

УДК 004.89:343.14

DOI <https://doi.org/10.24144/2307-3322.2025.92.3.37>

ШТУЧНИЙ ІНТЕЛЕКТ І БІОМЕТРИЧНІ ДАНІ В КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ: ДОПУСТИМІСТЬ, РИЗИКИ, СУДОВИЙ КОНТРОЛЬ

Маштальяр О.М.,
аспірант кафедри інформаційних технологій
Навчально-наукового інституту права та психології,
Національна академія внутрішніх справ
ORCID: 0009-0009-6979-333X
e-mail: o.mashtaliar@gmail.com

Маштальяр О.М. Штучний інтелект і біометричні дані в кримінальному процесі України: допустимість, ризики, судовий контроль.

У статті розглянуто питання впровадження технологій штучного інтелекту (ШІ) для обробки біометричних даних у кримінальному процесі України. Акцентовано увагу на потенціалі використання ШІ для ідентифікації осіб за відбитками пальців, рисами обличчя, голосом та іншими біометричними характеристиками, що може підвищити ефективність розслідування та доведення вини. Одночасно окреслено низку ризиків: можливі помилкові спрацювання алгоритмів та хибні збіги, які здатні призвести до неправомірних підозр або арештів; проблема надійності та прозорості «чорних скриньок» ШІ, коли сторони процесу не можуть перевірити методику отримання результату; загрози приватності, пов'язані з масовим збиранням і використанням чутливих персональних (біометричних) даних без достатніх правових гарантій. Встановлено, що чинне українське законодавство не містить спеціальних норм щодо допустимості доказів, отриманих із застосуванням ШІ, зокрема результатів автоматизованого розпізнавання облич або інших біометричних ідентифікацій. Обґрунтовано необхідність удосконалення нормативної бази: визначення процесуального статусу даних, згенерованих ШІ, впровадження критеріїв перевірки їх достовірності (через експертну оцінку, валідацію методів тощо), а також особливого порядку судового контролю за використанням таких технологій на стадіях досудового розслідування і судового розгляду. Зроблено висновок, що для збалансування інноваційних можливостей ШІ з гарантіями прав людини потрібен комплексний підхід – від внесення змін до Кримінального процесуального кодексу щодо фіксації та оцінки доказів, отриманих за допомогою ШІ, до врахування міжнародних стандартів (GDPR, Акта ЄС про ШІ) і створення механізмів незалежного нагляду. Належний судовий контроль та правове регулювання мінімізують ризики і забезпечать допустимість та об'єктивність використання біометричних даних, опрацьованих ШІ, у кримінальному провадженні. Наведено приклади зарубіжного досвіду: в окремих справах у США суди визнавали результати ШІ-аналізу, наприклад при ДНК-експертизі, водночас інші судові рішення відхиляли докази, отримані через технології розпізнавання облич, через сумніви у їх надійності та належному розкритті методики. На європейському рівні спостерігається тенденція до обережного підходу: Європарламент пропонує суттєві обмеження на використання систем масового біометричного спостереження, дозволяючи їх лише у виняткових випадках за рішенням суду. Підкреслено, що впровадження ШІ у практику кримінальної юстиції має супроводжуватися не лише технічними, але й правовими та етичними запобіжниками.

Ключові слова: штучний інтелект, біометричні дані, кримінальне провадження, допустимість доказів, ризики, судовий контроль, приватність.

Mashtaliar O.M. Artificial intelligence and biometric data in the criminal procedure of Ukraine: admissibility, risks, and judicial oversight.

The article examines the implementation of artificial intelligence (AI) technologies for processing biometric data in Ukraine's criminal proceedings. Emphasis is placed on the potential of AI use for

