

УДК 343.1(477):004.8]«364»

DOI: <https://doi.org/10.32631/pb.2025.3.07>

ЖАННА ВОЛОДИМИРІВНА УДОВЕНКО,

*доктор юридичних наук, доцент,
Національний університет «Києво-Могилянська академія»,
кафедра кримінального та кримінального процесуального права;*

 <https://orcid.org/0000-0002-4100-0723>,
e-mail: zhanna.udovenko@ukma.edu.ua;

ВОЛОДИМИР ІВАНОВИЧ ГАЛАГАН,

*доктор юридичних наук, професор,
Національний університет «Києво-Могилянська академія»,
кафедра кримінального та кримінального процесуального права;*

 <https://orcid.org/0000-0001-8224-0099>,
e-mail: galaganvi@ukma.edu.ua;

ВІКТОРІЯ АНАТОЛІЇВНА ШКЕЛЕБЕЙ,

*кандидат юридичних наук, доцент,
Національний університет «Києво-Могилянська академія»,
кафедра кримінального та кримінального процесуального права;*

 <https://orcid.org/0000-0002-2717-097X>,
e-mail: v.shkelebey@ukma.edu.ua

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ

У статті досліджено можливості, ризики та нормативно-правові аспекти використання штучного інтелекту у кримінальному провадженні, з особливим акцентом на виклики, зумовлені умовами воєнного стану в Україні. З огляду на сучасні тенденції цифровізації та необхідність підвищення ефективності розслідувань проаналізовано приклади застосування штучного інтелекту у правоохоронній практичній діяльності, зокрема автоматизований аналіз великих обсягів даних, біометричну ідентифікацію, використання дронів для розвідки, прогнозу аналітики та інші технології.

Особливу увагу приділено досвіду використання систем штучного інтелекту для розслідування воєнних злочинів, зокрема ідентифікації російських військовослужбовців, виявлення колаборантів, пошуку зниклих осіб і викрадених дітей. Проаналізовано перспективи застосування алгоритмів глибокого навчання, інструментів доповненого пошуку, тематичних баз даних, а також можливості автоматизації рутинних слідчих (розшукових) дій.

Критично осмислено ризики, пов'язані з використанням штучного інтелекту: недостовірність і «галюцинації» алгоритмів, непрозорість моделей, ризики дискримінації, порушення приватності, проблеми верифікації цифрових доказів і технічну неспроможність наявних систем. Аргументовано необхідність запровадження нормативних гарантій якості, надійності та підзвітності результатів, отриманих за допомогою штучного інтелекту. Обґрунтовано потребу впровадження принципів прозорості, підзвітності, інформованості та нагляду за алгоритмічними інструментами у кримінальному процесі.

Запропоновано напрями вдосконалення кримінального процесуального законодавства, зокрема зміни до статей 91 та 101 Кримінального процесуального кодексу України, спрямовані на регламентацію та визнання результатів роботи штучного інтелекту процесуальними джерелами доказів за умови їх належної фіксації, верифікації й експертної оцінки. Зміни передбачають чітку фіксацію застосування штучного інтелекту у процесуальних документах, запровадження відповідальної особи за використання технологій, а також механізми перевірки й оцінювання отриманих результатів. Такий підхід забезпечить баланс між технологічним прогресом та захистом прав людини, підвищуючи якість розслідувань і довіру до судової системи. Зроблено висновок про доцільність розроблення комплексної нормативної моделі правового регулювання штучного інтелекту в Україні з урахуванням положень Закону ЄС про штучний інтелект (EU AI Act), потреб воєнного часу та стандартів захисту прав людини. Наголошено на необхідності гнучкого та функціонального підходу до правового регулювання штучного інтелекту, що зосереджується не на його дефініції, а на оцінці реальних наслідків і можливостей.

Ключові слова: штучний інтелект, досудове розслідування, воєнний стан, доказування, цифрові докази, захист персональних даних, технології в юриспруденції, ефективність.

Оригінальна стаття

ВСТУП. Держава Україна, хоча й перебуває у стані повномасштабної війни, дедалі активніше інтегрується у світову дискусію щодо ролі штучного інтелекту (далі – ШІ) у кримінальному провадженні. Це питання, яке досліджують науковці і практики, нині постає на перетині технологічного прогресу та фундаментальних правових засад і потребує глибокого, збалансовано-критичного аналізу та визначення чітких правил щодо можливостей його застосування.

Штучний інтелект у кримінальному провадженні – це не стільки технологічний виклик, скільки реалізація етичного, правового й управлінського аспектів. Сучасне кримінальне провадження, особливо в умовах повномасштабної війни, що триває в Україні, стикається з колосальним напливом цифрових даних. Воєнний стан суттєво перевантажує правоохоронну та судову системи, генеруючи значні обсяги інформації, пов'язаної з воєнними злочинами, кібератаками, колабораціонізмом та іншими кримінальними правопорушеннями. Можливості програмного забезпечення у сфері підтримання правопорядку надають значні переваги людському потенціалу щодо фіксації, попередження та завчасного реагування на правопорушення (Шевчук, Свистун, 2021, с. 128).

Відео з камер спостереження, дописи в соціальних мережах, супутникові знімки, дані мобільних операторів та перехоплені комунікації – все це є потенційними фактичними даними, обсяг яких неможливо опрацювати лише людськими силами. За таких обставин цінна інформація може так і залишитися невикористаною, не перетворившись на процесуальні докази. У цьому разі на допомогу приходить ШІ, здатний аналізувати гігантські масиви інформації та виявляти закономірності, недоступні для людського ока. В інтерв'ю журналу TIME тодішній Генеральний прокурор України Андрій Костін щодо використання ШІ зауважував, що створення цих технологічних інструментів означає не лише виявлення злочинців, а й недопущення втрати жодних доказів, які можуть бути використані для побудови розслідування¹.

Хоча в дискусіях про ШІ часто панують дві крайності – оптимізм щодо його потенціалу для розвитку або песимізм через ризик заміщення робочих місць, реальність є значно складнішою. На наш погляд, не слід боятися, що ШІ замінить людей. Навпаки, ті, хто навчиться ефективно його використовувати, матимуть перевагу на ринку праці над тими, хто цього своєчасно не зробить. Страх перед упровадженням передових технологій не повинен паралізувати прогрес у час, коли вони стрімко входять у повсякденне життя людини. Штучний інтелект слід сприймати як помічника, здатного виконувати рутинні завдання, залишаючи людині простір для зосередження на складніших аспектах роботи. Він зберігає «холодний розум» в умовах великих масивів даних та емоційного тиску, що особливо важливо у сферах, де ключовими є неупередженість і точність, зокрема у правосудді. Однак, як зазначає Уляна Шадська, застосування ШІ потребує не лише інтеграції технологій, а й переосмислення традиційних правових принципів, забезпечення прозорості, надійності та збереження провідної ролі людини у процесі ухвалення судових рішень². Водночас слід пам'ятати, що використання ШІ у правосудді не зводиться лише до кримінального провадження, адже його інструменти можуть бути застосовані й у інших видах судових процесів.

