

УДК 004.93+004.8+629.73]:[34+351.74](477)

DOI: <https://doi.org/10.32631/pb.2025.1.08>

МИКОЛА ВОЛОДИМИРОВИЧ МОРДВИНЦЕВ,

кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 4,
науково-дослідна лабораторія з проблем інформаційних
технологій та протидії злочинності у кіберпросторі;

 <https://orcid.org/0000-0002-7674-3164>,
e-mail: lukoly@ukr.net;

ДМИТРО ВАЛЕНТИНОВИЧ ПАШНЄВ,

кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 4,
науково-дослідна лабораторія з проблем інформаційних
технологій та протидії злочинності у кіберпросторі;

 <https://orcid.org/0000-0001-8693-3802>,
e-mail: dvpashnev@gmail.com;

ВОЛОДИМИР СЕРГІЙОВИЧ НАКОНЕЧНИЙ,

доктор технічних наук, професор,
Київський національний університет імені Тараса Шевченка,
кафедра кібербезпеки та захисту інформації;

 <https://orcid.org/0000-0002-0247-5400>,
e-mail: volodym.nakonechnyi@knu.ua

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІДЕОАНАЛІЗУ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З РОЗПІЗНАВАННЯ ОБЛИЧ У КРИМІНАЛЬНОМУ АНАЛІЗІ

Проаналізовано сучасні технології відеоаналізу та програмне забезпечення для розпізнавання облич, оцінено їхню ефективність у кримінальному аналізі, а також досліджено етичні та правові аспекти використання цих інновацій у правоохоронній діяльності. Наголошено на актуальності впровадження новітніх технологій відеоаналізу та програмного забезпечення для розпізнавання облич з метою забезпечення громадської безпеки та боротьби зі злочинністю в Україні.

Визначено ключові технічні характеристики технологій відеоаналізу та розпізнавання облич, розкрито їхню роль у зменшенні впливу людського фактора та прискоренні процесів ідентифікації підозрюваних. Проаналізовано зарубіжний досвід використання подібних технологій і способи їх інтеграції у правоохоронну діяльність України. Особливу увагу приділено правовим аспектам, зокрема захисту персональних даних, а також етичним викликам, таким як забезпечення прозорості, недискримінації та дотримання прав людини. Методологія дослідження базується на аналізі нормативно-правових документів, наукових джерел і практичного досвіду використання технологій відеоаналізу. Використано системний підхід для узагальнення даних і порівняльний метод для оцінювання різних програмних рішень. Досліджено та враховано специфіку застосування штучного інтелекту в різних країнах, що дало змогу узагальнити найкращі практики. Надано рекомендації щодо вдосконалення впровадження технологій відеоаналізу у практичну діяльність правоохоронних органів України. Запропоновано заходи для покращення технічного забезпечення, створення законодавчих механізмів та етичних стандартів використання даних. Зокрема, наголошено на важливості навчання співробітників, розроблення політики захисту персональних даних та впровадження прозорих процедур моніторингу ефективності технологій. Особливу увагу приділено рекомендаціям щодо забезпечення правової підтримки інтеграції новітніх технологій, зокрема стандартизації процедур і мінімізації ризиків зловживання владою або службовим становищем працівниками правоохоронних органів.

Отримані результати можуть сприяти вдосконаленню методів кримінального аналізу, підвищенню ефективності діяльності правоохоронних органів і зміцненню громадської

безпеки. Запропоновані підходи позитивно впливатимуть на зміцнення безпекової інфраструктури держави, що підвищить рівень суспільної довіри до правоохоронних органів та забезпечить стабільність і безпеку в країні.

Ключові слова: відеоаналіз, розпізнавання облич, кримінальний аналіз, правоохоронні органи, штучний інтелект, етика, безпека даних.

Оригінальна стаття

ВСТУП. Сучасні виклики у сфері забезпечення безпеки громадян, об'єктів критичної інфраструктури та військових об'єктів вимагають упровадження інноваційних підходів і технологій. Зростання загроз, зокрема терористичних актів, порушень громадського порядку та злочинності, зумовлює потребу в ефективних інструментах для виявлення і запобігання потенційним ризикам. Технології відеоаналізу та програмного забезпечення (далі – ПЗ) з розпізнавання облич для виявлення підозрюваних є однією з інновацій, що надає можливість підвищити ефективність роботи правоохоронних органів.

Попри широкий міжнародний досвід застосування технологій відеоаналізу у правоохоронній діяльності, їхня інтеграція в Національну поліцію України стикається з низкою викликів. Серед основних можна виокремити:

- недостатній рівень правового регулювання використання відеоаналітичних систем, що може створювати загрози для захисту персональних даних;
- відсутність уніфікованих стандартів і рекомендацій щодо впровадження технологій відеоаналізу в діяльність українських правоохоронних органів;
- потребу в удосконаленні технічного забезпечення для роботи з великими обсягами відеоінформації, що надходить із камер спостереження;
- недостатню увагу до етичних аспектів використання технологій, зокрема запобігання дискримінації та забезпечення прозорості.

Технологічний прогрес суттєво впливає на різні сфери суспільного життя, зокрема на функціонування правоохоронних органів. Використання технологій відеоаналізу та розпізнавання облич стало важливим інструментом у боротьбі зі злочинністю. Ці інновації дозволяють зменшити людський фактор у кримінальному аналізі, прискорити розкриття злочинів і підвищити точність ідентифікації підозрюваних. Постійно вдосконалюються способи ефективного застосування відеоспостереження для забезпечення публічної безпеки¹.

Працівники підрозділів поліції отримують великий масив даних про злочинну діяльність, який необхідно обробляти. Одним з інструментів для обробки зібраних даних є кримінальний аналіз. Кримінальний аналіз – це сукупність дій, спрямованих на ідентифікацію та встановлення зв'язків між інформацією, що стосується злочину, особами, пов'язаними з ним, та даними з різних джерел, а також подальше використання проаналізованих даних правоохоронними органами. Великі обсяги накопичених даних можуть створювати проблеми з їхньою обробкою та аналізом, що може спричинити затримки в роботі правоохоронних органів. З метою оптимізації цих процесів у правоохоронних органах України доцільно впровадити використання штучного інтелекту (далі – ШІ).

Чимало країн у роботі правоохоронних органів використовують ШІ для прискорення та покращення їхньої роботи. У розвинених країнах великі міста обладнуються камерами відеоспостереження з можливістю розпізнавати обличчя, транспортні засоби та їхні номерні знаки, що допомагає в контролі й дотриманні громадського порядку шляхом цілодобового моніторингу громадських місць. Використання правоохоронними органами ШІ для ідентифікації злочинців за обличчям сприяє їх швидкому виявленню та затриманню. У Сполучених Штатах Америки точиться дискусія щодо використання ШІ для ідентифікації підозрюваних та їхніх родичів за загальнодоступними базами даних, побудови їхнього зовнішнього вигляду за даними ДНК, що може допомогти в розслідуванні злочинів (Wienroth, 2020).

У судових органах України ШІ використовують для автоматизації певних етапів судових процесів (Белов, Белова, 2023).

У контексті використання ШІ в діяльності правоохоронних органів особливий акцент

¹ Спосіб підключення зовнішніх камер відеоспостереження при здійсненні екстреного телефонного виклику : пат. 149028 Україна: МПК

(2021.01): H04N1/32, G08G1/00. № u202101018 ; заявл. 01.03.2020; опубл. 13.10.2021, Бюл. № 41/2021. 5 с.; Спосіб підключення зовнішніх камер відеоспостереження під час здійсненні екстреного телефонного виклику : пат. 158407 Україна: МПК (2024.01): G08B25/00, H04N7/18. № u202401054 ; заявл. 27.02.2024 ; опубл. 05.02.2025, Бюл. № 6/2025. 6 с.

