Статті за іншими напрямами досліджень у галузі знань 08 – "Право"

УДК / UDC: 34:004.8(477)
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364542

Максим Олександрович Валін
Тренінговий центр прокурорів України.
Київ, Україна
ORCID: https://orcid.org/0009-0002-2966-2887
Володимир Вікторович Нікітін
Київський національний університет будівництва і архітектури
Київ, Україна
ORCID: https://orcid.org/0000-0001-6915-6319

DEEPFAKE ЯК ДОКАЗ У КРИМІНАЛЬНОМУ ПРОЦЕСІ: СТАНДАРТИ ПЕРЕВІРКИ АВТЕНТИЧНОСТІ ТА ДОПУСТИМОСТІ

Анотація: *У статті здійснено комплексне доктринальне дослідження проблематики використання deepfake-матеріалів як доказів у кримінальному провадженні. На підставі міждисциплінарного аналізу технологічних, правових та криміналістичних аспектів синтезу медіаконтенту за допомогою генеративно-змагальних нейронних мереж (GAN) сформовано авторську концепцію процесуального статусу deepfake як виду електронного доказу. Досліджено нормативно-правову базу України щодо регулювання електронних доказів та встановлено системні прогалини, що унеможливлюють адекватну оцінку синтетичних медіаматеріалів у судочинстві. Здійснено порівняльний аналіз підходів до автентифікації цифрових доказів у праві США, ЄС та України. Детально проаналізовано методи форензичного виявлення deepfake та критерії їхньої придатності для кримінального процесу. Запропоновано концептуальну модель верифікації синтетичних медіаматеріалів та розроблено конкретні пропозиції щодо вдосконалення КПК України, законодавства про судову експертизу та кримінального закону. Наукова новизна полягає у формуванні цілісної доктрини допустимості deepfake-доказів як самостійного правового інституту.*

Ключові слова: *deepfake, докази у кримінальному процесі, допустимість доказів, автентичність цифрових матеріалів, електронні докази, штучний інтелект, форензика, генеративно-змагальні мережі, синтетичні медіаматеріали, кримінальне провадження, верифікація.*

Maksym O. Valin
Training Center of Prosecutors of Ukraine. Educational Consultant collaborating with EPAM Systems
Kyiv, Ukraine
ORCID: https://orcid.org/0009-0002-2966-2887
Volodymyr V. Nikitin
Kyiv National University of Construction and Architecture
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-6915-6319

DEEPFAKE AS EVIDENCE IN CRIMINAL PROCEEDINGS: STANDARDS FOR VERIFICATION OF AUTHENTICITY AND ADMISSIBILITY

Summary: *The article presents a comprehensive doctrinal study of the issue of using deepfake materials as evidence in criminal proceedings. Based on an interdisciplinary analysis of technological, legal, and forensic aspects of media content synthesis using generative adversarial neural networks (GAN), an original concept of the procedural status of deepfake as a type of electronic evidence has been developed. The regulatory framework of Ukraine governing electronic evidence is examined, and systemic gaps are identified. A comparative analysis of digital evidence authentication approaches in US, EU, and Ukrainian law is conducted. Forensic methods of deepfake detection are analyzed and criteria for their suitability in criminal proceedings are substantiated. A conceptual model for verifying synthetic media materials is proposed, and specific recommendations for improving Ukrainian legislation are developed. The scientific novelty lies in forming an integral doctrine of deepfake evidence admissibility as an independent legal institution.*

Keywords: *deepfake, evidence in criminal proceedings, admissibility of evidence, authenticity of digital materials, electronic evidence, artificial intelligence, forensics, generative adversarial networks, synthetic media materials, criminal proceedings, verification.*

1. Постановка проблеми та її загальна характеристика

Сучасне кримінальне судочинство переживає безпрецедентну технологічну трансформацію, яка корінним чином змінює природу та склад доказової бази. Серед найбільш дестабілізуючих чинників – стрімке поширення так званих “deepfake”-технологій (від англ. deep learning + fake), що уможливлюють створення синтетичного медіаконтенту, невідрізнюваного від справжнього за будь-яким зовнішнім критерієм. Технологія є продуктом архітектур глибокого навчання, передусім генеративно-змагальних мереж (Generative Adversarial Networks, GAN), запропонованих у 2014 р. та вдосконалених у численних наступних роботах [15]. Саме ця здатність deepfake-технологій до синтезу гіперреалістичного, але фіктивного відео-, аудіо- та фотоконтенту становить безпрецедентну загрозу для правосуддя.

