specific tasks of face image processing and analysis using artificial intelligence based tools» [2].

Отже, застосування сучасних інструментів обробки зображень суттєво розширює аналітичні можливості правоохоронних органів. Як свідчить практика, відмова від використання ізольованих програм на користь комплексних багатокрокових алгоритмів із поєднання генеративного штучного інтелекту, математичної кореляції та класичних графічних редакторів дає змогу ефективно вирішувати найскладніші оперативні завдання: від ідентифікації осіб за пікселізованими кадрами до розшуку зниклих безвісти та деобфускації номерних знаків. Подальша алгоритмізація цих процесів є ключовою умовою підвищення результативності підрозділів кримінального аналізу.

Список використаних джерел:

1. Манжай О. В. Поліцейська діяльність у кіберсфері : підручник / О. В. Манжай ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2024. 188 с. URL: https://dspace.univd.edu.ua/handle/123456789/23140.

2. Sokurenko V., Rusyn B., Manzhai O., Nosov V., Luchyk S., Luchyk V. Solving specific tasks of face image processing and analysis using artificial intelligence based tools. *Proceedings of the International Workshop on Applied Intelligent Security Systems in Law Enforcement (AISSLE-2025)* (Vinnytsia, Ukraine, October 30–31, 2025). Vinnytsia : KNUIA, 2025. P. 186–203. URL: https://ceur-ws.org/Vol-4126/paper13.pdf.

ЦИФРОВІ ПЛАТФОРМИ КРИМІНАЛЬНОГО АНАЛІЗУ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Моргунова Тетяна Іванівна
к.т.н., доцент, доцент кафедри
кримінального аналізу та інформаційних технологій
Одеського державного університету внутрішніх справ

Сучасна система забезпечення правопорядку вже давно не виглядає такою простою, як її іноді намагаються описати в підручниках. Кримінальні загрози ніби розповзаються у різні боки, стають складнішими, переплітаються між країнами, і все це ще й

активно підживлюється цифровими технологіями. Іноді складається враження, що швидкість змін тут навіть вища, ніж у бізнес-середовищі, хоча це різні сфери. За таких умов звичні підходи до кримінального аналізу починають виглядати дещо застарілими, навіть якщо формально вони працюють.

Тому поступово виникає потреба переходити до більш гнучких і «розумних» інструментів, зокрема цифрових платформ, які здатні не просто накопичувати дані, а щось із ними робити в режимі, близькому до реального часу.

Якщо говорити про самі ці платформи, то їх складно звести до якогось одного визначення. Це швидше набір взаємопов'язаних рішень, які одночасно і збирають інформацію, і обробляють її, і намагаються показати аналітику певну картину подій. Причому мова не лише про факти, а й про зв'язки між людьми, повторювані моделі поведінки, інколи навіть такі речі, які не лежать на поверхні. У традиційних системах зазвичай все обмежувалося фіксацією інформації, тоді як тут з'являється елемент «домислення», якщо так можна сказати, хоча це, звісно, алгоритми, а не інтуїція. Втім, іноді результат виглядає дуже схоже.

Штучний інтелект у цьому контексті використовується доволі широко, хоча не завжди це помітно на перший погляд. Машинне навчання, наприклад, дозволяє виявляти певні закономірності, які людина могла б і пропустити, особливо коли даних багато. Обробка текстів теж відіграє роль, бо значна частина інформації існує у вигляді звітів, повідомлень, пояснень. Десь поруч і комп'ютерний зір, який аналізує відео з камер, хоча якість цих даних буває різною, і це теж проблема. Усе це разом поступово змінює саму логіку аналітичної роботи, скорочує час на прийняття рішень, але повністю виключити людський фактор все одно не виходить, та й навряд чи це потрібно.