Насправді, у сучасному технологічному світі виникає фундаментальне питання використання ШІ у кримінальному провадженні: як уникнути стандартизації рішень алгоритмами та зберегти індивідуальний підхід до кожного розслідування і кожної кримінальної справи.

Наріжним каменем будь-якої технологічної трансформації має залишатися принцип: людське розуміння є важливішим за будь-який, навіть найточніший алгоритм. Це означає, що ШІ, попри всю свою потужність, має залишатися інструментом, а не заміною для критичного мислення, емпатії, морального судження та відповідальності, притаманних тільки людині. Важливо забезпечити право на

¹ Bergengruen V. How Ukraine is Pioneering New Ways to Prosecute War Crimes // Time : сайт. 06.11.2023. URL: <https://time.com/6331902/ukraine-war-crimes-prosecutor/> (дата звернення: 11.07.2025).

² Шадська У. Як штучний інтелект змінює судочинство? Нові можливості та ризики // Just Talk : сайт. 12.06.2025. URL: <https://justtalk.com.ua/post/yak-shtuchnij-intelekt-zminyue-sudochinstvo-novi-mozhливosti-ta-riziki> (дата звернення: 11.07.2025).

індивідуальність, аби технології не призводили до стандартизації чи нівелювання унікальних особливостей кожної особи. Майбутнє належить розумній людині, яка використовує технології не для зміни себе, а для посилення власних можливостей. Ці та інші важливі питання у контексті застосування ШІ у кримінальному провадженні свого часу докладно розглядали І. Басиста, Ж. Удовенко та М.-М. Кулинич (2024).

Проте поряд із людиноцентричністю, що ставить особистість у центр технологічного розвитку, не менш важливою є і державоцентричність. Це означає, що застосування ШІ у кримінальному провадженні має бути адаптованим до унікального правового контексту України, а не зводиться до копіювання іноземних моделей. Лише так можна гарантувати, що технології працюватимуть на благо українського суспільства. Для України, яка прагне модернізації, це означає розроблення та впровадження рішень із використанням ШІ, покликаних зміцнювати національну ідентичність і суверенітет. Важливо знайти баланс між використанням потенціалу ШІ для підвищення ефективності кримінального провадження та збереження основоположних засад, закріплених, зокрема, у ст. 7 Кримінального процесуального кодексу України (далі – КПК України). Це передбачає людиноцентричний підхід, системність і регулювання, що ґрунтується на чітких правилах: навчання та підвищення кваліфікації, прозорість (створення й упровадження систем ШІ, здатних пояснити власну логіку – наскільки це можливо – і забезпечити підзвітність розробників та користувачів), надійність і захист конфіденційних даних, оброблюваних ШІ, що є особливо актуальним в умовах воєнного стану. Унікальність сучасної ситуації полягає в тому, що ці засади набувають критичного значення в умовах воєнного стану та гібридних загроз. Використання ШІ у кримінальному провадженні потребує не просто технічної інтеграції, а й переосмислення його ролі як інструмента захисту національної безпеки та ідентичності. Це надає дискусії нової актуальності.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. Метою статті є комплексний аналіз можливостей, ризиків і перспектив застосування ШІ у кримінальному провадженні в умовах воєнного стану в Україні, а також обґрунтування доцільних напрямів правового регулювання з урахуванням європейських стандартів, технологічного прогресу та потреб національної безпеки України.

Для досягнення цієї мети були поставлені такі завдання:

- проаналізувати сучасні практики застосування ШІ у кримінальному провадженні в умовах воєнного стану в Україні;

- дослідити можливості ШІ щодо збору, обробки, аналізу та верифікації доказів;

- виявити ключові загрози, виклики й етичні дилеми, що виникають при використанні ШІ під час кримінального провадження;

- обґрунтувати необхідність створення механізмів перевірки, відповідальності та прозорості щодо використання алгоритмів ШІ в діяльності слідчих, дізнавачів, прокурорів та суддів;

- сформулювати пропозиції щодо внесення змін до кримінального процесуального законодавства України з метою легітимного і безпечного застосування технологій ШІ у кримінальному провадженні.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Методологічну основу дослідження становить системний підхід, що забезпечив комплексний аналіз проблеми використання ШІ у кримінальному провадженні в умовах воєнного стану. Завдяки цьому вдалося не лише виявити правові колізії та прогалини чинного законодавства України, а й сформулювати практично орієнтовані пропозиції щодо його вдосконалення з урахуванням як національного, так і міжнародного досвіду.

У процесі дослідження застосовувалися такі загальнонаукові та спеціально-юридичні методи:

- діалектичний метод – для розкриття взаємозв'язку між розвитком технологій ШІ та змінами у кримінальному процесі, а також для осмислення динаміки правового регулювання цієї сфери;

- аналіз і синтез – для глибокого вивчення окремих елементів досліджуваного явища (види використання ШІ, потенційні ризики, конкретні технології) та формування висновків щодо правових механізмів інтеграції ШІ у кримінальне провадження;

- формально-юридичний метод – для аналізу чинного законодавства України (зокрема норм КПК України) та міжнародних нормативно-правових актів, що регламентують застосування ШІ;

- порівняльно-правовий метод – для зіставлення підходів до регулювання ШІ у кримінальному провадженні в Україні та Європейському Союзі (зокрема аналіз положень Закону ЄС про штучний інтелект (EU AI Act) і Рамкової конвенції Ради Європи про штучний інтелект);

- метод емпіричного аналізу – для дослідження прикладів використання ШІ у правоохоронній діяльності під час воєнного стану в

Україні (зокрема використання програм розпізнавання обличчя, дронів, систем прогнозованої аналітики тощо).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Проблеми, що вивчаються у сфері використання ШІ, охоплюють значну кількість різних наукових напрямів. Водночас правозахисники лише нещодавно почали всебічно його аналізувати й висловлювати позиції щодо застосування ШІ у кримінальному провадженні. Зокрема, одним із таких досліджень, автори якого головною ідеєю вбачали аналіз готовності правничого середовища до застосування технологій ШІ, є «Перспективи та межі використання штучного інтелекту в кримінальному процесі». Реалізуючи цей проєкт, дослідники проводили інтерв'ю та опитування суддів, адвокатів і прокурорів, що забезпечило високу репрезентативність отриманих даних і формування реального бачення юридичної спільноти щодо перспектив та ризиків застосування технологій ШІ. Дослідження дало змогу дійти низки висновків, основним з яких є такий: «Наразі штучний інтелект – не суддя, не адвокат і не прокурор. Та він має всі шанси стати їхнім надійним помічником й інструментом у здійсненні правосуддя»¹.

Потужним сигналом та водночас зобов'язанням рухатися саме цим напрямом є підписання Україною у травні 2025 року Рамкової конвенції Ради Європи про штучний інтелект. Цей документ визначає принципи, яких держава має дотримуватися у формуванні законодавства та застосуванні продуктів ШІ в публічному секторі, зокрема це: повага до людської гідності, прозорість, недискримінація, захист приватності, надійність і безпека².

