ISSN 2524-0374

УДК [343.13:343.14](73)
DOI https://doi.org/10.32782/2524-0374/2025-12/50

ЦИФРОВІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ США

DIGITAL EVIDENCE IN THE CRIMINAL PROCEDURE OF THE UNITED STATES

Микитюк О.С., аспірант кафедри кримінального процесу
Національний юридичний університет імені Ярослава Мудрого
orcid.org/0009-0004-1595-711X

Стаття присвячена дослідженню актуальних для сучасного кримінального процесу України питань, що стосуються використання в кримінальному процесуальному доказуванні США цифрових доказів. Автор підкреслює, що у вітчизняній доктрині кримінального процесу відомими науковцями-процесуалістами закладено міцний фундамент сучасного розуміння доказів, процесу доказування, визначено його принципи, обставини, що підлягають доказуванню тощо. Проте стрімкий розвиток цифрових технологій актуалізує потребу у виробленні нових концептуальних підходів до визначення поняття цифрових доказів, їхніх характерних ознак, а також до вирішення питань їхнього закріплення, перевірки та оцінки. Водночас українським дослідникам бракує практичного досвіду оперування цифровими доказами, який накопичено у зарубіжних правових системах, насамперед у США, де проблематика цифрових доказів перебуває у центрі уваги доктрини та судової практики вже протягом тривалого часу. З огляду на це автор звертається до положень американської правової доктрини, судової практики та Федеральних правил доказування, аналізуючи критерії належності, автентичності, доказової цінності, а також застосування правила найкращого доказу та заборони показань з чужих слів. Окремий акцент зроблено на сучасних викликах, пов'язаних із використанням deepfake-технологій та доказів, згенерованих штучним інтелектом, а також на пропозиціях американських правників щодо вдосконалення процедур автентифікації цифрових доказів. У підсумку обґрунтовується значення американського досвіду для вдосконалення українського кримінального процесу, зокрема у сфері нормативної регламентації та практичного застосування цифрових доказів, що має сприяти формуванню сучасної доктрини доказування в умовах цифровізації правосуддя.

Ключові слова: кримінальний процес; докази, доказування, доказове право, джерела доказового права, цифрові докази, способи збирання доказів; кримінальний процес США.

The article examines issues highly relevant to the modern criminal procedure of Ukraine, particularly those concerning the use of digital evidence in the United States criminal justice system. The author emphasizes that prominent Ukrainian scholars in the field of criminal procedure have laid a solid foundation for the contemporary understanding of evidence and the evidentiary process, defining its principles as well as the circumstances subject to proof. However, the rapid development of digital technologies underscores the need to develop new conceptual approaches to defining digital evidence, identifying its characteristic features, and addressing issues related to its preservation, verification, and assessment. At the same time, Ukrainian researchers lack the practical experience in handling digital evidence that has been accumulated in foreign legal systems, primarily in the United States, where these issues have long been at the forefront of both legal doctrine and judicial practice. In this context, the author examines American legal doctrine, judicial practice, and the Federal Rules of Evidence, analysing the criteria of relevance, authenticity, and probative value, as well as the application of the best evidence rule and the prohibition against hearsay. Particular attention is devoted to contemporary challenges associated with the use of deepfake technologies and AI-generated evidence, as well as to proposals advanced by American legal scholars for improving the procedures for digital evidence authentication. In conclusion, the significance of the American experience for improving the Ukrainian criminal procedure is substantiated, particularly regarding regulatory framework development and the practical application of digital evidence. These improvements are expected to contribute to the formation of a modern evidentiary doctrine in the context of the digitalisation of justice.

Key words: criminal procedure; evidence, evidentiary process, evidence law, sources of evidence law, digital evidence, methods of evidence collection; U.S. criminal procedure.

