УДК 343.98:004.8
DOI: 10.21564/2414-990X.171.342859

Правові та криміналістичні аспекти роботи з електронними документами, згенерованими штучним інтелектом

Олександр Вікторович Габро*
Навчально-науковий інститут права
Державного податкового університету,
Ірпінь, Україна
**e-mail: Oleksandr763@proton.me*

Анотація
Актуальність дослідження обумовлена стрімким розвитком технологій штучного інтелекту та їх інтеграцією у процеси створення електронних документів, що спричиняє появу суттєвих проблем у правовій та криміналістичній сферах, зокрема щодо визнання таких документів доказами. Мета статті полягає у висвітленні правових та криміналістичних викликів, пов'язаних з атрибуцією, доказовою силою та встановленням відповідальності за електронні документи, згенеровані штучним інтелектом. Методи аналізу включали системний, порівняльно-правовий, формально-юридичний і криміналістичний методи дослідження електронних доказів. Отримані результати свідчать про необхідність розробки нових підходів до оцінки достовірності та належності електронних документів, створених штучним інтелектом, а також впровадження спеціалізованих криміналістичних методик для встановлення їхнього походження та можливого втручання. Особлива увага приділена питанням атрибуції, оскільки пряма відповідальність за діями штучного інтелекту відсутня. Перспективи подальших досліджень пов'язані з розробкою уніфікованих міжнародних стандартів для роботи з доказами ШІ-генерації та вдосконаленням національного процесуального законодавства.

Ключові слова: штучний інтелект; електронний документ; доказ; атрибуція; криміналістика; відповідальність.

Legal and Forensic Aspects of Working with Electronic Documents Generated by Artificial Intelligence

Oleksandr V. Gabro*
Educational and Scientific Institute of Law of the State Tax University, Irpin, Ukraine
**e-mail: Oleksandr763@proton.me*

Abstract
The relevance of the research is due to the rapid development of artificial intelligence (AI) technologies and their integration into the process of creating electronic documents, which creates significant problems in the legal and forensic fields, particularly regarding the admissibility of such documents as evidence. The purpose of the article is to highlight the legal and forensic challenges associated with the attribution, probative value, and establishment of liability for electronic documents generated by AI. Methods of analysis included systemic, comparative-legal, formal-legal, and forensic methods for the study of electronic evidence. The results obtained indicate the need to develop new approaches to assessing the reliability and relevance of electronic documents created by AI, as well as the implementation of specialized forensic techniques to establish their origin and possible intervention. Particular attention is paid to attribution issues, as there is no direct liability for the actions of AI. The prospects for further research are related to the development of unified international standards for working with AI-generated evidence and the improvement of national procedural legislation.

Keywords: artificial intelligence; electronic document; evidence; attribution; forensics; liability.

Вступ

Інтенсивне впровадження та стрімке поширення технологій штучного інтелекту (ІІІІ) в усіх сферах суспільного життя, зокрема у процесі створення та обігу електронної документації, ознаменували принципово нову еру, яка ставить безпрецедентні виклики перед юридичною практикою та криміналістичною наукою. Сучасні генеративні моделі ІІІІ здатні створювати тексти, зображення, аудіо- та відеоматеріали, які за своїми зовнішніми ознаками повністю відповідають критеріям електронних документів і можуть бути використані як докази у судових процесах [1]. Цей технологічний прорив висуває на перший план глибоку методологічну проблему: як забезпечити достовірність, належність та допустимість доказів, джерелом яких є не людина, а алгоритм. Традиційні криміналістичні підходи, які ґрунтувалися на ідентифікації людини-творця або встановленні його унікального почерку/стилю, виявляються недостатніми для атрибуції та верифікації ІІІІ-згенерованого контенту [2; 3].

Актуальність дослідження посилюється критичною відсутністю чіткого законодавчого регулювання статусу документів, згенерованих ІІІІ, як у національному, так і у міжнародному правовому полі. На сучасному етапі не визначені ані правові механізми встановлення юридичної відповідальності за зміст або використання такого контенту у злочинних цілях, ані процедури його фіксації та вилучення. Особливої гостроти проблема набуває в контексті створення високоякісних підробок, технології deepfakes, які за лічені секунди можуть сфабрикувати переконливі докази злочинної діяльності чи, навпаки, неправдиво викрити невинну особу. Цей феномен ускладнює процес атрибуції джерела (людина-оператор, ІІІІ-модель, або програмне середовище) та вимагає термінової розробки новітніх, адаптованих до алгоритмічної природи даних, криміналістичних методик [4].

Сучасний стан проблеми на вітчизняному та світовому рівнях свідчить про активне, але фрагментарне обговорення перерахованих питань. Українські науковці вже окреслили певні грані цієї теми: наприклад, П. Клімушин [5] досліджує нагальну потребу чіткого законодавчого врегулювання та стандартизації функціональної безпеки Інтернету речей (IoT), підкреслюючи, що чинні норми є недостатніми для забезпечення захисту користувачів від кіберризиків. Цей аспект безпосередньо корелює з необхідністю забезпечення безпеки обробки та зберігання даних, які згодом можуть стати електронними доказами, згенерованими ІІІІ. О. Герасимів [6] акцентує, що, попри невпинне зростання кіберзлочинності та активне використання електронних доказів (наприклад, скріншотів) у кримінальному судочинстві, чинне українське законодавство є недостатньо врегульованим і суперечливим. Технології ІІІІ лише багаторазово посилюють наявні розбіжності, ставлячи під сумнів доказову силу будь-якої неатрибутивної цифрової інформації.

Закордонні дослідження, зокрема наукові праці F. Zhang [7], які стосуються проблем авторського права на ІІІІ-генерований контент, та S. Gupta і P. Sharma [8], присвячені етиці та праву ІІІІ, підкреслюють глобальний характер викликів. Ці дослідження свідчать про те, що світова спільнота схиляється до пошуку рішень не стільки у сфері технічного виявлення підробок, скільки у розробці правових презумпцій щодо авторства, відповідальності та процесуальної легітимізації ІІІІ-документів. Аналіз останніх досліджень (за 2023–2025 рр.) вказує на зміщення фокусу з суто технічних аспектів роботи ІІІІ на його глибокі юридичні та криміналістичні наслідки, проте комплексного та системного вирішення проблеми статусу ІІІІ-документів як повноцінних доказів, зокрема у кримінальному процесі України, ще не знайдено.