identifying individuals by fingerprints, facial features, voice, and other biometric characteristics, which can enhance the efficiency of investigations and evidence gathering. At the same time, a number of risks are outlined: possible algorithm errors and false matches that could lead to unjustified suspicions or arrests; the issue of reliability and transparency of AI “black box” models, whereby parties in a trial cannot verify how a result was obtained; and privacy threats associated with the mass collection and use of sensitive personal (biometric) data without sufficient legal safeguards. It is determined that current Ukrainian legislation lacks clear provisions on the admissibility of evidence obtained through AI, in particular results of automated facial recognition or other biometric identifications. The need for improving the regulatory framework is substantiated: defining the procedural status of data generated by AI; introducing criteria for verifying their accuracy (through expert assessment, validation of methods, etc.); as well as establishing special procedures for judicial oversight over the use of such technologies at the pre-trial investigation and trial stages. Examples of foreign experience are provided: in some cases U.S. courts have admitted AI-driven analyses (e.g., DNA expert reports) as evidence, whereas other rulings have excluded evidence obtained via facial recognition technologies due to concerns about their reliability and the lack of disclosure of the AI methods. At the European level, a cautious approach is observed: the European Parliament advocates significant restrictions on the use of mass biometric surveillance systems, allowing them only in exceptional situations subject to a court order. It is highlighted that the introduction of AI into criminal justice practice must be accompanied by not only technical, but also legal and ethical safeguards. The conclusion is drawn that a comprehensive approach is required to balance the innovative capabilities of AI with human rights protections – from amending the Criminal Procedure Code to record and evaluate AI-derived evidence to taking into account international standards (GDPR, the EU AI Act) and creating mechanisms of independent oversight. Proper judicial control and tailored legal regulation will minimize risks and ensure the admissibility and objectivity of using AI-processed biometric data in criminal proceedings.

Key words: artificial intelligence, biometric data, criminal proceedings, admissibility of evidence, risks, judicial control, privacy.

Постановка проблеми: Стрімкий розвиток технологій штучного інтелекту та їх впровадження в діяльність правоохоронних органів відкриває нові можливості для розслідування злочинів і збору доказів. Зокрема, алгоритми ШІ здатні автоматично аналізувати біометричні дані (відбитки пальців, зображення обличчя, зразки голосу, ДНК тощо) для ідентифікації осіб, встановлення причетності до події та інше. Біометричні технології вже відіграють ключову роль у виявленні та розкритті злочинів, стаючи невід’ємною частиною кримінального процесу. Такі системи завдяки високій точності та швидкості здатні значно підвищити ефективність роботи слідчих підрозділів [1, с. 14].

Водночас активне використання ШІ у сфері кримінальної юстиції породжує серйозні правові виклики. Передусім постає питання забезпечення прав і свобод людини: обробка біометричної інформації стосується чутливих персональних даних, неналежний захист яких загрожує праву на приватність. Крім того, виникають сумніви щодо надійності і допустимості доказів, отриманих за допомогою автономних алгоритмів. Сторони кримінального провадження можуть поставити під сумнів результати, згенеровані ШІ, якщо методологія їх отримання є непрозорою або невідомою захисту. Застосування новітніх технологій випереджає законодавче регулювання, через що наразі відсутні чіткі правила, як інтегрувати такі цифрові докази у процес доказування [2, с. 14, 6, с. 15].

Актуальність проблеми особливо зросла в умовах воєнної агресії, коли постала потреба швидкого встановлення воєнних злочинців за цифровими слідами. Правоохоронці України вже вдаються до можливостей ШІ для ідентифікації осіб, наприклад, використовуючи технологію розпізнавання облич на кшталт системи Clearview AI для пошуку причетних до воєнних злочинів. Так, у 2022 році цю систему залучено для ідентифікації військових злочинців, що викликало обговорення правового статусу отриманих даних. Це свідчить про нагальну потребу вироблення підходів до легітимного використання біометричних доказів, здобутих із застосуванням ШІ [20, с. 17]. Загальна проблема полягає у тому, щоб визначити, за яких умов результати роботи алгоритмів ШІ можуть стати допустимими доказами у кримінальному провадженні України, і як при цьому мінімізувати ризики для прав людини та забезпечити дієвий судовий контроль.