Вступ. В умовах стрімкого розвитку інформаційно-комунікаційних технологій усе більшого значення набуває належне правове регулювання питань, пов'язаних із використанням цифрових (електронних) доказів. Серед країн, які першими усвідомили потребу у нормативному закріпленні правил допустимості таких доказів, особливе місце посідають Сполучені Штати Америки. Саме у США ще в 1990-х роках розпочалося становлення судової практики, що стосувалася цифрових доказів, а згодом формування системного підходу до їх використання у межах Федеральних правил доказування. Ця практика поступово еволюціонувала у цілісну концепцію, що поєднує нормативне регулювання, доктринальні засади та сталі підходи судових органів до оцінки електронної інформації як доказу. Досвід Сполучених Штатів є надзвичайно цінним не лише з точки зору історії розвитку цифрової доказової бази, але й як приклад концептуальної та практичної узгодженості у поєднанні норм права, технологічних можливостей і судової практики.

Постановка проблеми. Стрімка цифровізація суспільних процесів радикально трансформує природу та характер доказової інформації в кримінальному судочинстві. При цьому, цифрові докази мають низку специфічних ознак: іноді прихований характер, здатність перетинати межі юрисдикцій, технологічну вразливість до змін або знищення, великий обсяг і швидкість генерації, а також складність у технічній оцінці їхнього походження та цілісності. У межах кримінального процесу США ця технологічна реальність стала потужним каталізатором еволюції доказового права, сформувавши його сучасний вигляд: гнучкий, технологічно орієнтований і практично значущий, що становить особливий інтерес для вивчення та запозичення вітчизняною правовою системою.

Стан дослідження. Проблематика доказів та доказування стабільно перебуває у центрі уваги науковців протягом усього розвитку кримінальної процесуальної науки. У вітчизняній доктрині значний внесок у дослідження актуальних проблем доказового права здійснили такі відомі вчені, як В. В. Вапнярчук, Ю. М. Грошевий, В. П. Гмирко, М. М. Михеєнко, В. Т. Нор, М. А. Погорецький, Д. Б. Сергєєва, С. М. Стахівський, М. Є. Шумило та інші. Їхні праці заклали фундаментальні засади сучасного розуміння процесу доказування, визначили його принципи, межі та гарантії.

Водночас упродовж останніх семи років спостерігається істотне зростання наукового інтересу до проблематики цифрових доказів, що зумовлено стрімким розвитком інформаційних технологій та їхнім впливом

на кримінальне судочинство. У цьому контексті заслуговують на увагу дослідження І.В. Басистої, І. В. Гловюк, І. Г. Каланчі, А. В. Коваленка, С. О. Ковальчука, І. О. Крицької, Д. О. Літкевича, О. П. Метелева, А. В. Скрипника, І.А. Смаль, А. В. Столітнього, Д. М. Цехана, С. С. Чернявського та інших. Дослідження цих авторів спрямовані на осмислення правової природи цифрових доказів, визначення критеріїв їх допустимості, а також вироблення процесуальних механізмів їхнього належного закріплення й використання у кримінальному провадженні.

Однак, вітчизняним дослідникам істотно бракує досвіду оперування цифровими доказами у кримінальному процесі зарубіжних держав, зокрема, США, де цьому питанню значна увага приділяється вже багато років. Серед американських науковців особливу увагу заслуговують дослідники, у доробку яких наявні ґрунтовні праці, присвячені проблематиці використання цифрових доказів у кримінальному процесі, зокрема це Пол Грімм [1, 2], Маура Гроссман [2], Річард Д. Фрідман [3], Герберт Б. Діксон-молодший [4] та ін.

Метою статті є аналіз підходів до цифрових доказів у кримінальному процесі США, зокрема критеріїв їх допустимості, та окреслення викликів, пов'язаних із технологіями deepfake і ШІ, з урахуванням можливості використання цього досвіду в Україні.

