

Список використаних джерел

1. Білецький В. О., Матняк В. М. Сучасні виклики та напрями розвитку оперативно-розшукової діяльності в Україні. *Наукові перспективи*. 2025. № 2(56). С. 1249–1257. DOI: [https://doi.org/10.52058/2708-7530-2025-2\(56\)-1249-1257](https://doi.org/10.52058/2708-7530-2025-2(56)-1249-1257).
2. Tyshchuk V. O papel da análise criminal na proteção das fronteiras estatais: aplicações na Ucrânia. *Revista Quaestio Iuris*. 2026. Vol. 18, No. 3. P. 61–88. DOI: <https://doi.org/10.12957/rqi.2025.87868>.
3. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України : навч. посіб. / О. С. Кіреєва, Ю. В. Крутік, О. М. Махлай, А. С. Треус. Хмельницький : Вид-во НАДПСУ, 2022. 360 с. URL: <https://dspace.nadpsu.edu.ua/handle/123456789/3241>.
4. Кіреєва О. С. Використання альтернативних аналітичних інструментів у кримінальному аналізі. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки* : наукове видання. Хмельницький : Вид-во НАДПСУ, 2016. ґ 4(70). С. 64–76. URL: http://nbuv.gov.ua/UJRN/znpnapv_vtn_2017_4_14/
5. Басалик С. А., Туз О. С., Тищук В. В. Генезис інструментів OSINT та окремі аспекти їх використання у правоохоронній діяльності. *Український політико-правовий дискурс*. 2025. № 9. DOI: <https://doi.org/10.5281/zenodo.15086041>.

Клименко Вячеслав Анатолійович,

заступник начальника управління –
начальник відділу аналітичної роботи
Управління кримінального аналізу
Головного управління Національної
поліції в Одеській області

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ: ПРАКТИЧНИЙ ДОСВІД І ПРОБЛЕМНІ ПИТАННЯ

Розвиток технологій штучного інтелекту (ШІ) відкриває принципово нові можливості для кримінального аналізу в діяльності правоохоронних органів. Зокрема, системи комп'ютерного зору та розпізнавання обличчя дозволяють суттєво скоротити час встановлення особи підозрюваного і підвищити точність ідентифікації навіть за матеріалами низької якості.

Водночас їх застосування породжує низку правових, організаційних та кадрових проблем, які потребують системного вирішення.

Кримінальний аналіз у системі Національної поліції України здійснюється на підставі статті 71 Кримінального процесуального кодексу України – як залучення спеціаліста, що володіє спеціальними знаннями та навичками. Нормативною основою організації аналітичної роботи є наказ МВС України від 07.07.2017 № 575. Методологічно діяльність аналітичних підрозділів орієнтована на модель Intelligence-Led Policing (ILP) – поліцейської діяльності, керованої аналітикою, відповідно до якої аналітична інформація є підставою для оперативних заходів, а не їх наслідком [2, с. 18].

Практична діяльність аналітичних підрозділів здійснюється на двох основних рівнях. Оперативний аналіз спрямований на підтримку конкретних розслідувань і оперативно-розшукових заходів: ідентифікацію осіб, встановлення зв'язків між злочинами, аналіз «по гарячих слідах». Тактичний аналіз охоплює виявлення злочинних схем і угруповань, аналіз короткострокових тенденцій злочинності на визначеній території, підготовку аналітичних продуктів для планування поліцейських заходів. Поєднання обох рівнів забезпечує комплексну аналітичну підтримку як поточних проваджень, так і стратегічних рішень керівництва [3, с. 28].

У практиці Управління кримінального аналізу (УКА) Головного управління Національної поліції (ГУНП) в Одеській області використовуються три основні ШІ-системи розпізнавання обличчя.

Clearview AI – американська система з базою понад 10 млрд фотозображень, у тому числі понад 2 млрд знімків з соціальної мережі «ВКонтакте». За даними Національного інституту стандартів і технологій США (NIST), точність системи становить 99,6 %. Принципова перевага – здатність ідентифікувати особу навіть за матеріалами низької якості (розмиті зображення, зйомка під кутом, недостатнє освітлення). З початку повномасштабного вторгнення Російської Федерації в Україну за допомогою Clearview AI ідентифіковано понад 10 000 осіб, причетних до злочинів [1].

