УДК 343.131:004.8:004.056(4+477)
DOI https://doi.org/10.24144/2307-3322.2025.91.4.56

ШТУЧНИЙ ІНТЕЛЕКТ У ДОКАЗУВАННІ В ДОСУДОВОМУ ТА СУДОВОМУ ПРОВАДЖЕННЯХ: ДОКТРИНАЛЬНІ ЗАСАДИ І ПРАКТИКА ЗАСТОСУВАННЯ

Погорецький М.А.,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
заслужений діяч науки і техніки України,
професор кафедри кримінального процесу та криміналістики
навчально-наукового інституту права,
проректор з науково-педагогічної роботи
Київського національного університету
імені Тараса Шевченка
ORCID: 0000-0003-0936-0929
e-mail: mykola.pohoretskyi@knu.ua

Погорецький М.А. Штучний інтелект у доказуванні в досудовому та судовому провадженнях: доктринальні засади і практика застосування.

Стаття присвячена проблемним питанням використання штучного інтелекту у доказуванні в кримінальному провадженні в умовах стрімкої цифровізації. Зростання масивів даних із комунікаційних платформ, мобільних пристроїв, мережевих журналів та відкритих джерел інформації (OSINT) ускладнює їх процесуально коректну обробку, формуючи подвійний імператив: оперативний та відтворюваний аналіз за суворого дотримання критеріїв належності, допустимості, достовірності та достатності, із мінімізацією ризиків алгоритмічної упередженості й недостатньої прозорості процедур (проблема «чорної скриньки» – *black box*). Мета дослідження полягає в обґрунтуванні цілісної доктринально-процесуальної криміналістичної моделі інтеграції алгоритмів штучного інтелекту у доказування на досудовій і судовій стадіях у поєднанні із судовим контролем, принципом змагальності та рівності сторін. Методологія спирається на формально-догматичний і порівняльно-правовий підходи, практику Верховного Суду України, Європейського суду з прав людини (*Roman Zakharov v. Russia*; *Big Brother Watch and Others v. the UK*) та Суду ЄС у справі *EncroChat* (C-670/22), а також на криміналістичні стандарти Європейської мережі експертних установ (ENFSI), документи NIST SP 800-86/101r1 і Протокол Берклі. Наукова новизна полягає у: (1) конкретизації тестів допустимості й достовірності результатів алгоритмічної обробки; (2) регламентації «пакета відтворюваності» (*reproducibility dossier*), що включає версії програмного забезпечення, конфігурації, початкові значення (*seed*), журнали передоброблення та виведення, хеш-ідентифікатори, тест-плани й «паспорт моделі» (*model card*); (3) описі процесуальних фільтрів судового контролю (необхідність, пропорційність, мінімізація, обмеження вторинного використання) та тесту «внутрішньої еквівалентності» у транскордонних справах за Європейським наказом про розслідування (EIO); (4) операційних орієнтирах для сторін і суду. Результати дослідження окреслюють концепцію доказування, підсиленого штучним інтелектом (*AI-enabled proof*), яка забезпечує пояснюваність (*XAI*), відтворюваність результатів та вимогу кореспондуючих підтверджень. Розроблено пакет практичних рішень (типові ухвали, стандарти розкриття, уніфіковані формати експертних висновків, суддівський довідник – *benchbook*) і запропоновано інституційні кроки – міжвідомчі криміналістичні центри (forensic-центри), стандартні організаційно-технічні процедури (*SOP*) та програми фахового навчання. Запропонована нормативно-процесуальна конструкція інтегрує алгоритми штучного інтелекту в систему доказування без підміни процесуальної форми та зі збереженням балансу між ефективністю кримінального переслідування і гарантіями прав людини..

Ключові слова: штучний інтелект; цифрові докази; цифрова криміналістика»; належність; допустимість; відтворюваність; судовий контроль; досудове провадження; судове провадження; ЄСПЛ; OSINT; EIO; XAI; SOP.

Pohoretskyi M.A. Artificial Intelligence in evidence in pre-trial and judicial proceedings: doctrine principles and application practice.

The article addresses contentious issues surrounding the use of artificial intelligence in criminal proof within the context of rapid digitalization. The expansion of data streams from communication platforms, mobile devices, network logs, and open-source information (OSINT) complicates their procedurally sound handling, creating a dual imperative: rapid and reproducible analysis conducted under strict adherence to the criteria of relevance, admissibility, reliability, and sufficiency, while minimizing risks of algorithmic bias and insufficient procedural transparency (the "black box" problem). The aim of the study is to substantiate a coherent doctrinal-procedural model for integrating artificial-intelligence algorithms into proof at both the pre-trial and trial stages, combined with judicial oversight, the principle of adversarial proceedings, and equality of arms. The methodology relies on formal-dogmatic and comparative-legal approaches, the practice of the Supreme Court of Ukraine, the European Court of Human Rights (Roman Zakharov v. Russia; Big Brother Watch and Others v. the UK), and the Court of Justice of the EU in EncroChat (C-670/22), as well as on criminalistics standards of the European Network of Forensic Science Institutes (ENFSI), NIST SP 800-86/101r1 documents, and the Berkeley Protocol. The scientific novelty consists in: (1) specifying tests for admissibility and reliability of algorithmic outputs; (2) regulating a "reproducibility dossier" that includes software and model versions, configurations, seed values, preprocessing and inference logs, hash identifiers, test plans, and a "model card"; (3) describing procedural filters of judicial control (necessity, proportionality, minimization, restrictions on secondary use) and the "internal equivalence" test in cross-border cases under the European Investigation Order (EIO); (4) operational guidelines for the parties and the court. The results outline the concept of AI-enabled proof, which ensures explainability (XAI), reproducibility of results, and the requirement of corroborating evidence. A package of practical solutions has been developed (model court orders, disclosure standards, unified formats for expert opinions, and a judicial benchbook), together with proposed institutional steps–interagency criminalistics (forensic) centers, standard operating procedures (SOPs), and professional training programs. The proposed normative-procedural construct integrates artificial-intelligence algorithms into the system of proof without substituting the procedural form and preserves the balance between investigative efficiency and guarantees of human rights.

Key words: artificial intelligence; digital evidence; digital criminalistics (forensics); relevance; admissibility; reproducibility; judicial oversight; pre-trial proceedings; trial proceedings; ECtHR; OSINT; EIO.

Постановка проблеми. Цифрова трансформація суспільних відносин перетворила кримінальне провадження на середовище, у якому ключові фактичні дані виникають, циркулюють і зберігаються в електронній формі – у комунікаційних платформах, мобільних пристроях, мережевих журналах та відкритих джерелах інформації (Open Source Intelligence, OSINT). Це породжує водночас і нові можливості, і нові ризики для доказування: з одного боку – прискорення виявлення, тематизації та систематизації відомостей за допомогою алгоритмів штучного інтелекту, з іншого – виклики допустимості, відтворюваності, алгоритмічної упередженості (bias) і недостатньої прозорості та перевірюваності алгоритмічних процедур (проблема «чорної скриньки» – *black box*) [30; 26; 27]. Транскордонний вимір додатково ускладнює використання цифрових масивів: практика Суду Європейського Союзу (Court of Justice of the European Union, CJEU) у справі C-670/22 (*EncroChat*) закріпила тест «внутрішньої еквівалентності» як умову придатності «вже наявних» даних, отриманих у порядку Європейського наказу про розслідування (European Investigation Order, EIO), що вимагає від національних судів не лише формальної, а й змістовної перевірки гарантій їх здобуття, збереження та подальшого використання [22; 30]. У сфері прав людини Європейський суд з прав людини (European Court of Human Rights, ЄСПЛ) наголошує на «сильних запобіжниках» (robust safeguards) для секретних і масових втручань: необхідності, пропорційності, мінімізації, визначеності правил зберігання/знищення даних та, коли це можливо, повідомлення *post factum* (ex post notification) [26; 27]. У цьому контексті українська наукова доктрина та практика Верховного Суду послідовно підкреслюють: технологічні інструменти не

замінюють процесуальної форми та судової оцінки доказів; «алгоритмічні відповіді» як такі не є джерелом науково доведеної інформації та набувають доказового значення лише за умови належної процесуальної фіксації, розкриття сутнісної технічної інформації (disclosure) і перевірки у сукупності з іншими даними [3; 4; 11; 12; 14]. Відтак ключовою проблемою є вироблення цілісної доктринально-процесуальної криміналістичної моделі інтеграції штучного інтелекту в ланцюг «виявлення – збирання – перевірка – оцінка – представлення в суді» з такими процесуальними фільтрами, які одночасно забезпечують ефективність кримінального переслідування та дотримання прав людини, включно з реальним судовим контролем, рівністю сторін і можливістю незалежного відтворення результатів алгоритмічної обробки.

Аналіз останніх досліджень і публікацій.

Українська наукова традиція доказування у кримінальному провадженні сформувала усталену систему критеріїв належності, допустимості, достовірності та оцінки доказів у сукупності. В авторських працях (про застосування новітніх технологій у розслідуванні воєнних злочинів; про судовий контроль; про теорію та нову концепцію доказування) послідовно окреслено: (а) провідну роль судового контролю у легітимації втручання в права людини; (б) необхідність процесуальної форми для будь-яких технічних результатів; (в) вимогу кореспондуючих доказів при використанні інструментів аналізу даних [11; 12; 13; 14]. Позиції Верховного Суду кореспондують цій доктрині: «відповіді» систем штучного інтелекту самі по собі не становлять джерела науково доведеної інформації і набувають значення лише в межах процесуальної форми з можливістю незалежної перевірки; окремі напрацювання суддівського корпусу акцентують на прозорості технічних операцій і єдності підходів до цифрових доказів [3; 4].

Українські галузеві дослідження, присвячені запобіганню злочинності та використанню штучного інтелекту (ШІ), зокрема праці Р. Благути, А. Мовчана, О. Бугери, О. Заярного, О. Зачека, Я. Свистун, В. Шевчука, Т. Шевчук, В. Шепітька, М. Шепітька та ін., демонструють поступ від загальнотехнічного огляду можливостей до нормативно-практичної інтеграції інструментів аналізу даних у розслідування, водночас наголошуючи на ризиках алгоритмічної упередженості (bias), надмірності та необхідності етичних і процесуальних запобіжників [1; 2; 6; 7; 22]. Навчально-методичні матеріали технічних шкіл (КПІ: «Методи та системи штучного інтелекту», «Методи ШІ в кібербезпеці») підсилюють потребу у стандартизованій перевірці придатності (validation), тест-планах і контролі похибок для моделей комп'ютерного зору (Computer Vision, CV) / оброблення природної мови (Natural Language Processing, NLP) та аналітики журналів подій [10].

Європейський вимір задає подвійний вектор: права людини та транскордонна придатність цифрових масивів. Практика ЄСПЛ (ECtHR) у справах *Big Brother Watch and Others v. the United Kingdom* та *Roman Zakharov v. Russia* формулює вимогу «сильних запобіжників» (robust safeguards): законна мета, необхідність/пропорційність, мінімізація, регламентація зберігання/знищення, ефективний нагляд і, коли можливо, повідомлення постфактум (ex post) [32; 33]. СЄС (CJEU) у справі C-670/22 (*EncroChat*) закріпив тест «внутрішньої еквівалентності» для «вже наявних» цифрових масивів у межах Європейського наказу про розслідування (European Investigation Order, EIO), що вимагає не лише формальної, а й змістовної сумісності гарантій між державами [28; 30]. Оглядові та аналітичні публікації Європолу (Europol) засвідчують користь ШІ для оперативної аналітики, але підкреслюють різницю між «операційною ефективністю» й «судовою придатністю», яка потребує відтворюваності (reproducibility), прозорості та зовнішньої перевірки придатності (external validation) [24; 25]. Порівняльно-правові дослідження (K. Ligeti та ін.; H. Kuczyńska; O. Kutovyi) поглиблюють дискусію щодо автентифікації «алгоритмічних» доказів, допустимості ШІ-опосередкованих висновків та меж судового покладання на статистичні інструменти [39; 40; 41]. У публічному контексті увагу привертає масштаб використання систем розпізнавання облич (facial recognition) та дебати щодо недискримінації і пропорційності (BBC про Clearview; коментар щодо *Glukhin v. Russia*) [36; 37].

