення відповідного контенту, а також відшкодування моральної шкоди і компенсацію за неправомірне використання зображення чи інших елементів індивідуалізації особи. Окрему увагу приділено процесуальним аспектам захисту, включаючи застосування заходів забезпечення позову.

Досліджено як правомірні, так і неправомірні практики використання діпфейків. Показано, що за умови дотримання вимог закону вони можуть застосовуватися у сфері освіти, культури, медіа та реабілітації, тоді як їх використання без згоди особи або з метою введення в оману призводить до порушення її цивільних прав. Розглянуто міжнародно-приватноправові аспекти поширення діпфейків, зумовлені їх транскордонним характером, зокрема питання визначення юрисдикції та застосовного права.

Сформульовано пропозиції щодо вдосконалення цивільного законодавства України, які полягають у необхідності нормативного закріплення цифрової ідентичності особи як об'єкта цивільно-правового захисту та розвитку ефективних механізмів протидії неправомірному використанню діпфейків.

Методологічну основу дослідження становлять загальнонаукові та спеціально-юридичні методи, зокрема формально-юридичний, системно-структурний, порівняльно-правовий та метод правового моделювання, що дозволило комплексно проаналізувати цивільно-правову природу діпфейків і визначити напрями вдосконалення законодавства.

Ключові слова: діпфейк, особисті немайнові права, право на зображення, приватність, моральна шкода, цифрова ідентичність, цивільно-правовий захист.

Parasyuk M. V. Civil-legal protection of personal non-property rights in connection with the spread of deepfakes.

The article is devoted to the study of the features of the use of objects generated by artificial intelligence, with a focus on deepfakes as a new phenomenon of the digital environment. It is substantiated that the mass distribution of such technologies leads to the emergence of new challenges for civil law, in particular in the field of protection of personal non-property rights of an individual. It is established that the creation and use of deepfakes can lead to a violation of the right to honor, dignity, business reputation, image and privacy, as well as form the basis for the emergence of tortious obligations.

The civil-legal nature of deepfakes as a form of unlawful use of personal non-property benefits without the consent of their bearer is determined. The main methods of civil law protection are analyzed, in particular, refuting false information, stopping its distribution, removing the relevant content, as well as compensation for moral damage and compensation for the unlawful use of an image or other elements of a person's individualization. Special attention is paid to procedural aspects of protection, including the application of measures to secure the claim.

Both lawful and unlawful practices of using deepfakes are studied. It is shown that, provided that the requirements of the law are met, they can be used in the field of education, culture, media and rehabilitation, while their use without the consent of a person or for the purpose of misleading leads to a violation of his civil rights. The international and private law aspects of the spread of deepfakes, due to their cross-border nature, are considered, in particular the issue of determining jurisdiction and applicable law.

Proposals are formulated to improve the civil legislation of Ukraine, which consist in the need for regulatory consolidation of a person's digital identity as an object of civil law protection and the development of effective mechanisms to combat the illegal use of deepfakes.

Key words: deepfakes, personal non-property rights, image rights, privacy, moral damage, digital identity, civil law protection.

Постановка проблеми. Стрімкий розвиток технологій штучного інтелекту, зокрема у сфері машинного навчання, у другому десятилітті XXI століття зумовив трансформацію підходів до створення та використання цифрового контенту. Якщо на початкових етапах такі технології застосовувалися переважно у освітній, культурній та комунікативній сферах, то сьогодні їх використання дедалі частіше супроводжується втручанням у сферу приватних прав та інтересів особи.

Особливої актуальності ця проблема набуває у зв'язку з поширенням діпфейків – цифрових аудіовізуальних матеріалів, створених за допомогою алгоритмів штучного інтелекту, які імітують зовнішність, голос або поведінку реальної особи. Високий рівень правдоподібності таких матеріалів зумовлює ризики введення в оману третіх осіб та порушення особистих немайнових прав, зокрема права на честь, гідність, ділову репутацію, зображення та приватність.