Виклад основного матеріалу. У кримінальному процесуальному законодавстві США, як на федеральному рівні, так і на рівні окремих штатів, відсутнє нормативне визначення поняття «електронні (цифрові) докази» («digital evidence»). Така відсутність уніфікованого законодавчого регулювання компенсується напрацюваннями в науковій доктрині та правозастосовній практиці. Найбільш авторитетними офіційними джерелами, що надають визначення терміну «електронні докази» є «Розслідування місця злочину, пов'язаного з електронними доказами: посібник для працівників, які першими прибувають на місце події» Національного інституту юстиції США. Так в цьому посібнику електронні докази визначаються як «інформація та дані, що мають значення для розслідування і зберігаються або передаються за допомогою електронних пристроїв». Основними ознаками електронних доказів є: 1) прихований характер, що робить їх подібними до таких традиційних доказів, як відбитки пальців чи ДНК; 2) здатність швидко та безперешкодно перетинати юрисдикційні кордони; 3) вразливість до змін, пошкодження або знищення; 4) можлива обмеженість у часі щодо доступу або збереження [5, с. 10].

У свою чергу, Наукова робоча група з цифрових доказів (Scientific Working Group on Digital Evidence, SWGDE), яка об'єднує експертів правоохоронних органів, судової експертизи та академічних кіл, пропонує дещо ширше визначення, зазначаючи, що цифрові докази, це «будь-яка інформація доказового значення, що зберігається або передається у цифровому форматі» [6]. Таким чином, у правовій системі США сформувалося широке визначення поняття «електронні (цифрові) докази», що підтверджується доктринальним консенсусом.

Вперше Верховний Суд США вперше окреслив якісні відмінності електронних доказів від традиційних доказів у кримінальному процесі у рішенні по справі *Riley v. California* (2014). Суд дійшов висновку, що цифрова інформація, зокрема на мобільних пристроях, становить принципово новий вид доказів, який вимагає особливої обережності під час її вилучення, обробки та оцінки. У зв'язку з чим, суд згенерував три важливі риси, які виокремлюють цифрові докази з-поміж класичних матеріальних носіїв:

1) широта охоплення (цифрові пристрої містять колосальний обсяг інформації – фотографії, геолокаційні дані, історію пошуку, чати, документи, що може охоплювати роки особистого життя);

2) конфеденційність інформації (на відміну від паперових документів, цифрові носії можуть зберігати глибоко приватні й делікатні відомості: від медичних і фінансових даних до інтимних листувань);

3) системний характер (електронні докази нерідко стосуються системних процесів взаємодії особи із зовнішнім світом, що виходить за межі звичної оперативної ролі поліції і стосується вже сфер цифрової приватності, кіберпростору та міжнародного обміну даними) [7].

На підставі довідника «Цифрові докази та система кримінального правосуддя США. Визначення технологічних та інших потреб для більш ефективного отримання і використання цифрових доказів» («Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence») можна визначити наступні види цифрових доказів, які застосовуються в кримінальному процесі США: 1) електронна пошта та листування; 2) текстові повідомлення (SMS, MMS); 3) журнали викликів; 4) GPS-локації; 5) дані з мобільних телефонів; 6) історія браузера та cookie-файли; 7) журнали доступу до мережі; 8) фотографії та відео; 9) інформація з хмарних сховищ; дані з соціальних мереж (Facebook, Twitter тощо); 10) журнали дій користувача в операційних системах чи застосунках [8, с. 1–25].

