УДК 343.98
DOI: https://doi.org/10.24144/2307-3322.2026.94.3.40

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ У КРИМІНАЛІСТИЧНІЙ ПРАКТИЦІ: МОЖЛИВОСТІ КОМП'ЮТЕРНОГО ЗОРУ ТА РИЗИКИ ЗАСТОСУВАННЯ

Курман О.В.,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики,
Національний юридичний університет
імені Ярослава Мудрого
ORCID: 0000-0002-5432-7215

Курман О.В. Інтелектуальні технології у криміналістичній практиці: можливості комп'ютерного зору та ризики застосування.

У статті розглядається застосування технологій штучного інтелекту у криміналістичній практиці, зокрема у сфері відеоспостереження, ідентифікації об'єктів та аналізу цифрових доказів. Проаналізовано основні функції комп'ютерного зору, пов'язані з розпізнаванням облич, детекцію об'єктів, аналіз руху та сцен, а також оптичне визначення символів із подальшим використанням моделей глибокого навчання для підвищення точності криміналістичного прогнозування, аналітичного моделювання та комплексного оцінювання ризиків. Показано, що застосування штучного інтелекту дозволяє автоматизувати обробку великих обсягів даних, підвищити оперативність реагування правоохоронних органів, зменшити ймовірність пропуску важливих подій, ефективніше координувати дії різних служб у процесі розслідувань і забезпечити інтеграцію даних між підрозділами. Окремо висвітлено досвід використання систем відеоспостереження у рамках концепції «Безпечне місто», автоматичної фіксації адміністративних правопорушень на дорогах та застосування штучного інтелекту для контролю транспортних потоків і прогнозування потенційних ризиків для безпеки громадян. Водночас акцентовано на низці проблем і ризиків: законодавчій неврегульованості застосування штучного інтелекту у кримінальному провадженні, ризику помилок розпізнавання, що вже мали неодноразове місце на практиці, упереджених алгоритмічних рішень, порушення прав людини й конфіденційності даних, а також етичних викликах щодо прозорості ухвалення рішень та відповідальності. Наголошено на необхідності формування чітких етико-правових стандартів, удосконалення професійних компетенцій правоохоронців у сфері інтерпретації результатів штучного інтелекту та забезпечення балансу між ефективністю розслідувань, безпекою громадян і дотриманням прав людини. Стаття спрямована на комплексне дослідження сучасних тенденцій інтеграції цифрових технологій у криміналістику та визначення напрямів їх безпечного й законного впровадження у практику правоохоронних органів для підвищення ефективності запобігання, розкриття та розслідування злочинів.

Ключові слова: штучний інтелект, комп'ютерний зір, розкриття злочинів, криміналістична техніка, криміналістична профілактика, криміналістичне прогнозування.

Kurman O.V. Intelligent technologies in criminalistic practice: capabilities of computer vision and application risks.

The article examines the application of artificial intelligence (AI) technologies in forensic practice, particularly in the areas of video surveillance, object identification, and analysis of digital evidence. The main functions of computer vision are analyzed, including facial recognition, object detection, motion and scene analysis, as well as optical character recognition, with subsequent use of deep learning models to enhance the accuracy of forensic forecasting, analytical modeling, and comprehensive risk assessment. It is demonstrated that the use of AI enables the automation of large data processing, increases the operational responsiveness of law enforcement agencies, reduces the likelihood of missing important events, improves coordination among different services during investigations, and ensures data integration across departments. The experience of using video surveillance systems within the framework of the "Safe City" concept, automatic recording of administrative violations on roads, and the application of AI for traffic flow control and forecasting potential risks to public safety is highlighted. At the same time, attention is drawn to a number of problems and risks: the legal unregulated status of

AI application in criminal proceedings, the risk of recognition errors that have repeatedly occurred in practice, biased algorithmic decisions, violations of human rights and data privacy, as well as ethical challenges regarding transparency in decision-making and accountability. The necessity of establishing clear ethical and legal standards, improving law enforcement officers' professional competencies in interpreting AI-generated results, and ensuring a balance between investigative efficiency, public safety, and respect for human rights is emphasized. The article is aimed at a comprehensive study of current trends in the integration of digital technologies into forensic practice and the identification of directions for their safe and lawful implementation in law enforcement to enhance the effectiveness of crime prevention, detection, and investigation.