BigData People Artelligence – система побудови розширеного профілю встановленої особи: номери телефонів, прив'язані облікові записи у соціальних мережах, список пов'язаних осіб, інтереси, а також відомості щодо зв'язків з Російською

Федерацією та ставлення до збройної агресії. Пошук здійснюється за фотографією, номером телефону або посиланням на акаунт.

Face-check – пошуковий модуль Інформаційного порталу Національної поліції України. База системи налічує близько 2 млн фотозображень з облікових баз «Особа», «Розшук», «Безвісти зниклі», «Блокпост», «Сепаратисти» та «Зареєстрована зброя». Перевагою є відсутність правових ризиків, пов'язаних із захистом персональних даних, оскільки система є суто відомчою.

Алгоритм роботи аналітика з зазначеними системами охоплює шість послідовних кроків: отримання оригіналу відеозапису або фотозображення; завантаження матеріалу до системи розпізнавання; отримання переліку найбільш схожих осіб; критичний аналіз результатів аналітиком із верифікацією постійних (форма черепа, розріз очей, форма носа та вух) і тимчасових (зачіска, маса тіла) ознак зовнішності; перехресна перевірка у відомчих і міжвідомчих базах даних (ПНП «Цунамі», НАІС, ДМС, «Гепард»); формування аналітичного продукту з обґрунтованим висновком.

Четвертий крок є ключовим: відсоток збігу, розрахований ІІІ-системою, є лише орієнтиром, а не підставою для висновку. З практики відомо, що показник 40–60 % може відповідати правильному результату, тоді як 90 % – виявитись помилковим. Остаточне рішення завжди залишається за аналітиком [4, с. 112].

Результатом роботи аналітика є аналітичний продукт – документ із обґрунтованим висновком та доказовою базою. Відповідно до вимог КПК України, такий продукт може бути використаний у кримінальному провадженні як висновок спеціаліста. Це означає, що помилкова ідентифікація, не верифікована аналітиком, здатна призвести до порушення прав людини, тому дотримання алгоритму є не лише методичною, а й правовою вимогою [5, с. 54].

Аналіз практики застосування зазначених технологій дозволяє виокремити чотири системні проблеми.

По-перше, правова неврегульованість. Нині в Україні відсутнє спеціальне законодавство, яке б регулювало застосування ІІІ-систем розпізнавання обличчя правоохоронними органами. Система Clearview AI вже була визнана такою, що порушує законодавство про захист персональних даних у низці країн Євросоюзу, зокрема у вересні 2024 року Управління захисту даних Нідерландів наклало на компанію штраф у розмірі 30,5 млн євро. В умовах євроінтеграційного курсу України відповідне правове

регулювання є необхідною передумовою подальшого використання подібних систем [7].

По-друге, відсутність API-доступу до державних реєстрів. Аналітики змушені опрацьовувати дані з ІПНІ, НАІС, ДМС та інших систем вручну, оскільки ці ресурси не інтегровані між собою. Значна частина робочого часу витрачається на механічне структурування даних замість безпосереднього аналізу.

По-третє, відставання системи підготовки аналітиків. Нові види злочинності – дипфейки, кіберфрод, злочини з використанням криптовалют, ШІ-генерований контент – з'являються значно швидше, ніж оновлюються навчальні програми закладів вищої освіти системи МВС.

По-четверте, відсутність обліку камер відеоспостереження приватного сектору. Магазины, підприємства, об'єднання співвласників багатоквартирних будинків (ОСББ) встановлюють камери, спрямовані на вулицю або проїжджу частину, без будь-якого погодження з правоохоронними органами. Внаслідок цього поліція не має єдиного реєстру таких камер, що суттєво ускладнює та уповільнює розслідування.

Варто зазначити, що країни Євросоюзу вже напрацювали певний досвід у сфері правового регулювання ШІ у правоохоронній діяльності. Зокрема, Europol у своїх методичних рекомендаціях наголошує на необхідності забезпечення прозорості алгоритмів, обов'язкового людського контролю над рішеннями ШІ та дотримання принципу мінімізації даних [6]. Акт ЄС про штучний інтелект (AI Act, 2024) відносить системи ідентифікації осіб у режимі реального часу до категорії «високого ризику», що вимагає обов'язкової сертифікації та реєстрації. Україна як кандидат на вступ до ЄС має враховувати ці вимоги при формуванні національного законодавства у відповідній сфері.