Аналіз сучасної американської доктрини, присвяченої електронним доказам [див: 9, с. 15–61], [8, с. 1–25] дав змогу розробити авторську класифікацію цих доказів, спираючись на типи інформації, що зберігається у відповідному цифровому джерелі: 1) змістовна інформація (повідомлення, email, документи, зображення, відео, звук); 2) метадані (час створення, зміни, геолокація, автор, цифровий слід); 3) записи про активності користувача в системі (журнали входу/виходу, історія браузера, використання пристрою); 4) інформація про комунікацію (історія викликів, текстові повідомлення, IP-адреси); 5) дані про переміщення (GPS-треки, Wi-Fi локації); 6) системні дані/дані з додатків (файли cookie, системні журнали, інформація з месенджерів); 7) дані з «хмари» та соцмереж (Facebook, Instagram, Google Drive, Dropbox, Discord); 8) автоматично згенеровані дані (знімки з камер відеоспостереження, дані згенеровані штучним інтелектом (AI logic)); 9) копії / резервні дані (копії дисків, мобільних пристроїв).

Така класифікація електронних доказів є не лише теоретично виваженою, а й має прикладне значення для визначення обсягу доказової бази, а також для оцінки допустимості таких доказів у кримінальному провадженні.

Електронні докази в кримінальному процесі США оцінюються за тими ж загальними правилами, що й інші види доказів, але із урахуванням їхніх технічних особливостей. При цьому, у судовому провадженні, що стосується використання електронних доказів, критично важливим є дотримання вимог допустимості таких доказів. Ці вимоги сформульовані на основі принципів американського прецедентного права, закріплені у Федеральних правилах доказування та конкретизовані у судових рішеннях, зокрема у справі *Lorraine v. Markel American Insurance Company* (2007) [10]. У цій справі суддя Пол Д. Грімм виклав низку ключових критеріїв, які повинні бути враховані при вирішенні питання про допустимість електронних доказів у судовому процесі.

Перш за все, цифрові докази мають відповідати ***критерію належності/релевантності («relevancy»)*** – тобто мати прямий або опосередкований зв'язок із фактами, що підлягають доказуванню у справі. Умова належності є загальною передумовою для розгляду будь-якого доказу у суді.

Так, відповідно до правил 401 і 402 Федеральних правил доказування США, електронні докази можуть бути визнані як допустимі лише за умови їхньої належності. Згідно з Правилом 401, доказ вважається належним,

якщо: 1) він має здатність хоча б мінімально змінити ймовірність настання певного факту (тобто робить його більш або менш вірогідним), ніж без такого доказу; 2) цей факт має значення для вирішення справи по суті. В свою чергу, правило 402 закріплює, що всі належні докази є допустимими, якщо лише вони не суперечать Конституції США, федеральному законодавству, іншим положенням Федеральних правил доказування або правилам, встановленим Верховним судом [11].

Докази, що не відповідають критерію належності, визнаються недопустимими. Це положення відображає відомий у правовій доктрині принцип «належність як порогова вимога» («relevancy as a threshold requirement»), відповідно до якого належність доказу є первинною, базовою умовою, яку потрібно виконати, перш ніж суд розглядатиме інші характеристики доказу. Одним з перших цей принцип сформулював Дж. Тайлер [12, с. 269] і він застосовується, як і до цифрових, такі і до інших видів доказів.

У цьому контексті належність (релевантність) можна розглядати як змістовний вимір допустимості. Професор Мічиганського університету, фахівець у сфері доказового права Річард Д. Фрідман стверджує, що належність доказу не гарантує його допуск до судового розгляду, тому що іноді важливішим є умовний характер зв'язку між доказом і фактом, що потребує уточнення додатковими обставинами або оцінки в ширшому контексті справи [3, с. 458].

Другим критерієм допустимості є ***автентичність («authenticity»).*** Так, Правило 901 («Автентифікація або ідентифікація доказу») Федеральних правил доказування закріплює, що «сторона, яка подає доказ, зобов'язана надати достатні підстави для встановлення того, що об'єкт доказування є саме тим, за який він видається» [11]. Інакше кажучи, це правило вимагає надання такої доказової інформації, яка дає суду підстави вважати, що поданий цифровий об'єкт є оригінальним, не зміненим і належним чином збереженим та пройшов процедуру автентифікації.