Криміналістичний технічний стандарт закладено в європейських та американських настановах: ENFSI Best Practice Manuals для цифрової криміналістики; NIST SP 800-86 (інтеграція криміналістики у реагування на інциденти) і NIST SP 800-101, Rev. 1 (мобільні пристрої). Вони уніфікують вимоги до первинних/робочих копій (master/working copies), хеш-ідентифікації (hashing), блокаторів запису (write-blockers), журналів доступу (access logs), опису невизначеностей (uncertainty) та відтворюваності – що є критично важливим для перетворення технічного результату на доказ [25; 32; 39]. Для відкритих джерел розвідка з відкритих джерел (Open Source

Intelligence, OSINT) за Протоколом Берклі (Berkeley Protocol) встановлює процесуальні вимоги до пошукових стратегій, верифікації метаданих/походження, геолокації й збереження оригіналів, створюючи місток між OSINT і судовою придатністю [26]. Емпіричні дослідження щодо застосування ШІ у діяльності органів правопорядку додатково наголошують на потребі прозорого ланцюга оброблення (processing chain) та зовнішнього контролю інструментів з боку незалежних установ [30].

Окремий напрям порівняльної практики стосується оцінок ризику (risk scoring) та дисциплінарних наслідків зловживання ШІ: справа *State v. Loomis* встановила межі покладання на імовірнісні оцінки без розкриття методики та без кореспондуючих доказів; судова й дисциплінарна практика США, Канади й Австралії щодо «галюцинацій» і фіктивних посилань у процесуальних документах підтвердила неприпустимість делегування професійної ретельності машині [37; 38; 42; 43]. На політичному рівні європейські орієнтири «довірчого ШІ» та Європейська етична хартія для правосуддя вимагають прозорості, підзвітності, недискримінації, пояснюваності (explainability, XAI) і управління ризиками упродовж усього життєвого циклу моделі [27; 46].

Зіставлення масиву публікацій дозволяє виокремити лакуни, які ця стаття прагне заповнити. *По-перше*, у вітчизняній практиці бракує уніфікованих вимог до «пакета відтворюваності» (*reproducibility dossier*) для інструментів комп'ютерного зору (CV), оброблення природної мови (NLP), графової та блокчейн-аналітики із фіксацією версій програмного забезпечення/моделей, конфігурацій, контрольних початкових значень (*seed*), журналів виведення (*inference logs*), тест-планів і аудиту упередженості (*bias audit*) – попри наявність згаданих міжнародних криміналістичних стандартів [26; 30; 32; 45]. *По-друге*, неусталені межі та обсяг розкриття (*disclosure*) сутнісної технічної інформації стороні захисту для забезпечення реального контрольного незалежного відтворення результатів (replication) і рівності сторін (*equality of arms*), зокрема у справах із транскордонним елементом (EIO; «внутрішня еквівалентність») [28; 30]. *По-третє*, потребує деталізації судова методика мотивації рішень щодо покладання/непокладання на алгоритмічні висновки з урахуванням пояснюваності (XAI) і опису невизначеностей, а також стандартизація форм експертних висновків під вимоги ENFSI/NIST і Протоколу Берклі [26; 31; 38; 45]. *По-четверте*, на рівні політик – необхідна операційна уніфікація (Standard Operating Procedures, SOP; *benchbooks*; стандарти *disclosure*) та інституційна спроможність (міжвідомчі криміналістичні центри ШІ – *forensic*-центри) для забезпечення відтворюваності, підзвітності та недискримінації [24; 27; 45-46].

Таким чином, сучасний науково-практичний дискурс пропонує багаторівневу опору для інтеграції ШІ в доказування: національну доктрину кримінального процесуального доказування та позиції Верховного Суду [3; 4; 11–14], європейські стандарти прав людини та транскордонної взаємодії [22; 24; 32; 33], криміналістичні технічні настанови ENFSI/NIST і Протокол Берклі [26; 31; 38; 45], а також порівняльну практику щодо меж алгоритмічних інструментів у суді [24; 25; 36; 38–41; 43–44; 48–49]. На цьому тлі запропонована в статті модель «доказування, підсиленого ШІ» окреслює системні процесуальні фільтри, стандарти відтворюваності та орієнтири для сторін і суду, спрямовані на перетворення технічних результатів на переконливі докази у досудовому та судовому провадженнях.

Метою статті є концептуалізація доктринально-процесуальної криміналістичної моделі використання штучного інтелекту (ШІ) у доказуванні на досудовій та судовій стадіях з урахуванням європейських стандартів і національної практики. Для досягнення цієї мети сформульовано такі *завдання*: (1) уточнити місце ШІ в системі доказування з позицій належності, допустимості, достовірності та достатності; (2) окреслити нормативний і стандартизований масив – практику ЄСПЛ, СЄС, Європейський наказ про розслідування, а також керівництва Європейської мережі судово-експертних установ (European Network of Forensic Science Institutes, ENFSI) та Національного інституту стандартів і технологій США (National Institute of Standards and Technology, NIST), Протокол Берклі (Berkeley Protocol); (3) змоделювати «вставки» ШІ у життєвому циклі доказу та пов'язані з цим процесуальні й техніко-криміналістичні ризики; (4) визначити критерії оцінки результатів ШІ і вимогу відтворюваності результатів (*reproducibility*) як матеріальної основи змагальності; (5) запропонувати операційну «дорожню карту» для сторін і суду [24; 26–27; 30–31; 38; 45].

Матеріали і методи. Матеріальною базою дослідження є нормативно-правові акти та публічні політики України й Європейського Союзу (ЄС, EU), зокрема Закон України «Про оперативно-роз-

шукову діяльність», законодавство у сфері кібербезпеки, Концепція розвитку штучного інтелекту (розпорядження КМУ № 1556-р), а також європейські орієнтири «довірчого штучного інтелекту» (*trustworthy AI*) та Етична хартія Ради Європи для судових систем [5; 6; 27; 46]. Джерельна база включає практику Верховного Суду щодо ролі ШІ та єдності судової практики, рішення ЄСПЛ (ECtHR) у справах *Big Brother Watch* та *Roman Zakharov*, постанову СЄС (CJEU) у справі C-670/22 (*EncroChat*), а також порівняльні кейси західних юрисдикцій стосовно оцінок ризику (*risk scoring*) і дисциплінарних наслідків використання «галюцинацій» (*hallucinations*) систем ШІ у процесуальних документах [3; 4; 28; 32–33; 43–44; 49]. Використано міжнародні стандарти і керівництва: ENFSI Best Practice Manuals для цифрової криміналістики; NIST SP 800-86 та NIST SP 800-101 (інтеграція криміналістики та робота з мобільними пристроями); Протокол Берклі (Berkeley Protocol) щодо роботи з відкритими цифровими джерелами (OSINT) [26; 37–38; 39]. Аналітичний пласт становлять матеріали Європолу (Europol) про застосування ШІ у діяльності органів поліції, міждисциплінарні праці з цифрової криміналістики та доказування, а також українські дослідження щодо ШІ у протидії злочинності та у доказуванні [1–2; 10–14; 30–25; 39–41].

Методологічно застосовано: формально-догматичний аналіз норм кримінального процесу та спеціального законодавства з їх співвіднесенням із європейськими стандартами прав людини – необхідністю, пропорційністю, мінімізацією та «сильними запобіжниками» (*robust safeguards*) [27; 32–33]; порівняльно-правовий підхід через зіставлення національної практики з правом ЄС (Європейський наказ про розслідування – ЕІО, тест «внутрішньої еквівалентності» за C-670/22) та провідними західними юрисдикціями (оцінки ризику, санкції за фіктивні посилання) [22; 30; 43–44; 49]; криміналістичне *case study* з аналітичним моделюванням життєвого циклу доказу з «вставками» ШІ (комп'ютерний зір (Computer Vision, CV), текстова аналітика (Natural Language Processing, NLP), графова аналітика (*graph analytics*), блокчейн-аналіз (*blockchain forensics*), відкриті джерела) на основі ENFSI/NIST/Протоколу Берклі та практичних оглядів Європолу, з подальшою оцінкою судової придатності за критеріями належності, допустимості, достовірності та достатності [24; 26; 31; 38; 45]; стандартизований аудит процедур збирання, збереження та аналізу цифрових артефактів відповідно до вимог ланцюга збереження (*chain of custody*), журналювання доступів (*access logging*), хеш-ідентифікації (*hashing*), опису невизначеностей (*uncertainty*) і відтворюваності (*reproducibility*) [31–32; 45].

Для операціоналізації ключових понять *«допустимість»* розуміється як наявність законної підстави, дотримання судового контролю, відсутність провокації чи масової невибіркової інтервенції та непорушність ланцюга збереження, що забезпечує доброякісність доказу, отриманого із застосуванням ШІ; для транскордонних даних – додатково перевірка «внутрішньої еквівалентності» і співмірності відповідно до підходів ЄСПЛ, СЄС і технічних стандартів [22; 32–33; 38; 45]. *«Достовірність/надійність»* охоплює перевірку придатності інструмента (*validation*), контроль похибок із урахуванням показників хибнопозитивів/хибнонегативів (FPR/FNR), чутливості/специфічності (*sensitivity/specificity*), стійкості до зміни порогів (*thresholds*), аудит упередженості (*bias-audum*) та наявність «пакета відтворюваності» (*reproducibility dossier*) – версій програмного забезпечення/моделей і середовищ, конфігурацій, контрольних початкових значень (*seed*), журналів передоброблення та виведення (*processing/inference logs*), хеш-таблиць, тест-планів і «паспорта моделі» (*model card*) [26; 27; 31; 45–46]. *«Вага/достатність»* визначається оцінкою у сукупності з кореспондуючими доказами та забороною «автоматичного авторитету» алгоритму, зокрема для оцінок ризику [11; 49].

Для забезпечення відтворюваності та якості формується «пакет відтворюваності» (*reproducibility dossier*), що включає таблиці хешів первинних і робочих копій, зафіксовані версії програмного забезпечення/моделей і середовищ, конфігурації та *seed*, журнали передоброблення і виведення, тест-плани й результати перевірених метрик, «паспорт моделі» із визначенням меж застосовності (*scope*), а також протоколи мінімізації/знищення (*minimization/deletion*) та обмеження вторинного використання (*secondary use*) [26–27; 31; 45–46]. Контроль упередженості здійснюється через періодичний *bias-audum* (мовна, демографічна, контекстна упередженість), людську перевірку критичних висновків (*human-in-the-loop*) та вимогу кореспондуючих підтверджень [27; 46].