Незважаючи на наявність окремих правових механізмів захисту, сучасне цивільне законодавство не повною мірою враховує специфіку діпфейків як форми використання цифрової ідентичності особи. Відсутність чітких критеріїв розмежування правомірного та неправомірного використання таких технологій, а також ефективних способів оперативного захисту прав особи, зумовлює необхідність комплексного наукового дослідження цієї проблематики.

У зв'язку з цим виникає потреба у визначенні цивільно-правової природи діпфейків, їх класифікації з точки зору правомірності використання, а також у розробці ефективних механізмів захисту особистих немайнових прав особи в умовах цифровізації суспільства.

Мета статті полягає у визначенні цивільно-правової природи діпфейків та дослідженні механізмів захисту особистих немайнових прав особи у зв'язку з їх створенням і поширенням, а також у розробці пропозицій щодо вдосконалення цивільного законодавства України у сфері захисту цифрової ідентичності.

Аналіз останніх досліджень. Проблематика використання технологій штучного інтелекту та їх впливу на правову систему активно досліджується як у вітчизняній, так і в зарубіжній науці. Зокрема, загальні питання правового регулювання цифрових технологій, захисту персональних даних та приватності особи розглядалися у працях таких українських науковців, як О. Кохановської, Р. Майданика, В. Коссак та інших.

Окремі аспекти захисту особистих немайнових прав особи, зокрема честі, гідності, ділової репутації та права на зображення, були предметом дослідження І. Спасибо-Фатєєвої, Р. Майданика, О. Кохановської, які обґрунтовують необхідність розширення підходів до захисту особистих немайнових благ в умовах цифровізації суспільства.

Проблеми правового регулювання штучного інтелекту та відповідальності за його використання досліджуються також у працях зарубіжних учених, зокрема Вудро Барфілд, Уго Пагалло, Райан Калло, які аналізують вплив новітніх технологій на традиційні правові інститути.

Безпосередньо питання діпфейків як правового феномену досліджуються у працях Роберт Чесні та Даніель Сітрон, які розглядають їх як інструмент дезінформації та загрозу правам людини, зокрема у контексті порушення приватності та репутації.

Водночас у науковій літературі переважають дослідження, спрямовані на кримінально-правові, інформаційно-правові та безпекові аспекти використання діпфейків. Натомість цивільно-правова природа діпфейків як форми порушення особистих немайнових прав, а також механізми їх захисту у межах цивільного права та цивільного процесу залишаються недостатньо дослідженими.

Таким чином, існує потреба у подальшому комплексному аналізі діпфейків саме з позицій цивільного права, зокрема щодо визначення їх як підстави виникнення деліктних зобов'язань та розробки ефективних способів захисту прав особи у цифровому середовищі.

Виклад основного матеріалу. Термін «deepfake» поєднує у собі поняття «глибоке навчання» та «підробка» і використовується для позначення цифрового контенту, створеного із застосуванням алгоритмів штучного інтелекту, що імітує зовнішність, голос або поведінку реальної особи [1].

Етимологія терміну «deepfake» походить від англійської мови та поєднує елементи, пов'язані з глибоким навчанням – формою штучного інтелекту, яка імітує процеси людського мозку за допомогою штучних нейронних мереж. Друга частина терміна «fake», широко використовується в сучасних мовах для передачі різних значень, від неправдивих новин («фейкові новини») до фальшивих профілів публічних осіб у соціальних мережах. Одне з визначень фейкових новин полягає в тому, що це форма підробки, неправда, що поширюється спеціально для дезінформації аудиторії [2, с. 184-188].