Нині правоохоронні органи використовують програмні комплекси, що дозволяють автоматично розпізнавати обличчя, порівнювати їх з інформацією, яка вже зберігається в базах даних. При цьому висока точність досягається завдяки застосуванню технологій використання індексу за біометричними параметрами обличчя. Подібні можливості стали реальністю в Україні (Черевко, Луценко, 2023, с. 128). Зокре-

ма, Київська міська рада встановила камери спостереження із вбудованою системою розпізнавання облич. Важливим чинником є те, що слідчі органи мають відкритий доступ до відповідних баз даних, що часто відіграє визначальну роль у попередженні, виявленні та подальшому розслідуванні кримінальних правопорушень, встановленні місцезнаходження осіб, оголошених у розшук. Аналогічна система під назвою «Прозоре місто» діє також у Житомирі (Князєв, Грібов, 2021, с. 15).

Аналіз відео- та фотоматеріалів за допомогою ШІ суттєво спрощує обробку значних обсягів інформації, зокрема ідентифікацію потерпілих, свідків та навіть самих злочинців. Важливо й те, що технології ШІ дозволяють швидко знаходити ключові моменти та об'єкти на відеозаписах (Вергун, 2025, с. 57).

В умовах неспровокованої воєнної агресії РФ проти України особливого значення набуває допомога ШІ у встановленні особи кожного російського військового, який учинив тяжкі чи особливо тяжкі злочини. Це сприяє оптимізації кримінального провадження та притягненню винних до відповідальності. Як повідомив виконавчий директор компанії ClearView AI Хоан Тон-Тхат, у їхньому розпорядженні є понад 2 млрд зображень із російської соціальної мережі «ВКонтакте», а загальна база даних налічує понад 10 млрд фотографій³.

Окрім ідентифікації злочинців під час воєнного стану ШІ може бути корисним і для пошуку безвісти зниклих та викрадених із тимчасово окупованих територій дітей. Зокрема, він здатний аналізувати вихідні дані (фотографії, персональну інформацію, особливості зовнішності), здійснювати пошук і визначати можливе місцезнаходження українських громадян у російських медіа, на особистих сторінках «ВКонтакте» та в інших відкритих чи частково закритих джерелах. Отриману інформацію правоохоронці можуть перевіряти і в разі підтвердження збігів уживати необхідних заходів. Також із допомогою ШІ можливо аналізувати переписку осіб, підозрюваних у співпраці з ворогом, та автоматизувати відстеження фінансових транзакцій із підозрілих джерел (П'ятецька, Чукаєва, 2025, с. 183).

Ще одним напрямом використання ШІ в умовах воєнного стану є застосування безпілотних літальних апаратів. За їхньою допомогою

¹ Перспективи та межі використання штучного інтелекту в кримінальному процесі // Відродження : сайт. URL: <https://www.irf.ua/wp-content/uploads/2024/02/ai.pdf> (дата звернення: 11.07.2025).

² Ковальова А. Україна приєдналася до Рамкової конвенції Ради Європи про штучний інтелект. Що це означає // АІН : сайт. 16.05.2025. URL: <https://ain.ua/2025/05/16/ramkova-konvenciya-radi-jevropi-pro-si/> (дата звернення: 11.07.2025).

³ Забадишина Ю. Як Україна використовує штучний інтелект для перемоги. У Мінцифри розповіли деталі // ДОУ : сайт. 05.12.2022. URL: <https://dou.ua/lenta/news/clearview-ai-in-ukraine/> (дата звернення: 11.07.2025).

можна виявляти та відстежувати рух ворожих сил, місця розташування злочинних угруповань або зони ймовірного вчинення воєнних злочинів. Оснащені камерами високої роздільної здатності та іншими сенсорами, дрони здатні документувати руйнування, фіксувати позиції артилерії, збирати відеодокази жорсткого поводження з населенням, що є критично важливим для подальших розслідувань. Вони також дають змогу проводити безпечні й детальні огляди місць масових руйнувань і поховань, фіксуючи докази злочинів навіть у важкодоступних районах (Вергун, 2025, с. 55).

Актуальним напрямом є використання ШІ для попередження кримінальних правопорушень. Починаючи з 2021 року Міністерство юстиції України офіційно застосовує програмне забезпечення з елементами ШІ – «Касандра», яке аналізує ймовірність повторного порушення закону злочинцем. У контексті воєнного стану наукова розвідка та прогнозування ризиків набувають нового критичного значення. Упровадження такого програмного забезпечення, як «Касандра», є надзвичайно корисним для ефективного розподілу ресурсів в умовах обмежених можливостей та тривалих розслідувань, для прогнозування поведінки осіб, схильних до рецидиву, що може бути пов'язано з новими видами кримінальних правопорушень, актуальними під час війни (мародерство, колабораціонізм). Це сприяє підвищенню рівня безпеки громадян і запобігає повторним злочинам, що особливо важливо в деокупованих і прифронтових регіонах. Отже, застосування подібних інструментів стає ключовим елементом зміцнення національної безпеки в умовах війни.

У своєму дослідженні «Штучний інтелект у виявленні злочинів: наскільки він корисний» Дж. Садульські визначає такі способи використання ШІ в боротьбі зі злочинами та їх запобіганні: проникнення до даркнету за допомогою ШІ та викриття широкого спектра незаконних послуг; виявлення тенденцій злочинності за допомогою глибокого навчання; ідентифікація жертв за допомогою машинного навчання; моніторинг онлайн-платформ злочинної діяльності; майнінг для даних та використання аналізу шаблонів для визначення місця вчинення злочину або зони з високим ризиком підозрілої діяльності; створення прогнозної аналітики для пом'якшення та попередження злочинності, зниження рівня злочинності та підвищення рівня громадської безпеки; встановлення осіб злочинців, а також телефонних номерів та IP-адрес, пов'язаних зі злочинною діяльністю; протидія тор-

гівлі дітьми, зокрема через аналіз інтернет-трафіку; моделювання злочинної поведінки та імітація дій і рішень злочинців¹.

Ці підходи набувають особливої актуальності в умовах війни, яку РФ веде проти України. Зокрема, ШІ є важливим для:

- застосування ШІ-агентів (*bots*), які автоматично сканують форуми і торговельні майданчики в даркнеті, ідентифікуючи закономірності в текстах, зображеннях та зашифрованих повідомленнях для виявлення незаконних пропозицій (продаж зброї, персональних даних, послуг хакерських атак);

- використання глибокого навчання (*deep learning*) для аналізу великих масивів даних (записи з камер спостереження, інформація із соціальних мереж), що дозволяє виявляти приховані закономірності;

- автоматичного порівняння фотографій зниклих безвісти осіб із зображеннями, знайденими в інтернеті;

- виявлення дезінформаційних кампаній, мереж російської пропаганди та моніторингу онлайн-платформ, що використовуються для координації злочинної діяльності.