Key words: artificial intelligence, computer vision, crime detection, criminalistic techniques, criminalistic prevention, criminalistic forecasting.

Постановка проблеми. Цифрові технології міцно увійшли в життя кожної людини та проникли в усі сфери суспільства. Дослідження можливостей штучного інтелекту переважно здійснюється з погляду його технічної та цивільно-правової складових. Проте останніми роками технології штучного інтелекту активно впроваджуються і в правоохоронну діяльність, зокрема у практику запобігання, розкриття та розслідування злочинів, що є важливим кроком у напрямі підвищення її ефективності. Системи на основі штучного інтелекту активно застосовуються у криміналістичному прогнозуванні та профілактиці, будучи логічною складовою процесу цифровізації й алгоритмізації розслідування кримінальних правопорушень. Проте разом із позитивними моментами та тенденціями виникають і питання правового, технічного та етичного характеру, пов'язані з впровадженням штучного інтелекту в практику правоохоронних органів.

Мета дослідження – визначення переваг та проблем використання штучного інтелекту (комп'ютерного зору) у процесі виявлення та розслідування кримінальних правопорушень.

Стан опрацювання проблематики. Проблематиці використання штучного інтелекту в судовій та правоохоронній діяльності приділяється значна увага з боку криміналістів. Свої наукові праці цій тематиці присвятили такі дослідники, як Авдєєва Г.К., Великанова М.М., Шевчук В.М., Шепітько В.Ю., Латиш К.В., Негребецький В.В., Степанюк Р.Л., Перлін С.І. та інші. Водночас з огляду на стрімку динаміку розвитку штучного інтелекту, його активне впровадження у практику діяльності правоохоронних органів, а також пов'язані з цим виклики та проблеми, цей напрям наукових криміналістичних досліджень потребує постійного вивчення, оновлення та вдосконалення.

Виклад основного матеріалу. Одним із найефективніших напрямів використання штучного інтелекту у кримінальних розслідуваннях є ідентифікація об'єктів на відеозображеннях. Для цього використовується технологія комп'ютерного зору (Computer Vision).

Технологія комп'ютерного зору включає такі основні характеристики та можливості:

Аналіз зображень і відео. Технологія комп'ютерного зору може аналізувати фотографії та відео, визначаючи об'єкти, форми, рухи й інші візуальні елементи, що містяться в них.

Виявлення об'єктів. Системи дозволяють розпізнавати різні об'єкти (наприклад, людину, автомобіль, тварину тощо) на фотографіях або у відео та визначати їхнє місцезнаходження.

Розпізнавання облич. Сучасні системи комп'ютерного зору здатні відстежувати обличчя та ідентифікувати різних людей. Ця технологія широко використовується у сферах безпеки, криміналістичної ідентифікації та соціальних мереж.

Розуміння сцени. Штучний інтелект спрможний визначати загальний контекст зображення та аналізувати взаємозв'язки між об'єктами на ньому.

Оптичне розпізнавання символів. Автоматичне розпізнавання тексту із зображень або відсканованих документів і перетворення його на цифровий формат [1].

За допомогою таких систем можна автоматично розпізнавати обличчя, об'єкти або дії на відеозаписах. Комп'ютерний зір може використовуватися для: 1) аналізу відеоспостереження; 2) пошуку підозрюваних на основі зображень; 3) розпізнавання номерних знаків автомобілів; 4) виявлення певних об'єктів або ситуацій.

Однією з основних переваг штучного інтелекту в системах відеоспостереження є можливість обробки великих обсягів даних. Сучасні розслідування часто включають величезні масиви інформації, які складно аналізувати вручну. Штучний інтелект може значно прискорити цей процес. Алгоритми комп'ютерного зору здатні автоматично аналізувати дані з різних джерел і виявляти закономірності, які можуть бути непомітними для людини [2].