Згідно з дослідженням групи з інформатики DeepTrace Labs, кількість діпфейків в Інтернеті зростатиме експоненціально щороку. У 2018 році в Інтернеті було знайдено 7964 оригінальних відео, створених за допомогою цієї технології, а у 2019 році ця кількість досягла 14 600. Хоча більшість цих відео є порнографічними, деякі з них були створені з метою дезінформації та маніпуляції, а саме: 12% фейкових відео підривали імідж політиків; 5% були помітні в журналістських матеріалах; 2% стосувалися бізнес-діячів.

Крім того, дослідження виявило 20 незалежних веб-сайтів, які створюють такий контент. Результати показують, що, здавалося б, нешкідливі комп'ютерні програми, створені для розважальних цілей, можуть становити серйозний виклик для світової спільноти [3].

Діпфейки – це потужні інструменти, які можна використовувати як у благодійних, так і в маніпулятивних цілях, залежно від цільового призначення.

З цивільно-правової точки зору діпфейк слід розглядати не лише як технологічний продукт, а як результат використання персональних немайнових благ особи без її згоди.

Визначальною ознакою діпфейку є його гіперреалістичність, яка здатна вводити в оману третіх осіб, створюючи уявлення про достовірність інформації. Саме ця ознака обумовлює його потенційну протиправність у разі порушення прав конкретної особи.

Отже, діпфейк може виступати: об'єктом цивільних правовідносин; підставою виникнення деліктних зобов'язань; способом неправомірного використання образу особи.

Нижче наведено приклади законного та зловмисного використання діпфейків.

Отож, корисні діпфейки використовують в таких галузях:

1) виготовлення кінострічок. В них можна замінити як повністю актора, так і частину його тіла (обличчя, руки, поставу), голос, міміку, жести і економити мільйони коштів;
2) на цифрових освітніх платформах та в корпоративних навчальних системах, де використовують аватарів на основі ШІ. Тут поширеними є цифрові освітні інструктори, аватари персоналізованих відомих культурних діячів та історичних постатей; штучно створені коучі, які надають освітню інформацію;
3) технології доступності та допоміжні технології, які використовуються для клонування голосу людини при порушенні їх мовних функцій через хворобу (проблеми слуху, мовлення).

Діпфейки, які передбачають зловмисні дії, злочинні дії, дії кримінально караного характеру, спрямовані проти безпеки, здоров'я та життя суспільних мас:

1) політична дезінформація та пропаганда: фальшиві інтерв'ю, промови, кількасекундний ролик з цифровим аватаром тощо, який поширює неправдиву чи суперечливу інформацію;
2) клонування голосу, обличчя при просуванні фінансових махінацій, злочинів, що позначаються згодом як фінансові шахрайства;
3) в системі соціальної інженерії та крадіжці персональних даних;
4) фішингові шахрайства з використанням AI-генерованих голосів або відео для зміни платіжних реквізитів, голосове клонування для наказів підлеглим працівникам при переводах коштів тощо [4].

Обговорюючи сутність діпфейків, дослідник А. Гачкевич наголошує на питанні: на якому елементі слід зробити акцент: на здатності діпфейку виглядати правдоподібно, сприяючи імітації автентичності, чи на тому факті, що діпфейки створюються за допомогою спеціалізованого програмного забезпечення на основі глибокого машинного навчання, гілки штучного інтелекту [5, с. 14]. Ми погоджуємось з висновком дослідника, що ефект високої правдоподібності стосується, швидше, подання інформації, ніж її точності. Відео може здаватися реалістичним, доки ми не проаналізуємо ймовірність того, що зображена подія насправді відбудеться. У деяких випадках, навіть після аналізу, все ще може бути важко визначити правду. Тому визначення діпфейку повинно підкреслювати його гіперреалістичну форму та схожість з особою, яку він містить, а не його фактичну точність. Більше того, не всі діпфейки становлять небезпеку. Наприклад, гумористичне відео, яке легко сприймається як підробка, не несе таких самих ризиків, як відео, яке виглядає реалістичним.

