Научная статья
УДК 343.9
DOI 10.33184/pravgos-2024.2.23

КУТУЗОВ Алексей Владимирович
Севастопольский государственный университет, Севастополь, Россия,
e-mail: kutuzovlist@yandex.ru,
https://orcid.org/0000-0003-2296-7549

Original article

KUTUZOV Alexei Vladimirovich
Sevastopol State University, Sevastopol, Russia.

КРИМИНАЛИСТИЧЕСКАЯ ИДЕНТИФИКАЦИЯ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ РАСПОЗНАВАНИЯ ЛИЦ: СОСТОЯНИЕ ПРОБЛЕМЫ И ПОТЕНЦИАЛЬНЫЕ ПУТИ ЕЕ РЕШЕНИЯ

FORENSIC IDENTIFICATION USING FACIAL RECOGNITION SYSTEMS: STATE OF THE PROBLEM AND POTENTIAL WAYS TO SOLVE IT

Аннотация. *Криминалистическая идентификация личности с использованием систем распознавания лиц представляет собой научный интерес ввиду стремительной цифровизации общества и необходимости оперативного установления злоумышленника. Имплементация передовых технических решений в криминалистику позволяет обогатить теоретический базис, что прямо влияет на эффективность противодействия преступности, в том числе террористического и экстремистского характера. Цель: рассмотреть значение и возможности систем биометрической идентификации по изображению лица для раскрытия и расследования преступлений. Для достижения поставленной цели использовались диалектический, системные и логические методы (общенаучные). Среди частнонаучных методов исследования превалировали формально-юридический, обобщения и абстрагирования. Результаты: рассмотрены вопросы правового регулирования использования биометрических данных в процессе отождествления личности; изучены возможности использования систем распознавания лиц, установленных в общественных местах, на примере крупных городов России; предложены пути повышения эффективности биометрической идентификации по изображению лица в условиях противодействия преступности.*

Ключевые слова: *расследование преступлений, раскрытие преступлений, криминалистическая идентификация, распознавание лиц, биометрическая идентификация, биометрия, цифровые технологии, личность преступника*

Для цитирования: Кутузов А.В. Криминалистическая идентификация с использованием систем распознавания лиц: состояние проблемы и потенциальные пути ее решения / А.В. Кутузов. – DOI 10.33184/pravgos-2024.2.23 // Правовое государство: теория и практика. – 2024. – № 2. – С. 183–191.

Abstract. *Forensic personal identification using facial recognition systems is of scientific interest due to the rapid digitalization of society and the necessity to quickly identify the perpetrator. The implementation of advanced technical solutions in forensics allows to enrich the theoretical basis, which directly affects the effectiveness of countering crimes, including terrorist and extremist crimes. Purpose: to examine the value and capabilities of facial image biometric identification systems for the detection and investigation of crimes. Methods: to achieve the set purpose, dialectical, systemic and logical methods (general scientific) are used. Among specific scientific research methods, formal legal methods, methods of generalization and abstraction prevailed. Results: the issues of legal regulation of the use of biometric data in the process of personal identification are considered; the possibilities of using face recognition systems installed in public places are studied using the example of large cities in Russia. Ways are proposed to increase the efficiency of biometric identification using a facial image in the context of countering crimes.*

Keywords: *crime investigation, crime detection, forensic identification, facial recognition, biometric identification, biometric, digital technologies, criminal identity*

For citation: Kutuzov A.V. Forensic identification using facial recognition systems: state of the problem and potential ways to solve it. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2024, no. 2, pp. 183–191 (In Russian). DOI 10.33184/pravgos-2024.2.23.

Введение

Перед российским обществом наряду с фундаментальными и объективными внешними угрозами, обусловленными в том числе борьбой государства за отстаивание своего суверенитета, стоят внутренние вызовы, к которым, бесспорно, относится преступность. Невзирая на снижение общего количества зарегистрированных преступлений, в том числе совершенных в общественных местах, имеется тенденция к росту преступности в сфере компьютерной информации и незаконного оборота наркотиков[1]. Нельзя обойти вниманием и события последних лет, активизировавшие подпольную деятельность различных террористических группировок, планирующих и осуществляющих деструктивную деятельность, что обязывает правоохранительные органы использовать последние достижения технического прогресса для противодействия преступности.

