УДК 351.741:004.8 **DOI:** https://doi.org/10.32631/v.2024.2.22

Дмитро Олегович Жадан,
Харківський національний університет внутрішніх справ, науково-дослідна лабораторія з проблем інформаційних технологій та протидії злочинності у кіберпросторі;
https://orcid.org/0000-0001-8184-4800,
e-mail: dmttro.zhadan23@gmail.com;

Микола Володимирович Мордвинцев,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ, 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, науково-дослідна лабораторія з проблем інформаційних технологій та протидії злочинності у кіберпросторі;
https://orcid.org/0000-0001-8693-3802,
e-mail: dvpashnev@gmail.com;

Олексій Володимирович Хлестков,
Харківський національний університет внутрішніх справ, науково-дослідна лабораторія з проблем інформаційних технологій та протидії злочинності у кіберпросторі;
https://orcid.org/0000-0001-8777-8269,
e-mail: oleksii.xle69@gmail.com

УПРОВАДЖЕННЯ ТА ОПТИМІЗАЦІЯ ІНТЕЛЕКТУАЛЬНИХ ПОЛІЦЕЙСЬКИХ СИСТЕМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Досліджено сучасні рішення у сфері ідентифікації людей за обличчям за допомогою програм з інтегрованим у них штучним інтелектом, їх особливості та певні можливості використання в роботі Національної поліції України. Запропоновано кроки, що окреслюють послідовність дій для проведення об'єктивної ідентифікації людей за обличчям та забезпечення високої якості розпізнавання облич і необхідні для забезпечення відкритості, прозорості та найкращого результату застосування програм, здатних ідентифікувати людей за обличчям. Акцентовано увагу на необхідності подальшої роботи з удосконалення законодавства України, що регулює питання

захисту персональних даних та приватності громадян України, зокрема зображення обличчя людини, отриманого за допомогою камер відеоспостереження.

Ключові слова: відеоспостереження, ідентифікація людей, штучний інтелект, аналітична обробка даних, протидія злочинності.

Оригінальна стаття

Постановка проблеми

Правоохоронні органи розвинених країн світу все частіше звертаються до аналітичних інструментів із вбудованим штучним інтелектом (далі – ШІ). Через великі обсяги неструктурованих даних, що можуть становити докази в кримінальній або адміністративній справі, кількість яких у світі становить 80 % [1], оброблення таких даних за допомогою звичайних методів може потребувати дуже багато часу та залучення чималої кількості співробітників. У цьому разі можливості ШІ дадуть змогу скоротити час на обробку даних та допомогти працівникам правоохоронних органів у розкритті злочинів. Упровадження ШІ в роботу правоохоронних органів сприятиме покращенню безпеки громадян та допомагатиме у виявленні правопорушників. Розумні камери з інтегрованим у них ШІ дають змогу контролювати дорожній рух, відстежувати підозрілих людей та предмети. Впровадження систем типу «Безпечне місто» [2] або Domain Awareness System (DAS) [3] дозволяє контролювати публічний порядок та безпеку в зоні відеоспостереження та попереджати, окрім злочинів, терористичні акти завдяки можливості моніторингу залишених речей та підозрілих осіб. Використання програм, здатних ідентифікувати людей за обличчям, все частіше застосовується правоохоронними органами. Швидке виявлення розшукуваних людей за записами камер відеоспостереження допомагає правоохоронним органам у розшуку злочинців. Але все частіше з'являється критика щодо таких систем через можливості порушення прав громадян на захист персональної інформації та приватність. Отже, доцільно звертати на це увагу в процесі дослідження систем з інтегрованим ШІ, що використовуються в роботі правоохоронних органів інших країн, для їх можливого впровадження в роботу Національної поліції України для протидії злочинності та усунення можливих терористичних актів на території України. Важливо також розробляти рекомендації з використання програм ідентифікації людини за обличчям для врегулювання проблеми захисту персональних даних та приватності.

Стан дослідження проблеми

Дослідження у сфері застосування ШІ в роботі правоохоронних органів зараз перебувають у фокусі уваги багатьох науковців. Такі дослідники, як Г. К. Авдєєва, О. І. Бугера, О. І. Зачек, В. О. Гончаренко, Д. Ю. Узлов, В. М. Струков, Д. О. Вєтюков, О. В. Кривенко та

інші, розкривають аспекти впровадження в роботу правоохоронних органів систем з інтегрованим ШІ та проблеми, пов'язані із захистом персональних даних. Але з огляду на швидкий розвиток цієї високотехнологічної сфери необхідним є подальше дослідження впровадження в роботу Національної поліції України систем із ШІ, розроблення рекомендацій із раціонального використання програм ідентифікації людей за обличчям, що забезпечить правоохоронні органи новими можливостями та прискорить їхню роботу. Очевидним також є те, що слід постійно працювати над розвитком та удосконаленням законодавства України щодо захисту персональних даних і приватності громадян у зв'язку з можливим обмеженням прав людини через застосування вказаних технологій.