Таким чином, утворюється значний правовий та криміналістичний розрив (legal and forensic gap) між технологічною здатністю ІІІІ генерувати докази

та процесуальною нездатністю правової системи їх коректно оцінити та використовувати. Це зумовлює наукову потребу в розробленні чіткої методологічної бази.

Основна мета дослідження – проаналізувати юридичні та криміналістичні перешкоди на шляху визнання електронних документів, створених ІІІІ, повноцінними доказами у кримінальному провадженні та запропонувати шляхи вдосконалення процедур їх ідентифікації, верифікації й притягнення до відповідальності винних осіб.

Для досягнення поставленої мети було визначено такі завдання:

- проаналізувати чинне законодавство України щодо визнання електронного документа доказом у контексті його генерації ІІІІ та виявити ключові колізії;
- визначити та класифікувати криміналістичні проблеми ідентифікації й атрибуції ІІІІ-документів (зокрема, встановлення ланцюга постачання даних та програмного забезпечення);
- обґрунтувати необхідність розробки нових підходів до оцінки достовірності та належності електронних документів, створених ІІІІ, включно із запровадженням концепції «цифрового підпису алгоритму»;
- розглянути питання кримінальної юридичної відповідальності за зміст ІІІІ-документів та їх використання у протиправній діяльності, пропонуючи механізми ідентифікації кінцевого бенефіціара/оператора ІІІІ.

Огляд літератури

Проблема правового регулювання та криміналістичного дослідження продуктів діяльності ІІІІ є відносно новою, але динамічно розвивається, ставлячи перед юридичною наукою та правозастосовною практикою унікальні виклики. Поява ІІІІ-генерованого контенту, який може виступати як цифровий доказ чи об'єкт злочинного посягання, потребує ґрунтовної переоцінки традиційних підходів до збирання, перевірки та оцінки доказів. У вітчизняній науці правові аспекти регулювання ІІІІ та цифрових доказів активно досліджуються [9; 10]. Українські вчені зосереджують увагу на необхідності адаптації національного законодавства до реалій цифрової трансформації. Зокрема, В. Шаблистий [11] наголошує на невідкладній потребі адаптації кримінального та кримінального процесуального законодавства до сучасних цифрових реалій. Дослідник підкреслює унікальність цифрових слідів і необхідність розробки нових механізмів їхнього виявлення та фіксації, що прямо стосується ІІІІ-генерованих даних, які можуть бути як доказом, так і об'єктом фальсифікації.

Своєю чергою, К. Яровий [12] детально аналізує криміналістичні питання ідентифікації особи за електронними слідами. Ця проблема набуває принципово нового змісту в контексті ІІІ-генерації. Якщо раніше йшлося про ідентифікацію людини, яка створила слід, то зараз «особою», що залишила слід, може бути не людина, а алгоритм або програмний комплекс. Це вимагає розширення понятійного апарату криміналістики та розробки методів ідентифікації самого алгоритму як джерела інформації. Л. Мілімко [13] приділяє значну увагу питанням доказової сили електронних документів. Автор виокремлює виклики, пов'язані з їхньою змінною (мінливою) природою (volatility), а також із легкістю їх модифікації. Ці аспекти критично важливі для ІІІ-контенту, оскільки технології на кшталт deepfake можуть створювати ідеально імітовані, але повністю сфабриковані докази, що ставить під сумнів їхню автентичність та допустимість.

У зарубіжній літературі значний внесок зроблено у вивчення проблем атрибуції та відповідальності за діяльність ІІІ. Krishna Pasupuleti M. [14] у своїх працях акцентує увагу на основах цифрової криміналістики (Digital Forensics). Дослідник підкреслює необхідність її системного застосування для ефективного виявлення, збору та розкриття кібердоказів (cyber evidence). Підхід цифрової криміналістики є методологічною основою для дослідження будь-яких електронних слідів, включно з тими, що були створені або модифіковані ІІІ. Акцент наукових праць E. Hydara, M. Kikuchi, T. Ozono [15] зосереджено на гострій проблемі допустимості deepfakes як доказів. Вчені не лише підкреслюють важливість питання їхньої достовірності, а й пропонують конкретні механізми криміналістичної валідації таких матеріалів. Ключовою тезою їхньої роботи є висновок про те, що для належної атрибуції ІІІ-документа недостатньо встановити лише його кінцевого користувача або особу, яка натиснула кнопку «генерувати». Криміналістичне дослідження має містити також дослідження самого алгоритму, моделі даних, на якій він навчався, та середовища (платформи), в якому відбулася генерація цього контенту. Тільки комплексний аналіз цих елементів може забезпечити встановлення істинності та допустимості.

Попри те, що зазначені наукові праці, як вітчизняні, так і закордонні, є фундаментальними і становлять міцну теоретичну базу, вони часто не дають готових прикладних рішень для безпосереднього впровадження у правозастосовну практику в Україні. Наявні національні криміналістичні методики та процесуальні норми недостатньо гнучкі для роботи з динамічною природою ІІІ-доказів. Цей розрив між теоретичними напрацюваннями та практичними потребами підкреслює нагальну потребу у власному, специфічному для національної системи права, науковому пошуку. Останній має бути

спрямований на розроблення конкретних методик експертного дослідження ШІ-генерованих продуктів та відповідної процесуальної регламентації їхнього використання в доказуванні.

Матеріали та методи

Дослідження ґрунтується на всебічному аналізі нормативно-правової бази України, міжнародних актів та значного масиву наукових джерел з права, криміналістики та інформаційних технологій. Нормативну основу становлять ключові документи, що регулюють процесуальні та електронні відносини, зокрема: Кримінальний процесуальний кодекс (КПК) України [16], який визначає порядок збирання, перевірки та оцінки доказів, та Закон України «Про електронні документи та електронний документообіг» [17], що встановлює вимоги до юридичної сили електронних документів. Крім того, було проаналізовано відповідні положення Кримінального кодексу України, закони та кодекси країн ЄС, що стосуються кібербезпеки та електронної ідентифікації, а також інші акти, які регламентують використання інформаційних технологій у судочинстві.