Проблема має два взаємопов’язані виміри. По-перше, сторона обвинувачення або заінтересовані особи можуть намагатися використати сфальсифіковані deepfake-матеріали як начебто автентичні докази – відеозаписи злочину, звукові записи переговорів, фотографії підозрюваного на місці події. По-друге, виникає симетрична загроза “deepfake defense”: сторона захисту може без достатніх підстав заперечувати автентичність цілком справжніх відеодоказів, посилаючись на можливість їхнього підроблення. За даними аналітичної платформи Sensity AI (2023), кількість задокументованих deepfake-відео у відкритому доступі перевищила 500 000 одиниць, а річний темп зростання становить понад 900% [10].

В українському контексті проблема набуває особливої гостроти з огляду на триваючий збройний конфлікт, у ході якого deepfake-матеріали активно використовуються з метою дезінформації та дискредитації офіційних осіб. Водночас правова система України не має дієвих механізмів ані для виявлення, ані для процесуальної оцінки таких матеріалів у рамках кримінального провадження. Відсутність спеціальних норм у Кримінальному процесуальному кодексі України (далі – КПК України), брак атестованих методик судової форензичної експертизи синтетичного медіаконтенту, а також нерозвиненість судової практики у цій сфері утворюють системну правову прогалину, що потребує невідкладного заповнення [18; 19].

2. Результати аналізу наукових публікацій та визначення невирішених частин проблеми

Дослідження правових аспектів deepfake розпочалося переважно у зарубіжній науці на межі 2010–2020-х років. Фундаментальний внесок зробили дослідники, які у праці, опублікованій у California Law Review (2019), здійснили першу системну класифікацію правових загроз deepfake-контенту і запропонували законодавчі рекомендації для США [4]. Автори виокремили три основних сфери зловживань: шкода репутації та особистій гідності, маніпуляція демократичними процесами та загрози національній безпеці – усі з яких мають безпосередній процесуальний вимір.

У сфері криміналістики та форензики значний науковий доробок представлений дослідженнями, у яких здійснено систематизацію методів як генерації, так і виявлення синтетичного контенту [6]. Фундаментальні принципи форензичного дослідження цифрових доказів, що зберігають методологічну цінність для аналізу deepfake, закладені у класичних монографіях з цифрової криміналістики [5].

Надзвичайно важливим для концептуального осмислення проблематики є масив досліджень, присвячених правосуб'єктності та відповідальності в контексті штучного інтелекту. Дослідники у статті, опублікованій у журналі AI & Society (2024), поставили під сумнів традиційні категорії правосуб'єктності щодо систем ШІ та запропонували методологічні підходи до вирішення проблеми ідентифікації відповідального суб'єкта при заподіянні шкоди автономними системами ШІ [7]. Це дослідження є принципово важливим для визначення суб'єктів відповідальності за генерацію та використання deepfake-доказів у кримінальному процесі.

У монографічному дослідженні, присвяченому електронній юрисдикції та правовому статусу цифрових об'єктів, здійснено аналіз проблеми ідентифікації цифрових аватарів та нейронних мереж у правовому просторі [8]. Висновки цього дослідження безпосередньо стосуються питань встановлення походження deepfake-матеріалів та визначення кола осіб, відповідальних за їхнє створення і розповсюдження. Положення щодо правової відповідальності суб'єктів у системах з ШІ (IoT) [9] безпосередньо застосовні до визначення відповідальних осіб у справах про фальсифікацію доказів з використанням deepfake.

Питання використання доказів, отриманих за допомогою штучного інтелекту, в судовому провадженні досліджено у спеціалізованому виданні з криміналістики та судової експертизи [16]. Автор аналізує процесуальний статус таких доказів та розробляє критерії їхньої допустимості, що безпосередньо корелює з предметом цього дослідження.

В українській правовій науці загальні питання електронних доказів у кримінальному процесі розроблялися у низці спеціалізованих праць [13]. Криміналістичні аспекти цифрової форензики досліджувалися вченими Національного

юридичного університету імені Ярослава Мудрого та Харківського науково-дослідного інституту судових експертиз [14]. Разом з тим спеціальних монографічних досліджень, присвячених deepfake як виду доказів у кримінальному провадженні, в Україні на момент підготовки цієї статті не проводилося.