Окремо варто згадати про різні джерела інформації, які ці платформи намагаються об'єднати. Дані з внутрішніх баз, відкриті джерела, відеоспостереження, інформація з мобільних пристроїв або фінансових операцій – усе це збирається в одному місці, хоча на практиці не завжди ідеально стикується. Іноді виникають труднощі з сумісністю форматів або з якістю даних, але загальна тенденція очевидна: формується певний єдиний інформаційний простір, у якому можна дивитися на ситуацію ширше, ніж раніше.

Хоча це теж не панацея, бо надлишок інформації іноді створює нові складнощі.

Структура таких платформ теж не є чимось абсолютно чітким і раз і назавжди заданим. Вона змінюється під потреби конкретних органів або навіть під окремі завдання. Зазвичай можна говорити про певні базові елементи, але їх межі досить умовні, і в реальній роботі вони часто перетинаються. Тому функціональні можливості таких систем краще розглядати не як жорстко визначений перелік, а як набір інструментів, який постійно доповнюється і трохи змінюється залежно від ситуації. І, мабуть, саме ця гнучкість і є однією з ключових їх характеристик, навіть якщо про це не завжди прямо говорять.

У цьому контексті доцільно підкреслити, що саме платформний підхід у поєднанні з інструментами штучного інтелекту формує якісно новий рівень кримінального аналізу. Йдеться не просто про автоматизацію окремих функцій, а про створення єдиного середовища, у якому дані, аналітичні алгоритми та управлінські рішення взаємодіють у межах узгодженої логіки. Штучний інтелект у таких системах виступає не допоміжним елементом, а центральним механізмом, що забезпечує адаптивність, здатність до самооновлення моделей і підвищення точності аналітичних висновків. Завдяки цьому цифрові платформи набувають ознак динамічних систем, які можуть не лише відображати поточний стан криміногенної ситуації, але й активно впливати на процеси прийняття рішень у правоохоронній діяльності.

Важливою перспективою розвитку є застосування ШІ для предиктивного аналізу злочинності та створення профілів потенційних злочинців. Алгоритмічні моделі ШІ активно використовуються для ідентифікації та відстеження серійних злочинців шляхом виявлення спільних рис у різних кримінальних епізодах, підвищуючи рівень громадської безпеки. Завдяки прогностичним можливостям ШІ правоохоронні структури отримують інструменти для формування обґрунтованих прогнозів щодо часових, територіальних та якісних характеристик злочинності, що дозволяє більш ефективно розподіляти патрульні сили, слідчі групи та інші ресурси [1].

Застосування штучного інтелекту в криміналістичній діяльності є перспективним напрямом, що відкриває нові можливості для підвищення ефективності розкриття злочинів, автоматизації

рутинних завдань, прогнозування злочинності та аналізу великих обсягів даних [2].

Звернемо увагу на ключові складові цифрових платформ кримінального аналізу, які визначають їх ефективність (табл. 1).

Якщо дивитися на ці всі компоненти не окремо, а разом, то поступово стає зрозуміло, що вся ця історія з цифровими платформами тримається не стільки на самих технологіях, скільки на тому, як вони між собою «домовляються».

Слід відзначити, що можна мати доволі потужні модулі, але якщо вони працюють уривчасто або дані заходять із помилками, то результат виходить, м'яко кажучи, не дуже. Іноді проблема навіть не в складності алгоритмів, а в банальній якості інформації на вході, яка тягне все вниз.

Таблиця 1

Ключові компоненти цифрових платформ кримінального аналізу на основі штучного інтелекту

Компонент платформи	Зміст та функціональне призначення
Модуль збору даних	Забезпечує інтеграцію даних із внутрішніх і зовнішніх джерел, включаючи бази даних, сенсори, соціальні мережі
Аналітичний модуль	Використовує алгоритми машинного навчання для виявлення закономірностей, кластеризації та прогнозування
Модуль обробки природної мови	Дозволяє аналізувати текстову інформацію (заяви, протоколи, повідомлення в мережі)
Візуалізаційний модуль	Забезпечує графічне представлення результатів аналізу (карти, графи зв'язків, дашборди)
Модуль прийняття рішень	Формує рекомендації для правоохоронних органів на основі аналітичних висновків
Система безпеки даних	Гарантує захист інформації, контроль доступу та відповідність нормативним вимогам

У підсумку прогнози виглядають переконливо лише формально, а рішення, які на них спираються, можуть не давати очікуваного ефекту.