Крім того, залучення штучного інтелекту до створення діпфейків, а саме методу глибокого навчання, є палицею з двома кінцями у формулюванні визначення. З одного боку, штучний інтелект гарантує, що відео чи зображення, або, можливо, інші типи контенту, стають переконливими завдяки здатності генерувати короткий, унікальний аналог реальності. З іншого боку, результатом цього процесу є не реальність, а радше вигадане представлення, втілене в контенті, відповідно до параметрів, встановлених користувачем програмного забезпечення [5, с. 15].

Слід сказати, що хоча створення діпфейків в різних сферах налічує до десяти років, ні кримінальна наука окремої країни, ні міжнародні організації ще не розробили достатньо ефективної інструкції, методичних рекомендацій чи документу, як реагувати на виявлення діпфейків, їх класифікацію за шкалою «безпека – користь – небезпека – шкода – злочин», тому що розвиток штучного інтелекту, рівень машинного навчання і людські фантазії при створенні подібного контенту ще не настільки класифіковані та вивчені, перебувають в стані розвитку. Але реагувати на злочинне, шкідливе використання діпфейків необхідно. Тому у кількох країнах характеристики особистості (зовнішність, вираз обличчя, будова тіла) захищені правом на публічність, яке захищає різні прояви особи – від імені до підпису – від несанкціонованого комерційного використання. Право на публічність має спільні риси із захистом торговельних марок, пов'язуючи його зі сферою інтелектуальної власності [6, с. 1171].

Відповідно, будь-яке комерційне використання голосу, зображення та інших атрибутів особи повинно вимагати її згоди, щоб уникнути потенційних юридичних проблем. Щодо діпфейків, право на публічність та здатність особи контролювати значення власної особистості [7, с. 225-294.] застосовується у випадках, коли діпфейки використовуються для реклами або інших комерційних цілей.

Також діпфейки широко використовуються в такому типі шантажу чи образи честі та гідності людини, як порнографія помсти. Порнографія помсти пов'язана з публікацією фотографій та відео відвертого характеру без її згоди. Згідно зі словником Merriam-Webster, це трапляється, коли сексуально відверті зображення особи публікуються в Інтернеті без її згоди, особливо як форма помсти чи домагань [10]. Незважаючи на свою фальшивість, діпфейки також можна вважати порнографією помсти, враховуючи фактор їх сприйняття як точних. Одним із найгучніших випадків використання діпфейків для маніпуляцій та пропаганди є фейкове порновідео за участю відомої індійської опозиційної журналістки Рани Айюб. Фан-сторінка лідера партії Бхаратія Джаната (BJP) поширила фейкове відео, на якому нібито зображена журналістка, тим самим дискредитуючи Рану в очах індійської громади. Ще одним прикладом маніпуляцій з використанням нових технологій є випадок міністра фінансів Малайзії Азміна Алі. За допомогою діпфейка обличчя політика з'явилося на відео, де він займається гомосексуальним сексом, що є незаконним у Малайзії [3, с. 109].

Діпфейки можуть слугувати інструментом для шахрайства та інших незаконних дій, включаючи крадіжку особистих даних, нелегальну міграцію та шпигунство [9, с. 58–64]. Деякі країни, зокрема Сінгапур [10], вже прийняли закони, що криміналізують використання діпфейків.

Очікується, що виклики, що виникають через діпфейки, будуть розглянуті для вдосконалення кримінального законодавства та розвитку судової практики. Перевагу надасть порівняльний підхід, коли держави запозичують норми одна в одної для введення нових злочинів у свої правові системи. Таким чином, діпфейк не повинен бути засобом вчинення злочину на основі складу злочинів кримінального права.

В боротьбі за безпечне застосування діпфейків слід також згадати процедуру маркування контенту. Вчені все частіше вивчають ідею позначення походження контенту, створеного штучним інтелектом,

щодо створення та поширення діпфейків [11]. Ця пропозиція також підтримується на рівні урядових угод. Одним з ключових принципів G7 є «розробка та впровадження надійних механізмів автентифікації та походження контенту, де це технічно можливо, включаючи водяні знаки або інші методи, що дозволяють користувачам ідентифікувати контент, створений штучним інтелектом». Правила щодо маркування стають частиною законодавства, перш за все, відповідно до прогресивного Закону ЄС про штучний інтелект (стаття 50) [12].