Серед останніх розробок 2025–2026 рр. слід виокремити дослідження у сфері регулювання ШІ в правосудді в контексті Регламенту ЄС про штучний інтелект [18], а також праці, присвячені стандартам міжнародної правової допомоги у справах з deepfake-доказами [19; 20]. Перспективним є напрям, пов'язаний із застосуванням блокчейн-технологій для забезпечення незмінності цифрових доказів [21].

Невирішеними залишаються такі ключові питання: критерії процесуального розмежування автентичних і синтетичних цифрових матеріалів; порядок призначення та кваліфікаційні вимоги до судово-технічних експертів у справах із deepfake; правові наслідки встановлення факту підроблення медіадоказу для кримінального провадження; механізми захисту від необґрунтованої "deepfake defense".

3. Актуальність та наукова новизна дослідження

Актуальність дослідження визначається сукупністю чинників технологічного, правозастосовного та законодавчого характеру. У технологічному вимірі слід констатувати якісний стрибок можливостей deepfake-технологій: сучасні дифузійні моделі (Stable Diffusion, Elevenlabs та ін.) продукують відео та аудіоматеріали, практично неможливі для розрізнення від автентичних навіть для навченого ока [10; 20]. Відповідно до звіту Europol (2022), правоохоронні органи держав – членів ЄС зафіксували зростання кількості кримінальних проваджень, де deepfake-матеріали фігурували як докази або використовувалися з метою шахрайства [11].

У правозастосовному вимірі Україна вже стикається з конкретними викликами. Низка кримінальних проваджень, порушених у зв'язку зі збройним конфліктом, потребує оцінки відеозаписів, автентичність яких оспорюється. Слідчі підрозділи Національної поліції та Служби безпеки України не мають уніфікованого методичного забезпечення для проведення відповідних перевірок, а Науково-дослідний інститут судових експертиз не має затверджених методик дослідження deepfake-контенту.

Наукова новизна статті полягає у такому: (1) вперше у вітчизняній науці сформовано доктрину deepfake як самостійного виду електронного доказу зі специфічним процесуальним режимом верифікації; (2) розроблено авторську класифікацію форм участі deepfake-матеріалів у кримінальному судочинстві; (3) синтезовано міждисциплінарну методологію форензичної верифікації, адаптовану до процесуальних вимог КПК України; (4) вперше у вітчизняній доктрині досліджено питання кримінальної відповідальності за фальсифікацію deepfake-доказів у контексті концепцій правосуб'єктності ШІ; (5) розроблено конкретні законодавчі пропозиції, підкріплені порівняльно-правовим аналізом.

4. Мета та завдання дослідження

Метою статті є формування науково обґрунтованої доктрини допустимості deepfake-матеріалів як доказів у кримінальному провадженні та розробка системних пропозицій щодо вдосконалення кримінального процесуального законодавства України з урахуванням міжнародного досвіду та досягнень сучасної форензики.

5. Виклад основного матеріалу

5.1. Технологічна природа deepfake: від генерації до виявлення

Поняття “deepfake” охоплює широкий спектр технологій синтезу та маніпуляції медіаконтентом на основі алгоритмів машинного навчання. Архітектурно розрізняють кілька ключових підходів: класичні GAN [15], варіаційні автоенкодери (VAE), трансформерні моделі та дифузійні моделі (DDPM). Сучасні системи (FaceSwap, DeepFaceLab, SimSwap, FSGAN) здатні з мінімальним набором навчальних зразків синтезувати переконливе відео тривалістю від секунд до годин.

З точки зору судової форензики, методи виявлення deepfake поділяються на пасивні (аналіз наявного контенту) та активні (верифікація за допомогою попередньо вбудованих цифрових підписів або водяних знаків). Серед пасивних методів виокремлюють: (а) аналіз просторово-часових артефактів – нерівномірності текстури шкіри, аномалії меж підміненої ділянки, невідповідність освітлення; (б) rPPG-аналіз (remote photoplethysmography) – виявлення аномалій у мікровібраціях зображення, що відображають серцебиття; (в) аналіз рухів очей та повік – статистично неприродні патерни моргання; (г) спектральний аналіз аудіосигналу – виявлення артефактів вокодера, аномалій у спектрограмі; (д) аналіз метаданих файлу – невідповідності дат, програмного забезпечення, GPS-координат [6].