Одна людина вручну (або навіть група аналітиків) ніколи не зможе переглянути й проаналізувати велику кількість знімків або відеофрагментів, порівняти їх з оригіналами та зробити правильні висновки у найкоротші строки. Системи розпізнавання на основі комп'ютерного зору здатні виконувати це з високою точністю. Замість постійного спостереження за великою кількістю екранів співробітники отримують сповіщення лише у разі виявлення значущих подій. Це дає змогу підвищити оперативність реагування та зменшити ймовірність пропуску важливих інцидентів. Сучасні системи розпізнавання, що використовують машинне навчання, можуть аналізувати не лише зображення обличчя, а й одяг, структуру скелета, ходу та рухи тіла, тому такий аналіз активно застосовується у криміналістичній прогностичній діяльності.

Технології розпізнавання облич також активно використовуються для аналізу щільності потоків людей. Система може виявляти скупчення людей, падіння людини, тривале перебування об'єкта в забороненій зоні або залишений без нагляду багаж. Крім того, штучний інтелект дає змогу аналізувати поведінку людей. Система здатна виявляти нестандартні або підозрілі дії, наприклад бійку, агресивну поведінку чи спробу проникнення на закриту територію.

Однією з найважливіших функцій штучного інтелекту в системах відеоспостереження є виявлення (детекція) об'єктів. Система спроможна визначати присутність людини, автомобіля, тварини або інших об'єктів і виділяти їх на зображенні. Це дає змогу автоматично фіксувати появу певних об'єктів у заданій зоні та оперативно повідомляти операторів.

Технології інтелектуального відеоспостереження знайшли широке застосування у забезпеченні громадської безпеки в населених пунктах України. Концепція «Безпечне місто» передбачає використання мережі камер та інтелектуальних систем для моніторингу дорожнього руху, запобігання злочинам і підвищення ефективності роботи служб безпеки. Так, Г.К. Авдєєва та В.О. Коновалова зазначають, що ефективність системи штучного інтелекту стає очевидною під час виявлення порушень і забезпечення дотримання правил дорожнього руху, допомагаючи ідентифікувати транспортні засоби та осіб у несприятливих умовах (низька роздільна здатність фото- або відеокамери, темрява, снігопад, дощ тощо). Своєю чергою, прогнози зростання злочинності, створені спеціальними системами штучного інтелекту, дають змогу підвищити ефективність заходів її попередження [3, с. 37]. У транспортній сфері такі системи використовуються для контролю дорожнього руху, фіксації порушень правил дорожнього руху та керування транспортними потоками. Камери з використанням штучного інтелекту здатні автоматично визначати перевищення швидкості, проїзд на заборонений сигнал світлофора та інші порушення.

Сьогодні в Україні використовується система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі (з елементами штучного інтелекту) [4]. Фіксація цих правопорушень на дорогах здійснюється за допомогою комплексів автоматичної фіксації – спеціальних технічних засобів, здатних здійснювати фото- і відеозапис в автоматичному режимі, що дає змогу документувати та виявляти фактичні події, які містять ознаки адміністративних або кримінальних правопорушень у зазначеній сфері.

Встановлення стаціонарних технічних засобів здійснюється в аварійно небезпечних місцях та місцях концентрації дорожньо-транспортних пригод на автомобільних дорогах загального користування державного та місцевого значення, а також на вулицях і дорогах у містах та інших населених пунктах за погодженням із відповідним уповноваженим підрозділом Національна поліція України [5, с. 129].