Метою даного дослідження є комплексний аналіз правових питань, пов’язаних із використанням систем штучного інтелекту для обробки біометричних даних у кримінальному процесі

України, та вироблення пропозицій щодо забезпечення належної допустимості таких доказів і ефективного судового контролю. Для досягнення цієї мети основну увагу зосереджено на: визначенні поточного стану нормативного регулювання та наявних прогалин щодо використання біометричних даних, отриманих із застосуванням ШІ, у кримінальному судочинстві; виявленні потенційних ризиків і загроз правам людини, які виникають при впровадженні ШІ-технологій у процес доказування; обґрунтуванні критеріїв допустимості й достовірності цифрових (біометричних) доказів, згенерованих ШІ; а також формулюванні рекомендацій щодо вдосконалення законодавства та практики (включно з механізмами судового контролю) з метою збалансування інноваційних можливостей ШІ з вимогами справедливого правосуддя та захисту прав людини.

Аналіз останніх досліджень та публікацій: Питання впливу штучного інтелекту на сферу кримінальної юстиції останніми роками привертає значну увагу науковців як в Україні, так і за кордоном. З'явилися ґрунтовні роботи, присвячені загальним тенденціям і перспективам використання ШІ в кримінальному процесі. Зокрема, І. Басиста, Ж. Удовенко та М. Кулинич (2024) здійснили огляд сучасних трендів і можливостей ШІ при ухваленні процесуальних рішень, а Д. Белов і М. Белова (2023) проаналізували потенціал та ризики застосування ШІ у судовому провадженні та формуванні судових рішень [2, с. 14]. Окрему увагу приділено питанням використання ШІ у боротьбі зі злочинністю: так, К. Черевко та І. Луценко (2023) розглянули ШІ як інструмент протидії злочинності, а Т. Шевчук і Я. Свицун (2021) дослідили можливості ШІ у протидії злочинності на практиці [12, с. 16].

Аспекти правового регулювання і визначення статусу ШІ також відображені в науці. Наприклад, С. Корнєєва (2021) проаналізувала теоретичні підходи до правового визначення ШІ та необхідність відповідного нормативного врегулювання [8, с. 15]. Вітчизняні криміналісти звертаються до проблем доказування із використанням сучасних технологій: у працях С. Князева та М. Грібова (2021) порушено питання нормативного забезпечення застосування досягнень науки і техніки при розкритті злочинів [7, с. 15]. Дослідники М. Погорецький та ін. розглядають проблематику цифрових доказів і судового контролю: зокрема, наголошено на потребі нових процесуальних механізмів для гарантування справедливості у використанні даних, отриманих через цифрові технології (ШІ) [3, с. 14, 20, с. 17]. Такі аспекти, як використання даних із зашифрованих комунікацій (наприклад, мережі EncroChat) у доказуванні, а також документування воєнних злочинів з допомогою мультисенсорного аналізу даних, також стали предметом досліджень вітчизняних науковців (М. Погорецький, 2023–2025) [20, с. 17].

У світлі стрімкого розвитку подій 2022–2023 рр. з'явилися публікації, присвячені застосуванню ШІ у воєнний час та розслідуванні воєнних злочинів. Зокрема, праці Ж. Удовенко, В. Галагана, О. Гузія, І. Мартишко (2025) висвітлюють можливості використання ШІ для документування злочинів агресора та захисту персональних даних при цьому [14, с. 16, 16, с. 16, 17, с. 16]. І. Вергун (2025) акцентує увагу на цифрових слідах війни та ролі ШІ в їх аналізі [18, с. 17]. Водночас низка досліджень (В. Парасюк, О. Шумик, 2025; С. П'ятецька, А. Чукаєва, 2025; С. Тарасюк, 2025) на рівні тез конференцій окреслили загальні перспективи і виклики впровадження ШІ у судочинство, наголосивши на необхідності адаптації правових підходів [10, с. 15, 11, с. 15, 13, с. 16].

Зарубіжні вчені зосереджуються як на технічних аспектах (наприклад, проблемі пояснюваності рішень ШІ та подоланні ефекту «чорного ящика»), так і на питаннях достовірності й безпеки алгоритмів. Так, Н. Карліні та Х. Фарід (2020) продемонстрували вразливість детекторів так званих «глибоких підробок» (deepfakes) перед спеціальними атаками, що підкреслює ризик фальсифікації доказів на основі ШІ [4, с. 14]. Це доповнює дискусію про допустимість доказів: якщо алгоритми можуть бути обмануті, суд має враховувати можливість помилок. У європейському науковому просторі активно розвивається напрям пояснюваного ШІ (XAI), метою якого є забезпечення прозорості алгоритмів, особливо критично важливої у правовому застосуванні ШІ [6, с. 15].