Критично важливим для правозастосування є усвідомлення обмежень кожного методу. Жоден з них не забезпечує абсолютної точності: найкращі системи автоматичного виявлення демонструють похибку у 5–15% навіть на «чистих» тестових наборах, а при навмисному “обході” детектора (adversarial attack) похибка може сягати 30–40% [6; 20]. Це означає, що форензичний висновок у справі з deepfake завжди має ймовірнісний характер і не може слугувати єдиним доказом автентичності чи неавтентичності матеріалу.

Таблиця 1

Порівняльна характеристика методів форензичного виявлення deepfake у кримінальному процесі

Метод виявлення	Технологічна основа	Точність (за умови відсутності adversarial attack)	Процесуальна придатність	Нормативна база застосування
Аналіз просторово-часових артефактів	Детектори текстури шкіри, GAN-аномалій	78–85%	Висока – використовується як первинний скринінг	ISO/IEC 27042; ENISA Guidelines 2022 [12]
rPPG-аналіз (пульсовий аналіз)	Мікровібрації пікселів, серцебиття	82–88%	Середня – залежить від якості відео	FRE Rule 702 (США); ISO/IEC 27037 [12]
Спектральний аналіз аудіо	Аномалії спектрограми, артефакти вокодера	80–87%	Висока для аудіо-deepfake; потребує спеціалізації	Ст. 242 КПК України; Наказ МЮ № 1666/5 [1]
Аналіз метаданих та хеш-сум	Форензика файлової системи,	90–96%*	Дуже висока – є базовим доказом	Ст. 99 КПК України;

Метод виявлення	Технологічна основа	Точність (за умови відсутності adversarial attack)	Процесуальна придатність	Нормативна база застосування
	EXIF-даних		chain of custody	ISO/IEC 27037 [1; 12]
Комплексна машинно-навчальна детекція (ансамблеві моделі)	Мультимодальний DNN-аналіз (відео + аудіо + метадані)	88–94%	Найвища – рекомендується як основний метод судової експертизи	Проєкт Методичних рекомендацій МЮ України 2025 [1; 18]

** Точність знижується до 60–70% при навмисному adversarial attack; потребує комплексного застосування.*
Джерело: складено автором на основі [6; 12; 18].

5.2. Deepfake у системі доказів КПК України: правова природа та класифікація

Аналіз системи доказів за КПК України (статті 84–99) з урахуванням технологічних характеристик deepfake-матеріалів дозволяє сформулювати таке. Deepfake-матеріали за своєю правовою природою є гетерогенним поняттям, що охоплює різні процесуальні форми залежно від конкретного контексту їх появи у кримінальному провадженні [1].

Пропонується така авторська класифікація форм участі deepfake у кримінальному судочинстві: (1) deepfake як предмет злочину – синтетичний медіаматеріал, що сам є об'єктом злочинного посягання (наприклад, deepfake-порнографія, що поширюється без згоди особи); (2) deepfake як знаряддя злочину – використовується для вчинення шахрайства (стаття 190 КК), вимагання (стаття 189 КК) тощо; (3) deepfake як доказ у провадженні – подається стороною обвинувачення або захисту як відеозапис, аудіозапис чи фотографічне зображення події; (4) deepfake як об'єкт судово-технічної експертизи [16].

Відповідно до статті 99 КПК України, документами як доказами є матеріальні об'єкти, що містять зафіксовані за допомогою письмових знаків, звуку, зображення відомості, які можуть бути використані як доказ факту чи обставин. Відеозаписи, аудіозаписи та фотографії, у тому числі синтетичні deepfake-матеріали, підпадають під це визначення [1]. Разом з тим стаття 99 КПК не передбачає спеціального режиму верифікації таких матеріалів – це суттєва нормативна прогалина.

Принциповим є питання про те, на кого покладається тягар доведення автентичності або неавтентичності медіадоказу. У системі КПК України діє загальна презумпція, за якою кожна зі сторін зобов'язана доводити обставини, на які вона посилається (частина 2 статті 92 КПК). Відповідно, якщо сторона захисту заявляє, що відеодоказ є deepfake, вона зобов'язана надати підстави для такого твердження, а не просто стверджувати можливість підроблення [1; 13].