робиться на ефективному застосуванні розвідувальної аналітики. Вона забезпечує системний підхід до планування та управління поліцейськими операціями, ґрунтуючись на кримінальному аналізі. Завдяки отриманим аналітичним даним визначаються стратегічні й оперативні пріоритети у сфері попередження та протидії злочинності (Моца, 2022). Для втілення цієї концепції правоохоронними органами України необхідно мати потужні аналітичні можливості для обробки великого масиву даних. До аналітичних потужностей можна віднести як персонал, що складається з аналітиків, так і спеціалізоване ПЗ, що буде прискорювати аналіз великих обсягів даних. Варто зауважити, що, попри універсальність кримінальних аналітиків, їхня спеціалізація за окремими напрямками та завданнями є надзвичайно важливою. Деякі із цих завдань можуть бути схожими між собою, зокрема розпізнавання облич та інших об'єктів. Використання інструментів ШІ під час розслідування кримінальних злочинів стане у пригоді кримінальним аналітикам, оскільки значно зменшить похибки, спричинені людським фактором, допоможе оперативно збирати й обробляти інформацію. У результаті злочинців, які вчинили кримінальне правопорушення, буде розшукано значно швидше, і вони понесуть покарання.

Застосування технологій відеоаналізу та ПЗ для розпізнавання облич є одним із найефективніших рішень для правоохоронних органів. Важливими є не лише розроблення та інтеграція такого ПЗ в їхню роботу, а й упровадження рекомендацій щодо використання ШІ та відеоаналітичних технологій у кримінальному аналізі. Це сприятиме підвищенню об'єктивності розслідувань, заснованих на доказах, отриманих шляхом ідентифікації осіб за обличчям. Крім того, необхідно постійно вдосконалювати підходи до зберігання, обробки та використання персональних даних, а також адаптувати етичні стандарти застосування технологій відеоаналізу та розпізнавання облич.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. Метою цієї статті є аналіз сучасних технологій відеоаналізу та розпізнавання облич, оцінювання їхньої ефективності у кримінальному аналізі, а також обговорення етичних і правових аспектів їхнього використання. Окремий акцент зроблено на розробленні рекомендацій щодо подальшого впровадження цих технологій у практичну діяльність правоохоронних органів України.

Основними завданнями дослідження є:

1) визначення технічних особливостей технологій відеоаналізу та розпізнавання облич;

2) аналіз правових аспектів використання таких технологій у правоохоронній діяльності;

3) оцінювання етичних викликів, пов'язаних із впровадженням цих технологій;

4) розроблення рекомендацій щодо вдосконалення використання технологій відеоаналізу та розпізнавання облич у кримінальному аналізі.

ОГЛЯД ЛІТЕРАТУРИ. У сучасних наукових дослідженнях чимала увага приділяється аналізу технологій відеоаналізу та розпізнавання облич у правоохоронній діяльності. Зокрема, у роботі Д. М. Белова та М. В. Белової (2023) досліджується потенціал і ризики використання ШІ в судочинстві, а також висвітлюється вплив автоматизованих систем на ухвалення судових рішень.

В. В. Моца (2022) акцентує увагу на концептуальних засадах використання кримінального аналізу оперативними підрозділами правоохоронних органів України, що є важливим елементом для впровадження сучасних технологій відеоаналізу.

Зарубіжний досвід використання технологій ідентифікації обличчя висвітлено в роботах, присвячених розробленню таких програмних продуктів, як *Veritone Identify* (Baltimore, 2024), *Clearview AI* (Rezende, 2020) та *Corsight* (Sheera, 2024). Ці дослідження демонструють, як інтеграція ШІ дозволяє правоохоронним органам покращити розслідування злочинів, ідентифікацію підозрюваних та аналіз даних.

Водночас вітчизняні дослідники, зокрема К. Токарева і Н. Савліва (2021), зосереджуються на особливостях правового регулювання ШІ в Україні, наголошуючи на необхідності вдосконалення законодавства в цій сфері.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Методологічною основою дослідження є системний підхід, який дає змогу всебічно оцінити вплив технологій відеоаналізу на кримінальний аналіз і діяльність правоохоронних органів. Для досягнення поставленої мети застосовано метод аналізу нормативно-правових документів, що регламентують використання систем відеоаналітики та розпізнавання облич у правоохоронній діяльності.

Порівняльний метод став у пригоді під час вивчення міжнародного досвіду впровадження відеоаналітичних технологій, що дало змогу визначити найкращі практики й адаптувати їх до умов України. Для оцінювання ефективності застосування таких технологій проведено аналіз емпіричних даних, зокрема практичних кейсів із правоохоронної діяльності.

Метод експертного оцінювання було використано у процесі опрацювання поглядів

фахівців у галузі кримінального аналізу, кібербезпеки та права щодо переваг і викликів впровадження відеоаналітичних систем. Крім того, здійснено контент-аналіз наукових публікацій для узагальнення сучасних досліджень із тематики використання ШІ у сфері безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ

1. Використання технічних пристроїв і засобів відеофіксації в діяльності Національної поліції України

Працівники Національної поліції України, виконуючи свої обов'язки щодо забезпечення громадської безпеки, захисту прав і свобод громадян, а також запобігання правопорушенням, використовують сучасні технічні засоби, зокрема пристрої для фото- і відеофіксації (Жадан, Мордвинцев, Пашнєв, 2024). Таке обладнання відіграє важливу роль у превентивних заходах, оперативному реагуванні на інциденти та розслідуванні злочинів.

Відповідно до положень п. 9 ч. 1 ст. 31 Закону України «Про Національну поліцію» використання фото- та відеопристроїв є одним із превентивних заходів, які можуть застосовувати правоохоронці. Крім того, ст. 40 Закону передбачає право поліції встановлювати на односторонні, службових транспортних засобах, розміщувати по зовнішньому периметру доріг і будівель автоматичні камери спостереження для контролю громадського порядку та фіксації можливих правопорушень. Окрім цього, поліція може отримувати й аналізувати дані з відеотехніки, що належить третім особам, за умови дотримання законодавчих норм.

Регламентація використання засобів відео- та фотофіксації здійснюється не лише на рівні законодавства, а й відповідно до нормативних актів Міністерства внутрішніх справ України, внутрішніх розпорядчих документів Національної поліції та локальних положень, затверджених регіональними управліннями. Основна мета застосування цих засобів полягає у фіксації подій, пов'язаних із порушенням закону, забезпеченні охорони громадського порядку, збереженні майна та життів громадян, а також контролі дотримання норм дорожнього руху.

Використання зазначених технологій сприяє оперативному реагуванню на надзвичайні ситуації, а також допомагає в розслідуванні правопорушень, надаючи докази у вигляді фото- та відеоматеріалів. Водночас важливим залишається питання правового регулювання та дотримання норм щодо конфіденційності і захисту персональних даних громадян.

Системи централізованого управління нарядами патрульної служби «ЦУНАМІ»

Управління силами та ресурсами патрульної поліції здійснюється за допомогою системи централізованого управління нарядами патрульної служби «ЦУНАМІ». Ця система включає комплекс програмно-апаратних засобів і підготовлений персонал, що забезпечує координацію дій патрульних підрозділів (Коршенко та ін., 2020). Вона надає інформаційні, технічні й аналітичні ресурси для оперативного ухвалення управлінських рішень. Основним завданням «ЦУНАМІ» є реєстрація та збереження даних про події, а також контроль за ефективністю реагування на них.