Криминалистическая идентификация по изображению лица на современном этапе

Расследование преступлений, совершенных в условиях неочевидности, сопряжено со значительными сложностями установления личности злоумышленника. В случаях, когда преступления совершены лицами, ранее не попадавшими в поле зрения правоохранительных органов, особенно молодого возраста, целесообразно опираться на последние разработки криминалистической идентификации. Сказанное относится к широкому спектру уголовно наказуемых деяний: от распространения наркотических средств и психотропных веществ (как правило, с помощью тайников-закладок) до преступлений в сфере компьютерной информации, экстремистского и террористического характера.

Как отмечают исследователи, для идентификации злоумышленника целесообразно использовать разнообразные методики установления, особенно по внешним признакам [1, с. 227]. Не вызывает сомнения утверждение, что криминалистическая идентификация выступает базовым источником тактического обеспечения криминалистической науки и является одной из наиболее разработанной теорией. Слово «идентификация» происходит от латинского idem – «тот же самый». Соответственно, идентификация личности преступника является одной из задач, стоящих перед криминалистикой [2, с. 16]. Криминалистическая идентификация отвечает на один из фундаментальных вопросов криминалистики – позволяет найти сходство между исследуемым образцом и фактическим объектом материального мира. В то же время ошибочно полагать, что результатом идентификации является суждение об идентичности проверяемого и референсного объектов.

Представляется, что биометрическая идентификация лица – достаточно актуальное и важное направление в криминалистике и оперативно-розыскной деятельности. Разработками указанной проблематики занимались С.М. Потапов, Р.С. Белкин, В.Ф. Орлов, Ю.А. Дубягин, Д.А. Степаненко, В.Н. Терехович, А.А. Эксархопуло, И.А. Макаренко и другие представители научного сообщества.

В последние несколько лет публикации М.Ю. Катаева, А.С. Катасёва, Д.В. Катасёвой, А.П. Кирпичникова, В.Н. Чаплыгиной, Д.Ю. Писарева позволили переосмыслить данную категорию с учетом нововведений в законодательстве и последних достижений науки и техники.

Биометрическая идентификация по изображению лица: преимущества и недостатки в противодействии преступности

В широком смысле к биометрическим данным человека можно отнести отпечатки пальцев, фотоизображения, голос, ДНК и др., а наиболее эффективным инструментом является идентификация по отпечаткам пальцев, голосу, физиологическим особенностям (например, по ушной раковине, шрамам или увечьям) и изображению лица.

Идентификация с использованием биометрических данных, в том числе по изображению лица, представляет особый интерес

1 Состояние преступности в Российской Федерации за январь – сентябрь 2023 г. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/42989123/ (дата обращения: 27.11.2023).

в противодействии преступности. К преимуществам биометрической идентификации личности по изображению лица следует отнести скорость распознавания объекта и высокую эффективность. Среди минусов выделяют ресурсозатратность внедрения отдельных технических решений, необходимость создания различных баз данных, дополнительной защиты обрабатываемой информации, проведения последующего выходного контроля.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регламентирует порядок сбора, обработки и хранения персональных данных, в том числе содержащих биометрическую информацию о гражданине. При этом нормы данного закона регулируют обработку только сведений, использующихся непосредственно для идентификации [3, с. 83].

К биометрическим данным законодатель относит информацию как о физиологических особенностях человека, так и его изображение (биологическая характеристика). Постановление Правительства РФ от 4 марта 2010 г. № 125[2] конкретизирует нормы Федерального закона «О персональных данных» и вводит категорию «цветное цифровое фотографическое изображение лица», а приказ Минкомсвязи России от 25 июня 2018 г. № 321[3] устанавливает порядок получения биометрических данных (изображение и голос).

В рамках обозначенной проблематики считаем нецелесообразным детально анализировать и характеризовать нормы законодательства, лишь отметим, что криминалистическая идентификация лица в рамках выполнения правоохранительной функции государства не требует согласия гражданина (в отличие от банковской деятельности и других случаев).