Науково-теоретичну базу дослідження становлять праці вітчизняних і зарубіжних науковців, присвячені теорії доказів, цифровій криміналістиці (forensics), правовому регулюванню штучного інтелекту, а також міжнародні регуляторні ініціативи. Серед останніх – проєкт Регламенту Європейського Союзу про штучний інтелект (EU AI Act), який вперше намагається комплексно класифікувати та регулювати ШІ-системи відповідно до рівня ризику. Також було досліджено прецедентну практику щодо використання deepfakes як доказів у США та країнах Європи, що дозволило виявити спільні підходи та розбіжності у судовій оцінці ШІ-генерованого контенту.

Основні етапи проведеного дослідження були такими. Дослідження було структуровано і реалізовано шляхом послідовного виконання трьох взаємопов'язаних етапів, що забезпечили логічний перехід від теоретичного аналізу до формування практичних рекомендацій:

1) аналіз правового статусу ШІ-генерації. На цьому етапі було проведено детальний аналіз чинних положень щодо вимог до електронних документів як доказів (цілісність, автентичність, доступність), визначених КПК та профільним законодавством [16; 17]. Особлива увага приділялася виявленню правових прогалин і колізій, що виникають унаслідок відсутності суб'єкта-людини як єдиного творця документа. Було визначено момент набуття згенерованим ШІ-контентом статусу електронного документа, а також умови, за яких такий контент може бути легалізований у процесі доказування [13];

2) визначення криміналістичних викликів. Етап передбачав систематизацію ключових криміналістичних викликів, пов'язаних з ідентифікацією та атрибуцією електронних документів, створених ШІ. Проводилася класифікація можливих «авторів» електронного документа (користувача-оператора, розробника моделі, власника платформи або, гіпотетично, самого ШІ як квазісуб'єкта). Вивчалися методики трасування цифрових слідів, які залишає алгоритм (аналіз промптів, log files, метаданих), що є необхідною передумовою для встановлення джерела та цілісності інформації;
3) розробка концептуальних підходів. На фінальному етапі було сформульовано пропозиції щодо критеріїв допустимості та достовірності ШІ-документів у кримінальному процесі. Це включало обґрунтування необхідності запровадження спеціальних процесуальних процедур, таких як обов'язкове розкриття інформації про ШІ-модель, що використовувалася, та криміналістичних експертиз, спрямованих на верифікацію алгоритмічного походження доказу та встановлення відповідальності.

Обґрунтування вибору методів дослідження: для забезпечення глибини, всебічності та об'єктивності дослідження було застосовано комплекс загальнонаукових, логічних та спеціально-юридичних методів:

– діалектичний метод був застосований для вивчення ШІ-документа як діалектичної єдності форми (незмінний електронний слід) і змісту (інформація, згенерована алгоритмом, що може бути змінена або сфальсифікована). Метод дозволив проаналізувати суперечності між традиційними процесуальними нормами, які потребують встановлення умислу людини, та новими технологічними реаліями, де алгоритм виступає як квазітворець. Це забезпечило розгляд процесу генерації ШІ у динаміці його впливу на правовідносини;
– порівняльно-правовий метод використовувався для зіставлення вітчизняного законодавства про докази з міжнародним досвідом регулювання ШІ. Зокрема, було проаналізовано підходи, закладені в Регламенті ЄС про ШІ (AI Act) щодо прозорості та оцінки ризиків систем ШІ, а також законодавчі ініціативи інших країн щодо боротьби з deepfakes. Метою було виявлення та обґрунтування кращих міжнародних практик для їх імплементації в українське кримінальне процесуальне законодавство;
– формально-юридичний метод дав змогу здійснити чіткий, структурний аналіз положень КПК України [16], Закону України «Про електронні документи та електронний документообіг» [17] та інших нормативних

актів. Цей метод був критично важливим для визначення точного юридичного статусу ШІ-документа, аналізу термінології («оригінал електронного документа», «автор», «цілісність») та виявлення правових умов для його допустимості як доказу;
- системно-структурний метод використовувався для дослідження ШІ-документа не ізольовано, а як елемента складної системи «людина-алгоритм-інформаційне середовище». Застосування цього методу є ключовим для встановлення об'єктивної атрибуції та визначення відповідальності, адже дає можливість оцінити роль кожного компонента системи (введення даних користувачем, логіка роботи ШІ-моделі, налаштування платформи) у створенні кінцевого доказу;
- криміналістичний метод (методика дослідження електронних доказів) був застосований для формування гіпотез щодо необхідності запровадження спеціалізованих криміналістичних експертиз нового покоління. Ці експертизи мають бути спрямовані на трасування промптів (текстових або інших команд, що викликали генерацію), логів роботи ШІ-моделі (журналів її використання), та встановлення наявності «цифрових водяних знаків» (якщо вони застосовані розробником). Метою є не лише встановлення факту генерації ШІ, а й визначення, хто ініціював процес, з якою метою та чи було втручання після генерації.

Цей комплексний підхід забезпечив глибокий аналіз як правових, так і технічних аспектів проблеми, що дало змогу сформулювати науково обґрунтовані рекомендації.

Результати та обговорення

Правові виклики визнання ШІ-документа доказом у кримінальному провадженні

Аналіз чинного КПК України [16] у контексті інтеграції ШІ у сферу документування виявляє низку фундаментальних правових викликів щодо визнання електронних документів, згенерованих ШІ, належними, допустимими та достовірними доказами. Принципова відмінність ШІ-документа від традиційного електронного документа полягає в автономності його генерації, що трансформує класичні критерії оцінки доказів.