Попри значний інтерес до тематики, слід відзначити, що в українській науці питання саме допустимості біометричних доказів, отриманих за допомогою ШІ, та процедур судового контролю за їх використанням розроблене ще недостатньо. Наявні роботи закладають теоретичне підґрунтя та окреслюють проблеми, але потребують подальшого розвитку конкретні пропозиції щодо змін у кримінальному процесуальному законодавстві і практиці. Отже, дана стаття покликана заповнити цю прогалину шляхом синтезу наявних напрацювань та формулювання цілісного підходу до вирішення означених питань.

Виклад основного матеріалу.

Використання ШІ для аналізу біометричних даних у кримінальних розслідуваннях. Сучасні правоохоронні органи все частіше застосовують алгоритми штучного інтелекту при роботі з біометрією. Існують автоматизовані системи дактилоскопічної ідентифікації (AFIS), що за допомогою ШІ швидко порівнюють відбитки пальців підозрюваних із базами даних [1, с. 14]. Активно розвиваються технології розпізнавання обличчя: камери відеоспостереження у поєднанні з нейромережами дозволяють у режимі реального часу виявляти розшукуваних осіб у натовпі або ідентифікувати людей на відеозаписах. Наприклад, в умовах воєнного стану такі інструменти застосовувалися для встановлення осіб мародерів чи військових злочинців за фото- та відеоматеріалами [16, с. 16, 18, с. 17, 20, с. 17]. Подібні рішення приймаються і щодо голосових даних: програмне забезпечення з елементами ШІ здатне зіставляти зразки голосу (аудіозаписи розмов) з еталонними записами, допомагаючи визначити особу мовця. Також з'являються спеціалізовані алгоритми для менш традиційних біометричних характеристик – наприклад, ідентифікація людини за манерою ходи на відео [19, с. 17]. У результаті ШІ дедалі більше інтегрується у криміналістику, сприяючи автоматизації рутинних процесів аналізу доказів та прискорюючи отримання результатів [5, с. 15].

Правові прогалини та проблема допустимості доказів, здобутих із допомогою ШІ. Нинішнє законодавство України не дає прямої відповіді, як поводитися з доказами, отриманими за участі штучного інтелекту. Кримінальний процесуальний кодекс визначає джерела доказів (показання, речові докази, документи, висновки експертів), але алгоритмічні висновки ШІ прямо не згадані. На практиці результати роботи ШІ можуть оформлятися як довідки чи звіти спеціалістів і долучатися до матеріалів справи як документи (ст. 99 КПК), або ж використовуватися експертами при підготовці висновку (ст. 101 КПК) [2, с. 14]. Проте відсутність спеціальних норм створює правову невизначеність. Відомо, що Закон України «Про захист персональних даних» 2010 р. жодним чином не згадує біометричні системи розпізнавання обличчя чи інші подібні технології. Не врегульовано також застосування ШІ у сфері негласних слідчих (розшукових) дій – профільний Закон «Про оперативно-розшукову діяльність» не містить положень про збирання інформації з використанням біометричних засобів [20, с. 17]. За таких умов зібрані із застосуванням ШІ докази потенційно піддаються оскарженню в суді як недопустимі через порушення порядку збирання або сумніви в достовірності.