Упровадження системи спрямоване на покращення організації роботи патрульної служби, що дозволяє швидше реагувати на повідомлення про правопорушення. Однією з важливих складових системи є відеоспостереження, яке функціонує у взаємозв'язку із системою колективного відображення інформації.

Система відеоспостереження та колективного відображення

Система відеоспостереження створена для оперативного контролю за громадськими місцями, вулицями, транспортними потоками, а також для збереження відеоматеріалів, які можуть бути використані в розслідуваннях. Інтеграція цієї системи з іншими інформаційними платформами дозволяє правоохоронцям швидко отримувати доступ до необхідних даних.

Система колективного відображення передбачає використання великоформатного екрану, встановленого в оперативних центрах Національної поліції України. На ньому можуть відображатися відеозаписи з камер спостереження, інформація з комп'ютерних систем, а також записи з різних цифрових носіїв. Такий підхід дозволяє в реальному часі відстежувати ситуацію та вносити корективи в роботу патрульних нарядів.

Інформаційна підсистема «Гарпун»

Системи відеоспостереження також використовуються у межах інформаційної підсистеми «Гарпун» – спеціалізованої інформаційно-телекомунікаційної системи, що є частиною Інформаційного порталу Національної поліції України. Ця система займається обробкою даних про транспортні засоби та їхні номерні знаки, що перебувають у розшуку в межах кримінальних проваджень, адміністративних правопорушень та оперативно-розшукових заходів¹.

¹ Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун»

Програмне забезпечення «Гарпун» автоматично обробляє відео- і фотоматеріали, отримані з камер спостереження, службових транспортних засобів та інших джерел, зокрема приватних систем відеоспостереження. Воно дозволяє швидко виявляти підозрілі транспортні засоби, розпізнавати можливі випадки використання фальшивих номерних знаків або інших порушень.

Використання відеофіксації в роботі чергових служб

Система відеоспостереження активно застосовується для організації роботи чергових частин поліції¹. Старші інспектори-чергові використовують відео- та фотоматеріали для встановлення осіб, підозрюваних у правопорушеннях, перевірки їх за базами даних, а також документування подій. Окрім того, камери відеоспостереження встановлюються у приміщеннях для затриманих осіб, що забезпечує додатковий рівень контролю та запобігає можливим порушенням.

Перед розміщенням затриманих осіб у спеціальних приміщеннях вони отримують повідомлення про наявність систем відеонагляду, що відповідає вимогам законодавства України щодо захисту персональних даних.

Використання безпілотних літальних апаратів з метою відеоспостереження у правоохоронній діяльності

У сучасних умовах правоохоронні органи активно застосовують безпілотні літальні апарати (далі – БпЛА) для виконання широкого спектра завдань. Із метою координації діяльності таких підрозділів у структурі центрального апарату Національної поліції України функціонує Управління авіації та поліції на воді Національної поліції України². Основні

завдання цього Управління охоплюють організацію, контроль і забезпечення ефективного використання авіаційних ресурсів у діяльності Національної поліції України.

Ефективне виконання завдань Національної поліції України вимагає не лише оптимального використання наявних ресурсів, а й розвитку сучасних технологічних засобів. Важливими напрямками є охорона громадської безпеки, боротьба зі злочинністю, забезпечення публічної безпеки, захист державного кордону, запобігання надзвичайним ситуаціям тощо. З огляду на ці потреби Національна поліція України реалізовує заходи щодо розвитку повітряної підтримки, зокрема впровадження вертолітної авіації та безпілотних авіаційних комплексів.

Сьогодні БпЛА активно застосовуються в діяльності підрозділів поліції, зокрема в Департаменті патрульної поліції, Департаменті оперативної служби, Департаменті охорони та технічного забезпечення, а також регіональних управліннях.

Основні напрями використання БпЛА в поліцейській діяльності

Основними напрямками використання БпЛА в поліцейській діяльності є такі:

- 1) **моніторинг громадської безпеки** – спостереження під час масових заходів, акцій протесту, спортивних подій, а також контроль ситуації у криміногенних районах;
- 2) **супроводження оперативних заходів** – використання БпЛА у процесі розслідувань, фіксація доказів, аналіз місця злочину;
- 3) **виявлення правопорушень** – фото- та відеофіксація незаконної діяльності, патрулювання територій із підвищеною кримінальною активністю;
- 4) **контроль безпеки дорожнього руху** – нагляд за транспортними потоками, виявлення порушень правил дорожнього руху;
- 5) **авіарозвідка** – оцінювання оперативної обстановки, забезпечення візуального контролю територій під час надзвичайних подій;
- 6) **пошук і порятунок зниклих осіб** – оперативне обстеження важкодоступних місцевостей для виявлення загублених чи зниклих громадян.

Застосування БпЛА забезпечує можливість моніторингу обстановки в режимі реального часу, швидкої передачі інформації та ухвалення оперативних рішень. Новітні технічні розробки в цьому напрямі значно

інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України»: наказ МВС України від 13.06.2018 № 497 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: <https://zakon.rada.gov.ua/laws/show/z0787-18> (дата звернення: 09.02.2025).

¹ Про затвердження Інструкції з організації діяльності чергової служби органів (підрозділів) Національної поліції України: наказ МВС України від 23.05.2017 № 440 // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/z0750-17> (дата звернення: 09.02.2025).

² Положення про Управління авіації та поліції на воді Національної поліції України: затв. наказом Нац. поліції України від 08.10.2020 № 795 // Доступ до правди: сайт. URL: <https://dostup.org.ua/request/94791/response/344252/attach/3/1.pdf> (дата звернення: 09.02.2025).

dostup.org.ua/request/94791/response/344252/attach/3/1.pdf (дата звернення: 09.02.2025).

підвищують ефективність роботи поліції у критичних ситуаціях¹.

Протидія несанкціонованим польотам

Одним із важливих напрямів роботи Управління авіації та поліції на воді Національної поліції України є боротьба з незаконним використанням безпілотних апаратів. Це охоплює контроль за повітряним простором, запобігання терористичним загрозам, захист об'єктів критичної інфраструктури та державних установ. Співробітники поліції залучаються до заходів із протидії нелегальним польотам БПЛА під час масових заходів державного рівня та спеціальних операцій.

Подальший розвиток системи повітряної підтримки

У середньостроковій перспективі розвиток системи повітряної підтримки передбачає:

- удосконалення нормативно-правового регулювання застосування БПЛА в поліцейській діяльності;
- розвиток заходів протидії незаконному використанню БПЛА;
- підготовку та навчання персоналу для ефективного використання безпілотних систем;
- інтеграцію сучасних аналітичних платформ для оптимізації роботи БПЛА у сфері кримінального аналізу.

Велика номенклатура засобів фото- та відеозйомки, що використовуються правоохоронними органами для забезпечення громадського порядку, можуть застосовуватись під час проведення кримінального аналізу для пошуку й ідентифікації злочинців. Для цього можливе залучення фото- та відеоматеріалів, отриманих з камер відеоспостереження. Але з'являється інша проблема, пов'язана з роботою цих систем, а саме масовість і великий обсяг даних, який вони збирають. Через широке поширення камер відеоспостереження вони акумулюють величезні обсяги відеоматеріалів. Для прискорення їхньої обробки можна застосовувати спеціалізоване програмне забезпечення з інтегрованим ШІ.