Окремо слід зазначити, що під час війни розслідування воєнних злочинів пов'язане з цілою низкою викликів: безпекових, логістичних, тактичних, комунікаційних, геополітичних тощо, які впливають та обмежують можливість використання традиційних криміналістичних засобів і форм збирання доказів. [6, с. 370]. Сучасні підходи до розслідування воєнних злочинів дають змогу визначити джерела цифрової інформації, що зумовлюють напрями збирання й дослідження цифрових слідів для отримання необхідної інформації. Зокрема, така інформація може бути отримана з камер відеоспостереження комерційних та державних структур [7, с. 37] з наступним аналізом відеоряду за допомогою штучного інтелекту.

Попри значні переваги, використання штучного інтелекту в системах візуальної детекції пов'язане з низкою проблем і обмежень. В. О. Коновалова справедливо зазначає, що сучасний стан використання науково-технічних засобів у судочинстві України характеризується чітко обмеженим процесуальним режимом. Водночас науковий пошук у цьому напрямі тяжіє до розширення сфери застосування науково-технічних засобів у плані виявлення доказової інформації та оцінки

її достовірності. Названі проблеми потребують дослідження таких аспектів: 1) наукового стану рішень, що пропонуються у галузях створення пошукових і реєструвальних приладів; 2) доказової цінності інформації, отриманої внаслідок їх застосування, у плані введення її до системи доказів, прийнятої вітчизняною процесуальною наукою [8, с. 13].

Можна виокремити кілька проблем, що потребують всебічного наукового вивчення: 1) забезпечення законності використання штучного інтелекту та прозорості алгоритмів; 2) захист прав людини та основних свобод; 3) ризик помилок і упередженості алгоритмічних рішень. Розглянемо їх більш детально.

Законодавча неврегульованість використання таких систем у кримінальному судочинстві. Аналіз чинного законодавства України свідчить про відсутність належного нормативного врегулювання ключових аспектів застосування систем штучного інтелекту у сфері кримінального провадження. Аналогічна ситуація простежується й в інших галузях права, що обумовлює міждисциплінарний характер проблеми [9, с. 300].

Відсутність пояснень або доступу до механізму ухвалення рішень штучним інтелектом унеможливлює оскарження помилкових висновків, що порушує, зокрема, і принцип законності. Будь-яке рішення штучного інтелекту у кримінальних провадженнях повинно супроводжуватися поясненнями, зрозумілими не лише розробникам, а й суддям, адвокатам, обвинуваченим та громадськості. Крім того, правоохоронці повинні мати відповідні вміння та навички щодо інтерпретації результатів, згенерованих такими системами, щоб уникнути помилок або упереджених висновків під час прийняття рішень щодо застосування тих чи інших запобіжних заходів [10, с. 170]. У відповідності до Указу Президента України «Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки» визначено одним із пріоритетів розвитку і реформування правоохоронних органів широке застосування штучного інтелекту, блокчейну, хмарних обчислень для потреб досудового розслідування. Також планується запровадження в усіх правоохоронних органах уніфікованої системи особистої автентифікації та системи біометричного зіставлення із поступовим забезпеченням її сумісності з європейськими системами [11]. Першочерговим завданням постає формування чітких етико-правових рамок, що регламентуватимуть інтеграцію систем штучного інтелекту у діяльність правоохоронних структур. Фундаментом подібних стандартів мають слугувати принципи прозорості функціонування алгоритмів, недвозначної відповідальності за їх використання та надійного захисту персональних даних і приватного життя громадян [12, с. 214].

2. Ймовірність помилок розпізнавання. Система може неправильно ідентифікувати людину або об'єкт, особливо за поганого освітлення чи низької якості зображення. Так, наприклад, поліція Детройта у 2020 році використала зернисте фото з камери спостереження, щоб знайти грабіжника. Алгоритм видав «збіг» із Робертом Вільямсом. Його заарештували на очах у сім'ї, але згодом з'ясувалося, що він навіть не перебував у тому районі [13]. У 2023 році вагітну жінку Поршу Вудрафф звинуватили в угоні автомобіля на підставі старого фото в базі даних. Штучний інтелект зіставив її зі знімком восьмирічної давності, проігнорувавши той факт, що на момент злочину вона була на восьмому місяці вагітності [14].