Про незамінний інструмент для кримінальної юстиції як на етапі документування, так і під час розслідування та доказування пишуть Ж. Удовенко та О. Гузій (2025, с. 788). На переконання дослідниць, ШІ допомагає в автоматизованому виявленні сталих ознак обстановки вчинення злочинів (географічні особливості, часові закономірності), типових способів їх учинення (використання певних видів зброї, тактика дій окупантів), характерних рис особи злочинця (вікові категорії, військове звання, належність до певних підрозділів) та потерпілого (соціальний статус, стать, вік), а також особливостей слідової картини (види та локалізація матеріальних слідів, типові показання потерпілих і свідків). Використання ШІ дозволяє виявити приховані кореляції між цими елементами, що сприяє ефективнішій побудові слідчих версій і плануванню розслідування.

З огляду на важливість ідентифікації осіб, особливо в умовах воєнних дій, увагу привертає застосування ШІ в молекулярно-генетичних експертизах, зокрема під час ДНК-аналізу (Удовенко, Мартишко, 2025, с. 405). Сучасні алгоритми ШІ здатні опрацьовувати великі

¹ Sadulski J. Artificial Intelligence in Crime Detection: How It's Useful // American Military University : сайт. 06.12.2024. URL: <https://www.amu.apus.edu/area-of-study/information-technology/resources/artificial-intelligence-in-crime-detection/> (дата звернення: 11.07.2025).

обсяги даних із високою точністю, значно скорочуючи час, необхідний для встановлення ДНК-профілів. Штучний інтелект застосовується для автоматичного порівняння зразків ДНК із базами даних, виконуючи роботу, яка раніше потребувала значних людських ресурсів і часу. Це особливо важливо у воєнний час, коли швидке встановлення особи загиблих дає змогу оперативно надати інформацію їхнім родинам. Окрім аналізу ДНК, штучний інтелект використовується для аналізу папілярних узорів, що забезпечує додатковий рівень перевірки ідентифікації особи. Порівняння цих слідів допомагає виявляти збіги між зразками з місця події та наявною базою даних, зменшуючи ймовірність помилкової ідентифікації¹. Водночас змушені констатувати, що чинне законодавство України, зокрема КПК України та підзаконні нормативно-правові акти, що регулюють проведення судових експертиз, не містять положень, які б визначали порядок і правила використання ШІ експертами. Це питання було предметом нашого окремого дослідження (Удовенко, Мартишко, 2025).

На можливості ШІ вказує С. Тарасюк (2025, с. 199). Зокрема, на налаштування моделей під конкретні завдання (*fine-tuning*) – адаптацію системи ШІ до специфічного юридичного контексту, що значно підвищує точність аналізу процесуальних документів; на технологію доповненого пошуку (RAG) та дає змогу системі автоматично звертатися до бази правових документів (кодексів, постанов Верховного Суду тощо) для перевірки власних висновків; на спеціалізовані архітектури для обробки великих текстів – технічні рішення, які дозволяють системі аналізувати одночасно весь обсяг матеріалів справи, що критично важливо для виявлення суперечностей у доказах; на створення тематичних баз даних – упорядкування документів за категоріями (докази, процесуальні документи, свідчення); на паралельний аналіз – одночасна обробка різних частин справи з подальшим зіставленням результатів для первинного виявлення суперечностей, які надалі перевіряє людина.

Поза сумнівом, ШІ має низку сучасних можливостей та переваг, зокрема: 1) здатність аналізувати гігантські масиви цифрових доказів (відео, фото, перехоплення комунікацій, супутникові знімки) значно швидше за люди-

ну, встановлюючи закономірності та зв'язки, зокрема у справах про воєнні злочини; 2) сприяння виявленню кримінальних правопорушень, зокрема шляхом збирання та верифікації доказів воєнних злочинів, аналізу показань і визначення ймовірних місць їх учинення, що є критично важливим для міжнародного правосуддя.

З огляду на це ШІ може оптимізувати роботу слідчих, перебираючи на себе рутинні завдання (сортування документів, підготовка чернеток процесуальних документів, транскрипція аудіозаписів), однак за умови постійної вимоги фінального затвердження та перевірки людиною. Водночас, щоб гарантувати прозорість і підзвітність, необхідні чіткі законодавчі механізми. Чинний КПК України не містить положень, які б регулювали використання ШІ, що створює правову невизначеність. Тому для запобігання зловживанням і забезпечення належного судового контролю потрібно внести відповідні зміни до КПК України, зокрема шляхом доповнення ст. 91.

Погоджуючись із слушними зауваженнями В. Парасюка та О. Шумика (2025, с. 152) щодо проблем використання ШІ у правосудді, зокрема стосовно етичних і правових аспектів його застосування в судовому процесі, відсутності належного контролю за програмним забезпеченням, недостатньої прозорості алгоритмів, а також питань збереження конфіденційності та захисту персональних даних, слід наголосити, що кожен із цих викликів потребує детального аналізу. У цьому контексті доцільно виокремити, конкретизувати і доповнити їх найважливішими аспектами.

1. *Правові та етичні аспекти*, зокрема достовірність цифрових доказів та потреба у верифікації даних. В умовах війни зростає ризик маніпуляцій із даними, створення фейкових зображень і відео. Верифікація та забезпечення достовірності цифрових доказів, отриманих або проаналізованих за допомогою ШІ, стає надзвичайно складним завданням.

2. *Проблеми конфіденційності*. Автоматизовані системи, що обробляють великі обсяги даних, включаючи особисту інформацію учасників процесу, мають доступ до великої кількості чутливої інформації. Забезпечення належного рівня захисту таких даних є критично важливим для забезпечення прав людини і дотримання норм приватності. Погоджуємося, що кримінальні провадження, особливо під час війни, містять чутливу особисту інформацію, дані розвідки, свідчення потерпілих. Використання ШІ, особливо відкритих моделей, підвищує ризики витоків і несанкціонованого

¹ Перспективи та межі використання штучного інтелекту в кримінальному процесі // Відродження : сайт. URL: <https://www.irf.ua/wp-content/uploads/2024/02/ai.pdf> (дата звернення: 11.07.2025).

доступу до даних, що може мати катастрофічні наслідки. З огляду на це нами були запропоновані деякі ключові аспекти та заходи, які необхідно враховувати для забезпечення належного захисту персональних даних, які обробляються системами ШІ (Удовенко, Галаган, 2025а, с. 210).

3. *Освітній виклик і потреба в навчанні користувачів.* Підготовка майбутніх працівників поліції може позитивно вплинути на результати розслідувань, адже навчальний процес здатен відтворювати практичні ситуації, з якими постійно стикаються діючі правоохоронці, зокрема у воєнний час: затримання колаборантів, розбирання завалів, аналіз і вироблення алгоритму дій. Штучний інтелект може допомогти у відпрацюванні таких сценаріїв, забезпечуючи подальший аналіз, виявлення помилок, надання рекомендацій для вдосконалення навичок і навіть добір літератури для самостійного вивчення (П'ятецька, Чукаєва, 2025, с. 182). Для ефективного та безпечного використання ШІ потрібна відповідна підготовка не лише працівників правоохоронних органів, а й прокурорів і суддів. В умовах війни, коли кадровий ресурс обмежений і перевантажений, забезпечення належного рівня компетентності стає окремим викликом. Зокрема, 16 травня 2025 року для українських державних службовців стартував курс Ради Європи HELP «Штучний інтелект і права людини». Запуск курсу відбувся в межах конференції «Штучний інтелект у публічному управлінні: виклики, можливості, перспективи». У конференції взяли участь понад 100 державних службовців, науковців і дослідників, які обговорили виклики і можливості використання ШІ в публічному управлінні в Україні, розуміння ШІ та його можливого впливу на права людини¹.