Простежуваність (трасованість) і ланцюг збереження гарантуються веденням журналів доступів, застосуванням блокаторів запису (*write-blockers*), інвентаризацією артефактів, нормалізацією часових поясів та фіксацією джерел і каналів отримання; для матеріалів з відкритих джерел додатково зберігаються пошукові запити/фільтри, метадані, геолокація та оригінали, як того вимагає Протокол Берклі [26; 31; 38; 45].

Етичні та правозахисні засади узгоджено зі стандартами ЄСПЛ щодо «сильних запобіжників» і принципами «довірчого» ШІ: необхідність, пропорційність, мінімізація, прозорість, підзвітність, недискримінація; для транскордонних випадків застосовано процедурний інструмент ЕІО та тест «внутрішньої еквівалентності»; окремо забезпечено пріоритет прав людини, зокрема заборону ексклюзивного покладання на алгоритмічні висновки [27–28; 30; 38–39; 46; 49].

Критерії включення охоплюють офіційні акти, судові рішення та стандарти, рецензовані публікації і кейси верховних/вищих судів провідних юрисдикцій; виключено джерела без верифікованого походження, непроцесуальні довідки без методичної бази та матеріали без можливості підтвердження автентичності або відтворюваності (*replicability*). До обмежень віднесено відсутність доступу до закритих масивів і відомчого програмного забезпечення, залежність від публічних описів інструментів і різнорідність національних практик; ці ризики мінімізовано стандартизованим аудитом за ENFSI/NIST/Протоколом Берклі [3–6; 24–23; 36–39; 44–46; 49].

Узгоджене поєднання наведених джерел і методів забезпечує прозору простежуваність аргументації, відповідність європейським стандартам прав людини та відтворюваність запропонованих висновків щодо інтеграції ШІ у доказування на досудовій і судовій стадіях.

Виклад основного матеріалу. Доказування у кримінальному провадженні є цілеспрямованою, нормативно врегульованою діяльністю сторін обвинувачення і захисту зі збирання, перевірки та оцінки доказів, яка відбувається під контролем суду. На досудовій стадії цей контроль не може зводитись до формальної перевірки процесуальних атрибутів; він має бути змістовним фільтром, що визначає межі допустимого втручання у приватну сферу, окреслює предмет і обсяг доступу до відомостей, забезпечує мінімізацію обробки даних і встановлює стандарти подальшого поводження з ними. Верховенство права у кримінальному процесуальному доказуванні вимагає не формального, а змістовного судового контролю, що забезпечує справедливість, пропорційність і мотивованість кожного рішення [15]. У судовій стадії ця логіка трансформується у змагальний розгляд, який передбачає належно мотивовані рішення та реальну рівність сторін (*equality of arms*) як умову довіри до результату доказування [12; 14]. Саме тому процесуальна форма не є «обгорткою» для технічного результату: вона виконує роль гарантії від свавілля й помилок і забезпечує відтворюваність шляху від джерела інформації до судового висновку.

Визначальним є підхід, за яким технічні засоби – уся сукупність цифрових інструментів, алгоритмів, методів фіксації та аналізу – розглядаються як допоміжні механізми реалізації засад доказування, які не підміняють судової оцінки належності, допустимості, достовірності та достатності. Будь-який технічний результат набуває процесуального статусу лише за умови його «вбудованості» у належну форму (протоколи, експертні висновки, додатки з технічними журналами), підтвердження кореспондуючими джерелами і доступності для незалежної перевірки стороною захисту [11; 13; 14]. Такий підхід забезпечує не лише формальну, а й епістемічну надійність доказування: суд отримує можливість відтворити логіку здобуття, обробки та інтерпретації цифрових відомостей і дати їм зважену оцінку в сукупності.

Орієнтиром для правозастосування є усталена позиція Верховного Суду: «алгоритмічні відповіді» – попередні висновки, згенеровані інформаційними системами або алгоритмами, – самі по собі не становлять джерела науково доведеної інформації і можуть набувати доказового значення лише за умови процесуальної легітимації та оцінки у взаємозв'язку з іншими даними [3; 4]. Це вимагає від сторін не стільки посилань на «високу точність» інструмента, скільки демонстрації процесуальної коректності його застосування, прозорості технічних операцій і здатності забезпечити ефективне контрольне незалежне відтворення. У підсумку саме поєднання змістовного судового контролю на «вході» (санкціонування, межі, мінімізація) та змагальної, мотивованої оцінки на «виході» (перевірюваність, кореспондування джерел, оцінка у сукупності) формує той базовий стандарт доказування, який унеможливлює підміну судової дискреції технологічною «автоматичністю» і гарантує якість правосуддя [3; 4; 11–14; 25; 26; 50].

Ключові перешкоди для належного застосування ШІ сторонами полягають у: (1) неповному розкритті технічного «ядра» (версій ПЗ/моделей, *seed*, порогів, журналів), що позбавляє захист реальної контрперевірки з контрольним незалежним відтворенням; (2) відсутності стандартних тест-планів і валідованих метрик (FPR/FNR, чутливість/специфічність, AUC) для конкретної справи; (3) ігноруванні принципу мінімізації під час збирання великих масивів; (4) покладанні на «загальну точність» без кореспондуючих доказів. *Рішення:* (1) обов'язкова передача пакета відтворюваності (*reproducibility dossier*) у складі матеріалів відкриття; (2) запровадження уніфіко-

ваних чек-списків сторін (питання до експерта/оператора, вимоги до журналів *processing/access/inference logs*, модельного «паспорта»), а також локальних SOP, узгоджених з ENFSI/NIST; (3) процесуальне фіксування мінімізації (цільові часові «вікна», таргетовані акаунти/пристрої) у клопотаннях і ухвалах; (4) правило кореспонденції: кожен алгоритмічний висновок підкріплюється щонайменше одним незалежним джерелом (протокол, експертиза, свідчення чи інший цифровий слід), а межі застосовності та похибки прямо зазначаються у мотивуванні.

Цифрова джерельна база у сучасному кримінальному провадженні охоплює ширший спектр артефактів, ніж класичні документальні чи речові докази: електронні документи, телекомунікаційні записи, журнали доступу й системні логи, дані мобільних пристроїв і хмарних сервісів, а також метадані – часові мітки, геолокація, ідентифікатори пристроїв – та сліди користувацької активності (патерни дій, історія взаємодій) [32; 39]. Кіберпростір є самостійним середовищем учинення злочинів, яке формує нові криміналістичні умови для виявлення, фіксації та доказування цифрових слідів [18]. У межах цієї множини матеріали з відкритих джерел (OSINT) – зображення, відео, дописи в соціальних мережах, супутникові знімки – набувають процесуальної ваги лише за умови суворого дотримання Протоколу Берклі: фіксації пошукових стратегій (збереження запитів/фільтрів/часових міток і платформ доступу), перевірки походження та цілісності (метадані/EXIF), геолокаційно-хронологічної реконструкції подій, збереження оригіналів і контрольних копій та підтримання безперервного ланцюга збереження (*chain of custody*) [20]. Звідси випливає базовий висновок: цифровий артефакт є процесуально придатним не «за природою», а лише настільки, наскільки прозоро задокументовано його шлях від джерела до судової зали.

Криміналістична (форензічна) дисципліна задається технічними стандартами ENFSI/NIST і є однаковою для всіх класів цифрових джерел: створення первинних і робочих копій, хеш-ідентифікація для підтвердження цілісності, журналювання доступів (хто/коли/що), контроль середовищ виконання та відтворюваність процедур (*reproducibility*) [25; 32; 39]. Ці вимоги не зводяться до «технологічної педантичності» – вони матеріалізують процесуальні гарантії: дають змогу відновити послідовність дій, відокремити первинний образ від робочих копій, перевірити незмінність вмісту та виключити маніпуляції. У такий спосіб технічна коректність стає юридично значущою властивістю, що перетворює інформаційний масив на доказовий матеріал, придатний для перехресної перевірки.

Разом із тим, різниця між «операційною ефективністю» аналітики і «судовою придатністю» доказу залишається принциповою. Практичні огляди Європолу слушно застерігають: швидкість виявлення закономірностей або масштаб обробки даних самі по собі не гарантують прийнятності у суді; необхідні повна простежуваність, можливість незалежного відтворення та наявність процесуальних запобіжників на всіх етапах роботи з даними [24–25]. З цієї позиції випливає нормативна вимога до учасників провадження: кожен цифровий артефакт має супроводжуватися відтворюваним набором технічних і процесуальних атрибутів – копії/хеші/журнали/опис середовищ – які забезпечують перевірюваність походження, цілісності й способу оброблення.

Отже, цифрова джерельна база не є простою сумою технічних файлів чи «скидів» даних; її правове значення формується через криміналістичну дисципліну. OSINT стає доказом лише тоді, коли виконано вимоги Протоколу Берклі; будь-які інші цифрові сліди – коли дотримано ENFSI/NIST-процедур копіювання, хешування, логування та відтворюваності [26; 31; 38; 45]. Науковий висновок тут однозначний: у цифровій сфері юридична якість випливає з технічної відтворюваності, а не навпаки; саме тому забезпечення повної простежуваності та контрольного незалежного відтворення стає не допоміжною, а визначальною умовою судової переконливості доказів.

Матеріальні та процесуальні межі втручання у сферу цифрових доказів визначаються поєднанням гарантій Конвенції та вимог кримінального процесу, які разом утворюють належний режим безпеки для будь-яких слідчих дій, у тому числі з використанням алгоритмічних інструментів. Практика ЄСПЛ вимагає наявності законної мети, реального, а не декларативного, незалежного контролю до і після втручання, дотримання принципу мінімізації, чітких правил зберігання й знищення даних, регламентації доступу та обміну інформацією і, коли це можливо, повідомлення *post factum* особи, щодо якої здійснювалася інтервенція [26; 27]. Саме ці елементи запобігають «інституціоналізації» масових і невибіркових практик збору відомостей та є критеріями як допустимості втручання, так і надійності його результатів.

Операціоналізація зазначених гарантій відбувається через змістовний судовий контроль. Ухвала слідчого судді повинна не просто санкціонувати доступ, а конкретизувати джерела й канали

даних, обсяг і строки, правила копіювання та фіксації цілісності (хеш-ідентифікація), вимоги до журналювання доступів, а також умови пояснюваності алгоритмічних процедур (XAI) і обов'язок сформувати «пакет відтворюваності» (*reproducibility dossier*) для можливої незалежної перевірки стороною захисту [31; 38; 45]. Така деталізація перетворює абстрактні стандарти Конвенції на перевірні процесуальні обов'язки, забезпечує відтворюваність технічного шляху доказу та реальну змагальність. У подальшому мотивувальна частина судового рішення має фіксувати, чи і чому суд покладається на відповідний цифровий/алгоритмічний компонент; брак прозорості або неможливість відтворення неминуче веде до зниження доказової ваги або до виключення матеріалів [3; 4; 49].

Транскордонний вимір підвищує планку процесуальних вимог. У порядку Європейського наказу про розслідування (EIO) застосовується тест «внутрішньої еквівалентності», закріплений СЄС у справі C-670/22 (*EncroChat*): «вже наявні» цифрові масиви можуть бути використані лише за умови, що гарантії їх здобуття та нагляду відповідають тим, які вимагалися б у державі-виконавці; перевірці підлягає не лише формальний канал передачі, а й змістовна сумісність запобіжників [28; 30; 34]. Це означає, що національний суд має оцінювати пропорційність первинної операції, безперервність ланцюга збереження та обмеження на *secondary use*, інакше доказ стає процесуально вразливим до виключення.

