

УДК 343.98.065

ПАРФИЛО О.А., кандидат юридичних наук, старший науковий співробітник,
професор кафедри інформаційно-правової культури
та комунікативної політики Укртелерадіопресінституту
ЛЕОНОВ Б.Д., доктор юридичних наук, старший науковий співробітник,
провідний науковий співробітник
Національної академії Служби безпеки України

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ І МЕТОДІВ ВИЯВЛЕННЯ ТА РОЗПІЗНАВАННЯ ОСІБ, ЯКІ МАЮТЬ НАМІР ВЧИНИТИ ТЕРАКТ

***Анотація.** У статті розглядаються актуальні питання застосування сучасних технологій і методів виявлення та розпізнавання осіб, які мають намір вчинити теракт. Аналізується позитивний зарубіжний досвід експлуатації систем виявлення та розпізнавання осіб. Виділяються найбільш оптимальні способи розпізнавання облич.*

***Ключові слова:** розпізнавання облич, особи, які мають намір вчинити теракт, сучасні технології.*

***Summary.** The article deals with urgent questions of the use of state-of-art technologies and methods of person's identification and face recognition (persons who intend to commit a terrorist attack). The positive foreign experience of using the system of person's identification and face recognition is analyzed. Attention is drawn to the best ways of face recognition.*

***Keywords:** face recognition, persons who intend to commit a terrorist attack, state-of-art technologies.*

***Аннотация.** В статье рассматриваются актуальные вопросы применения современных технологий и методов выявления и распознавания лиц, имеющих намерение совершить теракт. Анализируется позитивный зарубежный опыт эксплуатации систем выявления и распознавания лиц. Выделяются наиболее оптимальные способы распознавания лиц.*

***Ключевые слова:** распознавание лиц, лица, имеющие намерение совершить теракт, современные технологии.*

Постановка проблеми. Результати аналізу щоденних повідомлень міжнародних інформангентств підтверджують високий рівень терористичної загрози у світі. Драматичні події, які відбулися 22 травня 2017 року у Манчестері та 17 серпня 2017 року у Барселоні, засвідчили, що проблеми тероризму набули глобального характеру та потребують нових ідей та рішень у боротьбі з цим явищем. Незважаючи на зусилля світового співтовариства у протидії тероризму, непоодинокі терористичні акти практично у всіх країнах світу свідчать про недостатню ефективність створюваних систем протидії терористичній загрозі.

Оскільки тероризм постійно змінює форми та набуває глобального масштабу, його способи і методи стають все більш витонченими та руйнівними. Вступ людства в інформаційну епоху, розвиток науково-технічного прогресу потребує розробки та впровадження новітніх технологій та технічних рішень з метою протидії проявам тероризму. Саме тому в останні роки відбувається все більш широке впровадження технологій біометричної ідентифікації осіб. Зростання інтересу до цих технологій пояснюється швидкозростаючою їх ефективністю та можливостями використання саме за напрямом протидії терористичним загрозам. Підвищення ефективності технологій

біометричної ідентифікації забезпечується зростанням потужності обчислювальної техніки, що робить можливим швидкий пошук у великих базах даних біометричних ознак і дозволяє в реальному часі реалізовувати дедалі складніші та ефективніші алгоритми і набори біометричних ознак.

Біометричні технології можуть бути використані для вирішення різноманітних завдань, серед яких головною є криміналістична ідентифікація людини. Її сутність полягає у пошуку у максимально наповненій базі даних зразків, найбільш схожих з тією, яку ідентифікують. У криміналістиці для цього широко використовують методи габітоскопічної ідентифікації, особливо ідентифікації людини за зображенням обличчя. До переваг системи ідентифікації особистості за зображенням обличчя можна віднести наступні: відсутність фізичного контакту із пристроєм введення даних (особі не потрібно обов’язково дивитися у відеокамеру), прихованість, доступність даних та простота їх отримання.

Водночас, успіх системи ідентифікації особи за фотопортретом багато в чому залежить від точності виявлення, локалізації та розпізнання особи на зображенні.

Результати аналізу наукових публікацій. Окремі аспекти криміналістичного дослідження зовнішності з метою ідентифікації особи висвітлено у працях, авторами яких є: Н. Ахтирська, В. Бахін, Р. Белкін, П. Біленчук, І. Борисенко, І. Винниченко, В. Гарбар, М. Герасимов, В. Гончаренко, Ю. Дубягін, О. Дубягіна, В. Житніков, В. Захаров, О. Зінін, В. Колдін, В. Колмаков, І. Крилов, П. Кузнецов, В. Кузьмічов, В. Лукашевич, Г. Мамедов, І. Мартиненко, Є. Моїсєєв, В. Образцов, М. Салтевський, З. Самошина, М. Сегай, В. Снетков, О. Сокиринська, М. Терзієв, А. Топорков, А. Ухаль, П. Цветков, М. Чернець, В. Шепітько, М. Яблоков та інших учених.

