

УДК 343

DOI 10.36919/3041-1149(Print).8.2025.161-165

В. Г. Хахановський,*доктор юридичних наук, професор,
професор кафедри інформаційних технологій
Навчально-наукового інституту права та психології,
Національна академія внутрішніх справ
email: super-hvg@ukr.net***ORCID 0000-0001-5676-5641;****В. В. Петрик,***адвокат, аспірант кафедри інформаційних технологій
Навчально-наукового інституту права та психології,
Національна академія внутрішніх справ
email: vitep11@gmail.com***ORCID 0000-0003-4723-7921**

ШТУЧНИЙ ІНТЕЛЕКТ І ЕЛЕКТРОННІ ДОКАЗИ: ПРОБЛЕМИ АВТЕНТИЧНОСТІ (ЮРИДИЧНИЙ АСПЕКТ)

Стаття зосереджується на дослідженні питань застосування електронних доказів у сучасному контексті розвитку штучного інтелекту. Підкреслено, що через прогрес у технологіях генерації штучного (синтетичного) мультимедійного контенту («deepfake» – фото-, аудіо-, відео-) та синтетичних матеріалів значно зросли ризики фальсифікації цифрових даних, здатних виступати доказами в судочинстві. Наразі вітчизняне законодавство не містить відповідних засобів верифікації та встановлення автентичності електронних доказів, зокрема тих, що створені чи змінені з використанням штучного інтелекту. Цей недолік зумовлює значні труднощі для забезпечення об'єктивності судового процесу, внаслідок чого виникає нагальна потреба в розробці відповідних правових інструментів. Наведено рекомендації щодо вирішення проблеми достовірності електронних доказів з огляду на розвиток технологій штучного інтелекту.

Ключові слова: *штучний інтелект, електронні докази, цифровізація, синтетичний контент, блокчейн, цифровий підпис, достовірність доказів, хешування.*

Постановка проблеми та її актуальність. У цифрову еру роль електронних доказів у правосудді невпинно зростає. Усе частіше використовуються відео-, поштові листи, метадані, аудіофайли й інші формати. З бурхливим розвитком штучного інтелекту (далі – ШІ), зокрема генеративних моделей, виникає дедалі більший ризик маніпулювання цими доказами через їхні фальсифікації, що наражає на небезпеку принципи об'єктивності, законності та справедливості судового процесу. Докази, виправлені ШІ-системами, втрачають допустимість та автентичність.

Для України, що нині випереджає чимало інших країн світу у сфері цифрового перетворення державних послуг і комунікації між громадянами та владою, ці виклики є питаннями першочергової важливості, особливо з огляду на активну цифровізацію системи правосуддя.

Розвиток технологій «deepfake» та синтетичного контенту значно підсилив загрозу підробки цифрових матеріалів, що здатні слугувати доказами в суді. Наразі українське законодавство не пропонує чітких методів перевірки та засвідчення автентичності електронних доказів, включно із тими, що були створені чи змінені із залученням штучного інтелекту. Ця невідповідність породжує серйозні питання щодо об'єктивності судового процесу й диктує потребу в розробці відповідних правових механізмів.

Аналіз останніх досліджень і публікацій. Дослідження проблематики електронних доказів у контексті розвитку штучного інтелекту привертає увагу як українських, так і зарубіжних науковців. Серед вітчизняних дослідників питання електронних доказів розглядали Г. К. Авдєєва, П. Є. Антонюк, М. В. Гуцалюк, А. Ю. Каламайко, В. С. Кобко-Одарій, О. М. Лазько, Н. О. Левицька,

Ю. Ю. Орлов, Ю. С. Павлова, Д. О. Савицький, Д. М. Цехан, С. С. Чернявський тощо. Із закордонних дослідників, які займалися проблемами електронних доказів, можна виділити С. Мейсона, М. Р. Аркфельда, А. І. Коена, Д. Дж. Лендера, Д. Е. Гренига, У. С. Глайзнера, Т. Ларсона, Д. Л. Керола, М. Ланге, К. Нимсгера, Д. Л. Пола та інших.

Мета статті полягає в науковому обґрунтуванні теоретичних засад правового регулювання питань застосування електронних доказів у сучасному контексті розвитку штучного інтелекту.

