

Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2024. № 4. С. 29–38.

7. Використання технологій штучного інтелекту у протидії злочинності та забезпеченні безпеки громад: монографія / за ред. проф. Ю. О. Лисенка. Харків : Інститут вивчення проблем злочинності, 2025. 210 с.

8. Малиновський О. В. Світові стандарти предиктивної правоохоронної діяльності: перспективи впровадження в Україні. *Наука і правоохоронна діяльність*. 2025. № 1 (67). С. 50–59.

Буренко Олег Володимирович,

викладач кафедри кримінології

та інформаційних технологій

Національної академії внутрішніх справ

ЗАРУБІЖНИЙ ДОСВІД ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ПЕРСПЕКТИВНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ У СУДОВО-ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

Стрімкий розвиток технологій четвертої промислової революції та цифровізація правосуддя зумовлюють необхідність модернізації судово-експертної сфери. Саме впровадження штучного інтелекту, машинного навчання, комп'ютерного зору, цифрової криміналістики та технологій аналізу великих даних істотно трансформує сучасну судово-експертну діяльність та дозволяє значно підвищити точність, об'єктивність та швидкість проведення експертних досліджень, мінімізуючи при цьому людський фактор.

Донедавна цифрові технології переважно використовувалися як допоміжний інструмент для дослідження електронних доказів, то сьогодні вони стають невід'ємною складовою процесу виявлення, аналізу, інтерпретації та оцінки доказової інформації. Особливо активно ці технології застосовуються під час дослідження матеріалів систем відеоспостереження, цифрових зображень, аудіозаписів, мобільних пристроїв, хмарних сервісів та інших джерел електронної інформації. Але не треба забувати, що впровадження штучного інтелекту має супроводжуватися системами управління ризиками, прозорістю та обов'язковою перевіркою отриманих результатів.

На сучасному етапі алгоритми штучного інтелекту вже широко використовуються для автоматизованого аналізу цифрових доказів. Найбільшого поширення вони набули у сфері відеоаналітики, біометричної ідентифікації, розпізнавання облич, аналізу мовлення, дослідження документів, цифрової криміналістики та виявлення підроблених мультимедійних матеріалів. Використання штучного інтелекту дозволяє значно скоротити час аналізу великих масивів даних та автоматизувати пошук необхідної інформації, при цьому підвищується ефективність роботи експертів, але в кінцевому рахунку це не замінює їх професійної оцінки.

В останні роки особливого значення штучний інтелект набув під час роботи з матеріалами с систем відеоспостереження. Сучасні алгоритми комп'ютерного зору дозволяють автоматично виявляти рухомі об'єкти, визначати траєкторії їх руху, класифікувати транспортні засоби, здійснювати трекінг людей, аналізувати поведінкові сценарії та виявляти аномальні події. Це надає можливість оперативно аналізувати тисячі годин відеозаписів, що майже неможливо опрацювати вручну. Але оскільки алгоритми можуть припускатися помилок та надавати різну точність залежно від умов зйомки, є необхідність перевірки результатів автоматичного аналізу експертом.

Одним із найпоширеніших та найбільш досліджених напрямів застосування AI є автоматичне розпізнавання облич. На сьогодні такі системи доволі широко застосовують правоохоронні органи США, Великої Британії, Франції, Німеччини, Нідерландів, Японії та інших держав з метою встановлення підозрюваних осіб, пошуку зниклих осіб, ідентифікації осіб використовуючи архівні записи та аналізу матеріалів камер відеоспостереження. Варто зауважити, що точність розпізнавання залежить від багатьох критеріїв, а саме якості відеозапису, освітлення, кута огляду, погодних умов, віку особи та інших факторів, тому результати роботи таких систем не можуть розглядатися як самодостатній доказ без додаткової експертної перевірки.

Сучасні системи відеоспостереження все частіше використовують алгоритми глибокого навчання, які дозволяють автоматично класифікувати об'єкти, виявляти підозрілу поведінку, здійснювати пошук за кольором та особливостями одягу, типом транспортного засобу або напрямком руху. Перевага при

застосуванні таких технологій полягає у можливості швидкого аналізу значних обсягів відеоданих, але остаточне тлумачення результатів має здійснюватися людиною-експертом.

Перспективним напрямом є використання технологій Super-Resolution. На сьогоднішній день технологія super-resolution продемонструвала великий потенціал у обробці інформації з систем відеоспостереження, а саме можливість покращувати деталізацію цифрових відеозаписів низької якості. За допомогою нейронних мереж здійснюється відновлення дрібних деталей, зменшення цифрового шуму, підвищення чіткості зображення та покращення видимості об'єктів. Водночас у судово-експертній практиці такі технології повинні застосовуватися вкрай обережно, оскільки вони створюють реконструйовані елементи зображення, а не відновлюють їх у буквальному розумінні. Це в свою чергу потребує належного документування методики обробки та оцінки її впливу на доказове значення матеріалу [1, с. 34].