Таким чином матеріальні та процесуальні межі втручання виконують подвійну функцію: задають «вхідні» умови допустимості цифрової інтервенції і водночас визначають «вихідні» стандарти надійності та ваги її результатів. Їх практичний сенс – не в абстрактних запобіжниках, а в тому, що кожна технічна дія має бути необхідною і співмірною, кожен цифровий артефакт – *простежуваним* і відтворюваним, а кожне посилання на алгоритм – поясненим і перевірним. Лише за таких умов технологічний інструментарій працює на верховенство права, а не замість нього.

Штучний інтелект у кримінальному процесуальному доказуванні має подвійне призначення: з одного боку, це інструмент виявлення, відбору та аналітичного опрацювання цифрових масивів; з іншого – самостійний об'єкт перевірки на відповідність процесуальним і етичним вимогам. Така дихотомія зумовлює підвищені стандарти прозорості та відтворюваності: технічний результат, що виникає внаслідок алгоритмічної обробки, може бути покладений в основу судового висновку лише настільки, наскільки зрозумілий і перевірний шлях переходу від вхідних даних до висновку. Для цього застосовуються вимоги пояснюваності (XAI) та недискримінації: суд і сторони повинні отримати змістовне пояснення механізму класифікації/ідентифікації, кола істотних факторів і меж застосовності моделі, а також підтвердження відсутності дискримінаційних ефектів (мовних, демографічних, контекстних) [27; 46]. Водночас XAI не підміняє процесуальної форми: пояснення має бути «вмонтоване» у належно оформлені процесуальні носії (протоколи, висновки), доступне для перехресної перевірки і співставне з іншими джерелами.

Матеріальною основою такої перевірності виступає «пакет відтворюваності» (*reproducibility dossier*), який уніфікує технічні та процесуальні атрибути доказу: фіксовані версії програмного забезпечення, моделей і бібліотек; конфігурації та пороги; контрольні початкові значення (*seed*); журнали передоброблення й виведення (*processing/inference logs*); таблиці хешів первинних і робочих копій; протоколи середовищ виконання; тест-плани і метрики якості (FPR/FNR, чутливість/специфічність, AUC); результати аудиту упередженості; «паспорт моделі» (*model card*) з межами застосовності та застереженнями [31; 38; 45]. Така структуризація виконує не лише функцію технічної «документації», а й процесуальну гарантію реальної рівності сторін: за наявності пакета інша сторона спроможна здійснити контрольне незалежне відтворення, виявити чутливість висновків до зміни порогів, перевірити цілісність даних і коректність ланцюга збереження. За відсутності цих елементів зникає можливість ефективної контрперевірки, а отже – підривається як допустимість, так і доказова вага результату.

Операціоналізація зазначених гарантій відбувається через змістовний судовий контроль. Ухвала слідчого судді повинна не просто санкціонувати доступ, а конкретизувати джерела й канали даних, обсяг і строки, правила копіювання та фіксації цілісності (хеш-ідентифікація), вимоги до журналювання доступів, а також умови пояснюваності алгоритмічних процедур (XAI) і обов'язок сформувати «пакет відтворюваності» (*reproducibility dossier*) для можливої незалежної перевірки стороною захисту [31; 38; 45]. Така деталізація перетворює абстрактні стандарти Конвенції на перевірні процесуальні обов'язки, забезпечує відтворюваність технічного шляху доказу та реальну змагальність. У подальшому мотивувальна частина судового рішення має фіксувати, чи і

чому суд покладається на відповідний цифровий/алгоритмічний компонент; брак прозорості або неможливість відтворення неминуче веде до зниження доказової ваги або до виключення матеріалів [3; 4; 49].

Транскордонний вимір підвищує планку процесуальних вимог. У порядку Європейського наказу про розслідування (ЕІО) застосовується тест «внутрішньої еквівалентності», закріплений СЄС у справі C-670/22 (*EncroChat*): «вже наявні» цифрові масиви можуть бути використані лише за умови, що гарантії їх здобуття та нагляду відповідають тим, які вимагалися б у державі-виконавці; перевірці підлягає не лише формальний канал передачі, а й змістовна сумісність запобіжників [22; 30; 34]. Це означає, що національний суд має оцінювати пропорційність первинної операції, безперервність ланцюга збереження та обмеження на *secondary use*, інакше доказ стає процесуально вразливим до виключення.

Таким чином матеріальні та процесуальні межі втручання виконують подвійну функцію: визначають «вхідні» умови допустимості цифрової інтервенції і водночас окреслюють «вихідні» стандарти надійності та ваги її результатів. Їх практичний сенс – не в абстрактних запобіжниках, а в тому, що кожна технічна дія має бути необхідною і співмірною, кожен цифровий артефакт – *простежуваним* і відтворюваним, а кожне посилання на алгоритм – поясненим і перевірним. Лише за таких умов технологічний інструментарій працює на верховенство права, а не замість нього.

Штучний інтелект у кримінальному доказуванні має подвійне призначення: з одного боку, це інструмент виявлення, відбору та аналітичного опрацювання цифрових масивів; з іншого – самостійний об'єкт перевірки на відповідність процесуальним і етичним вимогам. Така дихотомія зумовлює підвищені стандарти прозорості та відтворюваності: технічний результат, що виникає внаслідок алгоритмічної обробки, може бути покладений в основу судового висновку лише настільки, наскільки зрозумілий і перевірний шлях переходу від вхідних даних до висновку. Для цього застосовуються вимоги пояснюваності (XAI) та недискримінації: суд і сторони повинні отримати змістовне пояснення механізму класифікації/ідентифікації, кола істотних факторів і меж застосовності моделі, а також підтвердження відсутності дискримінаційних ефектів (мовних, демографічних, контекстних) [27; 46]. Водночас XAI не підміняє процесуальної форми: пояснення має бути «вмонтоване» у належно оформлені процесуальні носії (протоколи, висновки), доступне для перехресної перевірки і співставне з іншими джерелами.

Матеріальною основою такої перевірності виступає «пакет відтворюваності» (*reproducibility dossier*), який уніфікує технічні та процесуальні атрибути доказу: фіксовані версії програмного забезпечення, моделей і бібліотек; конфігурації та пороги; контрольні початкові значення (*seed*); журнали передоброблення й виведення (*processing/inference logs*); таблиці хешів первинних і робочих копій; протоколи середовищ виконання; тест-плани і метрики якості (FPR/FNR, чутливість/специфічність, AUC); результати аудиту упередженості; «паспорт моделі» (*model card*) з межами застосовності та застереженнями [31; 38; 45]. Така структуризація виконує не лише функцію технічної «документації», а й процесуальну гарантію реальної рівності сторін: за наявності пакета інша сторона спроможна здійснити *контрольне незалежне відтворення*, виявити чутливість висновків до зміни порогів, перевірити цілісність даних і коректність ланцюга збереження. За відсутності цих елементів зникає можливість ефективної контрперевірки, а отже – підривається як допустимість, так і доказова вага результату.

Логічний наслідок цієї конструкції є прямим і практичним: дефект на стадії доступу або фіксації неминуче трансформується у дефект допустимості. Відсутність належної санкції, непродемонстрована необхідність/пропорційність, порушення *криміналістичних* процедур (відсутність первинної копії, хешів, журналів, контролю середовищ), вихід за межі первинної мети без нової ухвали – кожен із цих недоглядів не лише створює загрозу для прав людини, а й позбавляє суд можливості переконатися у законному походженні та процесуальній чистоті цифрового матеріалу [31; 38; 45]. Саме тому допустимість у цифровій сфері – це не формальний «прохідний бал», а сукупність перевірюваних гарантій, без яких електронний артефакт не може стати повноцінним доказом у змагальному процесі.

Достовірність у цифровому середовищі охоплює дві взаємопов'язані площини: автентичність і цілісність даних та відтворюваність застосованої методики їх одержання й опрацювання. У першій площині перевіряється, чи походить електронний артефакт саме з того джерела, на яке посилається сторона, і чи залишався він незмінним упродовж усього життєвого циклу; у другій – чи можна, дотримуючись описаної процедури, відтворити ідентичний або порівнянний результат,

що перетворює висновок із випадкового на методологічно надійний [25; 32; 39]. Практичним втіленням цих вимог є безперервність криптографічного контролю (стабільні хеш-значення від моменту первинного доступу до судової презентації), розмежування первинного образу і робочих копій, застосування пристроїв блокування запису (*write-blockers*), а також повний ланцюг журналів, які відбивають кожну операцію з даними і середовищами виконання (хто, коли, що і з якою метою здійснював) [25; 32; 39]. Будь-яка непояснена модифікація або розрив у журналюванні руйнує «ланцюг довіри» й послаблює доказову силу артефакту.

Невід'ємним елементом є верифікація метаданих, що корелює зміст із атрибутами: часові мітки узгоджуються з реконструйованою хронологією, геолокаційні координати – з топографією події, системні ідентифікатори пристроїв і акаунтів – із суб'єктним складом; часові пояси нормалізуються, джерела часу синхронізуються, а будь-які розбіжності фіксуються й аргументовано пояснюються [31; 38; 45]. Для фото- і відеоматеріалів аналіз метаданих формату обмінюваних метаданих зображення (Exchangeable Image File Format – EXIF) як стандарту зберігання технічної інформації (метаданих) у цифрових фото- та відеофайлах, а також реконструкція послідовності перекодувань (*re-encoding chain*) дають змогу відрізнити оригінальний (первинний) файл (*original file*) від змінених або похідних копій (*derived copies*), що нерідко є вирішальним (*critical*) для оцінки цілісності (*integrity*) цифрового доказу.

Відтворюваність методики на рівні як ручних, так і автоматизованих оброблень забезпечується повнотою журналів: журнали оброблення даних (*processing logs*) мають демонструвати кроки передоброблення, параметри нормалізації та порогові значення; журнали доступу (*access logs*) – суб'єкта, час, операцію і результат; журнали виведення (*inference logs*) – версію моделі, конфігурацію, *seed*, пороги й часові мітки запусків. Саме наявність цих журналів робить можливою незалежну перевірку й контрольне незалежне відтворення за ідентичних умов – ядро змагальності у справах, що спираються на цифрові докази [25; 32; 39].

Достовірність неможлива без перевірених (апробованих) інструментів і процедур: застосовуються засоби з підтвердженою точністю та стабільністю, описаними межами застосовності й відомими похибками. Ці параметри фіксуються у тестових планах (*test plans*) та показниках якості (*performance metrics*), зокрема у частоті хибнопозитивних спрацьовувань (False Positive Rate, FPR), чутливості (*sensitivity*), специфічності (*specificity*) та площі під кривою робочої характеристики приймача (Area Under the Curve, AUC). Усі ці дані додаються до матеріалів справи й надають суду змогу об'єктивно оцінити ризик помилок і стійкість отриманих результатів [31; 38; 45].

Для алгоритмічно отриманих результатів є обов'язковими три складові. *По-перше*, «пакет відтворюваності» (*reproducibility dossier*), що охоплює фіксовані версії програмного забезпечення, моделей і бібліотек, конфігурації та пороги, контрольні початкові значення (*seed*), журнали попередньої обробки та виведення (*preprocessing/inference logs*), таблиці хешів первинних і робочих копій, протокол середовищ виконання, тест-плани і метрики. *По-друге*, пояснюваність (*XAI*) – зрозуміле і відтворюване пояснення механізму класифікації чи ідентифікації, переліку істотних факторів і меж інтерпретації, що робить алгоритмічний висновок придатним для судового мотивування. *По-третє*, аудит упередженості (*bias-audum*) із фіксацією відсутності дискримінаційних ефектів (мовних, демографічних, контекстних) або з описом компенсаторів у разі виявлених ризиків [27; 46]. Сукупний ефект цих вимог полягає в тому, що цифровий висновок отримує епістемічну опору: відомо, чому модель дійшла певного результату, чи повторюється він за ідентичних умов, у яких межах його слід тлумачити і які похибки супроводжують застосування.