Виклад основного змісту матеріалу дослідження. Електронний доказ як юридичне поняття вимагає переосмислення з огляду на прогрес технологій штучного інтелекту. Відповідно до статті 100 Цивільного процесуального кодексу України електронні докази – це інформація в електронному вигляді, що містить дані про факти, які мають значення для розгляду справи. До них належать електронні документи, вебресурси, текстові, мультимедійні й голосові повідомлення, бази даних та інші дані в електронній формі [1].

Параграф перший п'ятого розділу Цивільного процесуального кодексу України окреслює ключові характеристики доказів, охоплюючи їх незалежність, допустимість, достатність і достовірність. Водночас, на нашу думку, ці вимоги не беруть до уваги особливостей доказів, які були сформовані або змінені з використанням штучного інтелекту. Адже варто враховувати, що сучасні генеративні моделі штучного інтелекту демонструють неймовірні здібності у створенні контенту – синтетичні результати їхньої праці настільки якісні, що практично не відрізняються від справжніх.

В Україні вже спостерігається суттєвий поступ у нормотворчому процесі, спрямованому на регулювання застосування штучного інтелекту у сфері судочинства. Зокрема, Кабінетом Міністрів України було затверджено Концепцію розвитку штучного інтелекту в Україні, яка передбачає активне використання штучного інтелекту в правовій сфері та безпосередньо під час здійснення правосуддя. Вища рада правосуддя ухвалила проєкт розпорядження, що стосується початку пілотного проєкту з використанням штучного інтелекту на основі одного із судів першої інстанції, з метою розгляду справ про адміністративні правопорушення [2].

Важливим орієнтиром для України є також Європейська етична хартія щодо використання штучного інтелекту в судових системах та їхньому середовищі, яка визначає п'ять ключових принципів: повага до основних прав людини, недискримінація, якість і безпека, їхня прозорість під контролем користувача. Розглядаючи міжнародний досвід, потрібно також звернути увагу на Регламент Європейського парламенту та Ради (ЄС) 2016/679, що закладає підвалини для забезпечення надійності електронних даних. Однак навіть європейське законодавство ще не виробило комплексного підходу до регулювання питань автентичності електронних доказів, створених за допомогою ШІ.

У світовій практиці питання автентифікації електронних доказів вирішується через впровадження технологій блокчейн і цифрових підписів. Американська дослідниця Andrea Roth у своїй основній праці «Machine Testimony» презентує концепцію «машинних свідчень», використовуючи цей термін для опису доказової інформації, створеної алгоритмами штучного інтелекту. Вона звертає увагу на проблему «чорної скриньки» алгоритмів машинного навчання – суди не мають можливості розібратися з логікою ухвалення рішень машиною, що ускладнює оцінку достовірності таких доказів.

Авторка висуває концепцію «технічного хешу» для цифрових доказів, створених штучним інтелектом. Це своєрідний цифровий «слід», який дає змогу перевірити незмінність і справжність доказу. Крім того, нею була створена рамкова структура для експертизи так званих «машинних свідчень», що передбачає верифікацію вхідних даних, ревізію алгоритму, підтвердження достовірності результатів і документальне оформлення процесу формування доказів [3].

Проблема справжності електронних доказів стає критично важливою із впровадженням ШІ в правову систему України. Ця тема викликає жваві дискусії та перебуває в центрі наукових досліджень. Згідно з працею Ю. Москвитин та докторки Агне Ліманте в переліку перспективних можливостей використання систем штучного інтелекту в судочинстві України перебуває й перевірка автентичності доказів [4].

Зокрема, в рамках Всеукраїнського семінару суддів, що відбувся в квітні 2024 року, Верховний Суд зосереджувався на вивченні потенціалу використання інструментів, на зразок Open AI Chat GPT та Microsoft Gemini, з метою забезпечення перевірки автентичності доказів у судочинстві.

О. М. Дроздов, О. В. Малоземова та А. С. Мхітарян наголошують, що, попри здатність систем штучного інтелекту покращувати ефективність судової системи, його застосування мусить ґрунтуватися на засадах справедливості й верховенства права, враховуючи потенційні упередження алгоритмів. Це стає критично важливим у процесі оцінювання автентичності електронних доказів, оскільки упереджені алгоритми здатні зумовлювати хибні висновки щодо їхньої достовірності [5].

На превеликий жаль, в Україні досі ще не існує ні спеціалізованих інструментів для перевірки електронних доказів на їх відповідність дійсності, ні злагодженого механізму їхнього підтвердження. Очевидно, що така обстановка спричиняє значні проблеми в розгляді судових справ, де вирішальну роль відіграють цифрові дані.