Декілька наукових робіт, зокрема А. Мовчан [1], О. Свістільніков [2], було присвячено застосуванню сучасних технологій для вирішення завдань оперативного розпізнання терористичних загроз.

Разом з тим питання виявлення та розпізнавання осіб, які мають намір вчинити теракт, із застосуванням сучасних інноваційних технологій та методів залишається не до кінця розкритим, що й зумовлює актуальність даного дослідження.

Метою статті є виявлення на основі аналізу позитивного зарубіжного досвіду у сфері боротьби з тероризмом найбільш оптимальних способів розпізнавання осіб, які мають намір вчинити теракт.

Виклад основного матеріалу. Технології та методи розпізнавання осіб в історії криміналістики почали застосовуватися, коли з’явилися перші фотокартки (з XIX-го століття), ще до активного впровадження пошуку людей за відбитками пальців.

Спосіб розпізнавання обличчя людини заснований на тому, що є певні точки і відстані між ними – міжбровна відстань, відстань між зіницями та інші, які не змінюються, як не змінюють зовнішність. Вони відносяться до будови черепа, а не до м’яких тканин. Тобто, борода, вуса і навіть пластичні операції не можуть змінити обличчя настільки, щоб не можна було впізнати особу.

Раніше за допомогою лінійки вимірювали розташування таких точок на обличчі і звіряли з записами на папері. Тепер, в епоху цифрових технологій, камери з високою роздільною здатністю передають дані програмам, які міряють відстань між “вузловими точками” обличчя: довжину і ширину носа, відстань між очима тощо. Потім на інших знімках, навіть в різних ракурсах, можна порівняти відстань між заданими точками і з великою ймовірністю ідентифікувати людей.

Базовим принципом інтелектуальних систем відеоспостереження є відеоаналітика – технологія, що базується на методах та алгоритмах розпізнавання образів і обробки

зображення, автоматизованого збору даних в результаті аналізу відеопотоку. Створені алгоритми без участі людини здатні виявити і відстежити в реальному часі задані цілі (автомобіль, групу людей), потенційно небезпечні ситуації (задимлення, загорання, несанкціоноване втручання в роботу відеокамер) та вчасно видати тривожний сигнал.

Сьогодні одним з основних методів детектування (знаходження) осіб в кадрі є метод, який використовує каскади Хаара. Найчастіше висока точність виявлення досягається для осіб, зображення яких потрапили в кадр анфас, при цьому в загальному випадку класифікатор методу можна навчити розпізнавати зображення обличчя і в інших положеннях.

Що стосується сучасного етапу розвитку технології розпізнавання обличчя, новим рішенням стало використання тривимірного моделювання за допомогою стереокамер. 3D-модель обличчя допомагає досягти значно вищих показників точності. В алгоритм роботи системи додається ще один етап – це побудова 3D-моделі обличчя в режимі реального часу з подальшим аналізом особливостей обличчя вже просторової моделі.

Найбільш популярні системні рішення для розпізнавання осіб “Face-Інтелект” (розробник – компанія AxxonSoft), “Kipod” (компанія Синезис) і “VOCORD FaceControl” (компанія VOCORD) демонструють: високу ймовірність ідентифікації об’єкта (до 99 %); підтримку широкого діапазону кутів повороту відеокамер; можливість виявлення осіб навіть в щільному натовпі; варіативність складання аналітичних звітів. Зокрема, “Face-Інтелект” може використовувати сторонні бази даних осіб, наприклад, урядових установ або правоохоронних органів. Підтримка універсального протоколу обміну даними забезпечує ще більшу ефективність використання таких систем на об’єктах транспортної, спортивної та розважальної інфраструктур [3].

З кожним роком збільшується роздільна здатність відеокамер та удосконалюються самі алгоритми розпізнавання осіб. Сьогодні ці системи працюють досить ефективно в багатьох країнах світу. Наприклад, китайська компанія Cloud Walk тестує систему, що не тільки розпізнає обличчя, але й аналізує ходу людини, місця її перебування і які товари вона купує. Якщо людина, скажімо, відвідує магазини зброї, вона стає підозрілою. За словам представника Cloud Walk, немає нічого кримінального, якщо людина, наприклад, купила кухонний ніж. Але якщо разом з ножем вона ще купила мішок і молоток, а також часто з’являється в місцях масового скупчення, – така особа для системи вважається потенційно небезпечною [4]. Перевага такої системи полягає в тому, що вона працює автономно – сама збирає й обробляє масив даних з відеокамер, і сама повідомляє про підозрілих осіб в правоохоронні органи.