Проблема належності (Relevance) та атрибуції

Належність доказу (ст. 85 КПК України [16]) вимагає, щоб зміст інформації мав безпосереднє значення для встановлення обставин, які підлягають доказуванню. Попри те, що змістове наповнення ШІ-документа може бути

високорелевантним для справи, його походження та механізм генерації ускладнюють оцінку. У цьому випадку виникає питання нової парадигми походження, Так, у традиційному розумінні, походження доказу пов'язане з діями фізичної або юридичної особи. У випадку ШІ, походження зміщується до алгоритмічного процесу, що ставить під сумнів можливість прямої атрибуції до конкретного суб'єкта, відповідального за кінцевий зміст. Це вимагає розширення тлумачення поняття «джерело доказу» з включенням валідованої ШІ-системи як легітимного джерела інформації [7].

Наприклад, у справі про шахрайство ключовим доказом є звіт, згенерований системою фінансового моніторингу на основі ШІ, який виявив аномальні трансакційні патерни та автоматично склав узагальнену хронологію підозрілих операцій. Належність цього ШІ-документа є беззаперечною, оскільки зміст (хронологія та патерни) прямо доводить обставини, що підлягають доказуванню (схему шахрайства). Проте походження цього доказу є нетрадиційним: він є не прямим свідченням особи або документом, створеним людиною, а результатом складного алгоритмічного процесу (нейронної мережі), що робить неможливим атрибуцію кінцевого змісту до конкретного працівника банку або розробника системи. Для забезпечення допустимості такого доказу суд повинен визнати валідовану ШІ-систему (що пройшла аудит і відповідає критеріям надійності) легітимним джерелом інформації, розширюючи тлумачення «джерела доказу» за межі лише фізичних або юридичних осіб.

Проблема допустимості (Admissibility) та технічна автентифікація

Допустимість доказу (ст. 86 КПК України [16]) вимагає його отримання та фіксації у порядку, встановленому законом. Цей критерій є найбільш вразливим для ШІ-документів через необхідність контролю над процесом їх генерації. У зазначеному аспекті йдеться про регулювання вхідних даних (промптів). Ключовим моментом для забезпечення допустимості є дотримання процедури отримання та фіксації вхідних даних (промптів), які слугували основою для генерації. Потрібно розробити процесуальні стандарти, які б гарантували незмінність, законність отримання та повний облік усіх вхідних параметрів [5]. Крім того, важливо зазначити про Концепцію «Технічної автентифікації». Критично необхідне введення в науково-правовий обіг та законодавство поняття «технічна автентифікація» ШІ-документа. Це поняття має охоплювати не лише підтвердження цілісності самого файлу, а й верифікацію алгоритмічного ланцюжка, моделі ШІ та вхідних даних, використаних для його створення. Така автентифікація повинна підтверджувати, що документ був згенерований саме заявленою, немодифікованою моделлю ШІ на основі зафіксованих вхідних даних [1].

Так, у кримінальному провадженні щодо кіберзлочину слідчий має намір використати звіт про аналіз мережевого трафіку, згенерований спеціалізованою ІІІ-системою на основі масиву необроблених даних (логістичних файлів) [3]. Для забезпечення допустимості доказу (ст. 86 КПК України) важливим є не лише фіксація самого фінального звіту, а й дотримання процедури отримання та фіксації вхідних даних (промптів / логістичних файлів), що були надані ІІІ-моделі для аналізу, щоб гарантувати їх незмінність і законність отримання [2]. Якщо ці вхідні параметри не були належним чином процесуально задокументовані, доказ може бути визнаний недопустимим. Тому ключовою вимогою стає технічна автентифікація ІІІ-документа, яка повинна підтвердити цілісність не лише кінцевого файлу, а й верифікувати алгоритмічний ланцюжок та засвідчити, що звіт був створений саме заявленою, немодифікованою моделлю ІІІ на основі зафіксованих і законно отриманих вхідних даних, забезпечуючи, таким чином, дотримання встановленого законом порядку отримання доказу.

Проблема достовірності (Reliability) та судова експертиза

Достовірність доказу (ст. 87 КПК України [16]) передбачає об'єктивне відображення факту, що має значення для справи. Основною загрозою для достовірності ІІІ-документів є феномен галюцинацій (hallucinations) генерації ІІІ правдоподібної, але фактично неточної або вигаданої інформації. У такому аспекті виникає ризик галюцинацій та питання об'єктивності. Через внутрішню непрозорість деяких ІІІ-моделей (Black Box), без спеціалізованого аналізу неможливо встановити, чи є згенерований документ відображенням об'єктивних фактів, або результатом помилки, зміщення (bias) моделі, або ж її «галюцинації». Це прямо підриває фундаментальний принцип об'єктивної істини у процесі доказування. Безпосередньо з цим процесом пов'язана вимога судової комп'ютерно-технічної експертизи. Традиційний підхід до електронного документа як доказу вимагає встановлення його цілісності та автентичності [6]. У випадку ІІІ-генерації, автентичність переходить у площину атрибуції (до ІІІ-системи) та валідації (алгоритмічного процесу). Таким чином, документ, створений ІІІ, може бути визнаний достовірним доказом виключно за умови, що його генерація була валідована шляхом судової комп'ютерно-технічної експертизи. Ця експертиза повинна включати: а) аналіз вхідних даних (промптів); б) верифікацію стану та конфігурації ІІІ-моделі на момент генерації; в) оцінку ймовірності галюцинацій або впливу зловмисних дій; г) підтвердження цілісності та незмінності кінцевого електронного документа.

Уведення обов'язкового експертного валідаційного механізму є єдиним шляхом для інтеграції ІІІ-документів у систему кримінально-процесуального доказування без шкоди для принципів законності та справедливості [9].

Наприклад, у справі про авторське право сторона захисту надає звіт, згенерований великою мовною моделлю (LLM), який нібито цитує наукові джерела, що підтверджують її позицію, але ключовою загрозою для достовірності доказу (ст. 87 КПК України [16]) є феномен галюцинацій, оскільки через непрозорість моделі (Black Box) неможливо без додаткового аналізу встановити, чи є ці цитати об'єктивним відображенням наявних фактів, або вони є правдоподібною, але вигаданою інформацією. Щоб підтвердити достовірність такого ШІ-документа та мінімізувати ризик галюцинацій чи впливу зміщення моделі, він має пройти обов'язкову судову комп'ютерно-технічну експертизу, що має містити аналіз вхідних даних (промптів), верифікацію конфігурації ШІ-моделі на момент генерації, оцінку ймовірності галюцинацій та підтвердження цілісності кінцевого документа, оскільки лише цей валідаційний механізм дає можливість забезпечити об'єктивну істину та інтегрувати ШІ-документ у доказову базу. Відмінності традиційного та ШІ-документа як доказу наведені у табл. 1.