4. *Відсутність єдиних стандартів для використання ШІ на досудовому розслідуванні.* Особливо актуальними залишаються питання, що потребують чітких і недвозначних відповідей: які моделі ШІ дозволено застосовувати, хто несе відповідальність за їхні помилки, як має фіксуватися сам процес аналізу тощо. Для їх вирішення необхідно розробити єдиний державний стандарт або відомчу інструкцію

для всіх правоохоронних органів щодо використання ШІ у кримінальному провадженні. Такий документ повинен чітко визначати перелік моделей ШІ, які дозволено використовувати (наприклад, тільки сертифіковані).

5. *«Галюцинації» ШІ.* Йдеться про здатність алгоритмів генерувати неправдиву інформацію, у тому числі вигадані правові норми чи факти. Наслідки таких помилок у кримінальному провадженні можуть бути фатальними – від несправедливих вироків до уникнення покарання за тяжкі злочини. Проблема «галюцинацій» ШІ становить значну процесуальну загрозу і може проявлятися у: створенні неіснуючих судових прецедентів або викривленні практики Верховного Суду (наприклад, при аналізі складних юридичних питань ШІ може посилаватися на вигадані постанови Великої Палати Верховного Суду); некоректному цитуванні законодавчих норм, коли система може змішувати чинні положення з тими, що втратили силу, внаслідок численних змін і доповнень; неправильній інтерпретації фактів справи, особливо при аналізі складних причинно-наслідкових зв'язків; хибному аналізі процесуальних документів, що може призвести до помилкових висновків про дотримання процесуальних строків або порядок проведення слідчих дій тощо (Тарасюк, 2025, с. 200).

6. *Непрозорість алгоритмів.* Із розвитком систем ШІ дедалі складніше зрозуміти їхнє внутрішнє функціонування – нерідко навіть самі розробники не можуть пояснити логіку прийнятих алгоритмами рішень. У результаті ми бачимо висновок, але не розуміємо логіку, що лежить в його основі. Ба більше, такі системи мають властивість самоорганізовуватися і фактично залишаються без зовнішнього контролю, попри його формальну наявність².

Коли ШІ використовується для підготовки ключових аналітичних висновків, відсутність прозорості унеможливорює належну перевірку отриманих результатів і ставить під загрозу право на справедливий судовий розгляд. Це особливо небезпечно у випадках, що стосуються кваліфікації та визначення міри відповідальності, а також під час оскарження доказів, коли неможливо простежити, яким саме чином алгоритм дійшов до конкретного висновку.

¹ Стартував курс Ради Європи HELP «Штучний інтелект і права людини» для державних службовців // Офіс Ради Європи в Україні : офіц. сайт. 21.05.2015. URL: <https://www.coe.int/uk/web/kyiv/-/council-of-europe-help-course-on-artificial-intelligence-and-human-rights-launched-for-public-servants> (дата звернення: 11.07.2025).

² Bughin J., Hazan E., Ramaswamy S., Chui M., Allas T., Dahlström P., Henke N., Trench M. Artificial intelligence: The next digital frontier? // Australian Policy Online : сайт. 13.12.2018. URL: <https://apo.org.au/node/210501> (дата звернення: 11.07.2025).

7. *Упередженість і дискримінація*. Навіть у мирний час ШІ може відтворювати і посилювати упередження, що містяться в даних, на яких він навчався. В умовах війни, коли суспільство поляризоване, ризик закріплення та автоматизації упередженої інформації або навіть дезінформації зростає експоненційно.

Інтеграція ШІ в діяльність правоохоронних органів України супроводжується низкою технічних обмежень, які можуть впливати на її ефективність, серед яких: а) якість і доступність даних – через різноманітність практик збору та зберігання виникають неповні чи упереджені набори даних, що знижує точність результатів. Крім цього, часто дані збираються без урахування вимог ШІ, що обмежує їхню корисність. Наприклад, поліцейські звіти можуть не охоплювати неповідомлені інциденти, і це впливає на навчання нейронних мереж. Стандартизовані протоколи збирання, очищення та збагачення даних, а також їх надійний захист критично важливі для забезпечення точності, етичності та відповідності законодавчим вимогам; б) проблеми інтеграції ШІ з наявними системами правоохоронних органів – спроба поєднати ШІ зі старими технологіями створює проблеми сумісності. Необхідна модернізація застарілих платформ і розроблення рішень з акцентом на модульну інтеграцію; в) масштабованість і адаптивність – інструменти ШІ мають працювати ефективно за різних обсягів даних і умов. Однак значні труднощі створюють «чорні скриньки» ШІ – алгоритми, внутрішня логіка яких непрозора та часто охороняється як комерційна таємниця (Hassija et al., 2024, p. 45). Це ускладнює судові процеси, оскільки немає чіткої відповіді, чому саме система ШІ зробила той чи інший висновок. Тому моделі ШІ повинні бути масштабованими й адаптивними, щоб не втрачати продуктивність і достовірність висновків навіть за наявності складних сценаріїв; г) обслуговування і технічна підтримка – постійне оновлення й технічне обслуговування є необхідними для забезпечення ефективності та безпеки систем ШІ. Проте це може бути проблемою для правоохоронних органів, які мають обмежені ресурси та доступ до ІТ-спеціалістів. Крім цього, існує можливість кібератак на системи ШІ, що може призвести до витоку даних або маніпуляції результатами. Атакована хакерами та пошкоджена система ШІ може використовуватися для створення дипфейк-відео або підробки доказів (Carlini, Farid, 2020, p. 2804).

Поява значної кількості загроз, ризиків і викликів для прав, свобод і законних інтересів людини, спричинених новими досягненнями у

сфері ШІ, підсилює необхідність створення ґрунтовної та якісної правової бази. Водночас постає питання: як саме право має реагувати на стрімкий розвиток ШІ. Конфлікт між прагненням законодавців чітко й жорстко врегулювати сферу ШІ на законодавчому рівні та бажанням стимулювати інноваційний розвиток держави через створення сприятливих умов для технологічних компаній певною мірою гальмує формування правового регулювання цієї сфери (Корнєєва, 2021, с. 50).

Р. Лінес і Ф. Люсіверо (2014, р. 194) пропонують таку градацію підходів до правового регулювання розроблення і застосування технологій ШІ:

- регулювання розроблення та виробництва ШІ шляхом ухвалення спеціального законодавства в цій сфері;

- регулювання поведінки користувача технології ШІ за допомогою застосування чинних законодавчих інструментів;

- регулювання поведінки самого ШІ через установлення нормами технічної регламентації і стандартизації певних стандартів архітектури системи.