Зрештою, відкидання дефектних практик – обов'язкова умова наукової доброчесності в судовій оцінці. Якщо відсутні стабільні хеші, журнали доступу/оброблення, не описано середовищ, не визначено метрик і тестів стабільності, а розробник або власник інструмента прикривається «комерційною таємницею» і не надає критичних параметрів для перевірки, такий результат не витримує змагальної перевірки і втрачає доказову вагу; за наявності істотних порушень він підлягає виключенню [27; 31; 38; 45; 46]. Отже, достовірність цифрових доказів – це стандартизована, криміналістично відтворювана процедура, а не довіра до технології: лише поєднання тяглого криптографічного контролю, повного журналювання, верифікації метаданих, перевірених (апробованих) інструментів, а для алгоритмічних результатів – «пакет відтворюваності» (*reproducibility dossier*), пояснюваність системи штучного інтелекту (*explainable AI, XAI*) та аудит алгоритмічної упередженості (*bias audit*) – забезпечує рівень перевірності, який дозволяє суду мотивовано покладатися на цифровий доказ у сукупності з іншими матеріалами.

Достатність і «вага» цифрових доказів – це не арифметика байтів і не захоплення технологічною витонченістю інструмента; це здатність цифрових відомостей переконувати суд у сукупності з іншими джерелами, без «автоматичного авторитету» одиничного артефакту або алгоритмічного висновку. Висока агрегована точність моделі сама по собі не конституює доказової сили: вона має бути співвіднесена з кореспондуючими підтвердженнями – протоколами слідчих дій, експертними висновками, показаннями, іншими цифровими слідами – які узгоджено відтворюють подію без внутрішніх суперечностей, а також із процесуальним «родоводом» отриманих даних (санкція, мінімізація, безперервний ланцюг збереження доказів (*chain of custody*), відтворюваність процедур) [3; 4; 27]. Інакше кажучи, достатність виникає не з ізольованої «впевненості» алгоритму, а з цілісності доказової картини, що витримує перехресну перевірку у змагальному процесі.

Змістовний стандарт зважування у цифрових справах вимагає від суду кількох послідовних кроків. *По-перше*, окреслити межі застосовності цифрового артефакту або алгоритмічного висновку: за яких умов (якість вхідних даних, параметри, пороги, середовища) він генерує стабільний результат і де його інтерпретація виходить за припустимі межі. *По-друге*, прямо врахувати похибки та невизначеності: імовірнісна природа класифікацій, ризики хибнопозитивів/хибнонегативів, чутливість до зміни порогів і контексту – усе це має бути відображено у мотивуванні судового рішення, щоб уникнути підміни змістовної оцінки «загальною точністю» інструмента [27]. *По-третє*, перевірити узгодженість з іншими джерелами: чи підтримують протоколи, експертизи, показання та незалежні цифрові сліди той самий фактичний сценарій, чи навпаки – демонструють розриви, які знижують вагу «алгоритмічної» ланки.

Окрема вимога стосується висновків, здобутих за допомогою «чорних скриньок» і оцінок ризику (risk scoring): вони не можуть бути самостійною підставою вирішального процесуального рішення. Такі результати потребують розкриття методики, ключових параметрів і меж точності та зважування разом з іншими доказами, інакше суд опиняється перед нездоланною епістемічною «діркою» – невідомо, чому модель прийшла до такого результату і наскільки він стабільний за змінених умов [3; 4; 27; 49]. Отже, заборона «автоматичного авторитету» – не декларація, а процесуальна вимога: навіть висока точність на тестових вибірках – це лише відправна точка для перевірки, а не фінішна підстава для висновків по суті.

Практичний критерій достатності у цифровому вимірі можна сформулювати як трискладову перевірку: (1) епістемічна якість цифрового артефакту/висновку (чіткі межі застосовності, артикуляція похибок, стабільність за параметрами); (2) процесуальний «родовід» (санкція, пропорційність, копії/хеші/журнали, контроль середовищ, цільове використання); (3) кореспонденція у сукупності (наявність незалежних підтверджень і відсутність невмотивованих розривів із іншими джерелами). Лише збіг усіх трьох вимірів трансформує цифровий матеріал із «операційно корисного» у судово переконливий. Саме тому «вага» – це наслідок узгодженості та відтворюваності доказової картини, перевіреної у змагальній процедурі, а не похідна від «вишуканості» чи «точності» застосованої технології.

Сукупне застосування цих чотирьох критеріїв (*належність; допустимість; достовірність; достатність і «вага»)* забезпечує не лише формальну відповідність процесу, а й якість судового пізнання: мінімізація виключає нерелевантні нашарування, санкція і пропорційність – свавільне втручання, відтворюваність – технічну надійність, а заборона «автоматичного авторитету» – підміну судової дискреції технологічною видимістю точності. Саме в такій послідовності цифровий артефакт переходить із площини «операційної корисності» до статусу судово переконливого доказу.

Використання штучного інтелекту (ШІ) у кримінальному доказуванні не може розглядатися як ізольований технологічний акт – це багатофазовий процес, вбудований у цілісний ланцюг доказування, що починається з виявлення релевантних цифрових слідів і завершується їх судовою презентацією. На кожній із цих фаз ШІ виступає як асистивний інструмент, придатність якого обумовлена не лише його алгоритмічними характеристиками, а й суворим дотриманням процесуальної форми, криміналістичних стандартів і принципу рівності сторін.

Фаза виявлення цифрової інформації, у якій ШІ застосовується як фільтр і класифікатор, вимагає попереднього визначення чітких критеріїв інклюзії та ексклюзії (*inclusion/exclusion criteria*), а також запрограмованих порогів релевантності для відсіву шумових чи надлишкових даних. Обов'язковою є фіксація конфігурацій і параметрів моделей, які застосовувались на цьому етапі, з метою подальшої відтворюваності та критичної оцінки [24; 25; 45]. *Фаза збирання* передбачає дотримання жорсткої технічної дисципліни відповідно до стандартів ENFSI та NIST: створен-

ня первинних і робочих копій, хеш-ідентифікація (*hashing*), детальне журналювання доступів (*access logs*), застосування *write-blockers* та інвентаризація артефактів [31; 38; 45]. У разі роботи з відкритими джерелами (OSINT) до цього додаються вимоги Протоколу Берклі – зокрема, фіксація пошукових стратегій, збереження оригіналів, геолокаційна й хронологічна верифікація, збереження метаданих та побудова безперервного ланцюга збереження (*chain of custody*) [26]. *Застосування ШІ як передумови для обшуку/виїмки породжує ризики:* (1) невибіркове «вилучення про запас» без чітко окресленої мети і без урахування мінімізації; (2) опора на «чорну скриньку» без пояснюваності (XAI), що унеможливлює перевірку законності джерела відомостей; (3) порушення ланцюга збереження через відсутність первинних копій, хеш-ідентифікаторів та журналів доступу/середовищ; (4) повторне використання даних без нової санкції (*secondary use*); (5) транскордонні дефекти, коли «вже наявні» масиви не відповідають тесту «внутрішньої еквівалентності». *Процесуальні запобіжники:* (1) в ухвалі слідчого судді – конкретизація предмета та меж доступу (час/місце/суб'єкти/канали), вимоги до копіювання, хешування і журналювання, XAI-умови та обов'язок сформувати пакет відтворюваності для подальшої перевірки; (2) фіксація заборони *secondary use* без нової ухвали; (2) для EIO – долучення матеріалів, що підтверджують судовий контроль, пропорційність первинної операції і безперервність ланцюга збереження у державі-виконавці [22; 29].

Фаза збереження потребує подвійної простежуваності: як щодо даних, так і інструмента, що їх обробляв. Інакше кажучи, ланцюг збереження (*chain of custody*) має включати не лише інформацію про копії, доступи й зберігання цифрових масивів, а й технічну документацію про застосовану модель ШІ: її версії, конфігурації, контрольні початкові значення (*seed*), журнали виведення (*inference logs*) та змінні середовища [3; 4; 25; 45]. Фаза аналізу включає застосування ШІ до оброблення даних – NLP, комп'ютерного зору, графової чи блокчейн-аналітики. На цьому етапі обов'язковими є: документована перевірка придатності моделі на релевантних вибірках; фіксація метрик якості (наприклад, FPR/FNR, AUC, чутливість/специфічність); тестування «крихкості» до змін вхідних даних (наприклад, зміни освітлення, шум, мовна варіативність); а також *bias*-аудит, спрямований на виявлення дискримінаційних ефектів (демографічних, мовних, контекстних) [24; 27; 36; 45]. Фінальною є фаза судової презентації, на якій цифровий доказ із ШІ-компонентом набуває або втрачає свою доказову силу залежно від якості обґрунтування та відкритості процедур. У центрі стоїть повний пакет відтворюваності (*reproducibility dossier*) – сукупність матеріалів, яка дає змогу суду й стороні захисту контрольно незалежно відтворити алгоритмічний висновок. До нього входять: версії моделей, параметри, конфігурації, журнали оброблення (*processing/inference logs*), таблиці хешів, «паспорт моделі» (*model card*), результати перевірки придатності, *bias*-аудит та пояснення (XAI) [27; 31; 45].

Ключове значення має реалізація прав сторони захисту на незалежну контрперевірку з контрольним відтворенням: якщо доступ до пакета відтворюваності, параметрів чи журналів обмежено, це не лише порушує принцип рівності сторін, а й підриває довіру до результату як такого. У транскордонному вимірі – наприклад, при використанні «вже наявних» цифрових масивів, одержаних у межах Європейського наказу про розслідування (European Investigation Order, EIO) – обов'язковою є перевірка «внутрішньої еквівалентності» (*internal equivalence*) гарантій: якщо стандарт збирання, доступу й обробки у державі-виконавці нижчий, такий доказ може бути визнано непридатним для використання в національному провадженні [22; 30; 32–33].

Таким чином, ШІ може бути вбудований у ланцюг доказування лише за умови дотримання процесуально-технічного режиму, який охоплює: (1) чіткі критерії інклюзії при виявленні; (2) технічну дисципліну і відповідність ENFSI/NIST/Берклі; (3) прозору простежуваність і ланцюг збереження; (4) повну перевірку придатності, тести похибок і *bias*-аудит; (5) відтворювану й пояснювану судову презентацію. У протилежному випадку алгоритмічний результат, навіть будучи технологічно складним, не витримує перевірки на процесуальну якість і доказову придатність.

У межах загального ланцюга цифрового доказування окрему увагу слід приділити спеціальним модальностям застосування алгоритмів штучного інтелекту (ШІ), оскільки кожен технологічний напрям – незалежно від уніфікованої інфраструктури – вимагає специфічної правової й технічної верифікації, а відповідно – окремого набору процесуальних запобіжників. Йдеться, зокрема, про оброблення природної мови (Natural Language Processing, NLP), комп'ютерний зір (Computer Vision, CV), графову аналітику (*graph analytics*), блокчейн-аналіз і збір цифрових відомостей з відкритих джерел (OSINT). У кожному з цих випадків критичним є не сам факт застосування ШІ,

а дотримання вимог відтворюваності, меж застосовності, пояснюваності (XAI) та процесуальної контрольованості.