Мета і завдання дослідження

Метою статті є аналіз сучасних технологій відеоаналітики з розпізнавання облич у роботі правоохоронних органів та розроблення рекомендацій з оптимального застосування цих програмно-технічних засобів. Досягнення поставленої мети передбачає виконання таких *завдань*: аналіз сучасних технологій відеоаналітики, що зараз застосовуються країнами світу; аналіз можливостей впровадження їх у роботу Національної поліції України; розроблення рекомендацій із забезпечення якісного й об'єктивного розслідування з використанням програмно-технічних засобів ідентифікації обличчя людини.

Наукова новизна дослідження

Уперше розроблено рекомендації щодо забезпечення проведення якісного та об'єктивного розслідування з використанням технічних засобів відеоспостереження та програмного забезпечення з ідентифікації людей за обличчям. Удосконалено основи захисту персональних даних і приватності громадян у зв'язку з можливим обмеженням прав людини через застосування вказаних технологій.

Набула подальшого розвитку система знань та досвіду використання сучасних аналітичних систем ідентифікації людей за обличчям у сфері забезпечення публічної безпеки та порядку, впровадження яких у практичну діяльність правоохоронних органів сприятиме підвищенню ефективності та пришвидшенню їхньої роботи.

Виклад основного матеріалу

Штучний інтелект зараз перебуває в центрі уваги багатьох дослідників. Розвиток можливостей ШІ призводить до найрізноманітніших результатів, що впроваджуються в роботу в різних сферах життя сучасних людей. Зараз вже нікого не здивуєш можливостями чатботів, наприклад ChatGPT, що можуть генерувати текст, відповідати на запитання, генерувати програмний код (зокрема, GitHub Copilot), розрізняти картинки та генерувати їх. Наприклад, можна

розпізнавати татуювання на тілах людей для визначення стосунків людей та їх переконань [4] або місця, де було зроблено фото, за допомогою використання нейронної мережі [5].

Упровадження ШІ відбулося і в роботі правоохоронних органів. Зараз чимало правоохоронних органів використовують ШІ, зокрема привертає увагу програмний продукт ResourceRouter, який є аналітичним інструментом, що автоматизує планування патрулювання поліцією для підвищення ефективності роботи[1] або використання штучного інтелекту для аналізу ДНК, що пришвидшує цей складний процес і сприяє розкриттю злочинів [6].

Однією з технологій, яка використовується правоохоронними органами і зарекомендувала себе з позитивного боку у сфері забезпечення публічної безпеки та порядку, є відеоспостереження. У таких великих містах, як Лондон та Нью-Йорк, встановлено тисячі камер відеоспостереження, що допомагають у роботі поліції. Виявлення розшукуваних злочинців та підозрілих предметів, моніторинг публічних місць, відстеження дорожньої ситуації – усе це можуть виконувати розумні камери відеоспостереження. Велика кількість камер відеоспостереження дає змогу цілодобово стежити за публічним порядком. Наприклад, у 2014 р. стартував проєкт P-REACT, спрямований на розкриття дрібних злочинів шляхом відстеження порушень публічного порядку та попередження про них за допомогою камер відеоспостереження [7].

На особливу увагу заслуговують системи, здатні ідентифікувати людей за обличчям. Серед представлених на ринку вказаних систем можна виокремити три: Corsight AI[2], Clearview Ai[3] та Veritone Identify[4]. Corsight AI – це програма, що ідентифікує людей за обличчям за допомогою відеоданих, відзнятих камерами відеоспостереження. Відмінністю цієї програми є те, що вона дозволяє, окрім ідентифікації людей, ще й відстежувати їх за допомогою камер відеоспостереження. Розроблення Clearview Ai також спрямоване на розпізнавання облич людей, але зі своїми особливостями, центральною серед яких є метод пошуку

[1] Maximize Limited Patrol & Analyst Resources for Highest Impact. Automate Directed Patrol Planning to Better Serve Communities // SoundThinking : сайт. URL: https://www.soundthinking.com/law-enforcement/resource-deployment-resourcerouter/ (дата звернення: 06.04.2024).