Тому виникає потреба в започаткуванні посади судового технічного експерта, який спеціалізуватиметься на виявленні ознак використання штучного інтелекту в процесі створення або модифікації електронних доказів. Водночас варто впровадити технологію хешування для формування унікального «цифрового відбитку» електронного доказу. Адже аналіз таких доказів нерідко вимагає вузькоспеціалізованих технічних знань, якими судді зазвичай не володіють.

Крім того, питання перевірки електронних доказів загострює проблеми процесуальних гарантій і права на справедливий судовий розгляд. Застосування ненадійних електронних доказів здатне порушити ключові принципи правосуддя та права учасників судового процесу. З огляду на це створення дієвих інструментів для встановлення достовірності таких доказів – це не просто технічне, але й надзвичайно важливе юридичне питання.

Сьогодні вже розроблено принципи використання штучного інтелекту у сфері судової експертизи, до яких варто віднести:

законність: дотримання особою, що використовує ШІ, вимог нормативно-правових документів, які регламентують правила застосування ШІ в науковій, правовій та інших сферах діяльності;

відповідальність: експерти несуть передбачену законами й підзаконними актами відповідальність за результати проведених досліджень і висновків, навіть за ті частини, які створені із використанням інструменту ШІ;

роз'яснення та простежуваність: фахівець зобов'язаний пояснити замовнику процедуру експертизи, а також суду, згідно з вимогами законодавства, які інструменти і як саме застосовано під час дослідження. У разі потреби експерт повинен надати посилання на джерела, які містять використані інструменти ШІ;

надійність і неупередженість: використання ШІ має супроводжуватися критичною оцінкою отриманих даних. Спеціалісти зобов'язані перевіряти відповідність отриманих результатів темі дослідження. Адже штучний інтелект може видавати переконливі відповіді, які, проте, можуть бути помилковими, неповними чи упередженими.

Ці стандарти сприятимуть ефективному використанню переваг машинних алгоритмів і водночас допоможуть знизити ризики, пов'язані з прозорістю та конфіденційністю [10, с. 39–40].

Висновки. Проблема достовірності електронних доказів в умовах поступу технологій штучного інтелекту кидає виклик українській правовій системі. Аналіз наукових розвідок і міжнародної практики дає підстави стверджувати, що українське законодавство не містить конкретних правил для перевірки електронних доказів, створених чи змінених за допомогою технологій ШІ, що ускладнює їхню оцінку в судах. В Україні відсутні спеціалізовані інструменти та програмні рішення для перевірки автентичності електронних доказів, а також бракує комплексної процедури їхньої верифікації.

Для успішного вирішення поставленого завдання потрібен цілісний метод, який об'єднує технічні інструменти (блокчейн, цифрові підписи, хешування), законодавчі регулювання та професійні знання. Варто розглянути можливість запровадження посади судового технічного експерта та приведення вітчизняного законодавства у відповідність з міжнародними нормами щодо електронних доказів.

Отже, подолання викликів, пов'язаних з достовірністю електронних доказів у контексті розвитку технологій штучного інтелекту, вимагає застосування міждисциплінарного, комплексного підходу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40–41, 42. Ст. 492.
2. Кобко-Одарій В. С. Роль штучного інтелекту в судовій інтерпретації права. *Київський часопис права*. № 3. С. 7–13. DOI : <https://doi.org/10.32782/klj/2023.3.1.3>
3. Roth, A. (2017). «Machine Testimony». *Yale Law Journal*. 130 (4). Pp. 1972–2053.
4. Limante, Agne; Moskvityn, Yuliia. Integrating Artificial Intelligence in Ukraine's Courts: State of Play and Future Prospect, *VerfBlog*, 2024/12/12. URL : <https://verfassungsblog.de/ai-ukraine-judiciary/> ; DOI 10.59704/c472a6ec2910dae3
5. Дроздов О. М., Малоземова О. В., Мхитарян А. С. Дослідження стану та перспектив використання ШІ у сфері правосуддя. URL : http://www.lsej.org.ua/5_2024/124.pdf
6. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного ун-ту*. 2013. № 5/2013. С. 256–260.
7. Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2/2017. С. 112–124.
8. Гуцалюк М. В., Антонюк П. Є. Щодо сутності електронної (цифрової) інформації як джерела доказів у кримінальному провадженні. *Криміналістичний вісник : наук.-практ. зб. / редкол. : І. М. Охріменко (голов. ред.) та ін. ; ДНДЕКЦ МВС України; НАВС. Київ : ДНДЕКЦ МВС України, 2020. № 1. С. 37–49.*
9. Авдєєва Г. К. Цифрові докази і системи штучного інтелекту у правозастосовній діяльності. *Питання боротьби зі злочинністю : зб. наук. пр. Харків, 2023. Вип. 46. С. 32–40.*
10. Шмерего О. Б., Станішевський Ю. А. Методика проведення досліджень в галузі цивільного захисту. Київ : ДНДЕКЦ МВС України, 2025. 61 с.