Так, у сфері оброблення природної мови (NLP) первинною умовою є ведення журналів передоброблення (*preprocessing logs*), які фіксують усі етапи трансформації тексту – токенізацію, нормалізацію, визначення мови, виключення стоп-слів і застосовані пороги класифікації. У кримінальному провадженні це критично важливо, оскільки контекстуальні ризики (іронія, сарказм, двозначність, культурна кодифікація, *code-mixed* мовлення) можуть істотно впливати на зміст правової оцінки. Звідси імператив: результати NLP-аналізу можуть бути використані лише як асистивний інструмент, а остаточне правове тлумачення має бути верифіковане людиною – як судом, так і стороною захисту – через незалежну перевірку параметрів і контрольне відтворення результатів [36; 45].

У сегменті комп'ютерного зору (CV) – наприклад, при автоматичному розпізнаванні облич або об'єктів на відео – визначальне значення має якість вхідних даних (освітлення, роздільність, кут зйомки), а також тестування меж застосовності моделі: чи була вона навчена на відповідних сценаріях і чи не виходить поточне використання за її епістемічну зону. Усі моделі CV повинні бути перевірені на предмет помилок першого і другого роду (*false positive rate / false negative rate, FPR/FNR*), а результати – задокументовані в тест-планах і метриках точності [36; 45]. За відсутності цих параметрів навіть найвишуканіший візуальний висновок втрачає переконливість у суді.

Графова аналітика (*graph analytics*), яка застосовується для виявлення зв'язків у телекомунікаційних, фінансових або соціальних масивах, вимагає подвійного контролю. *По-перше,* мають бути визначені пороги значущості, наприклад, мінімальна кількість контактів, обсяг транзакцій або часові межі спілкування. *По-друге*, обов'язковим є чутливісний аналіз (*sensitivity analysis*): дослідження впливу зміни порогів на стабільність висновків. Найголовніше – мережеві висновки повинні мати змістовні підтвердження: сам по собі факт з'єднання вузлів ще не є доказом протиправної взаємодії і має бути підтверджений іншими цифровими слідами або комунікаційними даними [24].

Аналіз блокчейну (кластеризація адрес, виявлення руху активів, побудова графів транзакцій) має очевидну прикладну цінність у справах про обіг криптовалюти та пов'язані злочини. Водночас судова придатність таких висновків вимагає: (1) прозорості евристичних правил кластеризації (наприклад, за IP, часом або поведінковими маркерами); (2) верифікації від постачальника інструмента з наданням метрик точності, інформації про навчальні вибірки та журналів версій; (3) кореспондуючих підтверджень, зокрема, результатів KYC-процедур (*know-your-customer*), офіційних витягів з реєстрів або слідчих дій, що підтверджують зв'язок між адресою та особою [24; 31; 38; 45].

Нарешті, у сфері використання відкритих джерел (OSINT) застосовується Протокол Берклі, який задає високі стандарти верифікації. Усі зібрані зображення, відео, дописи або супутникові знімки повинні бути простежуваними: фіксується джерело, URL, дата та час доступу, умови публічності, метадані (EXIF), геолокація, а також зберігаються оригінали та створюються контрольні копії. Усі дії з матеріалами протоколюються, формуючи ланцюг збереження (*chain of custody*), придатний до незалежного аудиту стороною захисту або судом [26; 31; 45].

У підсумку, застосування ШІ в межах зазначених модальностей є легітимним лише за умови повної прозорості інструмента, чітко задокументованих меж застосовності, кореспондуючих підтверджень і можливості контрольного незалежного відтворення. Лише за таких умов результат алгоритмічної обробки відповідає стандартам належності, допустимості, достовірності та може набувати процесуальної ваги в межах кримінального провадження.

Процесуальні ролі сторін у провадженнях, що передбачають застосування штучного інтелекту (ШІ), визначаються основоположними принципами змагальності, рівності озброєнь і справедливого суду. Учасники кримінального процесу – обвинувачення, захист і суд – виконують взаємопов'язані функції, покликані гарантувати легітимність втручання, криміналістичну дисципліну при роботі з цифровими даними, повноту та достовірність технічної інформації, а також її доступність для незалежної перевірки.

Провідна роль сторони обвинувачення полягає у правовому обґрунтуванні (легітимації) застосування алгоритмічних інструментів. Це означає не лише наявність законної мети та обґрунтованої необхідності/пропорційності втручання, а й чітке визначення обсягу даних, строків доступу, меж використання, способу обробки та знищення надлишкової інформації. Законність і обмеже-

ність втручання мають бути підтверджені в ухвалі слідчого судді з фіксацією усіх параметрів, зокрема – допустимих інструментів, конфігурацій, метрик та принципів мінімізації [12; 20; 27].

Крім того, саме обвинувачення несе обов'язок забезпечення криміналістичної дисципліни: створення первинних і робочих копій, хеш-ідентифікація, журналювання доступів, контроль середовищ (за стандартами ENFSI/NIST) [20; 25; 32; 45], а також перевірка придатності інструментів на релевантних контрольних підмножинах із фіксацією рівнів похибок (FPR/FNR), чутливості, специфічності, AUC та результатів *bias*-аудиту [20; 24; 27]. Безумовною є вимога пояснюваності (XAI): будь-який алгоритмічний висновок має супроводжуватися обґрунтуванням логіки моделі, її меж застосовності та застережень. Завершальним обов'язком сторони обвинувачення є розкриття (*disclosure*) – надання захисту повного пакета відтворюваності, що включає конфігурації, пороги, версії ПЗ/моделей, контрольні значення (*seed*), журнали, хеш-таблиці, тест-плани та результати *bias*-аудиту [31; 32; 39].

Сторона захисту, реалізуючи право на змагальність і ефективну контрперевірку, формує цільові клопотання про розкриття «технічного ядра» доказу – походження масиву, параметри класифікації, журнал обробки, ланцюг збереження, дані про доменну перевірку придатності й упередженість [19; 27; 32–3; 50]. У разі отримання доступу – здійснює контрольне незалежне відтворення, повторно запускаючи модель за наданими параметрами (версії, *seed*, пороги, середовище виконання, тест-плани) та фіксує будь-які відхилення, нестабільність результатів або ознаки доменної непридатності. На основі цього захист вибудовує контрнаратив: аргументовано ставить під сумнів допустимість, достовірність або вагу доказу з огляду на селекційну упередженість, непрозорість логіки моделі або порушення принципу мінімізації [17; 31; 36; 38; 45;].

Суд виконує функцію змістовного фільтра як на досудовій стадії (санкціонування втручань), так і під час судового розгляду. На етапі санкціонування суддя перевіряє законність мети, необхідність і пропорційність заходу, фіксує технічні обмеження й умови знищення надлишкових даних. У разі транскордонного провадження – здійснює оцінку «внутрішньої еквівалентності» стандартів за процедурою ЕІО: лише за умови змістовної сумісності процесуальних гарантій із національними можливе використання вже наявних масивів [12; 30; 32–33]. У судовому процесі суд зобов'язаний перевіряти відтворюваність результатів (*reproducibility*), рівень пояснюваності алгоритмів (*explainable AI, XAI*), показники точності та результати перевірки на упередженість (*bias*-аудит). Також підлягають оцінці наявність і зміст пояснень, які формує модель, відсутність дискримінаційних ефектів та визначення меж її застосовності. У своєму рішенні суд повинен надати мотивовану оцінку допустимості, достовірності та доказового значення такого результату в сукупності з іншими даними, чітко пояснивши, з яких причин він покладається або не покладається на алгоритмічний компонент доказу [12; 27; 32–33].

У такий спосіб вибудовується єдина логіка процесуального управління цифровими доказами з елементами ШІ: на кожному етапі – від легітимації втручання до оцінки доказів – дотримання вимог розкриття, контрольного незалежного відтворення, пояснюваності та кореспондуючих підтверджень є передумовою перетворення технічного результату на судово переконливий доказ.

Ризики, пов'язані із застосуванням штучного інтелекту (ШІ) у кримінальному доказуванні, є не випадковими винятками, а системними викликами, що випливають із самої природи алгоритмічних моделей, масштабності оброблюваних даних і складності їх перевірки (верифікації) у межах змагального процесу. Вони охоплюють технічний, процесуальний, етичний і правозастосовний виміри та потребують відповідного компенсаторного інструментарію для нейтралізації або мінімізації процесуальних ризиків.

Першу групу становлять ризики точності та стабільності моделей. Алгоритмічні інструменти, особливо в галузі розпізнавання образів (*computer vision*), аналізу текстів (*natural language processing*) або прогнозування ризиків, завжди оперують із певною імовірністю помилки. Показники помилок першого й другого роду (false positive rate – FPR, false negative rate – FNR), чутливості (*sensitivity*), специфічності (*specificity*) та загальної точності (area under the curve – AUC) прямо залежать від якості вхідних даних, налаштувань порогів, контексту застосування та так званої доменної придатності (*domain validity*) моделі. Моделі можуть виявитися «крихкими» (*fragile*), тобто нестабільними до мінімальних змін у формулюваннях (у випадку NLP), умовах освітлення (у випадку CV) або параметрах класифікації – що спричиняє різке зниження точності та спотворення висновків [31; 38; 45].

Друга група – це структурні проблеми «чорної скриньки» (*black-box models*), коли внутрішня логіка алгоритму, дані навчання або налаштування не розкриваються (навіть частково) через

посилання на комерційну таємницю. У такому випадку сторона захисту втрачає можливість провести контрперевірку з контрольним незалежним відтворенням, а суд – оцінити достовірність і межі застосовності результату, що ставить під сумнів саму змагальність. Третім викликом є так звані «галюцинації» (*hallucinations*) генеративних моделей: автоматичне створення неіснуючих посилань, джерел або фактів, які не мають реального підґрунтя в матеріалі справи [43; 44; 48].

Третя група ризиків стосується процесуальних дефектів збирання, обробки та збереження цифрових артефактів. Відсутність первинних копій або хеш-ідентифікаторів (SHA), незастосування *write-blockers*, відсутність журналів доступу (*access logs*) або неконтрольоване середовище виконання підривають безперервність ланцюга збереження (*chain of custody*) і створюють підстави для визнання доказів недопустимими або сумнівними [31; 38; 45]. До того ж непропорційне або надмірне втручання без чітко окресленої мети (наприклад, масове «вилучення про запас») та повторне використання даних без нової санкції (ухвали суду) (*secondary use*) прямо суперечить стандартам ЄСПЛ щодо необхідності, пропорційності та мінімізації [32–33]. Це ж стосується транскордонних масивів, які не проходять перевірку «внутрішньої еквівалентності» стандартів держави-виконавця у процедурі ЕІО [28; 30].

Етичний вимір ризиків охоплює як індивідуальні упередження, так і системні ефекти. Моделі, натреновані на нерепрезентативних або демографічно обмежених вибірках, здатні відтворювати або навіть посилювати дискримінаційні патерни. Особливо це стосується розпізнавання облич у разі низької якості зображень або прогнозних оцінок ризику щодо вразливих груп. Європейська етична хартія щодо ШІ (European Ethical Charter on AI in Justice) та політика «довірчого» ШІ ЄС (*trustworthy AI*) прямо вимагають аудит упередженості (*bias audit*), документацію меж застосовності моделі (*model card*) і заборону ексклюзивного покладання на автоматичний висновок без кореспондуючих підтверджень [27; 46].