2. Застосування технологій розпізнавання облич у кримінальному аналізі правоохоронних органів

Відеоспостереження завжди було критично важливим компонентом забезпечення громадської безпеки: від персоналу служби

безпеки, який стежить за трансляцією з камер відеоспостереження для запобігання злочинам, до працівників поліції, які переглядають записи для пошуку відеодоказів для підтримки розслідувань. Широке поширення камер відеоспостереження дає змогу збирати більше інформації про злочини та злочинців, які потрапили в їхній об'єктив. Водночас поява технології аналізу відеоконтенту значно підвищила цінність цих відеоматеріалів. Здатність ефективно та результативно переглядати й аналізувати відео змінює правила роботи для правоохоронних органів. Відеоспостереження відіграє особливу роль у кримінальному аналізі.

Кримінальний аналіз охоплює комплекс заходів, спрямованих на встановлення та оцінювання взаємозв'язків між кримінальними подіями, залученими особами і даними, отриманими з різних джерел. Ця інформація використовується слідчими органами, прокуратурою та судовими інстанціями для всебічного розгляду справи.

Основними завданнями кримінального аналізу є формування гіпотез щодо обставин злочину, відтворення послідовності його вчинення, визначення ймовірної причетності однієї чи кількох осіб, встановлення підозрюваних та їхніх зв'язків. Окрім того, аналіз дозволяє виявити важливі докази, дослідити структуру злочинних угруповань та оцінити масштаби й особливості їхньої діяльності.

Як зазначено вище, кримінальний аналіз завдяки своїй специфіці накопичує великий обсяг даних, пов'язаних зі злочином, до яких також належать дані про обличчя людей, які потрапили в об'єктив камери відеоспостереження. У криміналістиці інформація про зовнішні ознаки людини відіграє ключову роль у її встановленні, розшуку й ідентифікації (ототожненні) (Степанюк та ін., 2023). У цьому разі для ідентифікації особи за обличчям необхідно провести її ототожнення з наявними фото- та відеоданими. Ототожнення проводиться методом порівняння зовнішнього вигляду певної людини із зображенням розшукуваної особи (фотознімків, відео, відзнятих камерами відеоспостереження, опису свідків тощо). Залежно від типу зображень, що використовувались для розшуку особи, ототожнення проводять за фото- чи відеозаписом, рисунком, суб'єктивним або словесним портретом, уявним образом у пам'яті свідка.

У разі використання відеозапису як даних для ототожнення людини постає проблема в обробці таких даних. Окрім ідентифікації людини, існує необхідність у пошуку самої людини у відеофайлі та необхідність обробки

¹ Спосіб підключення зовнішніх камер відеоспостереження при здійсненні екстреного телефонного виклику : пат. 155418 Україна: МПК (2024.01): G08B25/00, H04N7/18, B64U101/30. № u202302479 ; заявл. 23.05.2023 ; опубл. 28.02.2024, Бюл. № 9/2024. 6 с.

декількох відеофайлів через можливу присутність підозрюваного на них. Тому виникає необхідність у розробленні, впровадженні й оптимізації програм з ідентифікації людей за обличчям.

Сьогодні ПЗ для ідентифікації людей за обличчям представлено такими розробками: *Veritone Identify* (Careless, 2024), *Clearview AI* (Shepitko et al., 2024), *Corsight* (Simmler, Canova, 2025) – від закордонних розробників; *ТиХто* (Томіна, Мукоїда, 2023), *Artellence* (Овсянюк, Худенко, 2023) – від вітчизняних розробників. Кожна з представлених програм має свої особливості, недоліки та переваги в застосуванні. *Veritone Identify* розроблена спеціально для правоохоронних органів і забезпечує пошук та ідентифікацію людей за обличчям у відео, знятому камерами відеоспостереження. *Clearview AI* використовується для пошуку людей за обличчям у відкритих базах даних, зокрема у соціальних мережах. *Corsight* також ідентифікує людей за обличчям у відеоматеріалах із камер відеоспостереження, але додатково може відстежувати переміщення осіб, чиї обличчя потрапили в об'єкти камери. Вітчизняні розробки *ТиХто* та *Artellence* здійснюють ідентифікацію людей на основі фотографій.

Veritone Identify – це високотехнологічна система швидкої ідентифікації підозрюваних, розроблена спеціально для потреб правоохоронних органів. Вона забезпечує можливість ефективного пошуку осіб, причетних до правопорушень, використовуючи фото- та відеоматеріали. Програма дозволяє застосовувати фільтрацію за такими ключовими параметрами, як вік, стать, зріст, колір очей, волосся, а також етнічні особливості.

Система дає змогу об'єднувати дані про можливих підозрюваних у межах розслідувань, формувати їх у базу для подальшого аналізу, а також обмінюватися зібраною інформацією між співробітниками відповідних відомств. Для зручності роботи *Veritone Identify* інтегрує всі зібрані матеріали на єдиній онлайн-платформі, де зберігаються докази, фотографії, адреси та інші відомості, важливі для проведення слідства.

Структура програми містить кілька основних модулів: «Управління справами», «Деталізація», «Дії», «Докази», «Обробка даних», «Підозрювані» та «Примітки».

Робота з *Veritone Identify* розпочинається зі створення нової справи, що передбачає заповнення відповідної форми, у якій вказується унікальний ідентифікатор (ID), дата і час події, назва справи, її короткий опис, структурний підрозділ, який займається розслідуван-

ням, відповідальна особа та місце, де подія відбулася. Модуль «Управління справами» надає можливість переглядати справи за трьома категоріями: активні, закриті або архівовані.

Модуль «Деталізація» містить всі зібрані та додані до справи докази й інформацію. Тут також можна завантажити й обробити додаткові докази, відредагувати деталі справи, додати примітки, обмінюватися інформацією між підрозділами та підтвердити збіг обличчя.

Модуль «Дії» надає можливість створити примітки для додавання інформації до справи. Також у цьому розділі можна завантажити відео- та фотодані як докази до справи, поширити справу серед колег в інших підрозділах за допомогою електронної пошти, дізнатися інформацію про справу, редагувати її матеріали, закрити, архівувати, видалити і повторно відкрити справу.

У модулі «Докази» містяться всі медіафайли, які завантажені у справу та впорядковані у форматі галереї. У цьому розділі можна виконати додаткові дії з файлами, зокрема обітнути або обробити відео, дізнатися про обсяг відеофайлу, запустити процес розпізнавання облич.

Модуль «Обробка» містить список файлів відео- та фотоданих, у яких відбулося розпізнавання облич. Тут можна переглянути обличчя, що збігаються з базою даних злочинців та невпізнаних людей. За допомогою фільтрів можна сортувати ідентифікованих людей за віком, расою та статтю.

Якщо обличчя підозрюваного відсутнє в будь-якій із доступних баз даних, його можна занести до спеціального реєстру невпізнаних осіб. Це дозволить у разі потреби оперативно здійснити пошук людини та ідентифікувати її в майбутньому.

Модуль «Підозрювані» містить перелік осіб, яким оголошено підозри у справі. Такі особи відображаються на картках у форматі галереї, які розташовані за датою їх додавання. Кожна картка містить дані та дозволяє виконати такі дії: порівняти ідентифікаційне зображення підозрюваного можна з еталонним зображенням, що використовується для ідентифікації відповідності, поділитися інформацією про підозрюваного електронною поштою, а також видалити особу зі списку підозрюваних.

Модуль «Примітки» містить колекцію нотаток, доданих до справи. Він також надає інструменти для редагування, спільного використання та видалення нотаток справи.