Питання допустимості цифрових доказів нерозривно пов'язане з їхньою надійністю. Суд, вирішуючи питання про допустимість, повинен впевнитися, що метод отримання даних не суперечить закону і отриманий результат відповідає критеріям достовірності. У зарубіжній практиці вироблені підходи до оцінки наукових (у тому числі алгоритмічних) доказів – зокрема, в США застосовуються критерії **Фрая** та **Дауберта** для перевірки методології на загальновизнаність у науковій спільноті, рівень похибки тощо. В контексті ШІ-аналізу даних спостерігається різнобічний підхід: в одній зі справ американський суд визнав допустимими результати ДНК-експертизи, проведеної з використанням програми TrueAllele на основі ШІ (справа *People v. Wakefield*), оскільки технологія отримала загальне визнання. Натомість в іншій справі (*Matter of Weber*) суддя вимагав довести надійність конкретної ШІ-системи перед тим, як допустити згенеровані нею дані [2, с. 14]. Ще показовішим є приклад з розпізнаванням обличчя: суд Клівленда (штат Огайо) відхилив докази, отримані за допомогою Clearview AI, через ненадання стороні захисту повної інформації про використаний алгоритм та сумніви у його надійності [22, с. 18]. Більше того, згадано випадки неправомірних арештів, спричинених хибними спрацюваннями систем розпізнавання обличчя (зокрема, помилкова ідентифікація невинних осіб). Європейський Союз наразі приділяє цим ризикам особливу увагу: у проекті Акта ЄС про штучний інтелект запропоновано віднести системи біометричного розпізнавання у режимі реального часу до практик, що становлять високий ризик або навіть підлягають забороні у публічних місцях, за винятком вузьких обставин тяжких злочинів за рішенням суду. Таким чином, тенденція така, що без належних гарантій суди схильні не довіряти «чорним скринькам» ШІ і радше відхилять сумнівні докази, ніж допустять їх з порушенням прав учасників процесу [6, с. 15].

Ризики порушення прав та зловживань при використанні ШІ з біометричною метою. Використання штучного інтелекту для масового збору й аналізу біометричних даних містить суттєві ризики для прав людини. Найперше – це загроза права на приватність та захист персональних даних [2, с. 14]. Біометрична інформація належить до категорії чутливих персональних даних,

що підтверджується і міжнародними стандартами (GDPR прямо відносить біометричні дані до особливих категорій, які потребують підвищеного захисту). В умовах відсутності спеціального регулювання існує небезпека, що такі дані можуть збиратися та використовуватися без достатніх правових підстав і згоди суб'єктів [14, с. 16]. В Україні поки не прийнято окремого закону про біометричні дані, а чинні норми про захист персональних даних не враховують специфіку технологій розпізнавання обличчя чи інших ШІ-систем. Це створює ситуацію, за якої державні органи та приватні структури можуть впроваджувати системи біометричного моніторингу без прозорих процедур контролю. Як наслідок, громадяни не поінформовані належним чином про те, де і як їхні біометричні характеристики збираються і обробляються, що підриває довіру до правоохоронної діяльності [22, с. 18].

Інший спектр ризиків стосується точності та неупередженості алгоритмів. Відомо, що моделі ШІ можуть мати похибки та схильність до хибних спрацьовувань. Якщо алгоритм навчений на нерепрезентативних даних, можливі випадки, коли він менш точно розпізнає обличчя осіб певної статі чи етнічної групи, що призводить до дискримінаційних наслідків. Хоча подібні проблеми більш досліджені на заході, українські правоохоронці мають враховувати ці ризики при закупівлі і впровадженні готових рішень. Окрім того, існує ризик цілеспрямованих маніпуляцій: злочинці можуть використовувати технології для створення фальшивих біометричних доказів (наприклад, *deepfake*-відео з підробленим зображенням або голосом) з метою введення слідства в оману [4, с. 15]. Наукові дослідження вже зафіксували, що навіть сучасні детектори *deepfake*-контенту можуть бути обійдені спеціально створеними атаками. Якщо подібний фальсифікат потрапить до матеріалів справи, його виявлення потребуватиме складної експертизи, а ризик помилки зростає. Таким чином, неконтрольоване використання ШІ у зборі та аналізі доказів може потягнути системні зловживання – від масового стеження за населенням без достатніх підстав до судових помилок через надмірну довіру до автоматизованих висновків [6, с. 15].