Автентичність цифрових доказів може бути підтверджена: свідком із особистим знанням (Правило 901(b)(1)); висновком експерта або порівнянням з автентичними прикладами (Правило 901(b)(3)); впізнаваними характеристиками та непрямими доказами (Правило 901(b)(4)); системами чи процесами, здатними гарантувати достовірний результат (Правило 901(b)(9)); торговими написами та знаками (Правило 902(7)); сертифікованими копіями бізнес-записів (Правило 902(11)); сертифікованими даними, створеними електронними системами (Правило 902(13), (14)).

Судова практика США демонструє два основні підходи до автентифікації цифрових доказів. У науковій літературі та судовій практиці їх умовно поділяють на так званий Мерілендський підхід («Maryland Approach») та Техаський підхід («Texas Approach»).

Одним із найвідоміших є так званий Мерілендський підхід, що базується на рішеннях судів штату Меріленд і має репутацію обережного та суворого підходу. Хрестоматійним прикладом цього підходу є справа *Griffin v. State* (2011), у якій прокуратура намагалася використати роздруківки зі сторінки соціальної мережі «MySpace» подруги обвинуваченого як доказ погроз свідку. Акаунт містив ім'я, дату народження, фотографії та пости із погрозами. Однак суд визнав ці дані недостатньо автентичними та недопустимим, як докази. Суд аргументував свою позицію тим, що в епоху соціальних мереж можливість зламу, підробки чи використання акаунтів третіми особами надто велика, щоб визнати автентичність на основі лише зовнішніх ознак [13]. Таким чином, сутність цього підходу полягає у тому, що процесуальний обов'язок (тягар доказування) покладається на сторону, яка ініціює подання таких доказів. Вона має підтвердити, що матеріал не був сфальсифікований або створений іншою особою.

Техаський підхід, пов'язаний із практикою судів штату Техас. Цей підхід є більш гнучким. У межах цього підходу на сторону, яка подає такі докази, покладається обов'язок надати достатньо підтверджень, які б дозволили розсудливому присяжному дійти висновку, що доказ із соціальної мережі є саме тим, за що його видає ініціатор подання. Техаський підхід дозволяє визнання доказу автентичним у разі наявності сукупності непрямих ознак, таких як характерне мовлення, псевдоніми, специфічні фотографії чи інша інформація, що може бути притаманна лише одній особі. У справі *Tienda v. State* (2012) суд визнав, що сукупність непрямих ознак була достатньою для того, щоб присяжні могли розумно дійти висновку про авторство повідомлень [14].

Доцільно підкреслити різницю між поняттям автентичності доказів у кримінальному процесі США та достовірності доказів, що використовується у вітчизняному кримінальному процесуальному законодавстві. У американській судовій практиці навіть змістовно достовірний доказ може бути визнаний недопустимим, якщо не доведено його автентичність. Наприклад, коли невідоме джерело його походження або існують підстави сумніватися в цілісності електронного файлу. При цьому встановлення автентичності не означає, що відомості, які містяться у доказі, є правдивими. Отже, категорія автентичності в американському праві охоплює ширший спектр питань, пов'язаний із перевіркою надійності та походження джерела доказової інформації, тоді як українське поняття достовірності переважно стосується оцінки істинності змісту доказу.

Третім ключовим критерієм оцінки допустимості електронних доказів у кримінальному процесі США є ***доказова цінність («probative value»)***. Цей критерій визначає, наскільки доказ має значення для встановлення істини у справі, тобто наскільки він сприяє підтвердженню або спростуванню певного факту, що має значення для вирішення спору. Відповідно до Правила 403 Федеральних правил доказування, навіть доказ, який формально відповідає вимогам належності та автентичності, може бути виключений із розгляду, якщо його доказова цінність є меншою, ніж потенційний упереджуючий ефект або інші негативні наслідки для справедливого судового розгляду [11].

Іншими словами, суд має здійснити балансування між користю від використання доказу для встановлення істини та можливими ризиками його впливу на об'єктивність судового процесу. До таких ризиків відносяться такі випадки.