Поширення діпфейків безпосередньо пов'язане з ризиком порушення низки особистих немайнових прав, закріплених у цивільному законодавстві України.

Право на честь, гідність і ділову репутацію. Діпфейки можуть містити недостовірну інформацію, що дискредитує особу, створює хибне уявлення про її поведінку або висловлювання. Це є підставою для захисту у формі спростування недостовірної інформації.

Право на зображення особи. Використання обличчя, міміки чи зовнішності особи без її згоди є прямим порушенням права на зображення. Діпфейки значно розширюють можливості такого порушення, оскільки дозволяють створювати новий контент без фактичної участі особи.

Право на приватність. Діпфейки можуть втручатися у приватне життя особи, зокрема шляхом створення неправдивих сцен особистого характеру.

Цифрова ідентичність як об'єкт захисту. Сучасні умови вимагають визнання цифрової ідентичності особи (зображення, голос, поведінкові моделі) як самостійного об'єкта цивільно-правового захисту.

Особа, права якої порушені шляхом створення чи поширення діпфейку, може скористатися широким спектром цивільно-правових способів захисту, передбачених чинним законодавством України. До таких способів, зокрема, належать:

- визнання інформації недостовірною та її спростування;
- припинення поширення діпфейку;
- видалення відповідного контенту;
- відшкодування моральної шкоди;
- компенсація за неправомірне використання зображення, голосу чи інших елементів індивідуалізації особи.

Зазначені способи захисту випливають із загальних положень Цивільного кодексу України, зокрема статей 16, 277, 280, 307, 308, які встановлюють механізми захисту особистих немайнових прав та визначають можливість спростування недостовірної інформації, заборони її поширення і відшкодування завданої шкоди [13].

У науковій літературі підкреслюється, що особисті немайнові права мають абсолютний характер і підлягають ефективному судовому захисту незалежно від способу їх порушення. Як зазначає Р. Стефанчук, особисті немайнові права фізичної особи є невідчужуваними та непорушними, а їх захист здійснюється шляхом припинення дій, що їх порушують, та відшкодування моральної шкоди [14, с. 206].

Особливе значення у випадку поширення діпфейків має інститут відшкодування моральної шкоди, оскільки такі дії здатні спричиняти істотні нематеріальні втрати, пов'язані із приниженням честі, гідності, ділової репутації, а також психологічним дискомфортом особи. Моральна шкода охоплює не лише фактичні страждання особи, але й негативні наслідки для її соціального становища та репутації.

Водночас, ефективність захисту особистих немайнових прав значною мірою залежить від своєчасності реагування на правопорушення, особливо у сфері поширення інформації в мережі Інтернет, де шкода може швидко набувати масштабного характеру. Дане твердження відображає правову позицію Касаційного цивільного суду у складі Верховного Суду (справа № 756/10624/21), де суд вказав, що вимога про видалення статті є належним способом захисту саме через неможливість іншим чином зупинити швидке поширення порушення в мережі [15].

У межах цивільного процесу важливим є застосування заходів забезпечення позову, які дозволяють оперативно припинити порушення прав особи ще до ухвалення рішення у справі. До таких заходів може належати блокування або видалення відповідного цифрового контенту, заборона його подальшого поширення, а також обмеження доступу до нього.

Таким чином, цивільно-правові способи захисту прав особи у випадках створення та поширення діпфейків є комплексними та включають як матеріально-правові, так і процесуальні механізми, спрямовані на відновлення порушених прав, припинення протиправної поведінки та компенсацію завданої шкоди.