[2] Identify Threats in Real Time and Conduct Forensic Investigations with Facial Intelligence // Corsight : сайт. URL: https://www.corsight.ai/law-enforcement/ (дата звернення: 06.04.2024).

[3] Clearview AI. URL: https://www.clearview.ai/clearview-2-0 (дата звернення: 06.04.2024).

[4] Intelligent, rapid suspect identification // Veritone : сайт. URL: https://www.veritone.com/applications/identify/ (дата звернення: 06.04.2024).

людей. Він заснований на пошуку схожих облич у відкритих базах даних, таких як відкриті сайти, соціальні мережі та інші інформаційні ресурси, що надає надзвичайно велику базу даних для ідентифікації та пошуку людей, що може використовуватися для пошуку зниклих безвісти людей. Третю систему – Veritone Identify – розглянемо детальніше.

Veritone Identify – розумна та швидка система ідентифікації підозрюваних для правоохоронних органів. Ця система дає змогу здійснювати пошук правопорушників за відео- та фотоданими, фільтрувати знайдених правопорушників за певними ознаками (вік, стать, зріст, колір волосся, колір очей та етнічна приналежність), об'єднувати потенційних підозрюваних для подальшого розслідування, ділитися списками підозрілих осіб всередині підрозділу та з іншими установами (включно з даними: фото, ім'я, остання відома адреса), об'єднувати інформацію про підозрюваних на централізованій вебплатформі (докази, фотографії, остання відома адреса тощо), упорядковувати докази за справами включно з деталями (ідентифікатор справи, відділ, офіцер, опис, місцезнаходження, час і доступні примітки). Зараз ця система використовується департаментом поліції Південної Каліфорнії.

Робота з програмою Veritone Identify розпочинається зі створення нової справи, для цього необхідно натиснути на кнопку «NEW CASE» (рис. 1, А) відкриється форма, яку необхідно заповнити[1]. У формі зазначається ідентифікатор справи (id), дата та час, назва, опис, до якого підрозділу належить, відповідальна особа, адреса. Далі з'явиться вікно, в якому можна завантажити відеодані, що стосуються цієї справи. Після натиснення кнопки «PROCESS» та обрання необхідної бази даних із зображеннями, здійснюється пошук у ній облич, виявлених на завантажених відеоданих. Спочатку у відеофайлі виділяються всі обличчя, а далі вони вже порівнюються з внутрішньою базою даних. Для перегляду всіх можливих збігів необхідно натиснути на кнопку «VIEW MATCHES», навівши курсор на відеофайл, у якому здійснювався пошук та розпізнавання облич. Також у цьому вікні можна відсортувати отримані збіги за декількома критеріями та визначити людину, схожу на підозрювану. Якщо обличчя підозрюваного не знайшлося в жодній із баз даних, його можна зберегти в базі даних неідентифікованих облич, щоб у подальшому, коли бази даних поповняться новими обличчями, ця людина була ідентифікована.

[1] Intelligent, rapid suspect identification // Veritone : сайт. URL: https://www.veritone.com/applications/identify/ (дата звернення: 06.04.2024).

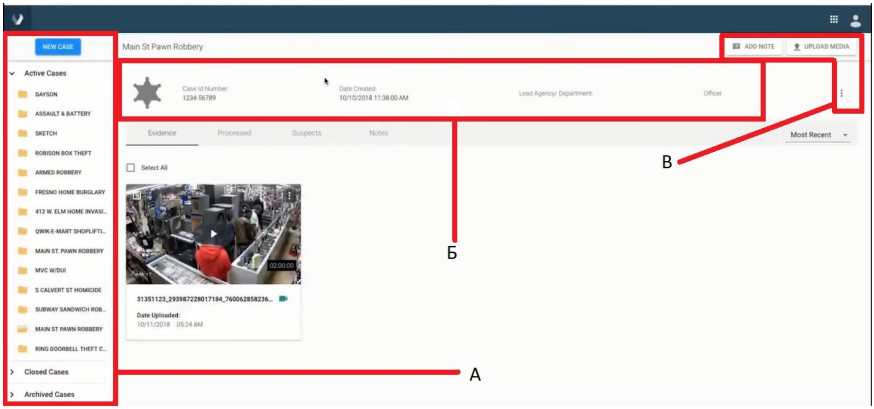

Рис. 1. Робота з програмою Veritone Identify:
А – панель управління справами; Б – вкладка подробиці справи;
В – дії

Коротка інформація про справу (рис. 1, Б) надає інформацію про номер справи, дату і хто відповідальний за неї. За необхідності до створеної справи можна додавати додаткові докази у форматі відеофайлів та додаткові дані про злочин (рис. 1, В).