Таблиця 1

Відмінності традиційного та ШІ-документа як доказу

Традиційний електронний документ	**Документ, згенерований ШІ (AI-generated Document)**
Автор. Фізична або юридична особа, яка ідентифікується підписом	Атрибутор. Користувач, розробник ШІ-моделі, або сама модель (як джерело інформації) [18]
Цілісність. Перевірка ЕЦП та хеш-суми	Цілісність. Перевірка метаданих генерації, логів взаємодії з ШІ-моделлю [19]
Достовірність. Оцінка змісту щодо відповідності фактам, часто за допомогою суб'єкта, що його створив	Достовірність. Оцінка на предмет галюцинацій, залежності від промпта (bias), потребує експертизи алгоритму [20]

* *Сформовано автором на підставі аналізу [18–20].*

Криміналістичні механізми атрибуції та виявлення фальсифікації

Проблема атрибуції ШІ-документів є центральною криміналістичною проблемою сучасності, оскільки традиційні методи ідентифікації автора чи джерела походження стають неефективними в контексті алгоритмічної генерації

[11]. На відміну від доказів, створених людиною, де атрибуція фокусується на ідіосинкразії письма чи дій, атрибуція ІІІІ-документа вимагає аналізу цифрового сліду та верифікації самого процесу генерації. Криміналістичний аналіз має бути спрямований на низку спеціалізованих техніко-криміналістичних механізмів [14].

Проблеми юридичної відповідальності

Відсутність суб'єктності у ІІІІ виключає можливість притягнення його самого до юридичної відповідальності. Основні концепції відповідальності:

1) відповідальність кінцевого користувача (оператора). Якщо користувач цілеспрямовано використовував ІІІІ для створення протиправного документа;
2) відповідальність розробника / провайдера (виробника). Якщо ІІІІ-система мала критичну ваду або розробник не вжив достатніх заходів безпеки.

Пропонується закріпити принцип контролю: відповідальність несе та особа, яка здійснювала контроль над процесом генерації або мала можливість йому запобігти.

Аналіз цифрового ланцюжка генерації

Насамперед критично важливим є аналіз промпт-інжинірингу, що передбачає глибоке вивчення вхідних даних (промптів), які використовувалися для ініціації та керування процесом генерації документа. Вивчення специфіки промптів, їхньої послідовності та параметрів, наданих користувачем, дозволяє встановити намір особи, що стоїть за генерацією, а також звузити коло потенційних суб'єктів, обізнаних із необхідною для промпту інформацією.

Паралельно, необхідне дослідження лог-файлів та метаданих взаємодії користувача з ІІІІ-платформою. Системні журнали (логи) містять хронологічні записи про доступ, запити та відповіді системи, які в сукупності створюють атрибутивний цифровий слід. Метадані генерації (включаючи ідентифікатор сесії, точний час, версію використаної ІІІІ-моделі та параметри конфігурації) мають бути обов'язковим елементом доказової бази, оскільки вони забезпечують верифікацію процесуальної чистоти та цілісності документа.

Виявлення технологічних ідентифікаторів

Крім того, критичну роль у боротьбі з фальсифікацією та встановленні джерела відіграє виявлення цифрових водяних знаків (Watermarking). Це невидимі мітки, які розробники ІІІІ-систем вбудовують у згенерований контент

(текст, зображення, аудіо) для його однозначної ідентифікації та прив'язки до конкретної моделі або навіть облікового запису користувача. Криміналістичні підрозділи мають бути оснащені спеціалізованими інструментами для виявлення та дешифрування цих стеганографічних міток, перетворюючи їх на надійний доказ походження.

Інституціоналізація спеціалізованої судової експертизи

Для забезпечення достовірності та допустимості ІІІ-документів у судовому процесі, потрібно запровадити спеціалізований вид судової експертизи – судову експертизу документів, згенерованих ІІІ. Основними завданнями цього інституту є:

1) встановлення факту генерації. Доведення того, що документ був створений заявленою, немодифікованою ІІІ-системою;
2) визначення параметрів моделі. Ідентифікація конкретної версії та конфігурації алгоритму, який продукував контент, для оцінки його потенційної схильності до зміщення або галюцинацій;
3) виявлення ознак модифікації. Комплексний аналіз щодо внесення змін як у вхідні промпти, так і в остаточний згенерований документ після його отримання від ІІІ-системи, що має ключове значення для підтвердження його цілісності та автентичності.

Цей спеціалізований експертний механізм є єдиним надійним способом подолання прозорості (Black Box) ІІІ-систем та забезпечення науково обґрунтованої інтеграції цифрових доказів нового покоління у правозастосовну практику.

Ураховуючи специфіку української правової системи, особливо принцип суворої формалізації кримінального процесу та жорсткі вимоги до допустимості доказу (ст. 86 КПК України [16]), малопридатними для прямої імплементації є надмірно дерегульовані або гнучкі підходи, що можуть існувати в деяких країнах ЄС (наприклад, у системах, в яких судді мають більшу дискрецію у визнанні «нетрадиційних» доказів). Будь-яка модель, яка намагається надати ІІІ-системі квазісуб'єктності або дозволяє її звітам використовуватися як доказ без обов'язкової технічної автентифікації та експертної валідації алгоритмічного ланцюжка, суперечитиме українській процесуальній традиції. Запозичення повинне уникати механізмів, які б розмивали поняття прямої атрибуції (контролю кінцевого користувача) та об'єктивної істини, підміняючи їх виключною довірою до «чорної скриньки» (Black Box) без можливості судового контролю (табл. 2).