1) Небезпека упередження присяжних («unfair prejudice»). Тобто, коли зміст доказу може викликати емоційні реакції або негативне ставлення до підсудного, що спотворить неупереджене сприйняття фактів присяжними.

2) Збентеження або дезорієнтація присяжних («confusing the issues or misleading the jury»). Тобто, коли доказ є занадто складним, технічно перевантаженим або містить інформацію, що може відволікти увагу від основного предмета розгляду.

3) Надмірне подання однотипних доказів («needless presentation of cumulative evidence»). Тобто, коли доказ лише дублює вже надану інформацію, не додаючи нової доказової ваги.

Зокрема, у справах, що стосуються електронних доказів, ці аспекти набувають особливого значення, оскільки цифрові матеріали можуть містити великі обсяги інформації, приватні дані або технічні деталі, незрозумілі для пересічного учасника процесу. Тому суди в США часто ретельно оцінюють, чи не створює подання електронного доказу ризику несправедливого впливу на хід судового розгляду або порушення прав сторін.

Четвертою вимогою допустимості електронних доказів виступає ***правило найкращого доказу («best evidence rule»)***. Це правило формувалось у доказовому праві США ще у 18 столітті. Воно знайшло відображення у роботах найви-

значніших дослідників доказового права США: В. Твінінга [15, с. 202], Г. Батерста [16, с. 1–2], Ф. Буллера [7, с. 293–94] та ін. На сучасному етапі його основи закладені у правилах 1001–1007 Федеральних правил доказування.

Це правило спрямоване на забезпечення максимальної достовірності та точності відомостей, що подаються суду, шляхом вимоги подання оригіналу документа або еквівалентної за надійністю копією. У контексті цифрових доказів це правило набуває особливої актуальності, адже електронні документи не існують у традиційному «паперовому» вигляді, і поняття «оригіналу» має специфічне трактування.

Наступною важливою вимогою до допустимості електронних доказів є **заборона показань з чужих слів («hearsay rule»)**. Це правило забороняє використання тверджень, зроблених поза судом, як доказів істинності заявлених фактів, за винятком випадків, коли таке твердження підпадає під одне з численних виключень, передбачених процесуальним законодавством. У випадку з електронними доказами це означає, що автоматично згенеровані системою дані, електронні листи або повідомлення можуть вважатися показаннями з чужих слів і бути недопустимими, якщо їх не підкріплено відповідним виключенням або підтвердженням достовірності [18].

Однією з ключових тем наукових дискусій щодо використання цифрових доказів у сучасному кримінальному процесі США є загроза застосування діпфейків, тобто маніпульованих або змінених мультимедійних матеріалів, які за допомогою технологій штучного інтелекту та машинного навчання замінюють оригінальне зображення чи відео на образ іншої особи) [19].

Широке застосування діпфейків у соціальних мережах та у судових процесах створює ризик здійснення захисту за допомогою так званого «deepfake defense» (тактики, коли сторона процесу ставить під сумнів автентичність доказу, посилаючись на можливість його фальсифікації за допомогою генеративного ШІ, навіть без фактичних підтверджень). Важливо, що у більшості випадків такі заперечення робляться без подання належних підтверджень факту підробки. Таким чином, сама наявність у сучасному світі технології deepfake стає аргументом для знецінення навіть цілком справжніх і належним чином здобутих доказів.

Дослідники відзначають, що «сам факт існування технології «deepfake» створює ефект «liar's dividend» (буквально – «дивіденд брехуна»), коли будь-який відео чи аудіозапис може бути поставлений під сумнів» [20, с. 9]. Іншими словами, технологічна можливість підробки сама по собі надає потенційним порушникам права додатковий інструмент маніпуляції процесом, дозволяючи їм відкидати несприятливі докази без реальних підстав.