Діпфейки також мають виражений транскордонний характер, що істотно ускладнює ефективний захист прав особи у випадку їх створення та поширення. Особливості функціонування глобального цифрового середовища, зокрема соціальних мереж та відеоплатформ, зумовлюють ситуації, коли контент створюється в одній державі, розміщується на серверах в іншій, а шкода завдається особі, яка перебуває в третій юрисдикції.

У зв'язку з цим виникає низка складних правових проблем, серед яких: визначення юрисдикції суду; встановлення застосовного права; притягнення до відповідальності іноземних суб'єктів.

Поширення діпфейків через глобальні платформи актуалізує необхідність застосування норм міжнародного приватного права, зокрема щодо визначення компетентного суду та права, що підлягає застосуванню до відповідних правовідносин. Як зазначає S. Symeonides, у справах із транскордонним елементом ключовим є встановлення найбільш тісного зв'язку правовідносин із певною юрисдикцією, що визначає застосовне право [16, с. 45].

Водночас важливе значення для формування підходів до вирішення подібних спорів має практика Суду Європейського Союзу. Зокрема, у справі eDate Advertising GmbH v X and Martinez v MGN Limited Суд ЄС сформулював підхід, відповідно до якого особа, права якої порушені в мережі Інтернет, може звертатися до суду як за місцем заподіяння шкоди, так і за місцем свого основного центру інтересів, що істотно розширює можливості захисту у транскордонних спорах [17].

Аналогічні підходи простежуються і в практиці Європейського суду з прав людини. У справі Delfi AS v Estonia Суд визнав відповідальність інтернет-платформи за поширення протиправного контенту третіми особами, підкресливши обов'язок забезпечення ефективного балансу між свободою вираження поглядів та захистом честі і гідності особи [18].

З урахуванням зазначеного, можна зробити висновок, що ефективний захист особистих немайнових прав у випадках поширення діпфейків потребує не лише вдосконалення національного законодавства, але й активного використання напрацювань європейської судової практики, розвитку міжнародного співробітництва та гармонізації правових підходів у сфері цифрових правовідносин.

З метою підвищення ефективності захисту прав особи в умовах стрімкого розвитку цифрових технологій доцільним є вдосконалення національного законодавства України у сфері регулювання діпфейків. Зокрема, пропонується:

- закріпити на законодавчому рівні поняття цифрової ідентичності як сукупності індивідуалізуючих ознак особи у цифровому середовищі;
- уточнити правовий режим використання зображення, голосу та інших біометричних характеристик особи;
- передбачити спеціальні цивільно-правові способи захисту від неправомірного використання діпфейків;
- удосконалити механізми оперативного обмеження доступу та видалення незаконного контенту;
- сприяти формуванню сталої судової практики щодо визначення розміру компенсації моральної шкоди у справах, пов'язаних із цифровими правопорушеннями.

На наше переконання, ефективне правове регулювання у цій сфері потребує формування чіткої дозвільно-заборонної системи класифікації діпфейків, яка б окреслювала межі їх добросовісного та недобросовісного використання, а також дозволяла відмежовувати правомірну діяльність від правопорушень і кримінально караних діянь.

До добросовісного застосування діпфейків доцільно віднести випадки, коли їх використання не порушує прав та законних інтересів інших осіб і має суспільно корисний характер. Зокрема, це:

- використання у сфері освіти, зокрема при створенні цифрових навчальних платформ та інтерактивних освітніх продуктів;
- застосування у культурно-мистецькій діяльності, включаючи цифрову реконструкцію історичних постатей та популяризацію культурної спадщини;
- використання у музейно-туристичній сфері з метою розширення доступу до культурних об'єктів;
- застосування у кіноіндустрії за умови дотримання прав осіб, зображення або голос яких використовуються;
- використання у медичній та реабілітаційній практиці, зокрема для відновлення комунікативних можливостей осіб із порушеннями мовлення.