Універсальної відповіді щодо використання ШІ у кримінальному провадженні наразі немає, тому доцільно розглянути кілька можливих сценаріїв подальшого розвитку цієї проблематики.

1. *Відмова від пошуку універсального визначення ШІ*. Відсутність єдиного та чіткого визначення робить цей підхід украй проблематичним. Натомість варто зосередитися на функціональності та потенційних наслідках, які несе ШІ у кримінальному провадженні. Регулювання має стосуватися не абстрактного поняття ШІ, а конкретних систем, наприклад програм розпізнавання обличчя чи програмного забезпечення для аналізу доказів. Це дозволить створювати більш гнучкі норми, адаптовані до нових технологічних розробок.

2. *Інтеграція норм, пов'язаних із ШІ, у чинні галузі права*. Можливим є створення спеціалізованих нормативно-правових актів відповідно до окремих галузей (цивільного, кримінального, адміністративного, господарського) або доповнення наявних кодексів новими нормами, що враховують особливості ШІ. У кримінальному та кримінальному процесуальному праві вже існують механізми доказування, визначені права й обов'язки учасників провадження та їхня відповідальність. Замість винаходження нових конструкцій можна розширити наявні механізми, інтегрувавши специфіку ШІ. Це зменшить опір суддів, прокурорів, слідчих і адвокатів, оскільки нові правила будуть

упроваджені в межах уже знайомих їм кодексів та законів.

3. *Запровадження відповідальної особи.* Необхідно закріпити поняття відповідальної особи, яка нестиме юридичну відповідальність за використання ШІ, навіть якщо система діє автономно. Такою особою має бути учасник кримінального провадження, який застосовує ці інструменти. Відповідальність повинна наставати не за дії ШІ як автономного суб'єкта, а за рішення людини, ухвалені на основі інформації, отриманої від нього.

4. *Розроблення абсолютно нової галузі права (Lex AI).* Прихильники цього підходу виходять із того, що старі норми не здатні врегулювати якісно нові суспільні відносини, які породжує ШІ, та що його вплив є надзвичайним. Водночас такий варіант несе ризики фрагментації правової системи, ускладнення взаємодії з іншими галузями та тривалого процесу становлення такої нової галузі права.

Схиляємося до необхідності враховувати специфіку практичної діяльності із застосування ШІ, аналізувати його наслідки та прогнозувати можливі трансформації. Це дає змогу сформувати гнучке регулювання, яке зосереджується не на абстрактних дефініціях, а на реальних викликах і можливостях, та встигає за стрімким розвитком технологій.

Розглядаючи питання правового регулювання ШІ у кримінальному провадженні, ми раніше пропонували часткову імплементацію Закону ЄС про штучний інтелект (EU AI Act) до законодавства України. На наш погляд, це забезпечить гнучку реакцію на швидкі зміни у сфері використання ШІ, а також дасть змогу поетапно впроваджувати його правове регулювання з урахуванням наявних ресурсів і можливостей (Удовенко, Галаган, 2025б, с. 245). У розвиток цієї позиції пропонуємо внести низку змін і доповнень до КПК України, спрямованих на гармонізацію національного законодавства з європейськими стандартами та забезпечення ефективного й етичного застосування ШІ у кримінальному провадженні, особливо в умовах воєнного стану. Це дозволить правоохоронним органам якісніше розслідувати кримінальні правопорушення. Адже незалежно від того, які алгоритми чи програми будуть розроблені та які відомості ШІ зможе змодельовувати у кримінальному провадженні, без надання їм офіційного статусу доказів або джерел доказів за КПК України вони залишатимуться лише непроцесуальною інформацією, непридатною для доказування.

Повністю підтримуємо позицію Д. Белова та М. Белової (2023, с. 315), які наводять пере-

конливі аргументи щодо того, що ШІ здатний автоматизувати процеси збирання, аналізу й оцінки доказів, підвищуючи ефективність та об'єктивність правосуддя. Зокрема, як зазначають науковці, ШІ може візуалізувати складні дані та докази, що допомагає суддям, адвокатам і прокурорам краще їх розуміти й аналізувати.

Фактичні дані, отримані з використанням ШІ, необхідно фіксувати у процесуальних документах для їх подальшого використання під час доказування. Як убачається зі змісту ч. 1 ст. 103 КПК України, фіксація дій під час кримінального провадження здійснюється за допомогою протоколу та носіїв інформації. При цьому саме на етапі досудового розслідування способами фіксації є протокол і технічні засоби фіксування процесуальних дій. На перший погляд може здатися, що застосування ШІ прямо ототожнюється із застосуванням технічних засобів (комп'ютерних мереж, спеціального програмного забезпечення тощо). Однак, на наше переконання, факт використання ШІ повинен фіксуватися саме у протоколі, до якого можуть бути додані додатки відповідно до ст. 105 КПК України. Такий спосіб оформлення процесуальних документів спрощує їх подальше використання: як під час доказування та відкриття матеріалів досудового розслідування, так і під час їх дослідження й оцінки всіма учасниками процесу – слідчим, прокурором, захисником, підозрюваним (обвинуваченим), потерпілим і судом на будь-якій стадії кримінального провадження.

З огляду на зазначене пропонуємо доповнити ст. 91 КПК України частиною 3 щодо використання ШІ, виклавши її в такий редакції:

«3. Усі процесуальні дії, спрямовані на збирання, перевірку чи оцінку доказів із використанням систем штучного інтелекту, повинні бути детально відображені у протоколі.

Протокол складається відповідно до частини 3 статті 104 цього Кодексу та додатково має містити:

повну назву системи штучного інтелекту, її версію та ідентифікаційні дані розробника;

детальний опис параметрів і налаштувань, з якими працював алгоритм під час провадження процесуальної дії;

чітке зазначення джерел вихідних даних, які були надані штучним інтелектом для аналізу;

інформацію про обсяг і характер оброблених даних».

Крім того, пропонуємо запровадити багаторівневий процес верифікації висновків ШІ як різновиду експертного висновку. Із цієї

метою доцільно доповнити ст. 101 КПК України новою частиною 11 такого змісту:

«11. Сторони кримінального провадження та суд мають право залучати незалежних технічних експертів для перевірки логіки роботи використаного алгоритму штучного інтелекту, його налаштувань, вхідних даних і відтворення отриманих результатів.

Експерти мають надавати висновки щодо надійності, прозорості та потенційних упереджень системи штучного інтелекту.

Жоден висновок, згенерований системою штучного інтелекту, не може бути використаний як джерело доказів без його ретельної перевірки та підпису уповноваженою особою, яка несе за нього повну відповідальність згідно з чинним законодавством».