США є одним із світових лідерів із впровадження штучного інтелекту у криміналістику. Значна частина досліджень проводиться під координацією Національного інституту стандартів і технологій США (NIST). Він здійснює незалежне тестування алгоритмів штучного інтелекту для правоохоронної діяльності (розробляє стандарти цифрової криміналістики та оцінює точність і швидкість алгоритмів розпізнавання облич від світових розробників). Особлива увага приділяється оцінці точності алгоритмів, їх відтворюваності, стійкості до помилок та можливості незалежної експертної перевірки.

Найвідомішим прикладом є програма **Face Recognition Vendor Test (FRVT)**, у межах якої NIST проводить незалежне тестування систем автоматичного розпізнавання облич. У 2023 році NIST перейменував основні напрямки тестування на FRTE (оцінка технології розпізнавання облич) та FATE (оцінка технології аналізу облич). Основні напрямки, за якими тестуються алгоритми сьогодні:

- FRTE (верифікація) – перевірка того, чи є дві фотографії однією людиною (наприклад, для розблокування смартфона);
- FRTE (ідентифікація) – пошук однієї людини в базі даних на мільйони зображень (використовується поліцією та прикордонниками);

– оцінка демографічних відмінностей – перевірка алгоритмів на предмет упередженості щодо віку, статі та раси;

– детекція морфінгу та підробок (PAD) – виявлення спроб обдурити систему за допомогою масок або модифікованих фото.

У тестуванні беруть участь десятки світових виробників програмного забезпечення. Отримані результати використовуються Федеральним бюро розслідувань (FBI), Міністерством внутрішньої безпеки США (DHS), прикордонною службою (CBP) та іншими правоохоронними органами для вибору найточніших алгоритмів. При цьому результати автоматичного розпізнавання не визнаються самостійним доказом і завжди підтверджуються експертним дослідженням [2].

У Великій Британії впровадження AI у судово-експертну діяльність здійснюється під контролем **Forensic Science Regulator**. Це державний орган в системі кримінального правосуддя Англії та Уельсу, який відповідає за встановлення та дотримання єдиних наукових стандартів. Діє незалежно від Міністерства внутрішніх справ від імені системи кримінального правосуддя в цілому Його головне завдання – гарантувати, що експертизи та докази, які використовуються в судах, є точними, надійними та відповідають найвищим професійним вимогам Основний принцип британської моделі полягає в тому, що будь-який алгоритм штучного інтелекту може використовуватися лише після наукової валідації, документування методики, оцінювання ризиків та підтвердження компетентності лабораторії відповідно до міжнародних стандартів.

Поліція Лондона та поліція Південного Уельсу використовують системи Live Facial Recognition (LFR). Це технологія відеоаналітики на базі штучного інтелекту, яка в режимі реального часу аналізує відеопотік із камер і зіставляє обличчя людей у кадрі зі спеціальними базами даних або «списками спостереження». На відміну від звичайного пошуку по фото (де завантажується знімок у базу і відшуковуються збіги у фотоархіві), Live-системи діють наживо. Вони самостійно виявляють обличчя серед натовпу, що рухається, незважаючи на сторонні об'єкти, і миттєво генерують тривожні сповіщення.

В урядовому «Плані дій щодо можливостей штучного інтелекту» опублікованого 13 січня 2025 року зазначено наступні сфери використання штучного інтелекту в поліції:

- обробка інформації, необхідної для виконання поліцейських обов'язків, для прикладу, у рамках розслідування – сортування та аналіз цифрових доказів, редагування текстових та аудіовізуальних файлів, узагальнення матеріалів справи, допомога у виконанні зобов'язань щодо розкриття інформації та виявлення дідфейків. Це може зробити розслідування швидшими та ретельнішими, дозволяючи офіцерам знаходити та обробляти ключову інформацію в розслідуванні за лічені хвилини, а не за дні;

- виявлення злочинної поведінки, розшукуваних підозрюваних або зниклих безвісти осіб – наприклад, за допомогою розпізнавання облич або автоматичного розпізнавання номерних знаків. Існує багато прикладів, коли використання штучного інтелекту для цієї мети призвело до арешту розшукуваних осіб, включаючи гвалтівників та сексуальних злочинців проти дітей, що зробило громади безпечнішими;

- покращення роботи диспетчерських пунктів поліції, наприклад, шляхом підтримки сортування нетермінових викликів 101, щоб ті, що не належать поліції, розглядалися відповідним органом, або шляхом розшифровки дзвінків, щоб поліція мала запис дзвінків і могла використовувати його для покращення своєї підготовки та реагування, але наразі мова не йде про використання поліцією штучного інтелекту для відповіді на екстрені виклики 999;

- підтримка у виконанні трудомістких завдань бек-офісу, таких як класифікація злочинів, ведення нотаток, оцифрування паперових файлів для розгляду нерозкритих справ, узагальнення документів, переклад документів, транскрибування свідчень свідків та заповнення форм. Це звільняє поліцейських та персонал для виконання обов'язків на передовій, включаючи патрулювання, розслідування та взаємодію з жертвами та свідками.