Упровадження таких систем у правоохоронну діяльність, так само як і поява ШІ в житті людей та інших сферах діяльності, викликає необхідність законодавчого врегулювання використання таких технологій. Уже неодноразово обговорювалася тема законодавчого врегулювання застосування програм з ідентифікації людей за їх обличчям [8; 9; 10]. Нині у Верховній Раді України зареєстрований Проект Закону про захист персональних даних від 25 жовтня 2022 р. № 8153[1], який повинен врегулювати в законодавстві України питання захисту персональних даних, зокрема зображення обличчя людини, автоматично збереженого камерою відеоспостереження. З урахуванням цього та для забезпечення якомога об'єктивного розслідування, в якому використовуються докази, отримані за допомогою програм з ідентифікації людей за обличчям, необхідно окреслити рекомендації щодо проведення таких робіт правоохоронними органами:

[1] Проект Закону про захист персональних даних : від 05.10.2022 № 8153 / ініціатори Р. О. Стефанчук, Є. В. Чернєв, Т. П. Тарасенко та ін. // База даних «Законодавство України» / Верховна Рада України. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення: 06.04.2024).

1) перед початком ідентифікації людини потрібно провести аналіз зображення, з якого проводитиметься розпізнавання підозрюваного. Необхідність цього кроку викликана тим, що процес розпізнавання людини буде більш точним, якщо буде високою якість фото- або відеофайлів, на підставі яких проводитиметься цей процес. Отже, для кращого результату в деяких випадках необхідно покращити якість зображення або відеозапису. Цей крок можна пропустити, якщо в програмі ідентифікації облич буде вбудована функція покращення зображень, що можна пропонувати як стандартну вимогу до таких програм;

2) після ідентифікації людини за допомогою будь-яких програмно-технічних засобів необхідно закріпити факт збігу обличчя, виявленого програмними методами, з тим зображенням, яке використовувалося для порівняння (еталонним зображенням), із застосуванням інших методів доказування: судової експертизи, впізнання. Що більше буде проведено інших слідчих (розшукових) дій, то краще. Зокрема, рекомендовано, щоб принаймні три особи підтвердили правильність ідентифікації людини шляхом її впізнання спочатку за зображеннями, а потім і наживо. Це забезпечить прозорість процесу ідентифікації людини;

3) найголовнішим є те, що збіг при розпізнаванні обличчя людини не повинен бути основною підставою для оголошення підозри та обвинувачення. Якісна слідча робота, спрямована на збір додаткових доказів для підтвердження особи людини та її винуватості, відіграє надзвичайно важливу роль у розслідуванні справи і сприяє ствердженню великого значення застосованих технологій розпізнавання обличчя для встановлення особи злочинця та прив'язки його до факту правопорушення;

4) повинен бути впроваджений журнал як у традиційному, захищеному від підробки, так і в електронному форматі, де буде фіксуватися: за яким фактом, ким, коли було використано програмне забезпечення та інші суттєві дані. Це забезпечить прозорість досліджуваного процесу та довіру суспільства до правоохоронних органів.

Висновки

Застосування програм з інтегрованим ШІ для ідентифікації людей за обличчям мають надзвичайно великі перспективи в забезпеченні публічної безпеки й протидії диверсійній і терористичній діяльності: від моніторингу ситуації в публічних місцях до контролю терористичних загроз шляхом відстеження залишених речей та ідентифікації підозрілих осіб. Нині існує чимало програмно-технічних продуктів, функціонал яких забезпечує виконання таких завдань. Серед розглянутих можна виокремити програму із ШІ Veritone Identify. Ця програма, спрямована на пошук підозрілих осіб за обличчям, має достатній потенціал для пришвидшення роботи правоохоронних органів.

Можливість швидкого поширення інформації про підозрюваного сприятиме прискоренню затримання злочинця.