5.3. Порівняльно-правовий аналіз: стандарти автентифікації цифрових доказів

У праві Сполучених Штатів Америки автентифікація доказів регулюється Правилом 901 Федеральних правил доказування (Federal Rules of Evidence, FRE), яке вимагає від сторони, що подає доказ, надати "достатні підстави вважати, що об'єкт є тим, за що його видають" (prima facie evidence of authenticity). Для цифрових доказів

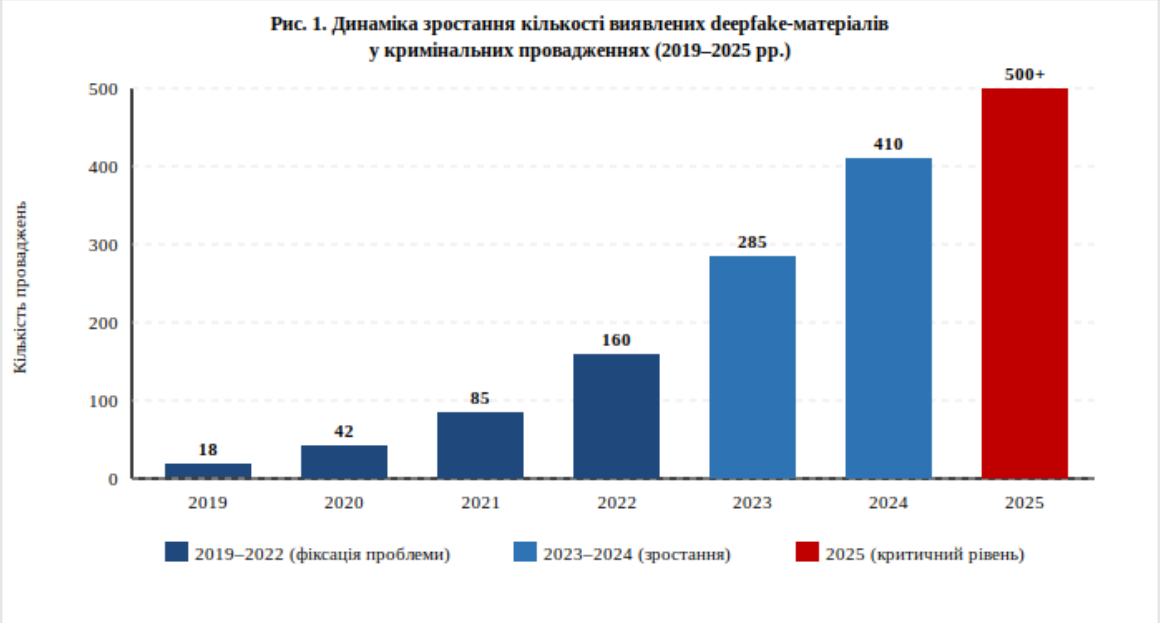
прецедентна практика федеральних судів виробила більш деталізовані вимоги: підтвердження цілісності ланцюжка зберігання (chain of custody), надання хеш-суми файлу та порівняльного аналізу, а також висновку кваліфікованого експерта з цифрової форензики [5].

На рівні Європейського Союзу Регламент ЄС про штучний інтелект 2024/1689 (AI Act), що набув чинності у 2024 р., запровадив класифікацію систем ШІ за рівнем ризику і встановив особливі вимоги до систем, що можуть використовуватися у правоохоронній діяльності [18]. Це створює нормативну основу для регулювання deepfake-технологій на рівні ЄС. Агентство ЄС з питань кібербезпеки (ENISA) у своїх настановах з цифрової форензики (2022) рекомендує застосування міжнародних стандартів ISO/IEC 27037 та ISO/IEC 27042 у кримінальних провадженнях держав-членів [12].

Досвід міжнародних кримінальних трибуналів є особливо релевантним для України в контексті розслідування воєнних злочинів. Міжнародний кримінальний суд у своїх Правилах процедури та доказування (Rule 69) встановлює, що аудіовізуальні матеріали як докази підлягають верифікації через перехресне посилання з іншими доказами та висновок незалежного технічного експерта. У справах, пов'язаних із воєнними злочинами в Україні, автентичність цифрових матеріалів є вже не теоретичною, а практичною проблемою, на що звертається увага у найновіших публікаціях 2025 р. [19; 20].