ВИСНОВКИ. На наше переконання, під час оцінювання висновків ШІ необхідно здійснювати обов'язкову перевірку алгоритму на наявність потенційних упереджень (расових, гендерних, соціальних тощо), які можуть впливати на результати аналізу. Це складний, але вкрай важливий процес, що вимагає поєднання технічних, юридичних та організаційних заходів. Серед них: створення спеціальних тестових наборів даних, які охоплюють різні демографічні групи (за віком, статтю, расою тощо); забезпечення можливості для розробників пояснювати логіку роботи системи та прийнятих нею рішень; створення спеціалізованої комісії із сертифікації ШІ-систем для їхнього використання у кримінальному провадженні.

Суд, вирішуючи питання про допустимість доказів, отриманих або опрацьованих за допомогою ШІ, повинен оцінювати надійність і прозорість застосованих алгоритмів, їх верифіковані характеристики та методологію навчання. Окремо має враховуватися кваліфікація та досвід експерта, який здійснив перевірку і підтвердив висновки ШІ-системи. Важливо також, щоб стороні захисту була забезпечена реальна можливість ознайомитися з даними, використаними для аналізу, піддати сумніву результати роботи ШІ та вимагати залучення альтернативних експертів.

Докази, опрацьовані за допомогою ШІ, слід розглядати судом як один із різновидів експертного висновку, що підлягає оцінюванню нарівні з іншими доказами відповідно до внутрішнього переконання судді. Запропоновані нами зміни до КПК України дадуть змогу законодавчо закріпити, що технологічний прогрес має зміцнювати правосуддя, а не створювати нові прогалини в системі захисту прав людини.

Майбутнє ШІ у кримінальному провадженні під час воєнного стану залежить не від потужності алгоритмів, а від мудрості правил, які їх регулюють. Передові технології можуть стати інструментом посилення справедливості й ефективності у розслідуванні воєнних злочинів або, у разі невмілого застосування, – джерелом нових загроз для прав людини та довіри до правосуддя. Вибір за нами!

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Басиста І. В., Удовенко Ж. В., Кулинич М.-М. 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, ч. 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 в судочинстві та судових рішеннях, потенціал та ризики. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 78, ч. 2. С. 315–320. DOI: <https://doi.org/10.24144/2307-3322.2023.78.2.50>.
3. Вергун І. Цифрові сліди війни: роль штучного інтелекту у розслідуванні воєнних злочинів // Штучний інтелект у правовій практиці: межі та можливості : зб. тез круглого столу (м. Львів, 14 берез. 2025 р.) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2025. С. 55–58.
4. Князєв 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, 25 лют. 2021 р.) / МВС України ; Нац. поліція України ; Нац. акад. внутр. справ. Київ : НАВС, 2021. С. 14–17.
5. Корнєєва С. Р. Теоретичні підходи до визначення поняття 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>.
6. П'ятецька С. О., Чукаєва А. В. Застосування штучного інтелекту в умовах війни: можливості та ризики // Штучний інтелект у правовій практиці: межі та можливості : зб. тез круглого столу (м. Львів, 14 берез. 2025 р.) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2025. С. 182–185.
7. Парасюк В., Шумик О. Використання штучного інтелекту в позовному провадженні: перспективи та виклики // Фінансова політика: теоретичні та практичні аспекти юридичної науки : зб. тез VII Міжнар. наук.-практ. конф. (м. Ірпінь, 3 квіт. 2025 р.) / М-во фінансів України ; Держ. податковий ун-т ; Віденський ун-т економіки та бізнесу та ін. Ірпінь : Держ. податковий ун-т, 2025. С. 152–155.

8. Тарасюк С. М. Використання штучного інтелекту у кримінальному провадженні: практичні аспекти та перспективи // Штучний інтелект у правовій практиці: межі та можливості : зб. тез круглого столу (м. Львів, 14 берез. 2025 р.) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2025. С. 199–202.

9. Удовенко Ж. В., Галаган В. І. Забезпечення захисту персональних даних, які обробляються системами штучного інтелекту: окремі аспекти // Штучний інтелект у правовій практиці: межі та можливості : зб. тез круглого столу (м. Львів, 14 берез. 2025 р.) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2025а. С. 210–215.

10. Удовенко Ж. В., Галаган В. І. Правове регулювання штучного інтелекту у кримінальному провадженні // Юридична наука: проблеми та шляхи їх вирішення : зб. матеріалів І Міжнар. наук.-практ. конф. (м. Київ, 6 берез. 2025 р.) / Приватний вищий навчальний заклад «Європейський університет». Київ, 2025б. С. 245–251.

11. Удовенко Ж. В., Гузій О. В. Криміналістична характеристика розслідування воєнних злочинів, вчинених окупантами 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).

12. Удовенко Ж., Мартишко І. Використання штучного інтелекту у судових експертизах в умовах збройного конфлікту. *Věda a Perspektivy*. 2025. № 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).

13. Черевко К. О., Луценко І. Г. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. № 1 (28). С. 124–132. DOI: <https://doi.org/10.32631/vca.2023.1.10>.

14. Шевчук Т. А., Свистун Я. В. Використання штучного інтелекту у протидії злочинності. *Вісник Кримінологічної асоціації України*. 2021. № 2 (25). С. 128–135.

15. Carlini N., Farid H. Evading deepfake-image detectors with white- and black-box attacks // IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (Washington, 14–19 June 2020). Washington, 2020. Pp. 2804–2813. DOI: <https://doi.org/10.48550/arXiv.2004.00622>.

16. Hassija V., Chamola V., Mahapatra A., Singal A., Goel D., Huang K., Scardapane S., Spinelli I., Mahmud M., Hussain A. Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. *Cognitive Computation*. 2024. Vol. 16. Pp. 45–74. DOI: <https://doi.org/10.1007/s12559-023-10179-8>.

17. 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, Iss. 2. Pp. 194–222.

Надійшла до редакції: 16.07.2025

Прийнята до опублікування: 13.09.2025

REFERENCES

1. Basysta, I. V., Udovenko, Zh. V., & Kulynych, M.-M. A. (2024). Review of trends regarding artificial intelligence and its prospects for procedural decisions during criminal proceeding. *Uzhhorod National University Herald. Series: Law*, 81(3), 19–38. <https://doi.org/10.24144/2307-3322.2024.81.3.3>.

2. Byelov, D. M., & Bielova, M. V. (2023). Artificial intelligence in judicial proceedings and court decisions, potential and risks. *Uzhhorod National University Herald. Series: Law*, 78(2), 315–320. <https://doi.org/10.24144/2307-3322.2023.78.2.50>.

3. Carlini, N., & Farid, H. (2020, June 14–19). *Evading deepfake-image detectors with white- and black-box attacks* [Conference presentation abstract]. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, Washington, USA. <https://doi.org/10.48550/arXiv.2004.00622>.

4. Cherevko, K. O., & Lutsenko, I. H. (2023). Artificial Intelligence as a tool for combating crime. *Bulletin of Criminological Association of Ukraine*, 1(28), 124–132. <https://doi.org/10.32631/vca.2023.1.10>.

5. Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M., & Hussain, A. (2024). Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. *Cognitive Computation*, 16, 45–74. <https://doi.org/10.1007/s12559-023-10179-8>.