Таблиця 2

Порівняльний аналіз регулювання доказової сили ШІ-документів: Україна vs. Країни ЄС

Країна	**Регулювання ШІ-документа як доказу (короткий опис)**	**Ключовий нормативно-правовий акт, який урегульовує окреслену сферу**	**Відмінність від Закону України «Про електронні документи та електронний документообіг»**
Україна	Визнає доказом електронний документ. Основний фокус на суб'єкті-авторі (особі) та його підписі. Не регулює технічну автентифікацію самого процесу генерації ШІ	КПК України [16], Закон України «Про електронні документи та електронний документообіг» [17])	
Німеччина, Франція, Італія, Іспанія та інші (національне право)	Визнають електронні документи рівнозначними паперовим у судовому процесі (за умови їхньої цілісності та автентичності). Прямого регулювання ШІ-доказу нині немає	Національні кримінально-процесуальні кодекси та закони про електронні докази [21; 22; 23; 24]	Пряма рівнозначність паперовим документам. Специфіка ШІ-доказу поки що вирішується через загальні правила вільної оцінки доказів
Європейський Союз (загальний вектор)	Встановлює горизонтальні вимоги до ШІ-систем високого ризику, що створює основу для допустимості їхніх результатів як доказів: прозорість, надійність, людський контроль	AI Act (Регламент; ЄС про ШІ) (введення в дію) [25]	Регулює сам процес створення доказу (систему ШІ), вимагаючи прозорості та контролю над моделями, що прямо впливає на критерії достовірності та допустимості в суді

**Сформовано автором на підставі аналізу [16; 17; 21–25].*

Висновки

Проведене дослідження підтверджує, що стрімкий розвиток технологій ШІ створив значний розрив між технологічними можливостями генерації електронних документів та чинним правовим і криміналістичним регулюванням їхнього статусу як доказів. Визнання документів, згенерованих штучним інтелектом (ШІ-документів), як належних, допустимих та достовірних доказів у кримінальному провадженні потребує комплексного переосмислення чинних правових та криміналістичних парадигм. Цей процес ґрунтується на необхідності трансформації традиційних критеріїв оцінки доказів, закріплених у КПК України, з метою адаптації до алгоритмічної природи походження інформації.

На підставі отриманих результатів дослідження можна зробити такі висновки.

Критерій належності доказу (ст. 85 КПК України) потребує законодавчого визнання нової парадигми походження інформації. Оскільки ШІ-документ виникає внаслідок алгоритмічного процесу, а не прямої волі або дії фізичної особи, традиційна атрибуція стає неможливою. Це змушує правову систему розширити поняття «джерело доказу», включивши до нього валідовану (сертифіковану) ШІ-систему. Тож, навіть якщо зміст є високорелевантним для справи, його юридична належність закріплюється через підтвердження легітимності самої системи-генератора, а не через ідентифікацію її людського автора.

Для дотримання вимоги допустимості доказу (ст. 86 КПК України), що передбачає його отримання у законний спосіб, потрібно запровадити Концепцію «Технічної автентифікації», яка виходить за рамки стандартної перевірки електронного підпису. Суть полягає в контролі за всім ланцюжком генерації. Процесуальні стандарти повинні вимагати фіксації та гарантування законності отримання і незмінності вхідних даних (промптів). Технічна автентифікація, таким чином, повинна верифікувати алгоритмічний ланцюжок та конфігурацію ШІ-моделі, засвідчуючи, що фінальний документ не був модифікований та був створений саме заявленою, незміненою системою на основі процесуально чистих вхідних параметрів.

Ключова загроза достовірності доказу (ст. 87 КПК України) полягає у феномені галюцинацій (hallucinations), коли ШІ генерує правдоподібну, але вигадану інформацію. Цей ризик посилюється непрозорістю деяких моделей (Black Box). Визнання ШІ-документа достовірним можливе лише за умови обов'язкового проведення судової комп'ютерно-технічної експертизи. Ця експертиза є валідаційним механізмом, який покликаний встановити об'єк-

тивність змісту шляхом: аналізу вхідних промптів, верифікації стану моделі на момент генерації та оцінки ймовірності помилок або зміщень. Виключно таке експертне підтвердження алгоритмічної надійності дає змогу інтегрувати ШІ-документ у доказову базу без шкоди для принципу об'єктивної істини.

Рекомендації

Наукова цінність статті полягає у формулюванні конкретних законодавчих і криміналістичних рекомендацій, спрямованих на забезпечення ефективності доказування в умовах використання ШІ.

На законодавчому рівні – внести зміни до КПК України та Закону України «Про електронні документи та електронний документообіг» шляхом запровадження поняття «електронний доказ, згенерований штучним інтелектом» та встановлення спеціальних правил його допустимості, які включають обов'язкову фіксацію метаданих генерації.

На криміналістичному рівні – розробити та затвердити науково-методичні рекомендації щодо проведення судової комп'ютерно-технічної експертизи для встановлення атрибуції та достовірності ШІ-документів, включаючи техніки аналізу промпт-інжинірингу та виявлення прихованих цифрових міток.

На рівні правозастосовної практики – при розгляді ШІ-документів як доказів судам та сторонам процесу необхідно вимагати надання не лише самого документа, а й валідаційних даних (логін-файлів взаємодії, промптів), які підтверджують ланцюжок його створення та цілісність.

Список використаних джерел

[1] Li C. Artificial Intelligence Evidence: Concepts, Nature and Applications. *Frontiers in Humanities and Social Sciences*. 2025. Vol. 5, No. 5. P. 62-69. https://doi.org/10.54691/6g9r5911.

[2] Dunsin D., Ghanem M. C., Ouazzane K., Vassilev V. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*. 2024. Vol. 48. P. 301675. https://doi.org/10.1016/j.fsidi.2023.301675.

[3] Ahmed A. A., Farhan K., Jabbar W. A., Al-Othmani A., Abdulrahman A. G. IoT Forensics: Current Perspectives and Future Directions. *Sensors*. 2024. Vol. 24, issue 16. P. 5210. https://doi.org/10.3390/s24165210.

[4] Sunkari V., Sri Nagesh A. Artificial intelligence for deepfake detection: systematic review and impact analysis. *IAES International Journal of Artificial Intelligence (IJ-AI)*. 2024. Vol. 13, No. 4. P. 3786. https://doi.org/10.11591/ijai.v13.i4.pp3786-3792.