3. Захист конфіденційності та персональних даних. Впровадження штучного інтелекту супроводжується серйозними викликами. Один із них є необхідність законодавчого регулювання, яке б забезпечувало баланс між ефективністю використання штучного інтелекту та захистом прав громадян, зокрема права на приватність. Особливого значення також набуває питання безпеки даних через ризики витоків конфіденційної інформації та можливі зловживання. Крім того, впровадження штучного інтелекту пов'язане з низкою етичних питань, зокрема щодо прозорості ухвалення рішень і відповідальності за їх наслідки [15, с. 56].

Виділяють цілу низку ризиків застосування штучного інтелекту, пов'язаних із порушенням приватності:

1. Ідентифікація. Одним із ключових ризиків є можливість встановлення особи. Системи штучного інтелекту, особливо технології розпізнавання облич, дають змогу визначати особу людини на основі біометричних даних. Це може призвести до масового спостереження та порушення права на анонімність у громадських місцях.

2. Розкриття інформації. Системи штучного інтелекту можуть виявляти приховані особисті характеристики, наприклад, вік, стан здоров'я або емоційний стан. Звідси існує ризик розкриття конфіденційної інформації без згоди людини.

3. Агрегація даних. Штучний інтелект здатний об'єднувати дані з різних джерел. Навіть якщо окремі дані не є конфіденційними, їх поєднання може дозволити створити детальний профіль особи, що значно підвищує ризики порушення приватності.

4. Фізіогноміка. Деякі алгоритми намагаються визначати особисті якості людини за зовнішністю – наприклад характер, інтелект або схильність до злочину. Подібні підходи викликають серйозні етичні проблеми й можуть призводити до дискримінації.

5. Розголошення. У процесі роботи систем штучного інтелекту можливе ненавмисне розкриття персональних даних. Наприклад, навчена модель може відтворювати фрагменти інформації з навчальних наборів даних.

6. Втручання у приватне життя. Для навчання алгоритмів потрібна велика кількість інформації про користувачів. Це може призводити до надмірного збирання даних, що порушує право на приватність.

7. Підвищена доступність даних. Цифрові бази даних роблять персональну інформацію більш доступною для різних організацій, що збільшує ймовірність її використання без згоди людини.

8. Небезпека даних. Зберігання великих масивів даних підвищує ризик кібератак і витоків інформації, особливо якщо системи захисту є застарілими і недостатньо ефективними.

9. Вторинне використання даних. Дані, зібрані для однієї мети, можуть використовуватися для інших завдань, про які користувач не був поінформований.

Виключення. Алгоритми можуть ухвалювати рішення, що призводять до виключення окремих груп людей із доступу до послуг або можливостей, наприклад через алгоритмічну дискримінацію [16].