Досить часто згадують машинне навчання, особливо коли мова заходить про прогнозування кримінальної активності. І воно справді дає цікаві результати, дозволяє побачити певні «гарячі точки», часові періоди, коли ризики зростають, або навіть виділити людей, які можуть бути дотичними до правопорушень. Але тут не все так однозначно. Є нюанси, про які інколи говорять неохоче: алгоритми можуть відтворювати старі перекоси, підсилювати їх, якщо дані були упередженими. Це вже виходить за межі техніки і заходить у площину етики, прав людини, і загалом довіри до таких систем. Без цього моменту вся «розумність» платформи виглядає трохи під питанням.

Ще один напрям, який останнім часом активно використовують, пов'язаний з аналізом соціальних мереж. Через ці інструменти намагаються розплутати структури груп, зрозуміти, хто з ким взаємодіє, хто відіграє ключову роль. Інколи це справді допомагає швидше вийти на організовані групи або побачити те, що раніше залишалося поза увагою. Хоча знову ж таки, не все так гладко: інформація з відкритих джерел буває суперечливою, і її інтерпретація може змінюватися залежно від контексту.

Разом із тим, впровадження таких платформ не обмежується лише технічними рішеннями. Тут одразу виникає цілий набір практичних моментів – фінанси, підготовка спеціалістів, питання безпеки даних. Іноді складається враження, що організаційна складова навіть складніша за технологічну. Додається ще й правове поле, яке не завжди встигає за розвитком технологій, особливо коли йдеться про штучний інтелект. Це створює певну невизначеність, яку доводиться якось обходити в реальній практиці.

В українських умовах усе це відчувається ще гостріше. Війна, кіберзагрози, нестабільність – ці фактори ніби підштовхують до швидшого впровадження нових рішень, але водночас ускладнюють сам процес. Іноді доводиться працювати з тим, що є, паралельно намагаючись модернізувати систему. Тут цифрові платформи могли б стати корисним інструментом, хоча їх ефективність напряму залежить від того, наскільки грамотно вони інтегровані у вже існуючі процеси.

Цікаво, що в інших країнах, особливо в Європі, подібні системи вже використовуються доволі активно. Там тестують різні підходи – від прогнозної аналітики до розпізнавання облич і аналізу поведінки. Це дозволяє економити ресурси, швидше реагувати, хоча й там не обходиться без дискусій щодо меж допустимого. Певною мірою ці приклади можна брати до уваги, але повністю копіювати їх, мабуть, не вийде.

Зрештою, все впирається в баланс. З одного боку – ефективність, швидкість, аналітика, яка дає нові можливості. З іншого – права людини, етичні обмеження, відповідальність за рішення, які приймаються на основі алгоритмів. Якщо цей баланс порушується, довіра до системи швидко зникає, навіть якщо вона технічно працює добре.

У підсумку можна сказати, що ці цифрові платформи виглядають перспективно, але їх розвиток не є прямолінійним. Це скоріше поступовий процес із великою кількістю нюансів, де технічні, організаційні та правові речі переплітаються між собою. І саме від того, як це все поєднається, залежить, чи дадуть вони реальний ефект, чи залишаться більше теоретичною перевагою.

Список використаних джерел:

1. Яровий К. Штучний інтелект як інструмент протидії злочинності. *Юридичний вісник. Повітряне і космічне право*. 2024. № 2. С. 68-76.

2. Черваньова Д.А., Курман О.В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики. *Аналітично-порівняльне правознавство*. 2025. Т. 3, № 3. С. 211-216. DOI: https://doi.org/10.24144/2788-6018.2025.03.3.31