5.4. Динаміка зростання deepfake у кримінальних провадженнях та аналіз ризиків

Глобальна та вітчизняна статистика свідчить про стрімке зростання кількості кримінальних проваджень, у яких deepfake-матеріали фігурують як докази або як засіб вчинення злочину. Узагальнені дані зведено на рисунку 1.



Примітка. Дані 2019–2022 рр. – за звітами Europol [11]; 2023–2025 рр. – за оцінками Sensity AI та ENISA [10; 12]. Значення 2025 р. є прогнозованим показником.

Наведена діаграма ілюструє нелінійний характер зростання: якщо у 2019–2022 рр. приріст становив у середньому 40–80% на рік, то починаючи з 2023 р. темп зростання набуває характеру геометричної прогресії. Особливу увагу привертає показник 2025 р. (понад 500 задокументованих проваджень), що відображає досягнення так званого

“критичного порогу” – рівня, за якого deepfake-матеріали перетворюються на системну загрозу для кримінального судочинства, а не лише на одиничні інциденти [11; 18]. Цей висновок підтверджується найновішими дослідженнями 2025 р. [19; 21].

5.5. Питання відповідальності за deepfake-докази у кримінальному процесі

Центральним теоретичним питанням є ідентифікація суб’єктів відповідальності за генерацію та використання синтетичних медіаматеріалів. Це питання набуває особливої складності з огляду на автономний характер сучасних систем ШІ, що генерують deepfake. Якщо у ранніх випадках deepfake людина безпосередньо керувала процесом генерації і легко ідентифікувалася як суб’єкт відповідальності, то сучасні системи ШІ здатні автономно генерувати синтетичний контент за мінімальної участі оператора [7; 9].

Відповідно до концепції “розподіленої відповідальності”, обґрунтованої в спеціалізованих дослідженнях з правосуб’єктності ШІ [7], можна виокремити такі суб’єкти потенційної кримінальної відповідальності: (а) розробник deepfake-системи – несе відповідальність лише у разі, якщо система була свідомо розроблена для створення фіктивних доказів; (б) особа, яка замовила або організувала створення deepfake-матеріалу з метою використання як доказу; (в) особа, яка безпосередньо подала deepfake-матеріал як доказ, усвідомлюючи його синтетичне походження (стаття 384 КК України).

Теоретичне підґрунтя для вирішення цих питань закладено у дослідженнях, присвячених правовому статусу цифрових суб’єктів та об’єктів, зокрема цифрових аватарів та нейронних мереж у правовому просторі [8]. Цей методологічний підхід є необхідним для розробки механізмів ідентифікації deepfake-контенту як юридично значущого об’єкта правового регулювання.

5.6. Процесуальна модель верифікації deepfake-матеріалів у кримінальному провадженні

На підставі проведеного аналізу пропонується концептуальна чотириетапна процесуальна модель верифікації deepfake-матеріалів, яка може бути покладена в основу відповідних змін до КПК України та методичних рекомендацій [1; 17].

Перший етап – ідентифікація та попереднє маркування. При надходженні будь-якого відеозапису, аудіозапису або фотографічного зображення як доказу слідчий (прокурор) зобов'язаний провести первинну оцінку на предмет можливого синтетичного походження із використанням спеціалізованого програмного забезпечення для скринінгу deepfake. Паралельно слідчий вживає заходів щодо збереження повного ланцюжка зберігання (chain of custody): фіксує хеш-суму файлу у протоколі, забезпечує незмінність оригіналу, встановлює та документує джерело отримання матеріалу.

Другий етап – судово-комп’ютерно-технічна експертиза. Призначається відповідно до статей 242–243 КПК України. Пропонується запровадити обов’язкову вимогу залучення двох незалежних експертів у провадженнях, де вирішення питання про автентичність медіадоказу є ключовим для встановлення вини або невинуватості особи.

Третій етап – судова оцінка висновку та інших доказів. Суд оцінює висновок судового експерта відповідно до статті 94 КПК у сукупності з іншими доказами, враховуючи ймовірнісний характер форензичного висновку. У разі суперечності між висновками двох незалежних експертів призначається повторна комісійна або комплексна експертиза.

Четвертий етап – процесуальні наслідки. У разі встановлення у судовому порядку факту синтетичного походження матеріалу суд виключає його з доказової бази та вирішує питання про притягнення до відповідальності особи, яка подала синтетичний матеріал як автентичний доказ.