Висновки. Використання технологій штучного інтелекту значно підвищує ефективність правоохоронної діяльності, даючи змогу швидше виявляти злочини, аналізувати великі обсяги даних і прогнозувати потенційні загрози. Водночас застосування таких систем супроводжується низкою проблем, серед яких правова неврегульованість, імовірність помилок розпізнавання та ризик порушення прав людини. Тому впровадження штучного інтелекту у сферу безпеки суспільства потребує чіткого законодавчого регулювання та дотримання балансу між забезпеченням громадської безпеки й захистом конфіденційності та персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. What is computer vision? Jet school. URL: https://jetschool.az/az/glossary/term/computer-vision (дата звернення: 12.03.2026).
2. AI and policing the benefits and challenges of artificial intelligence for law enforcement. An Observatory Report from the Europol Innovation Lab. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf (дата звернення: 12.03.2026).
3. Авдєєва Г.В., Коновалова В.О. Штучний інтелект у боротьбі зі злочинністю: напрями використання та проблеми законодавчого врегулювання. *Цифрова трансформація кримінального провадження в умовах воєнного стану*: матер. круглого столу, присвяч. Всеукр. тижню права (м. Харків, 23 груд. 2022 р.) С. 36-37. URL: https://dspace.nlu.edu.ua/items/e512275b-9c0b-4195-a254-5c2251e1f72e (дата звернення: 12.03.2026).
4. Запуск системи автоматичної фіксації порушень Правил дорожнього руху**.** URL: https://mvs.gov.ua/avtofotovideofiksaciia-porusen-pdr/zapusk-sistemi-avtomaticnoyi-fiksaciyi-porusen-pravil-doroznyogo-ruxu (дата звернення: 12.03.2026).
5. Черевко К.О., Луценко Г.О. Штучний інтелект як інструмент протидії злочинності. *Вісник кримінологічної асоціації України*. 2023. № 1 (28) С. 124-133. URL: https://vca.univd.edu.ua/index.php/vca/article/view/43/589 (дата звернення: 12.03.2026).
6. Дуфенюк О. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. № 4. С. 369-374. URL: https://doi.org/10.32782/2524-0374/2022-4/88 (дата звернення: 12.03.2026).
7. Матуєлене, С., Шевчук, В., Балтрунене, Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. *Теорія та практика судової експертизи і криміналістики*. 2022. Вип. 4 (29). С. 12-46. URL: https://khrife-journal.org/index.php/journal/issue/view/18/4-22 (дата звернення: 12.03.2026).
8. Коновалова В.О. Проблеми правомірності використання науково-технічних засобів у кримінальному судочинстві. Використання досягнень науки і техніки у боротьбі зі злочинні-

стю: матер. наук.-практ. конф. (м. Харків, 19 листоп. 1997 р.) / відп. ред. В.С. Зеленецький та Л.В. Дорош. Харків, Право, 1998. С. 12-15.
9. Курман О.В. Переваги та проблемні питання використання штучного інтелекту при дослідженні цифрових слідів. *Науковий вісник Ужгородського національного університету*. Серія Право. 2025. № 90. Том 4. С. 297-302. URL: https://doi.org/10.24144/2307-3322.2025.90.4.42 (дата звернення: 12.03.2026).
10. Журавель В.В. Принципи запобігання злочинності з використанням технологій штучного інтелекту. *Питання боротьби зі злочинністю*. 2024. Вип. 48. С. 167-174. URL: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=http://pbz.nlu.edu.ua/article/view/321770/312290&ved=2ahUKEwiUhsrD7JKTAxViT1UIHX5JHVMQFnoECBoQAQ&usg=AOvVaw1d2tSEDXgu2ZVkK7aSxXSe (дата звернення: 12.03.2026).
11. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 року: Указ Президента України № 273/2023 від 11 травня 2023 року. URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text (дата звернення: 12.03.2026).
12. Черваньова Д.А., Курман О.В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики. *Аналітично-порівняльне правознавство*. 2025. № 3. Ч.3. С. 211-215. URL: https://doi.org/10.24144/2788-6018.2025.03.3.31 (дата звернення: 12.03.2026).
13. Williams v. City of Detroit: Face Recognition False Arrest. *American Civil Liberties Union.* URL: https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest (дата звернення: 12.03.2026).
14. Hill K. Eight Months Pregnant and Arrested After a False Facial Recognition Match. *The New York Times*. 2023. 6 серпня. URL: https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html (дата звернення: 12.03.2026).
15. Гудзь Т.І., Синжерян А.А. Інтеграція технології штучного інтелекту у діяльність національної поліції України: перспективи та виклики. *Українська поліцеїстика: теорія, законодавство, практика*. 2024. (3). С. 53-59. URL: https://doi.org/10.32782/2709-9261-2024-3-11-9 (дата звернення: 12.03.2026).
16. Lee H.-P., Yang Y.-J., von Davier T.S., Forlizzi J., Das S. Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks. arXiv. 2023. URL: https://arxiv.org/abs/2310.07879 (дата звернення: 12.03.2026).

Дата першого надходження рукопису до видання: 14.03.2026
Дата прийняття до друку рукопису після рецензування: 23.04.2026
Дата публікації: 10.05.2026