Водночас застосування таких систем повинно завжди супроводжуватися судовим контролем, оцінкою впливу на права людини та незалежним аудитом алгоритмів [3].

Німеччина є одним із лідерів у сфері судової мультимедійної експертизи. Значний внесок у розвиток технологій аналізу цифрових доказів здійснює **Fraunhofer Institute for Digital Media Technology (IDMT)**. Це відомий німецький науково-дослідний

інститут, що спеціалізується на розробці технологій для аудіовізуальних медіа, штучного інтелекту (ШІ) та аналізу даних. Інститут розробляє алгоритми штучного інтелекту для встановлення автентичності аудіо- та відеозаписів, виявлення монтажу, синтетичного мовлення та DeepFake.

Алгоритми штучного інтелекту застосовуються для:

- автоматичного встановлення ознак монтажу відео;
- аналізу цифрових артефактів;
- визначення джерела походження аудіозаписів;
- виявлення синтетичного мовлення;
- експертної перевірки DeepFake-матеріалів [4].

Китай є одним із світових лідерів за масштабами впровадження технологій комп'ютерного зору у сфері громадської безпеки. У багатьох містах функціонують інтегровані системи відеоспостереження, що використовують штучний інтелект для автоматичного розпізнавання облич, транспортних засобів та відстеження переміщення осіб. Місцеві органи влади додають камери з підтримкою ШІ, оновлені сервери та програмне забезпечення, яке може інтерпретувати сцени, позначати «ненормальну» поведінку, виявляти натовпи або несанкціоновані заходи, а також шукати відео за письмовими підказками замість ручного перегляду.

З самого початку система відеоспостереження спиралася на розпізнавання облич, сканування номерних знаків та стандартні системи комп'ютерного зору; проте вона була створена в першу чергу для ідентифікації конкретних осіб, працювала на застарілому обладнанні та передавала відео до централізованих центрів обробки даних. Оновлення усуне необхідність ручного аналізу записів і дозволить ширше впливати на людей, які не перебувають у так званих «списках спостереження». Ці технології застосовуються під час розслідування кримінальних правопорушень, пошуку зниклих осіб і розшуку підозрюваних. Китай модернізує найбільшу у світі мережу спостереження до чогось на кшталт автоматизованої поліцейської машини. Компанії, такі як Hikvision і Huawei, впроваджують комп'ютерний зір і великі мовні моделі у системи спостереження, а постачальники чипів допомагають переносити більше обробки безпосередньо у камери та локальні пристрої. В той же час міжнародні експерти звертають увагу на необхідність

дотримання стандартів захисту прав людини та конфіденційності при використанні таких систем [5].

Порівнюючи практики США, Великої Британії, Німеччини та Китаю можна виділити наступні спільні тенденції:

- штучний інтелект застосовується як інструмент підтримки експерта, а не як заміна судового експерта;
- перед практичним використанням алгоритми обов'язково проходять валідацію та незалежне тестування;
- результати штучного інтелекту підлягають обов'язковій перевірці людиною;
- судово-експертні лабораторії діють відповідно до міжнародних стандартів та спеціалізованих криміналістичних рекомендацій;
- особлива увага приділяється пояснюваності алгоритмів, аудиту, документуванню всіх етапів аналізу та забезпеченню можливості перевірки висновків у суді.

Список використаних джерел

1. Огляд підходів до програмної реалізації super-resolution. О. С Грубнік, І. М. Бушин – Інформаційні моделюючі технології, системи та комплекси (ІМТСК-2024) : V Міжнар. наук.-практ. конф. (Черкаси, 18–19 квітня 2024 р. Черкаси : Черкаський національний університет імені Богдана Хмельницького, 2024. 319 с.

2. Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Gaithersburg, MD : National Institute of Standards and Technology, 2019. (NIST Interagency/Internal Report 8280). DOI: 10.6028/NIST.IR.8280.

3. Home Office. Police use of artificial intelligence (AI): factsheet. London : Home Office, 2026. Опубліковано 9 June 2026. URL: <https://www.gov.uk/government/publications/police-use-of-artificial-intelligence-ai-factsheet>

4. Bartle A., Boss D., Boyarov A. G., Cuccovillo L., Grigoras C., Michałek M., Nyberg D. Best Practice Manual for Digital Audio Authenticity Analysis. ENFSI-FSA-BPM-002. Version 01. European Network of Forensic Science Institutes, 2022. URL: https://enfsi.eu/wp-content/uploads/2022/12/FSA-BPM-002_BPM-for-Digital-Audio-Authenticity-Analysis.pdf

5. Yan M., Mou L., Chen L. Digital Innovation and Legal Protection in China's Predictive Policing // Computer Law & Security Review. 2026. Vol. 60. Article 106273. DOI: 10.1016/j.clsr.2026.106273