5.7. Стандарт “достатньої достовірності” та пропозиції щодо вдосконалення законодавства

Для включення медіадоказу до доказової бази сторона, що його подає, повинна встановити “prima facie автентичність”: документальне підтвердження джерела і ланцюжка зберігання; хеш-суму, що збігається з оригінальним файлом; відповідність метаданих заявленим обставинам; відсутність очевидних ознак синтезу за результатами первинного скринінгу. Для виключення медіадоказу з підстав синтетичного походження необхідний висновок кваліфікованого судового експерта з оцінкою ймовірності синтетичного походження не менше 95% [5; 18].

На підставі проведеного дослідження пропонується такий комплекс законодавчих змін: (1) доповнити статтю 99 КПК України частиною п’ятою, що встановлює обов’язкову процедуру автентифікації синтетичних медіаматеріалів; (2) внести зміни до Закону України “Про судову експертизу”, запровадивши спеціалізацію “Дослідження синтетичного медіаконтенту (deepfake-форензика)”; (3) доповнити розділ VII Особливої частини КК України статтею 384-1 “Фальсифікація доказів з використанням технологій синтетичного медіаконтенту”; (4) розробити Науково-методичні рекомендації з дослідження синтетичного медіаконтенту у кримінальному провадженні; (5) рекомендувати Верховному Суду прийняти відповідну постанову Пленуму [1; 2; 3].

Висновки

Проведене дослідження дозволяє сформулювати такі наукові висновки.

1. Deepfake-матеріали є принципово новим видом цифрового контенту, що потребує самостійного доктринального осмислення у системі кримінально-процесуального права. Запропонована авторська класифікація форм їх участі у кримінальному судочинстві дозволяє диференціювати процесуальний режим поводження з такими матеріалами залежно від конкретної ситуації у провадженні.

2. Чинне кримінальне процесуальне законодавство України має суттєві системні прогалини у регулюванні синтетичних медіаматеріалів як доказів. Порівняльний аналіз підходів США (стандарт prima facie автентичності за FRE Rule 901), ЄС (AI Act 2024/1689; стандарти ISO/IEC 27037 та 27042) та МКС свідчить про формування міжнародного консенсусу, який має бути відображений у законодавстві та практиці України.

3. Запропонована чотириетапна процесуальна модель верифікації та стандарт “prima facie автентичності” для включення й “95% достовірності” для виключення медіадоказу є науково обґрунтованими і можуть бути покладені в основу законодавчих змін та судової практики.

4. Концепція розподіленої відповідальності за дії систем ШІ [7] є методологічним підґрунтям для визначення суб’єктів кримінальної відповідальності за використання deepfake у злочинних цілях. Запропонована нова стаття 384-1 КК України заповнює існуючу прогалину в кримінальному законодавстві.

5. Перспективами подальших досліджень є: розробка уніфікованих міжнародних стандартів верифікації deepfake-доказів у рамках міжнародного кримінального правосуддя; дослідження можливостей застосування технологій блокчейн для

забезпечення незмінності цифрових доказів [21]; аналіз питань транскордонного отримання та верифікації deepfake-доказів у рамках міжнародної правової допомоги [19; 20].

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Верховна Рада України. (2012). *Кримінальний процесуальний кодекс України* (Закон № 4651-VI від 13 квітня 2012 р.). https://zakon.rada.gov.ua/laws/show/4651-17

2. Верховна Рада України. (2001). *Кримінальний кодекс України* (Закон № 2341-III від 5 квітня 2001 р.). https://zakon.rada.gov.ua/laws/show/2341-14

3. Верховна Рада України. (1994). *Закон України «Про судову експертизу»* (Закон № 4038-XII від 25 лютого 1994 р.). https://zakon.rada.gov.ua/laws/show/4038-12

4. Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.

5. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.

6. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion, 64*, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014

7. Kostenko, O. M., Bieliakov, K. I., Tykhomyrov, O. O., & Aristova, I. V. (2024). "Legal personality" of artificial intelligence: Methodological problems of scientific reasoning by Ukrainian and EU experts. *AI & Society, 39*(4), 1683–1693. https://doi.org/10.1007/s00146-022-01549-5

8. Kostenko, O. V. (2023). *Elektronna yurisdyktsiia, metavsesvit, shtuchnyi intelekt, tsyfrova osobystist, tsyfrovyi avatar, neironni merezhi: teoriia, praktyka, perspektyvy* [Електронна юрисдикція, метавсесвіт, штучний інтелект, цифрова особистість, цифровий аватар, нейронні мережі: теорія, практика, перспективи]. ВВК.