Згідно з даними дослідницької компанії IHS Markit, в Китаї налічується більше 176 мільйонів камер спостереження, очікується, що далі їх число буде лише зростати. На сьогоднішній день владою Китаю вже встановлені системи розпізнавання осіб в навчальних закладах, на вулицях і в місцях масового скупчення людей для запобігання порушенню правил громадської поведінки, дорожнього руху і виявлення випадків девіантної поведінки. За словами заступника Міністра науки й технологій КНР Лі Мена, використання розумних систем і технологій штучного інтелекту дозволить визначати заздалегідь, хто може скоїти щось протизаконне та хто може бути потенційним терористом [5].

Після терактів у Парижі керівництво громадським транспортом у Франції почало впровадження низки заходів із забезпечення безпеки пасажирів. Завдяки припиненому нападу на пасажирів потягу Thalys влітку 2016 року, на всіх вокзалах, що відправляють потяги міжнародних ліній, були встановлені програмно-апаратні комплекси з камерами, датчиками і рамками з металодетекторами. Програмне забезпечення цих

комплексів здатне реєструвати аномальні зміни голосу, температури тіла, ходи, а потім на основі аналізу цих даних попереджати про підозрілу поведінку того або іншого пасажира. Фахівці, знайомі з технікою аналізу поведінки пасажирів, зазначають, що можливо заздалегідь визначити потенційну небезпеку людини, яка має намір здійснити теракт [6].

У Німеччині також запроваджено систему розпізнавання облич. Зокрема, на берлінській залізничній станції Зюдкройц розпочали тестувати систему розпізнавання облич, яка покликана підвищити безпеку людей у громадських місцях. Відеокамери цієї системи розташовані на контрольному пункті і система фіксує всіх пасажирів, що перетинають контрольний рубіж. При виявленні ознак схожості пасажира з розшукуваним злочинцем (що знаходиться в розшуку не лише за злочини терористичного характеру, а й за інші протиправні діяння) система сигналізує про це співробітникам поліції [7].

Існує вулична мережа камер зі схожими алгоритмами розпізнавання і в лондонському Сіті. Поліція Уельсу почала тестування аналогічної технології під час проведення фіналу Ліги чемпіонів в м. Кардіфф. Якщо цей досвід буде визнаний успішним, правоохоронні органи Великої Британії сподіваються розширити використання нових методів для запобігання злочинам. Вони можуть застосовуватися для забезпечення громадської і національної безпеки, наприклад, для контролю ситуації в аеропортах [8].

Слід зазначити, що до цього часу спеціалістами провідних країн світу продовжується розробка програмних продуктів та технічних рішень на працездатність яких не повинні впливати інтенсивність освітлення, раса і вік особи, зміна зачіски, макіяж, окуляри, а також інші фактори.

Завдяки нейромережам системи комп'ютерного зору досягли рекордної точності в розпізнанні облич. Особа людини майже безпомилково розпізнається на звичайних фотографіях, навіть на тих де обличчя видно лише частково. Створені алгоритми, що враховують навіть одяг, ходу та вік людини. Наприклад, OpenFace у 80 % випадках змогла ідентифікувати осіб на змінених “старінням” фото людей.

Розглянемо на прикладі системи розпізнавання на основі відеосканування “FaceVACS” можливості та функціональність таких систем, зокрема:

- відслідковує та ідентифікує одне або багато облич за допомогою відеокамер прямої трансляції або матеріалів відео-зйомки;
- здійснює порівняння у реальному часі з базами даних зображень і списками особливого контролю;
- паралельно обробляє численні потоки зображень з камер і відеоданих;
- здійснює спостереження за громадськими місцями (наприклад, за стадіонами, залізничними вокзалами, аеропортами або конференц-центрами для виявлення та ідентифікації конкретних осіб);
- здійснює спостереження за режимними об'єктами, доступ до яких дозволено лише службовим особам (наприклад, за АЕС, військовими базами, хімічними заводами тощо) для виявлення та ідентифікації зловмисників і сторонніх осіб;
- порівнює зображення обличчя людини з цільовими даними (розшукуваними людьми або підозрюваними у вчиненні терористичних злочинів особами);
- порівнює збіги з наявними оперативними даними або з архівом відеоданих;
- порівняння відбувається з даними, що зберігаються в системі, або з наявними правовими базами даних (національною базою даних, базами ФБР, Інтерполу, власними базами даних тощо), з якими система з'єднана;

- систему можна під'єднати до графічної надструктури систем безпеки, що робить можливим поточний он-лайн-контроль місця, де перебуває особа, за якою ведеться спостереження.