Обов'язковою умовою правомірності у таких випадках має бути належне інформування користувачів про застосування технологій штучного інтелекту при створенні відповідного контенту.

Водночас до недобросовісного та протиправного використання діпфейків слід віднести дії, що порушують особисті немайнові права особи або спрямовані на введення в оману третіх осіб. До таких, зокрема, належать:

- відтворення або клонування зовнішності, голосу чи поведінки особи без її згоди;
- використання персональних даних з метою маніпуляції суспільною думкою або введення в оману;
- застосування діпфейків у шахрайських схемах, зокрема фінансового характеру;
- використання образу особи без її дозволу у творчих або комерційних продуктах;
- поширення діпфейків, що містять матеріали інтимного характеру без згоди особи.

Таким чином, запропонована класифікація має динамічний характер і може бути розширена з урахуванням розвитку судової практики та появи нових форм використання технологій штучного інтелекту. Її впровадження сприятиме формуванню збалансованого підходу до правового регулювання діпфейків, що забезпечить належний захист прав особи та водночас не перешкоджатиме розвитку інноваційних технологій.

Висновки. У результаті проведеного дослідження встановлено, що діпфейки як продукт розвитку технологій штучного інтелекту становлять складне міждисциплінарне явище, яке набуває самостійного значення у сфері цивільно-правового регулювання. Їх специфіка полягає у поєднанні високого рівня технологічної достовірності із потенційною здатністю порушувати особисті немайнові права фізичної особи, зокрема право на честь, гідність, ділову репутацію, зображення та приватність.

Обґрунтовано, що діпфейк у цивільно-правовому розумінні слід розглядати не лише як результат технічної діяльності, а як форму використання індивідуалізуючих ознак особи без її згоди, що може створювати підстави для виникнення деліктних зобов'язань. Визначальною ознакою діпфейків є їх гіперреалістичність, яка зумовлює здатність вводити в оману третіх осіб і, відповідно, підвищує ризик заподіяння немайнової шкоди.

Доведено, що чинне цивільне законодавство України загалом містить базові механізми захисту прав особи у випадках поширення діпфейків, однак не враховує повною мірою специфіку цифрового середовища та новітніх технологій. У зв'язку з цим особливого значення набуває застосування таких способів захисту, як спростування недостовірної інформації, припинення її поширення, видалення контенту, а також відшкодування моральної шкоди. Водночас ефективність їх реалізації значною мірою залежить від оперативності реагування та можливості застосування заходів забезпечення позову.

Встановлено, що транскордонний характер поширення діпфейків істотно ускладнює захист прав особи та потребує активного застосування норм міжнародного приватного права, а також врахування практики європейських судових інституцій. У цьому контексті особливого значення набувають підходи щодо визначення юрисдикції, застосовного права та відповідальності інформаційних посередників.

Обґрунтовано необхідність удосконалення національного законодавства України шляхом закріплення поняття цифрової ідентичності, уточнення правового режиму використання зображення та голосу особи, а також запровадження спеціальних механізмів реагування на неправомірне використання діпфейків. Запропоновано формування дозвільно-заборонної класифікації діпфейків, яка дозволить чітко розмежувати правомірне та протиправне їх використання.

Загалом, забезпечення ефективного захисту прав особи в умовах розвитку технологій штучного інтелекту потребує комплексного підходу, що поєднує вдосконалення цивільно-правових механізмів, розвиток судової практики та гармонізацію національного законодавства з європейськими стандартами. Це дозволить досягти балансу між свободою інноваційного розвитку та належним рівнем охорони особистих немайнових прав у цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Deepfake. *Encyclopaedia Britannica*. URL: https://www.britannica.com/ technology/deepfake
2. Мудра І. Поняття «фейку» та його уявлення у ЗМІ. *Теле- та радіожурналістика*. 2016. №15. С. 184-188. URL: https://publications.lnu.edu.ua/collections/ index.php/teleradio/article/viewFile/694/69