[5] Клімушин П. С., Рог В. Є., Колісник Т. П. Правові аспекти стандартизації функціональної безпеки Інтернету речей. *Право і безпека*. 2023. № 3(90). С. 200–213. https://doi.org/10.32631/pb.2023.3.17.

[6] Гарасимів О. І., Марко С. І., Ряшко О. В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2023. Вип. 75, ч. 2. С. 158–162. https://doi.org/10.24144/2307-3322.2022.75.2.25.

[7] Zhang F. Copyright Issues in Artificial Intelligence: A Comprehensive Examination from the Perspectives of Subject and Object. *Communications in Humanities Research*. 2023. Vol. 15. P. 172–182. https://doi.org/10.54254/2753-7064/15/20230664.

[8] Gupta S., Sharma P. Artificial Intelligence and Ethics. *SSRN Electronic Journal*. 2025. https://doi.org/10.2139/ssrn.5076025.

[9] Співак О. М. Правові засади регулювання штучного інтелекту в Україні та Польщі. *Юридичний науковий електронний журнал*. 2024. № 4. С. 815–817. https://doi.org/10.32782/2524-0374/2024-4/198.

[10] Іващенко С. Правові засади регулювання штучного інтелекту в Україні: сучасний стан та перспективи розвитку. *Адміністративне право і процес*. 2025. № 2. С. 24–32. https://doi.org/10.32782/2227-796x.2025.2.02.

[11] Шаблистий В. В. Цифрова ера кримінального процесу: можливості ІТ-систем у досудовому розслідуванні. *Юридичний науковий електронний журнал*. 2025. № 1. С. 630–633. https://doi.org/10.32782/2524-0374/2025-1/146.

[12] Яровий К. Штучний інтелект як інструмент попередження злочинності. *Юридичний вісник*. 2024. № 2. С. 68–76. https://doi.org/10.32782/yuv.v2.2024.9.

[13] Мілімко Л. В., Жидовцев Ю. В. Електронні докази в кримінальному судочинстві України. *Вісник Ужгородського Національного Університету. Серія: Право*. 2025. Вип. 88, ч. 3. С. 302–308. https://doi.org/10.24144/2307-3322.2025.88.3.45.

[14] Pasupuleti M. Kr. Digital Forensics Uncovering Cyber Evidence. *Digital Forensic Science*. 2024. Vol. 04, issue 1. P. 41-49. https://doi.org/10.62311/nesx/97422614.

[15] Morgan J. Digital Evidence. *Wrongful Convictions and Forensic Science Errors*. Boca Raton, 2023. P. 305-314. https://doi.org/10.4324/9781003202578-14.

[16] Кримінальний процесуальний кодекс України від 13.04.2012 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.10.2025).

[17] Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 20.10.2025).

[18] Sarker I. H. AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. *SN Computer Science*. 2022. Vol. 3:158. P. 1-20. https://doi.org/10.1007/s42979-022-01043-x.

[19] Ebers M., Tupay P. K. Delegation of Administrative Powers to AI Systems. *Artificial Intelligence and Machine Learning Powered Public Service Delivery in Estonia*. Cham, 2023. P. 85–102. https://doi.org/10.1007/978-3-031-19667-6_5.

[20] Anh-Hoang D., Tran V., Nguyen L.-M. Survey and analysis of hallucinations in large language models: attribution to prompting strategies or model behavior. *Frontiers in Artificial Intelligence*. 2025. Vol. 8. P. 1-21. https://doi.org/10.3389/frai.2025.1622292.

[21] Omlor S., Dilek D. German Electronic Securities Act. *European Company Law*. 2022. Vol. 19, issue 3. P. 67-72. https://doi.org/10.54648/eucl2022012.

[22] Nazarova I. N. Electronic document in the context of international economic and legal framework. *Journal of European Economy*. 2023. Vol 22, No. 1(84). P. 32-47. https://doi.org/10.35774/jee2023.01.031.

[23] Dr. Ammar Mahmoud Ayoub Al-Rawashed, Dr. Feras Mohmd Alyacoub, Dr. Ahmad Fahed Mohammad AlBtoosh, Adnan Salih Mohamad Alomar, Abdessalam Ali Mohamad Alfadel, Dr.Mamoon Suliman Alsmadi, Nashat Mohammad Abdul Qader Bani Hamad. The Law Applicable to Electronic Signatures Comparative Study. *Evolutionary Studies in Imaginative Culture*. 2024. Vol. 8.2, S2. P. 561–573. https://doi.org/10.70082/esiculture.vi.1066.

[24] Varbanova G. Electronic Documents as Electronic Evidence. *International Journal of Law in Changing World*. 2025. Vol. 4. No. 3. P. 43–54. https://doi.org/10.54934/ijlcw.v4i3.142.

[25] Irbe L. Regulation of artificial intelligence in the European Union. *INDIVIDUAL. SOCIETY. STATE: Proceedings of the 26th International Student and Teacher Scientific and Practical Conference*. (17 May, 2024). P. 199–206. https://doi.org/10.17770/iss2024.8338.

References

[1] Li, C. (2025). Artificial Intelligence Evidence: Concepts, Nature and Applications. Frontiers in *Humanities and Social Sciences, 5*(5), 62-69. https://doi.org/10.54691/6g9r5911.

[2] Dunsin, D., Ghanem, M.C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, *48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675.

[3] Ahmed, A.A., Farhan, K., Jabbar, W.A., Al-Othmani, A., & Abdulrahman, A.G. (2024). IoT Forensics: Current Perspectives and Future Directions. *Sensors, 24*(16), 5210. https://doi.org/10.3390/s24165210.

[4] Sunkari, V., & Sri Nagesh, A. (2024). Artificial intelligence for deepfake detection: systematic review and impact analysis. IAES *International Journal of Artificial Intelligence (IJ-AI), 13*(4), 3786. https://doi.org/10.11591/ijai.v13.i4.pp3786-3792.