За результатами дослідження пропонується:

1. Розробити та затвердити Положення «Про застосування штучного інтелекту у правоохоронній діяльності», яке визначатиме допустимі системи, порядок їх використання та відповідальність за порушення, з урахуванням вимог Загального регламенту про захист даних (GDPR). Запровадити відомчий наказ МВС із регламентом роботи з системами розпізнавання обличчя та обов'язкову реєстрацію кожного запиту (номер провадження, мета запиту, посадова особа).

2. Надати підрозділам кримінального аналізу захищений REST API-доступ до ІПНП, НАІС, ДМС та інших профільних реєстрів; розробити єдину міжвідомчу інтеграційну шину даних Національної поліції України.

3. Запровадити практично орієнтовані курси з ШІ-інструментів у системі підготовки аналітиків у закладах вищої освіти МВС у партнерстві з регіональними підрозділами кримінального аналізу.

4. Прийняти нормативно-правовий акт, який зобов'язуватиме юридичних і фізичних осіб, що встановлюють камери відеоспостереження, спрямовані на вулицю або проїжджу частину, отримувати погодження від управління кримінального аналізу відповідного ГУНП та вносити відомості до єдиного реєстру камер із зазначенням адреси розміщення, кута огляду та контактних даних власника. Це надасть аналітикам можливість оперативно визначати, які камери покривають конкретну ділянку місцевості, і без зволікань отримувати відеоматеріали.

Отже, ефективне застосування технологій штучного інтелекту в кримінальному аналізі можливе лише за умови одночасного вирішення правових, технічних та кадрових проблем. ШІ є потужним інструментом підтримки аналітика, проте не замінює його: критичне мислення і фахова верифікація результатів залишаються необхідними складовими аналітичної діяльності.

Список використаних джерел

1. Clearview AI. Офіційний сайт. URL: <https://www.clearview.ai>
2. Основи кримінального аналізу : підручник / А. М. Бабенко та ін. ; за заг. ред. О. Є. Користіна. Київ, 2020. 296 с.
3. Заєць О. М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні: сучасний стан і перспективи розвитку. *Вісник кримінального судочинства*. 2016. № 4. С. 17–25.
4. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.
6. Zaiets O. M. The Institute for Analytical Support of Pre-trial Criminal Proceedings in Ukraine: current status and prospects of development. *European Reforms Bulletin*. 2017. № 1. P. 54–62.
7. Europol. Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement. Publications Office of the European Union, 2019. URL:

<https://www.europol.europa.eu/publications-events/publications/facial-recognition-technology>

8. Dutch Data Protection Authority fines Clearview AI. Autoriteit Persoonsgegevens. 03.09.2024. URL: <https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-fines-clearview-ai>

Козлюк Людмила Олексіївна,

т.в.о. начальника відділу кримінального
аналізу Головного управління
Національної поліції в Рівненській області

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ Й OSINT У КРИМІНАЛЬНОМУ АНАЛІЗІ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

Сучасний етап розвитку суспільства характеризується стрімкою цифровізацією всіх сфер життєдіяльності, що, поряд із позитивними змінами, сприяє трансформації злочинності та появі нових форм кримінальних загроз. Злочинці активно використовують інформаційно-комунікаційні технології, соціальні мережі, месенджери, криптовалютні платформи та інші цифрові сервіси для підготовки, вчинення й приховування кримінальних правопорушень. У таких умовах особливого значення набуває кримінальний аналіз як інструмент інформаційно-аналітичного забезпечення діяльності правоохоронних органів, спрямований на своєчасне виявлення кримінальних ризиків, встановлення взаємозв'язків між подіями та особами, а також підтримку процесу прийняття управлінських і процесуальних рішень [1, с. 45].

Одним із найбільш перспективних напрямів розвитку кримінального аналізу є використання технологій штучного інтелекту та методів розвідки на основі відкритих джерел інформації (Open Source Intelligence, OSINT). Застосування зазначених інструментів дозволяє значно підвищити ефективність збору, обробки та аналізу великих масивів даних, що є критично важливим в умовах постійного зростання обсягів інформації.

Відкриті джерела інформації вже давно стали важливим елементом інформаційно-аналітичної діяльності правоохоронних органів. Соціальні мережі, інтернет-форуми, медіаресурси,