3. *Відеоаналітика та її застосування у кримінальному аналізі*

У кримінальному аналізі використання програм відеоаналізу для швидкої ідентифікації людей, об'єктів і транспортних засобів може сприяти прискоренню розкриття злочинів. У цьому разі сортування ідентифікованих об'єктів за багатьма категоріями, такими як колір, розмір, модель транспортного засобу, напрямок руху підозрюваного чи транспортного засобу тощо, може покращити можливості кримінального аналізу та допомогти правоохоронним органам у пошуку всіх причетних до злочину.

Як приклад продуктів, здатних аналізувати відеодані, можна розглянути розробки від компанії *BriefCam* (Vrba, Švadlenka, Galkin, 2024). Це програмне забезпечення, яке здатне аналізувати необроблений відеофайл та розуміти контекст всієї сцени та фон, виявляти, відстежувати й класифікувати кожен об'єкт, а також створювати структуровану базу даних із відеоданих, що полегшує обробку відеоконтенту.

Основне керування програмою розташоване в таких розділах:

- перелік відеофайлів, у яких буде проводитись розпізнавання;
- мапа з місцем розташування камер відеоспостереження, підключених до програми, та всіма ідентифікованими об'єктами, що потрапили в об'єкти камери відеоспостереження;
- дії – розділ програми, в якому можна відсортувати ідентифіковані об'єкти за різними властивостями, ідентифікувати людину, що була знята відеокамерою, та розпізнати номерний знак транспортного засобу.

Для аналізу відеоматеріалів у програмі *BriefCam* необхідно додати їх до програми. Це можна зробити, обравши камеру спостереження на мапі або просто завантаживши відео для обробки. Для того, щоб провести ідентифікацію людини, необхідно натиснути на її фото, після чого з'явиться інформація про неї. У разі, якщо людину не вдалося впізнати, її фото можна додати до бази для подальшого розслідування.

Окрім ідентифікації людей, невід'ємною частиною кримінального аналізу є також ідентифікація об'єктів, пов'язаних зі злочином. Сюди також можна віднести ідентифікацію транспортного засобу, що можливо був залучений до вчинення злочину, та його номерних знаків. Можливості *BriefCam* дозволяють швидко аналізувати відеодані на наявність різних транспортних засобів, визначати їхній колір, швидкість і напрямок руху.

4. *Рекомендації щодо впровадження технологій відеоаналізу і ПЗ для розпізнавання облич та інших об'єктів у кримінальному аналізі*

Сьогодні правоохоронні органи України дедалі частіше впроваджують технології ШІ, що зумовлює потребу не лише в нормативному врегулюванні їхнього використання, а й у розробленні практичних методичних рекомендацій щодо їхнього застосування (Жадан та ін., 2024). Питання правового регулювання ідентифікації осіб за допомогою технологій розпізнавання облич активно обговорюється в наукових дослідженнях (Токарева, Савліва, 2021; Зачек, Дмитрик, Сеник, 2023; Войнов, 2023).

Важливим кроком у цьому напрямі стало ухвалення Верховною Радою України Проекту закону про захист персональних даних від 25 жовтня 2022 р. (реєстраційний № 8153)¹, що був розглянутий на її засіданні 20 листопада 2024 р. Документ передбачає оновлені правові механізми захисту персональної інформації, зокрема щодо використання зображень осіб, автоматично збережених камерами відеоспостереження.

Крім нормативного регулювання, важливо розробити конкретні рекомендації для правоохоронних органів, які сприятимуть об'єктивному розслідуванню злочинів з використанням технологій відеоаналізу та систем розпізнавання облич. Це гарантує прозорість, законність та ефективність застосування таких інструментів у кримінальному аналізі.

1. На рівні законодавчої бази пропонуємо такі рекомендації щодо використання технологій відеоаналізу і ПЗ з розпізнавання облич та інших об'єктів у діяльності правоохоронних органів України:

1) дотримання положень Конституції та чинного законодавства України, що є ключовим аспектом правової держави та захисту прав громадян. Це стосується і діяльності правоохоронних органів, які застосовують технології розпізнавання облич. Згідно зі статтями 32 та 34 Конституції України кожен громадянин має гарантоване право на недоторканність приватного життя і збереження персональної інформації, а збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою є втручанням в її особисте та сімейне життя;

2) дотримання принципів законного збору, обробки та зберігання особистої інформації, забезпечуючи її конфіденційність і належний

¹ Проекту закону про захист персональних даних : від 25.10.2022 № 8153 / ініціатори Р. О. Стефанчук, Є. В. Чернів, Т. П. Тарасенко та ін. // БД «Законодавство України» / ВР України. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/40707> (дата звернення: 09.02.2025).

рівень безпеки, відповідно до вимог Закону України «Про захист персональних даних»;

3) використання технологій для розпізнавання осіб у межах оперативно-розшукової діяльності повинно відповідати положенням Закону України «Про оперативно-розшукову діяльність», який регламентує правові засади застосування таких технологій у сфері кримінального аналізу.

Ці норми спрямовані на забезпечення балансу між ефективністю правоохоронної діяльності та дотриманням фундаментальних прав людини.

2. Щодо громадської згоди та інформування доцільно запровадити:

1) інформування громадян про використання технологій розпізнавання обличчя шляхом розміщення відповідної інформації на офіційних вебресурсах, у медіа, а також установлення попереджувальних знаків у громадських місцях;

2) отримання в разі можливості явної згоди громадян на обробку персональних даних, особливо в закритих приміщеннях і приватних зонах.

3. Із погляду технічних аспектів використання технологій відеоаналізу та ПЗ з розпізнавання обличчя:

1) необхідно забезпечити високу точність систем розпізнавання обличчя. Для цього доцільно використовувати передові алгоритми розпізнавання обличчя, які демонструють високу точність, постійно покращуючи й оновлюючи їх;

2) перед початком процесу ідентифікації особи слід здійснити попереднє оцінювання якості зображення чи відеоматеріалу, з якого проводитиметься розпізнавання особи. Точність визначення особи на пряму залежить від якості вихідного зображення. У разі, коли оригінальні файли мають недостатню чіткість або розмиті деталі, доцільно застосовувати методи покращення якості графічного матеріалу. Якщо ж ПЗ для ідентифікації вже містить вбудовані функції покращення зображень, цей етап може бути автоматизованим і здійснюватися без додаткового втручання оператора;

3) після ідентифікації особи за допомогою програмно-аналітичних засобів слід підтвердити збіг обличчя, виявленого системою, з контрольним (еталонним) зображенням. Для цього рекомендується застосовувати додаткові методи доказування, зокрема судово-криміналістичну експертизу або процедуру ідентифікації. Надійність ідентифікації значно підвищується за умови залучення незалежних підтверджень. Оптимальною практикою є

проведення ідентифікації за участю трьох і більше осіб, що забезпечує додатковий рівень перевірки і знижує ризик помилкової ідентифікації;

4) важливо розуміти, що встановлений збіг під час розпізнавання обличчя не може бути єдиною підставою для винесення підозри або пред'явлення обвинувачення. Ідентифікація за допомогою алгоритмів має використовуватися як один із допоміжних інструментів, а не як остаточний доказ. Для підтвердження причетності особи до злочину необхідно здійснити комплексне розслідування, що включає аналіз інших доказів, покази свідків та додаткові перевірки. Дотримання цього підходу дозволяє уникнути помилкових звинувачень і гарантує об'єктивність слідчих дій;

5) використання засобів ідентифікації людей за обличчям пов'язано з накопиченням та обробкою персональних даних, що зумовлює необхідність забезпечення їхнього захисту на високому рівні. Використання сучасних методів шифрування, фізичного та логічного захисту серверів і мереж, де зберігаються ці дані, повинно забезпечити належний рівень захисту. Не менш важливі заходи із забезпечення збереження даних спрямовані на регулярні перевірки безпеки для виявлення вразливостей та потенційних загроз, розроблення та впровадження політик безпеки, що відповідають міжнародним стандартам.