Необхідність ефективного судового контролю і вдосконалення правового регулювання. З огляду на викладені виклики, ключову роль у забезпеченні законності та справедливості повинні відігравати суди. Судовий контроль покликаний стати запобіжником проти зловживань технологіями. По-перше, суд на стадії досудового розслідування має санкціонувати найбільш втручальні слідчі дії, пов'язані зі збором біометричних даних (наприклад, примусове отримання зразків ДНК, проведення експертиз з розпізнавання обличчя серед великого масиву записів тощо) [21, с. 17]. По-друге, на етапі судового розгляду судді повинні критично оцінювати представлені стороною обвинувачення докази, отримані із застосуванням ШІ: перевіряти, чи не порушено права людини при їх збиранні, та чи є достатні підстави довіряти висновкам алгоритму. При найменшому сумніві в достовірності таких доказів суд зобов'язаний визнати їх недопустимими. Примітно, що Верховний Суд України у своїй практиці вже висловив позицію щодо інформації, створеної ШІ: у постанові від 8 липня 2025 р. зазначено, що відповіді штучного інтелекту не можуть розцінюватися як джерело надійної, науково обґрунтованої інформації для суду. Цей підхід підтверджує необхідність обережного ставлення до новітніх технологій у судочинстві [2, с. 14, 20, с. 17].

В юридичній доктрині пропонуються конкретні механізми для посилення судового контролю і нормативного врегулювання. Зокрема, висловлено ідею закріпити в КПК порядок фіксації використання ШІ у ході слідства та суду, щоб кожен випадок застосування алгоритму був прозоро відображений у процесуальних документах. Пропонується покладати на ініціатора використання ШІ (слідчого, експерта) обов'язок довести належність і надійність отриманих результатів, а також визначити відповідальну за це технологію особу. Деякі автори наполягають на внесенні змін до статей 84, 99, 101 КПК з тим, щоб результати, здобуті із застосуванням ШІ, за умови їх належної верифікації та оцінки, прямо визнати новим видом (підвидами) доказів. Одночасно рекомендується оновити законодавство про захист персональних даних, імплементувавши положення GDPR щодо біометричної інформації та забезпечивши створення незалежного наглядового органу у сфері персональних даних, який би контролював правомірність використання технологій ШІ органами влади [14, с. 16]. Експерти також пропонують розробити етичні стандарти використання штучного інтелекту у правоохоронній діяльності та запровадити регулярні аудити алгоритмів на предмет упередженості і точності. Не менш важливою є вимога **пояснюваності**: якщо на підставі висновку ШІ ухвалюється процесуальне рішення, сторони повинні мати можливість перевірити логіку та вихідні дані алгоритму (не розкриваючи ноу-гау, але принаймні отримавши інформацію

про рівень похибки, використаний обсяг даних тощо). У цьому напрямі перспективним є розвиток концепції ХАІ – «пояснюваного ШІ», що дозволить інтегрувати принцип прозорості у дизайн алгоритмів.

Отже, поєднання належного нормативного регулювання і дієвого судового контролю здатне мінімізувати описані ризики. Законодавче уточнення статусу та порядку використання біометричних даних, отриманих ШІ, встановлення вимоги обов'язкової експертної перевірки таких доказів, впровадження незалежного контролю за діяльністю державних органів у цій сфері – усе це забезпечить більшу правову визначеність. Судовий контроль же слугуватиме гарантією від порушень: суди, як остання інстанція перевірки, зможуть відсіяти неналежно отримані або сумнівні з точки зору достовірності матеріали. В підсумку, кримінальна юстиція зможе скористатися перевагами штучного інтелекту у розкритті злочинів, не виходячи за рамки верховенства права та забезпечуючи захист основоположних прав громадян.

Висновки. Штучний інтелект у поєднанні з біометричними технологіями поступово стає дієвим інструментом кримінального судочинства, дозволяючи ефективніше розкривати злочини та ідентифікувати осіб. Водночас його застосування висуває нові вимоги до правової системи. Проведений аналіз показав, що в Україні наразі відсутні спеціальні норми, які б регулювали допустимість та порядок використання доказів, отриманих за допомогою ШІ-аналізу біометричних даних. Це створює ризики як для захисту прав учасників процесу (особливо права на приватність та на справедливий суд), так і для об'єктивності самого процесу доказування.

Передусім, слід на законодавчому рівні визначити процесуальний статус даних, згенерованих ШІ: чи можуть вони вважатися документами, висновками експертів або іншим видом доказів, та за яких умов. Важливо передбачити обов'язкові процедури перевірки достовірності таких доказів – наприклад, через призначення експертизи алгоритму чи вимогу надання інформації про показники точності. Паралельно потребує оновлення законодавство про захист персональних даних з урахуванням викликів цифрової доби, зокрема впровадження поняття біометричних даних та режиму їх обробки за стандартами ЄС.