Висновки.

Підсумовуючи вищенаведене, зазначимо, що з огляду на позитивний зарубіжний досвід експлуатації систем виявлення та розпізнавання осіб ці технології ефективно можуть бути використані і в антитерористичній діяльності. Водночас слід відзначити окремі аспекти застосування сучасних технологій виявлення та розпізнавання осіб, які мають намір вчинити теракт, а саме:

1. Більшість провідних країн світу запроваджують системи розпізнавання облич, використовуючи різні технології. Найбільш оптимальним способом розпізнавання облич є 3D-розпізнавання – алгоритм якого має суттєві переваги перед більш ранніми системами, реалізованими за допомогою двовимірного відеозображення. Метод вимагає установки декількох спеціальних стереокамер, синхронізованих між собою.

2. Сьогодні існує декілька легальних способів захисту від оперативного розшуку за допомогою систем розпізнавання облич. Наприклад, як справжні футбольні вболівальники, так і особа, яка має намір проникнути на стадіон інкогніто зі злочинною метою, можуть за допомогою спеціального макіяжу, який візуально змінює геометрію і пропорції обличчя людини, розфарбуватися в кольори футбольного клубу (чи збірної), і тим самим порушити визначення лицьових опорних точок. Оскільки сучасними об'ємними тривимірними камерами обладнано не дуже багато таких систем, розпізнавання розмальованого у такий спосіб обличчя людини з двовимірного “плоского” знімку є досить проблематичним.

3. Політика більшості провідних країн світу виходить із необхідності створення комплексної системи протидії тероризму з боку світової спільноти, що включає: посилення взаємодії правоохоронних та розвідувальних органів, надання допомоги та сприяння в боротьбі з тероризмом, у т.ч. шляхом обміну інформацією щодо терористичних організацій та бойовиків-терористів, включаючи їх біометричні ідентифікаційні дані.

4. Впровадження програмно-апаратних комплексів біометричної ідентифікації людини в правоохоронну діяльність створить технічні можливості для виявлення осіб, причетних до терористичної та іншої протиправної діяльності. Реалізація цієї пропозиції вимагає розробки та впровадження на міжнародному рівні уніфікованого програмного забезпечення, що за критерієм вибіркості охоплюватиме всі ідентифікаційні дані осіб, які підозрюються у терористичній діяльності, відомості про яких містяться у відповідних інформаційних базах правоохоронних органів та спеціальних служб.

Використана література

1. Мовчан А.В. Застосування сучасних технологій для вирішення завдань оперативного розпізнавання терористичних загроз // Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал. – 2013. – № 1(29). – С. 53-61.

2. Свистильников А.Б. Использование автоматизированных информационно-поисковых систем в идентификации личности террориста и предупреждении террористических актов на объектах транспорта. – Режим доступа : <https://cyberleninka.ru/article/n/ispolzovanie-avtomatizirovannyh-informatsionno-poiskovyh-sistem-v-identifikatsii-lichnosti-terrorista-i-preduprezhdenii>

3. Розпізнавання і пошук схожих осіб. – Режим доступу : <http://www.axxonsoft.com/ua/products/intellect/faceintellect>

4. Система распознавания лиц. – Режим доступу : <http://carnegie.ru/commentary/73279>

5. Как в Китае готовятся арестовывать за будущие преступления. – Режим доступа : <https://news.tj/ru/news/world/20171005/kak-v-kitae-gotovyatsya-arestovivat-za-budutshie-prestupleniya>

6. Железные дороги Франции тестируют программу распознавания террористов. – Режим доступа : <http://www.penki.lt/Informacionnye-tehnologii/ZHeleznye-dorogi-Francii-testiruyut-programmu-raspoznavaniya-terroristov.im?id=354192&f=c>

7. У Берліні тестують систему розпізнавання облич у громадських місцях. – Режим доступа : <http://www.eurointegration.com.ua/news/2017/08/23/7070084>

8. Атака на Лондон : 15 главных мер в борьбе с террором. – Режим доступа : http://www.bbc.com/russian/uk/2015/07/150707_london_bombing_changes

9. FaceVACS – система розпізнавання на основі відеосканування. – Режим доступа : <http://vabb.com.ua/service/innovation/faces>

~~~~~ \* \* \* ~~~~~