4. Дотримання етичних аспектів при використанні технологій відеоаналізу та ПЗ із розпізнавання обличчя охоплює:

1) пропорційність і необхідність, які стосуються оцінювання ризиків та цільового використання програм із розпізнавання обличчя. Оцінювання ризиків перед упровадженням технологій розпізнавання передбачає визначення конкретних цілей і завдань, щодо яких буде застосовуватись ця технологія. Використання технологій розпізнавання обличчя можливе тільки для досягнення конкретних цілей та законно обґрунтованих результатів, а саме запобігання злочинам, пошуку зниклих та розшукуваних осіб тощо;

2) запобігання дискримінації. Щоб запобігти упередженості систем розпізнавання обличчя, слід регулярно їх аналізувати і перевіряти на наявність відповідних упереджень. Крім того, для навчання систем необхідно використовувати тестові набори даних, які відображають різноманітність населення. Запобігання дискримінації сприяє розробленню та налаштуванню систем таким чином, щоб вони враховували розмаїття людських обличчя. Не буде зайвим залучення експертів з етики та

прав людини для оцінювання систем перед їх використанням.

5. Використання технологій відеоаналізу та ПЗ із розпізнавання облич передбачає відповідний контроль і нагляд, зокрема:

1) незалежний нагляд за використанням технологій розпізнавання облич із залученням Уповноваженого Верховної Ради України з прав людини, що передбачає забезпечення доступу до інформації про їх застосування. Створення незалежних комісій, які будуть постійно перевіряти використання технологій та їхню відповідність вимогам чинного законодавства. Комісія повинна включати представників громадськості, експертів з прав людини та експертів у галузі технологій розпізнавання облич;

2) аудити і перевірки, які передбачають регулярний контроль системи з метою оцінювання її ефективності та відповідності закону. Для об'єктивних висновків таких перевірок доцільно залучати зовнішні компанії.

Крім того, необхідно впровадити практику публікації результатів таких аудитів і перевірок. Звіти з інформацією про кількість ідентифікацій, помилкових спрацювань і випадків неправомірного використання систем забезпечити прозорість цього процесу та довіру суспільства до правоохоронних органів.

6. Належне застосування технологій відеоаналізу та ПЗ з розпізнавання облич неможливе без відповідного тренування та підготовки персоналу, що охоплює:

1) навчання, зокрема організацію навчальних курсів для співробітників, які працюють із системами розпізнавання облич, не лише з технічних аспектів використання систем, й з етичних питань. Також необхідне проведення регулярних тренінгів і семінарів для оновлення знань та навичок;

2) розроблення та впровадження кодексу етики, який визначає правила поведінки та використання технологій розпізнавання облич. Кодекс повинен містити положення про захист прав людини, конфіденційність даних і відповідальність за неправомірне використання технологій. Крім того, доцільним є проведення практичних занять для співробітників з акцентом на етичні питання та права людини з використанням реальних прикладів для симуляцій та навчання.

7. Запровадження звітування про використання технологій відеоаналізу та ПЗ з розпізнавання облич і механізмів зворотного зв'язку. Система обліку використання ПЗ, що здійснює розпізнавання облич, має вестися на захищених від фальсифікації носіях як у традиційному форматі, так і в електронному ви-

гляді. У такому журналі має фіксуватися інформація про кожен випадок використання системи, зокрема дату, час, відповідального працівника, підстави для застосування технології та отримані результати.

Крім того, правоохоронні органи зобов'язані забезпечити регулярне оприлюднення узагальнених звітів про функціонування систем розпізнавання облич. Такі звіти повинні містити дані про кількість ідентифікованих осіб, рівень точності розпізнавання, випадки помилкових спрацювань та ефективність технології в межах кримінального аналізу. Для забезпечення прозорості ці звіти мають бути доступними для громадськості через офіційні вебресурси правоохоронних органів.

Необхідним також є надання доступу дослідницьким і громадським організаціям до відкритих даних про використання технологій розпізнавання облич, до яких має бути включено інформацію про точність системи, частоту хибних спрацювань та інші технічні параметри.

Зворотній зв'язок передбачає створення механізмів для подання скарг громадянами щодо використання технологій розпізнавання облич, зокрема через інтернет, телефонні лінії та особистий прийом, наявність процедури розгляду скарг із визначеними термінами та відповідальними особами, забезпечення прозорості процесу розгляду скарг та інформування заявників про його результат.

8. Строки зберігання даних і доступ до них. Необхідно визначити чіткі строки зберігання даних для різних типів завдань, після спливу яких вони повинні знищуватись, шляхом розроблення чіткої політики зберігання даних, яка буде визначати терміни, умови зберігання та видалення.

Слід упровадити механізми контролю доступу до даних, які передбачають доступ до них тільки уповноважених осіб та використовують багаторівневий захист доступу, зокрема паролі, біометричні дані й інші методи автентифікації. Крім того, доцільно вести журнал обліку осіб, які мають доступ до даних, для відстеження їхніх дій. Це забезпечить можливість проведення аудитів на основі цих журналів для виявлення протиправних дій.

ВИСНОВКИ. Упровадження систем відеоаналізу та розпізнавання облич у діяльність правоохоронних органів сприяє зниженню впливу людського фактора, прискоренню процесу ідентифікації осіб, підозрюваних у скоєнні злочинів, та підвищенню ефективності оперативної роботи. Використання цих технологій дає змогу здійснювати глибокий аналіз великих

обсягів даних, зокрема відеоматеріалів із систем спостереження.

1. Досвід зарубіжних країн свідчить про те, що інтеграція інноваційних програмних рішень у сферу правоохоронної діяльності дає змогу суттєво підвищити рівень ефективності кримінального аналізу та скоротити час, необхідний для розслідування злочинів. Для успішного запровадження таких технологій в Україні необхідно враховувати національні особливості їхнього використання та специфіку правового регулювання.

2. Упровадження систем відеоаналізу та розпізнавання обличч потребує розроблення чітко визначених правових механізмів, які гарантуватимуть захист персональних даних, запобігатимуть дискримінаційним ризикам і мінімізуватимуть можливість зловживань. Особливу увагу слід приділити створенню етичних стандартів застосування таких технологій, що забезпечить баланс між ефективністю кримінального аналізу та дотриманням прав людини.

3. У межах дослідження запропоновано рекомендації щодо вдосконалення кримінального аналізу, підвищення ефективності ро-

боти правоохоронних органів та забезпечення прозорості їхньої діяльності:

1) розроблення та впровадження спеціалізованих навчальних програм для співробітників правоохоронних органів із метою оволодіння технічними навичками та дотримання правових норм;

2) створення єдиних стандартів для використання технологій відеоаналізу та розпізнавання обличч, зокрема технічні вимоги, методи обробки даних та оцінювання ефективності;

3) формування законодавчої бази, яка регулюватиме порядок застосування подібних технологій, із забезпеченням високого рівня захисту персональних даних громадян;

4) розроблення інструментів моніторингу й оцінювання ефективності впроваджених технологій, зокрема прозорі процедури звітності.