В ходе раскрытия и расследования преступлений перед оперативными и следственными органами встает вопрос об установлении личности злоумышленника. Наряду с традиционными криминалистическими методами используются передовые цифровые технологии. Благодаря активному внедрению систем фото-, видеофиксации, установленным в общественных местах, позволяющим фиксировать на магнитный носитель данные об окружающей обстановке (транспортных средствах, людях и событиях), значимость идентификации преступника по геометрии лица не вызывает сомнения. По мнению исследователей, данная технология наиболее приемлема для использования общественными институтами и органами государственной власти [4].

К востребованным направлениям в биометрической идентификации по изображению лица относится так называемая 2D и 3D идентификация. Фундаментальным отличием детектирования в трехмерном пространстве является построение соответствующей 3D модели [5, с. 96]. Данный способ более точен, однако технически сложно реализуем и дорогостоящ (наличие нескольких камер, необходимость внедрения дополнительного специализированного программного обеспечения и др.). Обнаружение сходства в 2D пространстве (фотоизображения) имеет значительные недостатки, что приводит к вероятности появления ошибок ввиду малого объема биометрических данных.

Выделяют 2 основных вида ошибок:

FRR – ошибка неправильного отказа в случае нераспознания объекта по представленному образцу;

FAR – ошибка неправильного пропуска, то есть детектирование объекта, не соответствующего образцу.

При решении задач оперативно-розыскной деятельности и в рамках криминалистической идентификации, как правило, используются именно статичные изображения лиц, объектов, предметов (в том числе ввиду накопления различных банков фотоизображений). Распознание же лиц происходит в несколько этапов. Первоначально система детектирует

2 О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию : постановление Правительства РФ от 04.03.2010 № 125 // Доступ из справ.-правовой системы «КонсультантПлюс».

3 Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации : приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.06.2018 № 321 // Доступ из справ.-правовой системы «КонсультантПлюс».

лицо из видеопотока, если имеются несколько лиц, каждому присваивается отдельный номер (атрибут). Второй этап предполагает построение точек на лице идентифицируемого объекта. Программные комплексы в большинстве случаев оперируют различными геометрическими характеристиками лица, то есть расстоянием от его определенных точек. Геометрический метод базируется на основе различных геометрических расстояний и углов между чертами. На третьем этапе система преобразовывает полученное изображение, на четвертом создается математический образ (используются дескрипторы, оценивающие лицо без посторонних факторов – прическа, головной убор и пр.). Заключительным этапом выступает непосредственно сопоставление полученной математической модели с изображениями, загруженными в банк данных [6, с. 169].

Потенциальное решение проблемы низкой точности распознавания лица лежит в плоскости использования нейронной сети глубинного типа. Типовая нейронная сеть являет собой математическую модель, базирующуюся на нескольких слоях элементов, выполняющих параллельные вычисления [7, с. 159]. Нейросети последнего поколения позволяют ориентироваться на иные параметры, а не только на контрольные точки, так как обладают возможностью комплексного оперирования миллионами ранее проанализированных критериев. Также нейросети позволяют реконструировать поврежденные фотоизображения, воссоздавать утраченные особенности, что важно при розыске без вести пропавших лиц или идентификации неопознанных трупов по фрагментам тела [8, с. 332].

В 2020 г. МВД России была разработана и внедрена в эксплуатацию система биометрической идентификации лиц по фотоизображениям – ИБД-Ф «Опознание». Данная система написана на языке Python, а обработка значительного массива данных происходит с помощью фреймворка Celery. По состоянию на начало 2021 г. модуль «Опознание» обрабатывал до 10 млн фотоизображений в сутки [9, с. 14].

Таким образом, обозначив правовой базис, некоторые технические особенности, а также обосновав необходимость применения возможностей биометрической идентификации лиц в целях противодействия преступности, остановимся на опыте правоохранительных органов и органов государственной власти различных субъектов Российской Федерации, что особенно актуально в настоящее время.