Ключову гарантію має становити судовий контроль. Суди повинні залишатися фінальним бар'єром, що відсіює недопустимі або ненадійні докази, отримані з використанням ШІ. Вироблення судової практики, в якій високо цінуються принципи прозорості й перевірюваності алгоритмічних доказів, стимулюватиме і слідчі органи діяти більш відповідально. Судді, посилячись на кращі світові стандарти (приміром, критерії оцінки наукових доказів), можуть вимагати від сторони, що подає доказ, довести його достовірність та пояснити метод його отримання.

Отже, запорукою успішного і безпечного впровадження штучного інтелекту у кримінальний процес є вдосконалення правового регулювання в поєднанні з ефективним судовим наглядом. Лише за таких умов вдасться використати переваги інновацій – швидкість, масштабність аналізу даних – не жертвуючи фундаментальними засадами правосуддя. У перспективі подальших досліджень залишається моніторинг практики застосування ШІ в правоохоронній діяльності України та розробка детальніших рекомендацій щодо імплементації міжнародних стандартів у національне законодавство.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Басиста І.В., Удовенко Ж.В., Кулинич М.А. Огляд тенденцій щодо штучного інтелекту та його перспектив для процесуальних рішень під час кримінального провадження. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2024. Вип. 81(3). С. 19–38. DOI: <https://doi.org/10.24144/2307-3322.2024.81.3.3>.
2. Белов Д.М., Белова М.В. Штучний інтелект у судовому провадженні та судових рішеннях, потенціал та ризики. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2023. Вип. 78(2). С. 315–320. DOI: <https://doi.org/10.24144/2307-3322.2023.78.2.50>.
3. Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., & Toporetska Z. (2022). Detection and proof of cybercrime. *Amazonia Investiga*, 11(53), 259–269. <https://doi.org/10.34069/AI/2022.53.05.26>.
4. Carlini N., Farid H. Evading deepfake-image detectors with white- and black-box attacks. *IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Washington, USA, June 14–19, 2020. DOI: <https://doi.org/10.48550/arXiv.2004.00622>.