Ця тенденція становить серйозну загрозу для доказового процесу, оскільки підриває традиційну довіру присяжних та суддів до цифрових носіїв інформації, які в умовах сучасного кримінального процесу відіграють визначальну роль. Якщо кожне відео чи аудіо може бути поставлене під сумнів лише на тій підставі, що технологія deepfake існує, це створює небезпеку втрати доказової сили навіть у беззаперечних матеріалів. Саме тому в американській доктрині дедалі більше авторів акцентують на необхідності розроблення нових процесуальних рішень, зокрема щодо удосконалення правил визнання цифрових доказів допустимими.

Науковці наголошують на необхідності розширення функцій судді у визначенні допустимості та автентичності доказів. Так, Герберт Б. Діксон-молодший у своїй статті «Захист на підставі діпфейку»: доказове ускладнення», опублікованій у журналі Американської асоціації адвокатів аналізує пропозиції сучасних дослідників щодо вирішення цього питання. Так професор Ребекка Дельфіно стверджує, що через ризики, пов'язані з фейковими матеріалами, автентичність доказів слід визначати судді, а не присяжним. Вона зазначає, що присяжні не здатні об'єктивно оцінити, чи є відео підробленим, оскільки діпфейкі виглядають реалістично. У зв'язку з цим пропонується запровадити нове положення у Федеральних правилах доказів, яке розширить роль судді у «фільтруванні» доказів і покладе на нього виняткову відповідальність за таке визначення [4, с. 38]. З огляду на це пропонується активніше застосовувати положення Правила 104(а) Федеральних правил доказування, згідно з яким саме суддя вирішує попередні питання автентичності, а не присяжні.

Дослідник доказового права Маура Гроссман та почесний суддя у відставці Пол Грімм пропонують внести цілеспрямовані зміни до Федеральних правил доказування США, а саме до Правила 901(b)(9), яке регулює порядок автентифікації доказів, створених технічними процесами або системами. Зміни, які пропонуються, є точковими, але змістовно важливими. Автори, зокрема, пропонують доповнити вимогу про те, що сторона, яка подає доказ згенерований штучним інтелектом, повинна: 1) описати джерела навчальних даних («training data»), використаних для створення моделі або алгоритму; 2) назвати програмне забезпечення чи модель штучного інтелекту, якою було згенеровано доказ; 3) довести, що в конкретному випадку цей алгоритм або програма дали дійсні та надійні результати [2, с. 14]. На думку авторів, така поправка сприятиме підвищенню стандартів допустимості доказів, згенерованих штучним інтелектом, і водночас не створюватиме зайвих перешкод для їх використання.

Висновки. Підхід Сполучених Штатів Америки до цифрових доказів є одним з найрозвиненіших і найпослідовніших у світі. Американська модель базується на поєднанні норм Федеральних правил доказування та прецедентного права, що забезпечує практичну гнучкість і технологічну адаптивність. Відсутність законодавчого визначення «цифрових доказів» компенсується доктринальними напрацюваннями, стандартизованими керівництвами та усталеною судовою практикою.

Основні критерії допустимості (належність; автентичність; доказова цінність; «правило найкращого доказу» та відсутність порушення вимог до показання з чужих слів) формують багаторівневу систему оцінки, яка гарантує баланс між технічними можливостями та процесуальними гарантіями.

Сучасні виклики, зокрема використання deepfake-технологій і доказів, створених штучним інтелектом, спонукають американських науковців і суддів до перегляду правил автентифікації та розширення ролі судді у перевірці достовірності таких матеріалів. Саме тому, досвід США демонструє ефективну інтеграцію правових, технічних і етичних стандартів, що може стати орієнтиром для вдосконалення українського кримінального процесу у сфері регулювання та оцінки цифрових доказів.