6. Kniazev, S. M., & Hribov, M. L. (2021, February 25). *Legal regulation of the use of achievements of modern science and technology in solving crimes* [Conference presentation abstract]. Interagency scientific and practical round table “Using the achievements of modern science and technology in solving crimes”, Kyiv, Ukraine.

7. Kornieieva, S. R. (2021). Theoretical approaches to the definition and legal regulation of artificial intelligence. *Uzhhorod National University Herald. Series: Law*, 66, 50–55. <https://doi.org/10.24144/2307-3322.2021.66.9>.

8. Leenes, R., & Lucivero, F. (2014). Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design. *Law, Innovation and Technology*, 6(2), 194–222.

9. Parasiuk, V., & Shumyk, O. (2025, April 3) *The use of artificial intelligence in litigation: prospects and challenges* [Conference presentation abstract]. VII International scientific and practical conference “Financial policy: theoretical and practical aspects of legal science”, Irpin, Ukraine.
10. Piatetska, S. O., & Chukaieva, A. V. (2025, March 14). *Application of artificial intelligence in wartime: opportunities and risks* [Conference presentation abstract]. Round table “Artificial intelligence in legal practice: limits and opportunities”, Lviv, Ukraine.
11. Shevchuk, T. A., & Svytsun Ya. V. (2021). Use of artificial intelligence in the crime combating. *Bulletin of Criminological Association of Ukraine*, 2(25), 128–135.
12. Tarasiuk, S. M. (2025, March 14). *The use of artificial intelligence in criminal proceedings: practical aspects and prospects* [Conference presentation abstract]. Round table “Artificial intelligence in legal practice: limits and opportunities”, Lviv, Ukraine.
13. Udovenko, Zh. V., & Halahan, V. I. (2025a, March 14). *Ensuring the protection of personal data processed by artificial intelligence systems: specific aspects* [Conference presentation abstract]. Round table “Artificial intelligence in legal practice: limits and opportunities”, Lviv, Ukraine.
14. Udovenko, Zh. V., & Halahan, V. I. (2025b, March 6). *Legal regulation of artificial intelligence in criminal proceedings* [Conference presentation abstract]. I International scientific and practical conference “Legal science: problems and solutions”, Kyiv, Ukraine.
15. Udovenko, Zh. V., & Huzii, O. V. (2025). Criminalistic characterisation of investigating war crimes committed by occupying forces in Ukraine: possibilities and prospects of using AI. *National Interests of Ukraine*, 5(10), 788–797. [https://doi.org/10.52058/3041-1793-2025-5\(10\)-788-796](https://doi.org/10.52058/3041-1793-2025-5(10)-788-796).
16. Udovenko, Zh., & Martyshko, I. (2025). Using artificial intelligence in forensic examinations in armed conflict. *Věda a Perspektivy*, 2(45), 405–414. [https://doi.org/10.52058/2695-1592-2025-2\(45\)-405-413](https://doi.org/10.52058/2695-1592-2025-2(45)-405-413).
17. Verhun, I. (2025, March 14). *Digital traces of war: the role of artificial intelligence in investigating war crimes* [Conference presentation abstract]. Round table “Artificial intelligence in legal practice: limits and opportunities”, Lviv, Ukraine.

Received the editorial office: 16 July 2025

Accepted for publication: 13 September 2025

ZHANNA VOLODYMYRIVNA UDOVENKO,

Doctor of Law, Associate Professor,
National University of Kyiv Mohyla Academy,
Department of Criminal and Criminal Procedure Law;
ORCID: <https://orcid.org/0000-0002-4100-0723>,
e-mail: zhanna.udovenko@ukma.edu.ua;

VOLODYMYR IVANOVYCH GALAGAN,

Doctor of Law, Professor,
National University of Kyiv Mohyla Academy,
Department of Criminal and Criminal Procedure Law;
ORCID: <https://orcid.org/0000-0001-8224-0099>,
e-mail: galaganvi@ukma.edu.ua;

VIKTORIA ANATOLIIVNA SHKELEBEI,

Candidate of Law, Associate Professor,
National University of Kyiv Mohyla Academy,
Department of Criminal and Criminal Procedure Law;
ORCID: <https://orcid.org/0000-0002-2717-097X>,
e-mail: v.shkelebey@ukma.edu.ua

THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS DURING MARTIAL LAW

This article examines the possibilities, risks, and regulatory aspects of using artificial intelligence in criminal proceedings, with a particular focus on the challenges posed by martial law in Ukraine. Given current trends in digitalisation and the need to improve the effectiveness of investigations, examples of the use of artificial intelligence in law enforcement practice are analysed, including automated analysis of large amounts of data, biometric identification, the use of drones for reconnaissance, predictive analytics and other technologies.

Particular attention is paid to the experience of using artificial intelligence systems to investigate war crimes, in particular the identification of Russian military personnel, the detection of collaborators, and the search for missing persons and abducted children. The prospects for the

application of deep learning algorithms, augmented search tools, thematic databases, and the possibility of automating routine investigative (search) activities are analysed.

The risks associated with the use of artificial intelligence are critically examined: the unreliability and “hallucinations” of algorithms, the opacity of models, the risks of discrimination, privacy violations, problems with the verification of digital evidence, and the technical inadequacy of existing systems. The need to introduce regulatory guarantees of quality, reliability and accountability of results obtained with the help of artificial intelligence is argued. The need to introduce the principles of transparency, accountability, awareness and oversight of algorithmic tools in criminal proceedings is justified.

Proposed directions for improving criminal procedural legislation, in particular amendments to Articles 91 and 101 of the Criminal Procedure Code of Ukraine, aimed at regulating and recognising the results of artificial intelligence as procedural sources of evidence, provided that they are properly recorded, verified and expertly assessed. The amendments provide for the clear recording of the use of artificial intelligence in procedural documents, the introduction of a person responsible for the use of technologies, as well as mechanisms for verifying and evaluating the results obtained. This approach will ensure a balance between technological progress and the protection of human rights, improving the quality of investigations and trust in the judicial system. It has been concluded that it is advisable to develop a comprehensive regulatory model for the legal regulation of artificial intelligence in Ukraine, taking into account the provisions of the EU AI Act, the needs of wartime and human rights standards. The need for a flexible and functional approach to the legal regulation of artificial intelligence is emphasised, focusing not on its definition but on the assessment of its real consequences and possibilities.

Keywords: *artificial intelligence, pre-trial investigation, martial law, evidence, digital evidence, personal data protection, technology in jurisprudence, effectiveness.*

Цитування (ДСТУ 8302:2015): Удовенко Ж. В., Галаган В. І., Шкелебей В. А. Використання штучного інтелекту у кримінальному провадженні під час дії воєнного стану. *Право і безпека*. 2025. № 3 (98). С. 78–90. DOI: <https://doi.org/10.32631/pb.2025.3.07>.

Citation (APA): Udovenko, Zh. V., Galagan, V. I., & Shkelebei, V. A. (2025). The Use of Artificial Intelligence in Criminal Proceedings During Martial Law. *Law and Safety*, 3(98), 78–90. <https://doi.org/10.32631/pb.2025.3.07>.