3. Подус С. Діпфейки в інформаційній війні. Сучасна війна: гуманітарний аспект: *IV Міжнародна наукова конференція ХНУПС ім. І.Кожедуба*, 21-22 травня 2020. С. 108-110. URL: https://www.hups.mil.gov.ua/assets/doc/science/stud-conf/suchasna-viyna-gumanitarniy-aspekt-05-2020/32.pdf
4. Загроза діпфейків і як їх вчасно розпізнати. *Eska Global*. 08.06.2025. URL: https://eska.global/blog/zagroza-dipfejkiv-i-yak-yih-vchasno-rozpiznati
5. Hachkevych A. Deepfakes: Definition of the Concept and Criteria for Distinguishing Between Harmful and Harmless Deepfakes. Veritas: *Legal and Psychological-Pedagogical Research.* 2025. № 1(2). С. 12–20. DOI: doi.org/10.23939/veritas2025.02.012. URL: https://science.lpnu.ua/veritas/all-volumes-and-issues/volume-1-number-2-2025/deepfakes-definition-concept-and-criteria
6. Dogan S., Lemley M. What the Right of Publicity Can Learn from Trademark *Law. Stanford Law Review*. 2006. № 58. P. 1161–1220.
7. McKenna M. The Right of Publicity and Autonomous Self-Definition. University of Pittsburgh. *Law Review*. 2005. № 67. С. 225–294.
8. Merriam-Webster. (n. d.). Revenge Porn. In Merriam-Webster.com dictionary. March 10, 2025. URL: https://www.merriam-webster.com/dictionary/revenge%20porn
9. Alanazi S., Asif S., Moulitsas I. Examining the societal impact and legislative requirements of deepfake technology: a comprehensive study. *International Journal of Social Science and Humanity.* 2024. № 14(2). С. 58–64. URL: https://www.researchgate.net/publication/379615642_ Examining_the_Societal_Impact_and_Legislative_Requirements_of_Deepfake_Technology_A_Comprehensive_Study
10. Werner J. Singapore's parliament passes bill to combat manipulated online election content. 24.10.2024. URL: https://babl.ai/singapores-parliament-passes-bill-to-combat-manipulated-online-election-content/
11. Gamage D., Sewwandi D., Zhang M., Bandara A. Labeling Synthetic Content: User Perceptions of Warning Label Designs for AI-generated *Content on Social Media*. 2025. URL: https://arxiv.org/abs/2503.05711
12. European Commission. Hiroshima Process International Guiding Principles for Advanced AI system. 30.10.2023. URL: https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-internationalguiding-principles-advanced-ai-system
13. Цивільний кодекс України від 16.03.2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15.
14. Стефанчук Р. О. Особисті немайнові права фізичних осіб (поняття, зміст, система, особливості здійснення та захисту): монографія. відп. ред. Я. М. Шевченко. К: КНТ, 2007. 626 с.
15. Постанова Верховного Суду у складі колегії суддів Другої судової палати Касаційного цивільного суду. Справа № 756/10624/21 від 11.10.2023 р. URL: https://reyestr.court.gov.ua/Review/114187195
16. Symeonides S.C. Private International Law: Idealism, Pragmatism, Eclecticism. Brill Nijhoff, 2021 462 p.
17. Judgment of the Court (Grand Chamber) of 25 October 2011. *eDate Advertising GmbH v X; Martinez v MGN Limited*. Joined Cases C-509/09 and C-161/10. URL: https://www.5rb.com/case/edate-advertising-gmbh-v-x-and-olivier-martinez-and-robert-martinez-v-mgn-limited/
18. Judgment of the European Court of Human Rights. *Delfi AS v Estonia*. 16 June 2015. URL: https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/

Дата першого надходження рукопису до видання: 21.03.2026
Дата прийняття до друку рукопису після рецензування: 23.04.2026
Дата публікації: 10.05.2026