5. Черевко К.О., Луценко І.Г. Штучний інтелект як інструмент боротьби зі злочинністю. *Вісник Кримінологічної асоціації України*. 2023. № 1(28). С. 124–132. DOI: <https://doi.org/10.32631/vca.2023.1.10>.
6. Hassija V., Chamola V., Mahapatra A., Singal A., Goel D., Huang K. та ін. Інтерпретація моделей «чорного ящика»: огляд пояснюваного штучного інтелекту. *Cognitive Computation*. 2024. Т. 16. С. 45–74. DOI: <https://doi.org/10.1007/s12559-023-10179-8>.
7. Князев С.М., Грібов М.Л. Правове регулювання використання досягнень сучасної науки й техніки в розкритті злочинів. Використання досягнень сучасної науки й техніки в розкритті злочинів: матеріали міжвідом. наук.-практ. круглого столу (м. Київ, 21 лют. 2021 р.). Київ, 2021. С. 14–17. URL: <https://www.navs.edu.ua/files/kafedru/ord/2021/ks-250221.pdf>.
8. Корнеєва С.Р. Теоретичні підходи до визначення та правового регулювання штучного інтелекту. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2021. Вип. 66. С. 50–55. DOI <https://doi.org/10.24144/2307-3322.2021.66.9>.
9. Leenes R., Lucivero F. Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design. *Law, Innovation and Technology*. 2014. Vol. 6, No. 2. P. 194–222. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546759.
10. Парасюк В., Шумик О. Використання штучного інтелекту в позовному провадженні: перспективи та виклики. Фінансова політика: теоретичні та практичні аспекти юридичної науки: тези доп. VII Міжнар. наук.-практ. конф. (Ірпінь, 3 квіт. 2025 р.). Ірпінь, 2025. URL: https://dpu.edu.ua/images/2025/Photo_dlya_novyn_2025/Naukovi%20zahodi/06%20cerven%20Naukovi%20zahodi/Zbirnik%20tez%20Miznarodnoi%20konferencii%2003_04_2025.pdf.
11. П'ятецька С.О., Чукаєва А.В. (2025). Застосування штучного інтелекту у воєнний час: можливості та ризики. Тези доповіді круглого столу «Штучний інтелект у юридичній практиці: обмеження та можливості» (Львів, 14 березня 2025 р.).
12. Шевчук Т.А., Свицун Я.В. Використання штучного інтелекту у протидії злочинності. *Вісник Кримінологічної асоціації України*. 2021. № 2(25). С. 128–135. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/26d850e6-49ce-4cc6-bf59-a0f14b6b4d40/content>.
13. Тарасюк С.М. Використання штучного інтелекту в кримінальному судочинстві: практичні аспекти та перспективи. Штучний інтелект у юридичній практиці: обмеження та можливості: матеріали круглого столу (м. Львів, 14 берез. 2025 р.). Львів, 2025. С. 199–202. URL: https://if.uu.edu.ua/wp-content/uploads/2025/05/14_03_2025.pdf.
14. Удовенко Ж.В., Галаган В.І. Забезпечення захисту персональних даних, що обробляються системами штучного інтелекту: окремі аспекти. Штучний інтелект у юридичній практиці: обмеження та можливості: матеріали круглого столу (м. Львів, 14 берез. 2025 р.). Львів, 2025.
15. Басиста І.В., Удовенко Ж.В., Кулинич Марта-Марія А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. *Науковий вісник Ужгородського Національного Університету*. Серія: Право. 2024. Вип. 81. Том (частина) 3. С. 19–38. https://visnyk-juris-uzhnu.com/wpcontent/uploads/2024/03/81_part-3.pdf.
16. Удовенко Ж.В., Гузій О.В. Криміналістична характеристика розслідування воєнних злочинів, скоєних окупаційними силами в Україні: можливості та перспективи використання штучного інтелекту. *Національні інтереси України*. 2025. № 5(10). С. 788–797. DOI: [https://doi.org/10.52058/3041-1793-2025-5\(10\)-788-796](https://doi.org/10.52058/3041-1793-2025-5(10)-788-796).
17. Удовенко Ж.В., Мартишко І. Використання штучного інтелекту в судово-медичних експертизах в умовах збройного конфлікту. *Věda a Perspektivy*. 2025. Т. 2(45). С. 405–414. DOI: [https://doi.org/10.52058/2695-1592-2025-2\(45\)-405-413](https://doi.org/10.52058/2695-1592-2025-2(45)-405-413).
18. Вергун І. Цифрові сліди війни: роль штучного інтелекту у розслідуванні воєнних злочинів. Штучний інтелект у юридичній практиці: обмеження та можливості: матеріали круглого столу (м. Львів, 14 берез. 2025 р.). Львів, 2025. С. 54–57.
19. Хахановський В.Г., Чашницька Т.Г. Ідентифікація особи за ходом, зафіксованою в матеріалах відеозапису. *Криміналістичний вісник*. 2020. № 1(33). С. 72–79. DOI: <https://doi.org/10.37025/1992-4437/2020-33-1-72>.
20. Погорецький М.А., Меленті Є.О. Документування атак держави-агресора на об'єкти критичної інфраструктури України: методика інтелектуального аналізу мультисенсорних даних

- та використання його результатів у кримінальному процесуальному доказуванні. *Право і суспільство*. 2025. № 4(1). С. 251–274. DOI: <https://doi.org/10.32842/2078-3736/2025.4.1.36>.
21. Горбач І.Ю. Біометричні дані як інструмент розкриття злочинів: правові й технічні аспекти. Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів: тези доп. Всеукр. наук.-практ. конф. (м. Вінниця, 16 трав. 2025 р.). Харків: ХНУВС, 2025. С. 478–481. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/156bc7ee-1fdc-413c-a0a6-c8eec2f29b4d/content> (дата звернення: 15.12.2025).
22. Вища школа адвокатури НААУ. Докази, отримані за допомогою штучного інтелекту, та їх використання в суді. *Блог ВША НААУ*. 2025. 19 жовт. URL: <https://www.hsa.org.ua/blog/dokazi-otrimani-za-dopomogoiu-stucnogo-intelektu-ta-yix-vikoristannia-v-sudi> (дата звернення: 15.12.2025).