Нарешті, надмірне або непрозоре використання алгоритмічних систем породжує *chilling effect* – ефект «охолодження» правової активності: наприклад, масове розпізнавання облич у публічному просторі здатне стримувати реалізацію свободи зібрань або вираження поглядів, що ЄСПЛ розглядає як інтервенції, які вимагають підвищеного рівня обґрунтування [32–33].

Для нейтралізації вищезазначених ризиків потрібні багатоетапні компенсатори. *По-перше*, аудит алгоритмів як до їх застосування (*ex ante*), так і після (*ex post*): документування методів, параметрів, версій, меж застосовності, тест-планів, метрик похибок, а також – обов'язково – результатів *bias*-аудиту [27; 45–46]. *По-друге*, впровадження стандартних операційних процедур (SOP) за моделлю ENFSI/NIST: кожен крок – від вилучення до зберігання – має фіксуватися у пакеті відтворюваності (*reproducibility dossier*), з відображенням журналів доступу, інструментів, середовищ, хешів тощо [31; 39; 45].

По-третє, незалежна експертиза та контрольне незалежне відтворення: сторона захисту має отримати доступ до усіх необхідних елементів – версій ПЗ, параметрів, *seed*, хешів – для відтворення і перевірки результату. Якщо це неможливо – доказова сила результату знижується, або такий результат виключається [3; 4].

Крім того, мають бути впроваджені прозорі політики збереження й знищення даних, обмеження на *secondary use*, контроль версій і середовищ виконання та – що найголовніше – заборона «автоматичного авторитету» алгоритму: будь-який технічний результат повинен оцінюватися у сукупності з іншими доказами та з обов'язковим мотивованим судовим поясненням.

Таким чином, ризики не можуть бути усунені остаточно – але можуть і повинні бути контрольовані через комплексну систему процесуальних, технічних та етичних компенсаторів, що уможливлюють перетворення ШІ з джерела правової невизначеності на інструмент, підзвітний верховенству права.

Практична імплементація стандартів застосування штучного інтелекту (ШІ) у кримінальному провадженні потребує не лише концептуальних підвалин і нормативної регламентації, а й створення чітких інструментів, що забезпечують реалізацію принципів прозорості, відтворюваності та змагальності на рівні щоденної слідчої, експертної й судової практики.

У межах процесуального регулювання першочергове значення мають стандартизовані шаблони ухвал слідчих суддів. Така ухвала має чітко фіксувати: (1) законну мету доступу до цифрових даних або використання алгоритмічних засобів; (2) часові, предметні та суб'єктні межі збору/обробки; (3) політику мінімізації і знищення надлишкових даних; (4) дозволені інструменти, моделі і версії програмного забезпечення; (5) обов'язок копіювання, хешування та ведення журналів до-

ступу; (6) вимоги до пояснюваності (*explainability, XAI*); (7) обов'язковість формування повного пакета відтворюваності (*reproducibility dossier*); (8) обмеження на повторне використання даних без нової санкції (*secondary use*); (9) у транскордонних провадженнях – матеріали для перевірки «внутрішньої еквівалентності» (*test of internal equivalence*) у межах Європейського наказу про розслідування (EIO) [22; 30–33; 45].

Уніфікована структура експертного висновку щодо аналізу результатів, отриманих із застосуванням штучного інтелекту (ШІ), повинна бути чітко визначена і зорієнтована на забезпечення процесуальної відтворюваності, технічної обґрунтованості й реальної змагальності сторін. Такий висновок має включати: стисле формулювання запитання до експерта; джерела та канали одержання даних із фіксацією ланцюга збереження (*chain of custody*); технічні інструменти – із зазначенням версій програмного забезпечення, моделей, середовища виконання, конфігурацій і контрольних початкових значень (*seed*); опис застосованих методів оброблення та встановлених параметрів; результати перевірки придатності на контрольних вибірках із відповідними тест-планами та метричними показниками (чутливість – *sensitivity*, специфічність – *specificity*, рівень хибнопозитивних і хибнонегативних результатів – FPR/FNR, площа під кривою – AUC); межі застосовності моделі та чинники невизначеності; аудит упередженості (*bias audit*) із зазначенням компенсаторів (балансування вибірок, людська перевірка, підтвердження іншими джерелами); візуалізацію результатів і можливість їх контрольного незалежного відтворення; фінальний висновок, який прямо підкреслює, що жоден результат алгоритму не може мати автоматичний авторитет без підтримки іншими кореспондуючими доказами [27; 31; 38; 45; 49]. Ключовим елементом доказової структури є пакет відтворюваності (*reproducibility dossier*) – повноцінний комплекс технічної документації, що забезпечує повну відтворюваність результату й дає змогу стороні захисту або суду здійснити контрольне незалежне відтворення. Такий пакет повинен містити: версії програмного забезпечення, моделей і бібліотек; конфігураційні файли; контрольні початкові значення (*seed*); журнали передоброблення й виведення (*preprocessing/inference logs*); таблиці хеш-ідентифікаторів первинних і робочих копій; тест-плани і метрики точності; результати *bias*-аудиту; «паспорт моделі» (*model card*) з межами застосовності; а також опис джерел даних і правових підстав їх одержання.

На інституційному рівні обґрунтованим кроком є створення міжвідомчих криміналістичних центрів штучного інтелекту, які виконуватимуть функції акредитації інструментів, зберігання первинних копій і конфігурацій, проведення контрольних незалежних відтворень на запит суду або сторони захисту, формування реєстрів «паспортів моделей» та системної фіксації результатів *bias*-аудитів. Ефективність таких центрів доцільно вимірювати кількістю справ, у яких забезпечено повний пакет відтворюваності, часткою успішних контрольних незалежних відтворень і відсутністю обґрунтованих процесуальних зауваг до ланцюга збереження.

Важливою є уніфікація знань та практик застосування ШІ у кримінальному процесуальному доказуванні усіх учасників процесу. Регулярні тренінги для суддів, прокурорів, слідчих і адвокатів повинні охоплювати стандарти ЄСПЛ щодо «сильних запобіжників» (*strong safeguards*), транскордонні вимоги Європейського наказу про розслідування (EIO) та принцип «внутрішньої еквівалентності», криміналістичну дисципліну відповідно до керівництв ENFSI і NIST, правила роботи з відкритими джерелами за Протоколом Берклі, принципи пояснюваності (XAI) й аудиту упередженості (*bias audit*), а також практику Верховного Суду щодо допустимості, достовірності та ваги доказів, отриманих за участю ШІ [3–4; 11–12; 14; 24–27; 31–33; 38; 44–46; 49].

Суддівські довідники (benchbooks) мають містити комплекс прикладних інструментів: типову структуру судового рішення із зазначенням процесуальних умов застосування технологій штучного інтелекту; орієнтовний перелік запитань для судової експертизи; зразок *reproducibility dossier*; а також контрольний перелік критеріїв оцінки допустимості, достовірності та доказової сили цифрових і алгоритмічних матеріалів. Сукупність цих елементів формує цілісну нормативно-процесуальну та технічну інфраструктуру, яка трансформує технологічну можливість отримання доказів із використанням ШІ на досудовій стадії у їхню судову придатність – не шляхом спрощення, а через поетапну формалізацію й забезпечення контрольованої прозорості кожного етапу алгоритмічного доказування.

Висновки. Штучний інтелект дедалі активніше інтегрується у сферу кримінального провадження, виконуючи функції виявлення, фільтрації, класифікації та первинної аналітики цифрових даних. Проте він не є самостійним суб'єктом процесу доказування, а лише технічним інстру-

ментом сторін і суду, який підпорядковується доктринальним і процесуальним вимогам. Доказ у цифровому середовищі – це не ізольований артефакт, а ланцюг дій, що починається з виявлення і збирання та завершується його судовою оцінкою. На кожному етапі цього ланцюга має бути забезпечено відтворюваність (*reproducibility*), прозорість (пояснюваність, *explainability*) і змагальність сторін (*equality of arms*).

Правовою основою цифрового доказування є *чотирикомпонентний комплекс критеріїв* належності, допустимості, достовірності та достатності. У цифровому вимірі *належність* тісно пов'язана з принципом мінімізації – інформація повинна стосуватися предмета доказування, збиратися в чітко окреслених межах і не перевищувати обґрунтовану мету.

Допустимість є фільтром законності та пропорційності доступу до цифрових даних: судова санкція, технічна дисципліна (копії, хеш-ідентифікація, журналювання) та заборона вторинного використання без нової ухвали є обов'язковими умовами. У транскордонному вимірі доказовість підпорядковується принципу «внутрішньої еквівалентності» (*internal equivalence*), сформульованому Судом ЄС у справі *EncroChat*: масив цифрових даних може бути використано лише тоді, коли гарантії, за яких він був здобутий, співмірні з тими, що вимагалися б у державі-запитувачі.

Достовірність у цифровому середовищі передбачає автентичність і цілісність даних, верифіковану через стабільні хеш-ідентифікатори, повний ланцюг журналів (*processing, access, inference logs*), аналіз метаданих і геолокації, а також відтворюваність методики одержання й аналізу. Для результатів, сформованих за допомогою ШІ, обов'язковим є пакет відтворюваності (*reproducibility dossier*) – сукупність технічної документації, що містить конфігурації, версії ПЗ, контрольні початкові значення (*seed*), параметри, журнали та метрики, а також результати *bias*-аудиту. Без нього результат втрачає доказову переконливість і не витримує змагального оскарження.

Достатність і вага доказу вимагають не технічної досконалості, а процесуальної узгодженості: алгоритмічний висновок не може бути самостійною підставою вирішального процесуального рішення, особливо за умов обмеженого доступу до його внутрішньої логіки. Навіть висока точність моделі не замінює потреби в кореспондуючих доказах, а межі похибки, застосовності та потенційні упередження мають прямо враховуватися судом під час оцінки. Орієнтиром тут слугує позиція Верховного Суду України та практика зарубіжних юрисдикцій, зокрема у справі *State v. Loomis*, яка встановлює: імовірнісні моделі (ризик-оцінювання, кластеризація, фільтрація) не можуть бути ексклюзивною основою для судового висновку.

Роль суду, сторони обвинувачення і сторони захисту в умовах застосування ШІ набуває оновленого змісту. *Обвинувачення* зобов'язане планувати втручання, дотримуючись принципу необхідності й мінімізації, забезпечити технічну дисципліну збирання та перевірку придатності інструментів, а також розкрити захисту технічне «ядро» алгоритму. *Сторона захисту* має право вимагати *disclosure*, здійснювати контрольне незалежне відтворення, виявляти технологічні вразливості (*bias, domain limits*) і формувати контрнаратив. *Суд* – як на стадії санкціонування, так і при розгляді по суті – зобов'язаний перевіряти XAI-пояснення, тестувати межі контрольного незалежного відтворення та мотивовано зважувати докази у сукупності, з урахуванням алгоритмічної природи та змагального оскарження.

Застосування ШІ створює нові ризики: технічні похибки, крихкість моделей, «галюцинації» генеративних систем, непрозорість («чорна скринька»), дефекти *chain of custody*, надмірне вторинне використання даних і *chilling effect*. Єдиною прийнятною відповіддю є впровадження компенсаторів: аудит алгоритмів до та після застосування (*ex ante/ex post*), ведення повного ланцюга збереження, фіксація версій і параметрів, регулярний *bias*-аудит, політики зберігання/знищення, незалежна експертиза й контрольне незалежне відтворення з доступом сторони захисту до технічної інформації.