Таким чином, інтеграція технологій відеоаналізу у правоохоронну діяльність дасть змогу підвищити рівень громадської безпеки, оперативність реагування на загрози й ефективність боротьби зі злочинністю, що є ключовими елементами забезпечення стабільності і безпеки в країні.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Белов Д. М., Белова М. В. Штучний інтелект в судочинстві та судових рішеннях, потенціал та ризики. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Т. 2, № 78. С. 315–320. DOI: <https://doi.org/10.24144/2307-3322.2023.78.2.50>.
2. Войнов М. Система розпізнавання обличчя: правові аспекти використання в Україні та в ЄС // Українська Гельсінська спілка з прав людини : сайт. 04.10.2023. URL: <https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes/> (дата звернення: 09.02.2025).
3. Жадан Д. О., Мордвинцев М. В., Пашнєв Д. В. Відстеження протиправних дій за допомогою систем відеоспостереження: огляд сучасного стану досліджень. *Право і безпека*. 2024. № 1 (92). С. 78–89. DOI: <https://doi.org/10.32631/pb.2024.1.07>.
4. Жадан Д. О., Мордвинцев М. В., Пашнєв Д. В., Хлестков О. В. Упровадження та оптимізація інтелектуальних поліцейських систем на основі штучного інтелекту. *Вісник Харківського національного університету внутрішніх справ*. 2024. Вип. 2 (105), ч. 1. С. 240–248. DOI: <https://doi.org/10.32631/v.2024.2.22>.
5. Зачек О. І., Дмитрик Ю. І., Сенік В. В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148–156. DOI: <https://doi.org/10.32782/2311-8040/2023-3-19>.
6. Коршенко В. А., Чумак В. В., Мордвинцев М. В., Пашнєв Д. В. Стан систем безпеки з використанням технічних засобів відеозапису та відеоспостереження: зарубіжний досвід, перспективи впровадження в діяльність Національної поліції України. *Право і безпека*. 2020. № 2 (77). С. 86–92. DOI: <https://doi.org/10.32631/pb.2020.2.12>.
7. Криміналістика: криміналістична техніка : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін. Харків : Харків. нац. ун-т внутр. справ, 2023. 388 с.
8. Моца В. В. Теоретико-методологічні засади використання кримінального аналізу оперативними підрозділами правоохоронних органів України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. Т. 2, № 73. С. 141–147. DOI: <https://doi.org/10.24144/2307-3322.2022.73.53>.
9. Овсянюк Д. І., Худенко Д. М. Використання підрозділами кримінального аналізу технологій розпізнавання обличч та фенотипування ДНК в умовах воєнного стану // Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану : матеріали міжвідом. наук.-практ. конф. (м. Київ, 30 берез. 2023 р.) / МВС України ; Нац. поліція України ; Нац. акад. внутр. справ. Київ, 2023. С. 231–235.

10. Токарева К., Савліва Н. Особливості правового регулювання штучного інтелекту в Україні. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. Т. 3, № 60. С. 148–153. DOI: <https://doi.org/10.18372/2307-9061.60.15967>.
11. Томіна В. Ю., Мукоїда Р. В. Особливості використання штучного інтелекту в умовах воєнного стану на території України // *Modern theories and improvement of world methods : Proceedings of the XXII International Scientific and Practical Conference (Helsinki, Finland, 6–9 June 2023)*. Helsinki, Finland : International Science Group, 2023. Pp. 150–154. DOI: <https://doi.org/10.46299/isg.2023.1.22>.
12. Baltimore A. Charlotte's Crime Landscape: Analyzing the Location of Criminal Activity; A Comprehensive Study of Crime Trends Over Six Years (2017–2023) // *Research Square* : сайт. 18.12.2024. DOI: <https://doi.org/10.21203/rs.3.rs-5567752/v1>.
13. Careless J. How law enforcement can surf the rising tide of digital evidence without drowning in details // *Police 1* : сайт. 12.03.2024. URL: <https://www.police1.com/police-products/investigation/evidence-management/how-law-enforcement-can-surf-the-rising-tide-of-digital-evidence-without-drowning-in-details> (дата звернення: 09.02.2025).
14. Rezende I. N. Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*. 2020. Vol. 11, Iss. 3. Pp. 375–389. DOI: <https://doi.org/10.1177/2032284420948161>.
15. Sheera F. Israel Deploys Expansive Facial Recognition Program in Gaza. *International New York Times*. 2024. 30 Mar. URL: <https://go.gale.com/ps/i.do?p=AONE&u=anon~3696e090&id=GALE%7CA788099163&v=2.1&it=r&sid=googleScholar&asid=25a8e947> (дата звернення: 09.02.2025).
16. Shepitko V., Shepitko M., Latysh K., Kapustina M., Demidova E. Artificial intelligence in crime counteraction: From legal regulation to implementation. *Social & Legal Studies*. 2024. Vol. 7, No. 1. Pp. 135–144. DOI: <https://doi.org/10.32518/sals1.2024.135>.
17. Simmler M., Canova G. Facial recognition technology in law enforcement: Regulating data analysis of another kind. *Computer Law & Security Review*. 2025. Vol. 56. DOI: <https://doi.org/10.1016/j.clsr.2024.106092>.
18. Vrba R., Švadlenka L., Galkin A. Monitoring Traffic Flow Using Breifcam Software to Improve Sustainable Urban Logistics // *Systems, Decision and Control in Energy VI. Studies in Systems, Decision and Control* / ed. by V. Babak, A. Zaporozhets. Cham : Springer, 2024. Pp. 377–387. DOI: https://doi.org/10.1007/978-3-031-68372-5_20.
19. Wienroth M. Socio-technical disagreements as ethical fora: Parabon NanoLab's forensic DNA Snapshot™ service at the intersection of discourses around robust science, technology validation, and commerce. *BioSocieties*. 2020. Vol. 15. Pp. 28–45. DOI: <https://doi.org/10.1057/s41292-018-0138-8>.

Надійшла до редакції 10.02.2025

Прийнята до опублікування 13.03.2025

REFERENCES

1. Baltimore, A. (2024, December 18). *Charlotte's Crime Landscape: Analyzing the Location of Criminal Activity; A Comprehensive Study of Crime Trends Over Six Years (2017–2023)*. Research Square. <https://doi.org/10.21203/rs.3.rs-5567752/v1>.
2. Byelov, D., & Bielova, M. (2023). Artificial intelligence in judicial proceedings and court decisions, potential and risks. *Uzhhorod National University Herald. Series: Law*, 2(78), 315–320. <https://doi.org/10.24144/2307-3322.2023.78.2.50>.
3. Careless, J. (2024, March 12). *How law enforcement can surf the rising tide of digital evidence without drowning in details*. Police 1. <https://www.police1.com/police-products/investigation/evidence-management/how-law-enforcement-can-surf-the-rising-tide-of-digital-evidence-without-drowning-in-details>.
4. Korshenko, V. A., Chumak, V. V., Mordvyntsev, M. V., & Pashniev, D. V. (2020). Security systems' status with the use of technical means of video recording and video surveillance: international experience, perspectives for implementation in the activities of the National police of Ukraine. *Law and Safety*, 2(77), 86–92. <https://doi.org/10.32631/pb.2020.2.12>.
5. Motsa, V. V. (2022). Theoretical and methodological bases for the use of criminal analysis by operative units of law enforcement agencies in Ukraine. *Uzhhorod National University Herald. Series: Law*, 2(73), 141–147. <https://doi.org/10.24144/2307-3322.2022.73.53>.
6. Ovsianiuk, D. I., & Khudenko, D. M. (2023, March 30). *Use of facial recognition and DNA phenotyping technologies by criminal analysis units under martial law* [Conference presentation abstract]. Interdepartmental Scientific and Practical Conference "Current issues and prospects for the use of operational and investigative means in solving crimes under martial law", Kyiv, Ukraine.
7. Rezende, I. N. (2020). Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, 11(3), 375–389. <https://doi.org/10.1177/2032284420948161>.