ЛІТЕРАТУРА

1. Grimm P.W., Brady K.F. Evidentiary admissibility chart: admissibility of electronic evidence. Tampa, 2018. 5 p. URL: https://www.flmb.uscourts.gov/judges/tampa/mcewen/GrimmBradyEvidAdmissChart.pdf (date of access: 22.05.2025).

2. Grossman M.R., Grimm P.W. Judicial approaches to acknowledged and unacknowledged AI-generated evidence. *Columbia Science and Technology Law Review*. 2025. Vol. 26, № 2. P. 110–125. URL : https://journals.library.columbia.edu/index.php/stlr/article/view/13890/7671 (date of access: 08.10.2025).

3. Friedman R.D. Refining conditional probative value. *Michigan Law Review*. 1995. Vol. 94, № 2. P. 457–465. URL: https://repository.law.umich.edu/articles/168 (date of access: 08.10.2025).

4. Dixon H. B. The “deepfake defense”: an evidentiary conundrum. *The Judges’ Journal*. 2024. Vol. 63, № 2. P. 38–40. URL: https://www.americanbar.org/content/dam/aba/publications/judges_journal/vol63no2-jj2024-tech.pdf (date of access: 25.11.2025).
5. Electronic crime scene investigation: a guide for first responders. 2nd ed. Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2015. 74 p. (NCJ 219941). URL: https://www.ojp.gov/pdffiles1/nij/219941.pdf (date of access: 25.11.2025).
6. Scientific working group on digital evidence (SWGDE). Digital evidence: standards and principles. *Forensic Science Communications*. 2000. Vol. 2, № 2. URL: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm (date of access: 25.11.2025).
7. Riley v. California, 573 U.S. 373 (2014).
8. Goodison S.E., Davis R.C., Jackson B.A. Digital evidence and the U.S. criminal justice system: identifying technology and other needs to more effectively acquire and utilize digital evidence. Santa Monica: RAND Corporation, 2015. 80 p. URL: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf (date of access: 08.10.2025).
9. Digital evidence in the courtroom: a guide for law enforcement and prosecutors. Washington, D.C.: National Institute of Justice, U.S. Department of Justice, 2007. 47 p. URL: https://www.ojp.gov/pdffiles1/nij/211314.pdf (date of access: 08.10.2025).
10. Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007).
11. Federal rules of evidence. 2024. URL : https://www.uscourts.gov/sites/default/files/2025-02/federal-rules-of-evidence-dec-1-2024.pdf (date of access: 08.10.2025).
12. Thayer J.B. A Preliminary treatise on evidence at the common law. Boston: Little, Brown and Co., 1898. 636 p.
13. Griffin v. State, 419 Md. 343, 19 A.3d 415 (Md. Ct. App. 2011).
14. Tienda v. State, 358 S.W.3d 633 (2012).
15. Twining W. Rethinking evidence: exploratory essays. 2nd ed. New York: Cambridge University Press, 2006. 511 p.
16. Bathurst H. The Theory of evidence. London, 1761. 146 p.
17. Buller F. An introduction to the law relative to trials at nisi prius. 4th ed. London, 1785. 383 p.
18. Микитюк О.С. Допустимість показань з чужих слів у кримінальному процесі США: історичний аспект та сучасні виклики. *Аналітично-порівняльне правознавство*. 2025. Вип. 3, ч. 3. С. 247–260. DOI: 10.24144/2788-6018.2025.04.3.37.
19. Deepfakes and the law // Clio Legal Dictionary. 2023. URL: https://www.clio.com/resources/legal-dictionary/deepfakes-and-the-law/ (date of access: 25.11.2025).
20. Salvi C. Deepfake evidence in criminal proceedings: procedural hurdles and forensic challenges. Luxembourg, 2024. 20 p. URL: https://aiandcriminaljustice.uni.lu/ (date of access: 25.11.2025).

Дата першого надходження рукопису до видання: 26.11.2025
Дата прийнятого до друку рукопису після рецензування: 12.12.2025
Дата публікації: 31.12.2025