Узагальнюючи: ШІ підсилює доказування лише в межах перевірної криміналістичної дисципліни та процесуальних гарантій справедливого суду. Будь-яке делегування дискреції машині (ШІ) без прозорості, відтворюваності та мотивованої людської оцінки – це не доказування, а технологічна ілюзія. Судовий процес має залишатися інструментом захисту прав, а не демонстрацією потужності алгоритмів. Саме тому автоматичний авторитет алгоритму – неприйнятний. Його результат переконливий лише тоді, коли він вбудований у процесуальну форму, перевірений, контрольно незалежно відтворений і оцінений у сукупності з іншими доказами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/3337.
2. Бугера О.І. Використання штучного інтелекту для запобігання злочинності. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Т. 32(71), № 6, 2021. С. 82–86. URL: https://www.juris.vernadskyjournals.in.ua/journals/2021/6_2021/15.pdf.
3. Верховний Суд. Відповіді штучного інтелекту не визнаються як джерело достовірної науково доведеної інформації. Постанова КГС ВС від 8 липня 2025 р. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1865949.
4. Верховний Суд. Роль ШІ у забезпеченні єдності судової практики в Україні. Презентація, 2025. URL: https://court.gov.ua/storage/portal/supreme/prezentacii_2025/_120_AI_uniformity_of_judicial_practice_bernaziuk.pdf.
5. Закон України «Про оперативно-розшукову діяльність»: Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
6. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19.
7. Заярний О.А. Концепція розвитку штучного інтелекту в Україні. Baltija Publishing, 2025. С. 7–25. URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/597/16071/33923-1.
8. Зачек О.І. Роль штучного інтелекту в підвищенні ефективності розслідувань кримінальних правопорушень. Вісник Львівського державного університету внутрішніх справ. 2023. № 3. С. 233–243. URL: http://journals.lvduvs.lviv.ua/index.php/law/article/view/637.
9. Клян Анастасія. Правове регулювання штучного інтелекту в Україні та світі. GOLAW, 02.2022. URL: https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti.
10. Методи та системи штучного інтелекту. Київ: КПІ, 2025. С. 112–145. URL: https://ipi.kpi.ua/wp-content/uploads/2025/01/Metody-ta-systemy-shtuchnogo-intelektu_24_25_3_6_denna.pdf.
11. Погорецький М.А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів… Вісник кримінального судочинства. 2023. № 3–4. С. 84–102. DOI: 10.17721/2413-5372.2023.3-4/84-102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf.
12. Погорецький М.А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. *Аналітично-порівняльне правознавство.* 2025. № 4, ч. 3. С. 269–279. DOI https://doi.org/10.24144/2788-6018.2025.04.3.40. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42-2.pdf.
13. Погорецький М. Теорія кримінального процесуального доказування: проблемні питання. *Право України*. 2014. № 10. С. 12–25. URL: https://pravoua.com.ua/uk/store/pravoukr/pravoukr_10_14/Pogoretskyi_10_14.
14. Погорецький М.А. Нова концепція кримінального процесуального доказування. *Вісник кримінального судочинства України*. 2015. № 3. С. 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf.
15. Погорецький М.А. Верховенство права у кримінальному процесуальному доказуванні: методологія та практика застосування. *Вісник Національної академії правових наук України*. 2025. Т. 32. № 3. С. 275–299. DOI: https://doi.org/10.31359/1993-0909-2025-32-3-275.
16. Погорецький М.А. Обшук: міжнародно-правові стандарти захисту приватності та їх застосування в Україні. *Юридичний науковий електронний журнал*. 2025. 7. С. 243–252. DOI https://doi.org/10.32782/2524-0374/2025-7/54. URL: http://lsej.org.ua/7_2025/56.pdf.
17. Погорецький М.А., Коровайко О.І. Застосування тимчасового доступу до речей і документів у кримінальних провадженнях про злочин, учинені організованими злочинними угрупуваннями. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*: наук.-практ. журн. Київ: Міжвід. наук.-досл. центр з проблем б-би з орг. злоч. 2013. № 1 (29). С. 234–242. URL: http://nbuv.gov.ua/UJRN/boz_2013_1_28.
18. Погорецький М.А., Шеломенцев В.П. Поняття кіберпростору як середовища вчення злочину. *Інформаційна безпека людини, суспільства, держави*: наук.-практ. журнал. Київ: НАСБУ, 2009. № 2 (2). С. 77–81.

19. Погорецький М.А. Захисник – суб'єкт доказування на досудовому провадженні за чинним КПК України: проблемні питання. *Актуальні питання державотворення в Україні*: матеріали міжнародної науково-практичної конференції (м. Київ, 23 травня 2014 р.). Київ: Прінт-Сервіс, 2014. С. 480–482.
20. Погорецький М. Прокурор у кримінальному процесі: щодо визначення функцій. *Право України*. 2015. № 6. С. 86–95. URL: https://pravoua.com.ua/storage/files/magazines/files/content-pravoukr-2015-6-pravoukr_6_15-3.pdf.
21. Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р «Про схвалення Концепції розвитку штучного інтелекту в Україні». URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.
22. Свистун Я.В., Шевчук Т.А. Використання штучного інтелекту у протидії злочинності. Вісник Кримінологічної асоціації України. 2021. № 2 (25). С. 128–134. URL: https://dspace.univd.edu.ua/xmlui/handle/123456789/10965.
23. Суддя Верховного Суду Я. Берназюк. Судова практика застосування ШІ для доступу до правосуддя. Суд.ua. 2025. URL: https://sud.ua/uk/news/sudebnaya-praktika/325362-sudya-verkhovnogo-suda-rasskazal-o-primenenii-iskusstvennogo-intellekta-v-pravosudii.
24. AI and policing: The benefits and challenges of artificial intelligence for law enforcement. Europol, 2023, pp. 1–28. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf.
25. A comprehensive analysis of the role of artificial intelligence in digital forensics. Forensic Science International: Digital Investigation. 2023. URL: https://www.sciencedirect.com/science/article/pii/S2666281723001944.
26. Berkeley Protocol on Digital Open Source Investigations. OHCHR & UC Berkeley, 2020. URL: https://www.ohchr.org/sites/default/files/Documents/Publications/BerkeleyProtocol.pdf.
27. Council of Europe. European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. 2018. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.
28. Court of Justice of the EU. Case C-670/22 (M.N.) – Judgment of 30 Apr 2024 (EIO / EncroChat). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0670.
29. Digital Justice: Ally or Threat? A Critical Analysis of Evidence Collection and Use in the Era of Artificial Intelligence in Colombia. ConnectOnTech (Baker McKenzie), 2025. URL: https://connectontech.bakermckenzie.com/digital-justice-ally-or-threat-a-critical-analysis-of-evidence-collection-and-use-in-the-era-of-artificial-intelligence-in-colombia.
30. Directive 2014/41/EU on the European Investigation Order. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0041.
31. European Network of Forensic Science Institutes (ENFSI). Best Practice Manuals – Digital Forensics. 2025. URL: https://enfsi.eu/documents/best-practice-manuals.
32. European Court of Human Rights (Grand Chamber). Big Brother Watch and Others v. the UK, nos. 58170/13, 62322/14, 24960/15. 2021. URL: https://hudoc.echr.coe.int/eng?i=001-203614.
33. European Court of Human Rights (Grand Chamber). Roman Zakharov v. Russia, no. 47143/06 (2015). URL: https://hudoc.echr.coe.int/eng?i=001-159324.
34. Погорецький М.А. Використання даних EncroChat у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий електронний журнал.* 2025. № 8. С. 223–229. DOI https://doi.org/10.32782/2524-0374/2025-8. URL: http://lsej.org.ua/8_2025/48.pdf.
35. Frontiers in Artificial Intelligence. Disinformation Countermeasures and Artificial Intelligence. 2024. URL: https://www.frontiersin.org/research-topics/58930/disinformation-countermeasures-and-artificial-intelligenceundefined.
36. Glukhin v. Russia: facial recognition is a highly intrusive technology, but the Court abstains from considering a potential inconsistency with fundamental rights. Strasbourg Observers, 2024. URL: https://strasbourgobservers.com/2024/01/09/glukhin-v-russia-facial-recognition-is-a-highly-intrusive-technology-but-the-court-abstains-from-considering-a-potential-inconsistency-with-fundamental-rights.
37. James Clayton, Ben Derico. Clearview AI used nearly 1m times by US police, it tells the BBC. BBC News. 27 March 2023. URL: https://www.bbc.com/news/technology-65057011.

38. Kent, K., Chevalier, S., Grance, T., & Dang, H. Integrating Forensic Techniques into Incident Response (NIST SP 800-86). NIST, 2006. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-86.pdf.
39. Kuczyńska H. The analysis and evaluation of evidence by artificial intelligence in a criminal trial. *Forensic Science*. 2025. № 1. С. 91–102. URL: https://journal.srcif.com.ua/index.php/main/article/download/20/33.
40. Kutovyi O. Artificial Intelligence in the Case-Law of the European Court of Human Rights. *Ehrlich's Journal*. 2025. № 12. С. 34–44. URL: http://journals.chnu.chernivtsi.ua/index.php/Ehrlich/article/view/144.
41. Ligeti K. et al. CRIM_AI – Unpacking AI Evidence and (Re-)Defining Authentication in Criminal Justice. University of Luxembourg, 2024, pp. 1–27. URL: https://aiandcriminaljustice.uni.lu/wp-content/uploads/sites/260/2024/11/Unpacking-AI-Evidence_Ligeti.pdf.
42. Moran C.R., Burton J., Christou G. US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. *Journal of Global Security Studies*. 2023. Vol. 8, Issue 2, ogad005. URL: https://academic.oup.com/jogss/article-abstract/8/2/ogad005/7128314.
43. Murray on behalf of the Wamba Wemba Native Title Claim Group v Victoria (Federal Court of Australia). BNlaw, 2025. URL: https://bnlaw.com.au/knowledge-hub/insights/ai-hallucinations-in-court-lessons-from-the-uk-us-and-australia.
44. Myers v. Tarion Warranty Corporation (Ontario, Canada). AI Hallucinations Cases Database, 2025. URL: https://www.damiencharlotin.com/hallucinations.
45. National Institute of Standards and Technology. Guidelines on Mobile Device Forensics (NIST SP 800-101, Rev. 1). U.S. Department of Commerce, 2014. https://doi.org/10.6028/NIST.SP.800-101r1.
46. Rules for trustworthy artificial intelligence in the EU. EUR-Lex, 2025. URL: https://eur-lex.europa.eu/EN/legal-content/summary/rules-for-trustworthy-artificial-intelligence-in-the-eu.html.
47. Seng D.K.B. Chapter 18: Artificial Intelligence as Evidence. *SSRN*. 2025. № 18. С. 340–365. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5275488.
48. Shahid v. Essam (Georgia Court of Appeals, US). Fabricated cases through use of AI – санкції до адвоката. BNlaw, 2025. URL: https://bnlaw.com.au/knowledge-hub/insights/ai-hallucinations-in-court-lessons-from-the-uk-us-and-australia.
49. State v. Loomis (Wisconsin Supreme Court, US). Використання AI-ризик-аналізу у кримінальному провадженні. *INNS of Court Review*, 2017. URL: https://inns.innsofcourt.org/media/199879/ai-case-law-and-resources.pdf.
50. Старенький О.С. Кримінальні процесуальні гарантії захисника як суб'єкта доказування у досудовому розслідуванні: теорія та практика: монографія. За загал. ред.д.ю.н., проф. М.А. Погорецького. К.: Алерта, 2016. 336 с.