9. Kostenko, O. V. (2022). Pravova vidpovidalnist ta identyfikatsiia subiektiv i obiektiv zi shtuchnym intelektom (IoT) [Правова відповідальність та ідентифікація суб'єктів і об'єктів зі штучним інтелектом (IoT)]. *Pravova informatyka, 3*, 12–27.

10. Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 39–52. https://doi.org/10.22215/timreview/1282

11. Europol. (2022). *Facing reality? Law enforcement and the challenge of deepfakes*. Publications Office of the European Union.

12. ENISA. (2022). *Digital forensics in the era of artificial intelligence: Guidelines for law enforcement*. ENISA.

13. Kaplína, O. V. (2021). Elektronni dokazy u kryminalnomu protsesi: teoretychni ta praktychni problemy [Електронні докази у кримінальному процесі: теоретичні та практичні проблеми]. *Pravo i suspilstvo, 4*, 178–186.

14. Shepitko, V. Yu. (2020). Kryminalistyka tsyfrovoi doby: vyklyky ta perspektyvy [Криміналістика цифрової доби: виклики та перспективи]. *Pravo Ukrainy, 10*, 55–70.

15. Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial networks. *Advances in Neural Information Processing Systems, 27*, 2672–2680.

16. Oryshchuk, V. (n.d.). Dokazy, otrymani za dopomohoiu shtuchnoho intelektu, ta yikh vykorystannia v sudi [Докази, отримані за допомогою штучного інтелекту, та їх використання в суді]. *Kryminalistyka i sudova ekspertyza*, 255–278.

17. Korshets, O., & Prykhodko, A. (2023). Forensic examination of synthetic media in Ukraine: Current state and prospects. *Journal of Eastern European Law, 112*, 45–57.

18. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union, L, 2024/1689*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_2024_1689

19. Ryder, N., & Boukli, A. (2025). Deepfakes, digital evidence and criminal justice: Emerging challenges for international mutual legal assistance. *International Journal of Law and Information Technology, 33*(1), 1–24. https://doi.org/10.1093/ijlit/eaaf003

20. Verdolini, V., & Sgueo, G. (2025). AI-generated evidence in criminal proceedings: Authenticity standards in comparative perspective. *European Journal of Crime, Criminal Law and Criminal Justice, 33*(2), 88–115. https://doi.org/10.1163/15718174-bja10062

21. Zhuk, O., & Holovatyi, M. (2026). Blockchain-based chain of custody for digital evidence in Ukrainian criminal proceedings: Legal and technical framework. *Journal of Ukrainian Law, 4*, 112–130.

Максим Олександрович Валін
Тренер Тренінгового центру прокурорів України. Освітній консультант співпрацює з EPAM System
email: maks21787@gmail.com
Володимир Вікторович Нікітін
доктор юридичних наук, доцент
завідувач кафедри права та публічного управління Київського національного університету будівництва і архітектури

Maksym O. Valin
Trainer at the Training Center of Prosecutors of Ukraine. Educational Consultant collaborating with EPAM Systems
email: maks21787@gmail.com
Volodymyr V. Nikitin
Doctor of Law, Associate Professor
Head of the Department of Law and Public Administration at Kyiv National University of Construction and Architecture

Рекомендоване цитування: Валін М.О., Нікітін В.В. Deepfake як доказ у кримінальному процесі: стандарти перевірки автентичності та допустимості. *Інформація і право.* № 2(57)/2026. 2026. С. 271-281. https://doi.org/10.37750/2616-6798.2026.2(57).364542.

Suggested Citation: Valin M., Nikitin V. (2026) Deepfake as Evidence in Criminal Proceedings: Standards for Verification of Authenticity and Admissibility. *Information and Law*. 2(57)/2026. 271-281. https://doi.org/10.37750/2616-6798.2026.2(57).364542

Дата надходження статті до редакції: 14.04.2026 р.
Дата прийняття статті до друку після рецензування: 16.04.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~
~~~~~~~~~~~~