[5] Klimushyn, P.S., Roh, V.Ye., & Kolisnyk, T.P. (2023). Legal aspects of functional security standardisation of the Internet of Things. *Law and Safety*, *3*(90), 200-213. https://doi.org/10.32631/pb.2023.3.17.

[6] Garasymiv, O.I., Marko, S.I., & Ryashko, O.V. (2023). Digital evidence: some problematic issues regarding its concept and use in criminal justice. *Uzhhorod National University Herald. Series: Law*, *75*(2), 158-162. https://doi.org/10.24144/2307-3322.2022.75.2.25.

[7] Zhang, F. (2023). Copyright Issues in Artificial Intelligence: A Comprehensive Examination from the Perspectives of Subject and Object. *Communications in Humanities Research, 15*, 172-182. https://doi.org/10.54254/2753-7064/15/20230664.

[8] Gupta, S., & Sharma, P. (2025). Artificial Intelligence and Ethics. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5076025.

[9] Spivak, O.M. (2024). Legal Basis of Regulation of Artificial Intelligence in Ukraine and Poland. *Juridical Scientific and Electronic Journal*, *4*, 815-817. https://doi.org/10.32782/2524-0374/2024-4/198.

[10] Ivashchenko, S. (2025). Legal basis for the use of artificial intelligence in jurisprudence in Ukraine. *Administrative Law and Process*, *2*, 24-32. https://doi.org/10.32782/2227-796x.2025.2.02.

[11] Shablystyi, V.V. (2025). The digital era of the criminal process: opportunities of it systems in pre-trial investigation. *Juridical Scientific and Electronic Journal*, *1*, 630-633. https://doi.org/10.32782/2524-0374/2025-1/146.

[12] Yarovyi, K. (2024). Artificial intelligence as a tool for crime prevention. *Law Herald*, *2,* 68-76. https://doi.org/10.32782/yuv.v2.2024.9.
[13] Milimko, L.V., & Zhydovtsev, Yu.V. (2025). Electronic evidence in criminal proceedings of Ukraine. *Visnyk UzhNU. Series: Legal, 88*(3), 302-308. https://doi.org/10.24144/2307-3322.2025.88.3.45.
[14] Pasupuleti, M.Kr. (2024). Digital Forensics Uncovering Cyber Evidence. *Digital forensic science, 4*(1), 41-49. https://doi.org/10.62311/nesx/97422614.
[15] Morgan, J. (2023). Digital evidence. In *Wrongful convictions and forensic science errors* (pp. 305-314). CRC Press. https://doi.org/10.4324/9781003202578-14.
[16] Criminal Procedure Code of Ukraine. (April 13, 2025). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[17] Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Workflow". (May 22, 2003). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15#Text.
[18] Sarker, I.H. (2022). AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. *SN Computer Science, 3*:158, 1-20. https://doi.org/10.1007/s42979-022-01043-x.
[19] Ebers, M., & Tupay, P.K. (2023). Delegation of Administrative Powers to AI Systems. In *Artificial Intelligence and Machine Learning Powered Public Service Delivery in Estonia* (pp. 85-102). *Springer International Publishing.* https://doi.org/10.1007/978-3-031-19667-6_5.
[20] Anh-Hoang D., Tran V., & Nguyen L.-M. (2025). Survey and analysis of hallucinations in large language models: attribution to prompting strategies or model behavior. *Frontiers in Artificial Intelligence*, *8*, 1-21. https://doi.org/10.3389/frai.2025.1622292.
[21] Omlor, S., & Dilek, D. (2022). German Electronic Securities Act. *European Company Law*, *19*(3), 67-72. https://doi.org/10.54648/eucl2022012.
[22] Nazarova, I.N. (2023). Electronic document in the context of international economic and legal framework. *Journal of European Economy*, *22*(1(84)), 32-47. https://doi.org/10.35774/jee2023.01.031.
[23] Dr. Ammar Mahmoud Ayoub Al-Rawashed, Dr. Feras Mohmd Alyacoub, Dr. Ahmad Fahed Mohammad AlBtoosh, Adnan Salih Mohamad Alomar, Abdessalam Ali Mohamad Alfadel, Dr.Mamoon Suliman Alsmadi, & Nashat Mohammad Abdul Qader Bani Hamad. (2024). The Law Applicable to Electronic Signatures Comparative Study. *Evolutionary Studies in Imaginative Culture*, *8.2*, 561-573. https://doi.org/10.70082/esiculture.vi.1066.
[24] Varbanova, G. (2025). Electronic Documents as Electronic Evidence. *International Journal of Law in Changing World*, *4*(3), 43-54. https://doi.org/10.54934/ijlcw.v4i3.142.
[25] Irbe, L. (May 17, 2024). Regulation of artificial intelligence in the european union. In *INDIVIDUAL. SOCIETY. STATE: Proceedings of the 26th International Student and Teacher Scientific and Practical Conference* (pp. 199-206). https://doi.org/10.17770/iss2024.8338.

Олександр Вікторович Габро
аспірант
Навчально-науковий інститут права Державного податкового університету
08205, вул. Університетська, 31, Ірпінь, Україна
e-mail: Oleksandr763@proton.me
ORCID 0009-0000-2363-6536

Oleksandr V. Gabro
Ph.D. Student
Educational and Scientific Institute of Law of the State Tax University
08205, 31 Universytetska Str., Irpin, Ukraine
e-mail: Oleksandr763@proton.me
ORCID 0009-0000-2363-6536

Рекомендоване цитування: Габро О. В. Правові та криміналістичні аспекти роботи з електронними документами, згенерованими штучним інтелектом. *Проблеми законності*. 2025. Вип. 171. С. 242–261. https://doi.org/10.21564/2414-990X.171.342859.

Suggested Citation: Gabro, O.V. (2025). Legal and Forensic Aspects of Working with Electronic Documents Generated by Artificial Intelligence. *Problems of Legality*, *171*, 242-261. https://doi.org/10.21564/2414-990X.171.342859.

Статтю подано / Submitted: 04.11.2025
Доопрацьовано / Revised:.05.12.2025
Схвалено до друку / Accepted: 18.12.2025
Опубліковано / Published: 29.12.2025