Зараз активно точаться дискусії щодо доцільності використання камер відеоспостереження та програм, здатних ідентифікувати людей за їх обличчям. Основою таких дискусій є відсутність законодавчого врегулювання захисту приватності та персональних даних людини, якими є зображення її обличчя. На цей час у чинному законодавстві України не врегульовані питання застосування камер відеоспостереження з можливістю ідентифікувати людей за обличчям. Проект Закону про захист персональних даних від 25 жовтня 2022 р. № 8153 містить необхідні законодавчі норми, отже, має врегулювати проблемні питання щодо захисту персональних даних. Додатково необхідно впровадити у практику запропоновані нами рекомендації до проведення розслідування з використанням програм з можливістю ідентифікації людей за обличчям.

Список бібліографічних посилань: 1. Захарчин Н. Г., Захарчин Н. Р. Ріст структурованих та неструктурованих даних та управління ними: загальні аспекти. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки.* 2021. Т. 32 (71), № 5. С. 83–87. DOI: https://doi.org/10.32838/2663-5941/2021.5/13. **2.** 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. **3.** Чашницька Т. Г. Аналіз зарубіжного досвіду у сфері використання систем відеоспостереження. *Нове українське право.* 2022. Т. 2, вип. 6. С. 207–214. DOI: https://doi.org/10.51989/NUL.2022.6.2.32. **4.** Maass D. FBI Wish List: An App That Can Recognize the Meaning of Your Tattoos // Electronic Frontier Foundation : сайт. 16.07.2018. URL: https://www.eff.org/deeplinks/2018/07/fbi-wants-app-can-recognize-meaning-your-tattoos (дата звернення: 06.04.2024). **5.** Weyand T., Kostrikov I., Philbin J. PlaNet – Photo Geolocation with Convolutional Neural Networks // Computer Vision – ECCV 2016 : Conference proceedings of the 14th European Conference (Amsterdam, The Netherlands, October 11–14, 2016) / ed. by B. Leibe, J. Matas, N. Sebe, M. Welling. Cham : Springer, 2016. Part VIII. Pp. 37–55. DOI: https://doi.org/10.1007/978-3-319-46484-8_3. **6.** Regalado A. Investigators searched a million people's DNA to find Golden State serial killer // MIT Technology Review : сайт. 27.04.2018. URL: https://www.technologyreview.com/2018/04/27/240734/investigators-searched-a-million-peoples-dna-to-find-golden-state-serial-killer/ (дата звернення: 06.04.2024). **7.** Revell T. Computer vision algorithms pick out petty crime in CCTV footage // NewScientist : сайт. 01.01.2017. URL: https://www.newscientist.com/article/2116970-computer-vision-algorithms-pick-out-

petty-crime-in-cctv-footage/ (дата звернення: 06.04.2024). **8.** Токарєва К., Савліва Н. Особливості правового регулювання штучного інтелекту в Україні. *Юридичний вісник. Повітряне і космічне право.* 2021. Т. 3, № 60. С. 148–153. DOI: https://doi.org/10.18372/2307-9061.60.15967. **9.** Зачек О. І., Дмитрик Ю. І., Сеник 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. **10.** 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: 06.04.2024).

Надійшла до редколегії 15.04.2024

Прийнята до опублікування 20.05.2024

Zhadan D. O., Mordvyntsev M. V., Pashniev D. V., Khlestkov O. V. Implementation and optimisation of intelligent police systems based on artificial intelligence

The rapid development of artificial intelligence provides new opportunities for law enforcement agencies. Nowadays, the developed countries of the world are increasingly using surveillance cameras to monitor public safety, detect criminals and suspicious objects. The facial identification systems on the market have tremendous potential to help law enforcement agencies. Facial recognition software helps to identify missing persons and criminals whose faces are caught on CCTV cameras. The use of artificial intelligence in such systems accelerates their operation, which, in turn, facilitates the quick search for suspects and their rapid apprehension. Modern video surveillance systems can help counter terrorist attacks by tracking and identifying people and suspicious objects. On the other hand, the issue of personal data protection and privacy when using CCTV cameras to identify people's faces is increasingly being discussed. The obvious solution to this problem is to regulate it at the legislative level, in particular, to introduce guidelines aimed at ensuring transparency and accountability of the use of facial recognition software.

For a more objective understanding of the circumstances which should be regulated by law, the author conducts a study of modern technical solutions in the field of facial identification with integrated artificial intelligence, their features and possibilities of use in the work of the National Police of Ukraine, and also identifies the steps which outline the sequence of actions during objective facial identification of people and ensure the high quality of this process and the reliability of its results.

Key words: video surveillance, identification of people, artificial intelligence, analytical data processing, crime prevention.