REFERENCES

1. Tsyvilnyi protsesualnyi kodeks Ukrainy : Zakon Ukrainy vid 18.03.2004 № 1618-IV. *Vidomosti Verkhovnoi Rady Ukrainy*. 2004. № 40–41, 42. St. 492.
2. Kobko-Odarii V. S. Rol shtuchnoho intelektu v sudovii interpretatsii prava. *Kyivskyi chasopys prava*. (3), 7–13. DOI : <https://doi.org/10.32782/klj/2023.3.1.3>
3. Roth, A. (2017). «Machine Testimony». *Yale Law Journal*. 130 (4), 1972–2053.
4. Limante, Agne; Moskvityn, Yuliia: Integrating Artificial Intelligence in Ukraine's Courts: State of Play and Future Prospect, *VerfBlog*, 2024/12/12. URL : <https://verfassungsblog.de/ai-ukraine-judiciary/> ; DOI 10.59704/c472a6ec2910dae3
5. Drozdov O. M., Malozemova O. V., Mkhitarian A. S. Doslidzhennia stanu ta perspektyv vykorystannia ShI u sferi pravosuddia. URL : http://www.lsej.org.ua/5_2024/124.pdf
6. Tsekhan D. M. Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia. *Naukovyi visnyk Mizhnarodnoho humanitarnoho un-tu*. 2013. № 5/2013. S. 256–260.
7. Cherniavskiy S. S., Orlov Iu. Iu. Elektronne vidobrazhennia yak dzherelo dokaziv u kryminalnomu provadzhenni. *Visnyk kryminalnoho sudochynstva*. 2017. № 2/2017. S. 112–124.
8. Hutsaliuk M. V., Antoniuk P. Ie. Shchodo sutnosti elektronnoi (tsyfrovoi) informatsii yak dzherela dokaziv u kryminalnomu provadzhenni. *Kryminalistychnyi visnyk : nauk.-prakt. zb. / redkol. : I. M. Okhrimenko (holov. red.) ta in. ; DNDEKTs MVS Ukrainy; NAVS. Kyiv : DNDEKTs MVS Ukrainy, 2020. № 1. S. 37–49.*
9. Avdieieva H. K. Tsyfrovi dokazy i systemy shtuchnoho intelektu u pravozastosovnii diialnosti. *Pytannia borotby zi zlochynnistiu : zb. nauk. pr. Kharkiv, 2023. Vyp. 46. S. 32–40.*
10. Shmereho O. B., Stanishevskiy Yu. A. Metodyka provedennia doslidzhen v haluzi tsyvilnoho zakhystu. Kyiv : DNDEKTs MVS Ukrainy, 2025. 61 s.

V. G. Khakhanovsky, V. V. Petryk. ARTIFICIAL INTELLIGENCE AND ELECTRONIC EVIDENCE: PROBLEMS OF AUTHENTICITY, LEGAL ASPECT

The article focuses on the study of issues of the use of electronic evidence in the modern context of the development of artificial intelligence (AI). It is emphasized that due to progress in technologies for generating artificial (synthetic) multimedia content ("deepfake" - photo, audio, video) and synthetic materials, the risks of falsification of digital data that can serve as evidence in legal proceedings have significantly increased. Currently, domestic legislation does not contain the necessary means of verification and establishing the authenticity of electronic evidence, including those created or modified using artificial intelligence. This shortcoming causes significant difficulties in ensuring the objectivity of the judicial process, as a result of which there is an urgent need to develop appropriate legal instruments. Recommendations are given to solve the problem of the reliability of electronic evidence in view of the development of artificial intelligence technologies.

Keywords: artificial intelligence, electronic evidence, digitalization, synthetic content, blockchain, digital signature, evidence authenticity, hashing.