8. Sheera, F. (2024, March 30). *Israel Deploys Expansive Facial Recognition Program in Gaza*. International New York Times. <https://go.gale.com/ps/i.do?p=AONE&u=anon~3696e090&id=GALE%7CA788099163&v=2.1&it=r&sid=googleScholar&asid=25a8e947>.
9. Shepitko, V., Shepitko, M., Latysh, K., Kapustina, M., & Demidova, E. (2024). Artificial intelligence in crime counteraction: From legal regulation to implementation. *Social & Legal Studies*, 7(1), 135–144. <https://doi.org/10.32518/sals1.2024.135>.
10. Simmler, M., & Canova, G. (2025). Facial recognition technology in law enforcement: Regulating data analysis of another kind. *Computer Law & Security Review*, 56. <https://doi.org/10.1016/j.clsr.2024.106092>.
11. Stepaniuk, R. L., Husieva, V. O., Kikinych, V. V. et al. (2023). *Forensics: forensic techniques*. Kharkiv National University of Internal Affairs.
12. Tokarieva, R., & Savliya, N. (2021). Peculiarities of legal regulation of artificial intelligence in Ukraine. *Scientific Works of Kyiv Aviation Institute. Series: Law Journal "Air and Space Law"*, 3(60), 148–153. <https://doi.org/10.18372/2307-9061.60.15967>.
13. Tomina, V. Yu., & Mukoida, R. V. (2023, June 6–9). *Peculiarities of using artificial intelligence in conditions of martial law in Ukraine* [Conference presentation abstract]. XXII International Scientific and Practical Conference "Modern theories and improvement of world methods", Helsinki, Finland.
14. Voinov, M. (2023, October 4). *Facial recognition system: legal aspects of use in Ukraine and the EU*. Ukrainian Helsinki Human Rights Union. <https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes/>.
15. Vrba, R., Švadlenka, L., & Galkin, A. (2024). Monitoring Traffic Flow Using Breifcam Software to Improve Sustainable Urban Logistics. In V. Babak, & A. Zaporozhets (Eds.), *Systems, Decision and Control in Energy VI. Studies in Systems, Decision and Control* (pp. 377–387). Springer. https://doi.org/10.1007/978-3-031-68372-5_20.
16. Wienroth, M. (2020). Socio-technical disagreements as ethical fora: Parabon NanoLab's forensic DNA Snapshot™ service at the intersection of discourses around robust science, technology validation, and commerce. *BioSocieties*, 15, 28–45. <https://doi.org/10.1057/s41292-018-0138-8>.
17. Zachek, O. I., Dmytryk, Yu. I., & Senyk, V. V. (2023). The role of artificial intelligence in increasing efficiency law enforcement activities. *Scientific Journal of Lviv State University of Internal Affairs. Law*, 3, 148–156. <https://doi.org/10.32782/2311-8040/2023-3-19>.
18. Zhadan, D. O., Mordvyntsev, M. V., & Pashniev, D. V. (2024). Tracking illegal actions using video surveillance systems: a review of the current state of research. *Law and Safety*, 1(92), 78–89. <https://doi.org/10.32631/pb.2024.1.07>.
19. Zhadan, D. O., Mordvyntsev, M. V., Pashniev, D. V., & Khlestkov, O. V. (2024). Implementation and optimisation of intelligent police systems based on artificial intelligence. *Bulletin of Kharkiv National University of Internal Affairs*, 2(105), 240–248. <https://doi.org/10.32631/v.2024.2.22>.

Received the editorial office: 10 February 2025

Accepted for publication: 13 March 2025

MYKOLA VOLODYMYROVYCH MORDVYNTSEV,

Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Educational and Research Institute No. 4,
Research Laboratory on the Problems of Information
Technologies and Combating Crime in Cyberspace;
ORCID: <https://orcid.org/0000-0002-7674-3164>,
e-mail: lukoly@ukr.net;

DMYTRO VALENTYNOVYCH PASHNIEV,

Candidate of Law, Associate Professor,
Kharkiv National University of Internal Affairs,
Educational and Research Institute No. 4,
Research Laboratory on the Problems of Information
Technologies and Combating Crime in Cyberspace;
ORCID: <https://orcid.org/0000-0001-8693-3802>,
e-mail: dypashnev@gmail.com;

VOLODYMYR SERHIIOVYCH NAKONECHNYI,

Doctor of Technical Sciences, Professor,
Taras Shevchenko National University of Kyiv,
Department of Cybersecurity and Information Protection;

ORCID: <https://orcid.org/0000-0002-0247-5400>,
e-mail: volodym.nakonechnyi@knu.ua

SPECIFICS OF USING VIDEO ANALYSIS TECHNOLOGIES AND FACIAL RECOGNITION SOFTWARE IN CRIMINAL ANALYSIS

The modern technologies of video analysis and face recognition software are analysed, their effectiveness in criminal analysis is assessed, and the ethical and legal aspects of using these innovations in law enforcement are investigated. The article emphasises the relevance of introducing the latest video analysis technologies and face recognition software for ensuring public safety and combating crime in Ukraine.

The key technical characteristics of video analysis technology and face recognition software are identified, and their role in reducing the human factor and accelerating the process of identifying suspects is revealed. The foreign experience of using such technologies and the ways of their integration into law enforcement in Ukraine are analysed. Particular attention is paid to legal aspects, in particular personal data protection, as well as ethical challenges, namely ensuring transparency, non-discrimination and respect for human rights.

The research methodology is based on the analysis of regulatory documents, scientific sources and practical experience in the use of video analysis technologies. A systematic approach was used to summarise the data and a comparative method was used to evaluate different software solutions. The specifics of the use of artificial intelligence in different countries were studied and taken into account, which allowed us to summarise the best practices of implementation. Recommendations are made to improve the implementation of video analysis technologies in the practical activities of law enforcement agencies of Ukraine. The article proposes measures to improve technical support, create legislative mechanisms and ethical standards for the use of data. In particular, the author emphasises the importance of training employees, developing a personal data protection policy and implementing transparent procedures for monitoring the effectiveness of technologies. Particular attention is paid to recommendations for providing legal support for the integration of new technologies, including standardisation of procedures and reducing the risks of abuse of power or position by law enforcement officers.

The results obtained can contribute to the improvement of criminal analysis methods, increase the efficiency of law enforcement agencies and strengthen public safety. The proposed approaches will help to strengthen national resilience and increase public confidence in law enforcement through the effective implementation of modern technologies.

Keywords: *video analysis, face recognition, criminal analysis, law enforcement, artificial intelligence, ethics, data security.*

Цитування (ДСТУ 8302:2015): Мордвинцев М. В., Пашнєв Д. В., Наконечний В. С. Особливості використання технологій відеоаналізу та програмного забезпечення з розпізнавання облич у кримінальному аналізі. *Право і безпека*. 2025. № 1 (96). С. 90–103. DOI: <https://doi.org/10.32631/pb.2025.1.08>.

Citation (APA): Mordvyntsev, M. V., Pashniev, D. V., & Nakonechnyi, V. S. (2025). Specifics of using video analysis technologies and facial recognition software in criminal analysis. *Law and Safety*, 1(96), 90–103. <https://doi.org/10.32631/pb.2025.1.08>.