Особый интерес вызывают именно системы распознавания лиц, установленные в общественных местах. Они позволяют в режиме реального времени детектировать конкретное лицо, маршрут его передвижения, определять потенциальные места интереса, а также устойчивые связи. Иные программные комплексы способны анализировать паттерны поведения определенных лиц и выявлять отклонения, характерные для потенциальных злоумышленников (образы террористов-смертников, агрессивных футбольных фанатов, приверженцев различных радикальных организаций), а некоторые аппаратно-программные комплексы (далее – АПК) располагают функционалом идентификации человека по его походке.

Использование аппаратно-программных комплексов видеофиксации данных, установленных в общественных местах, для раскрытия и расследования преступлений

Проведенный анализ технических особенностей используемых АПК показал, что в отдельных субъектах Российской Федерации введены в эксплуатацию системы распознавания, построенные на различных технических решениях, в том числе учитывающие опыт регионов, ранее их внедривших.

В подавляющем большинстве случаев используются аппаратно-программные решения компаний «ЦРТ», NtechLab. По заявлениям разработчиков, их комплексы сочетают возможности онлайн-реагирования на инциденты, интеграции в существующую инфраструктуру, имеют собственные базы данных и позволяют автоматически проводить поиск лиц. Примечательно, что оба решения использовались во время проведения чемпионата мира по футболу в 2018 г. и показали высокую эффективность.

Наиболее развита система биометрической идентификации по изображению лица в Москве. По состоянию на 2020 г. система видеоаналитики, функционирующая в составе

Государственной информационной системы «Единый центр хранения и обработки данных», использовалась 20 067 раз при осуществлении оперативно-розыскной деятельности. При этом идентифицировано 11 лиц, ранее причастных к совершению преступлений экстремистского характера [10, с. 178]. Кроме того, правительством Москвы введена в эксплуатацию государственная автоматизированная система «Сфера»[4], функционирующая в общественном транспорте столицы.

Анализ нормативной базы функционирования данной системы позволил выделить основные направления ее использования, среди них «повышение уровня антитеррористической защищенности объектов транспортной инфраструктуры и на транспорте». В этих целях осуществляется автоматический сбор, хранение и обработка информации с последующим анализом видеопотока с камер видеонаблюдения, расположенных в транспорте общего пользования и объектах транспортной инфраструктуры Москвы.

В Южном федеральном округе тоже активно внедряются возможности систем сбора, хранения и анализа изображений, установленных в общественных местах. В 2018 г. в целях обеспечения безопасности при проведении чемпионата мира по футболу в Ростове-на-Дону была запущена система идентификации лиц. По имеющимся сведениям, она оперировала информацией из базы данных о лицах, находившихся в федеральном или международном розыске[5]. В 2022 г. тестовая эксплуатация системы распознавания лиц, насчитывавшая 25 камер в Центральной части Ростова-на-Дону и 22 камеры, интегрированные в домофоны, показала свою эффективность в 90 %, что говорит о значительном потенциале данной технологии[6].

Представляется интересным опыт Краснодарского края. Так, по данным ряда СМИ, в 2021 г. возможности системы распознавания лиц применялись для идентификации лиц, участвовавших в несанкционированных акциях протеста в поддержку лидера экстремистской организации. По состоянию на май 2023 г. на территории Анапы запущена система «Купол», насчитывающая 650 камер видеонаблюдения, охватывающая 80 % пляжных территорий и обрабатывающая видеоданные из торговых центров, объектов инфраструктуры[7]. В планах до 2025 г. предполагается внедрение данного комплекса на территории всего Краснодарского края.

На совещании при Секретаре Совета Безопасности было заявлено об активизации работ по запуску системы видеоконтроля и видеоаналитики в рамках системы «Безопасный город»[8]. Заметим, что «Безопасный город» является наиболее распространенным названием подобных систем, используемым разработчиками. С определенной долей уверенности можно констатировать, что именно под данным названием будут в дальнейшем создаваться и функционировать большинство АПК на территории Российской Федерации.

В самом же Краснодаре АПК, разработанный на территории края, в 2022 г. позволил раскрыть 250 преступлений. Особенностью системы является синергия распознавания физических лиц и государственных номеров. По состоянию на указанный период планировалось введение в эксплуатацию порядка 1200 средств слежения, с акцентом на установку в жилых районах, что обусловлено спецификой совершения противоправных действий[9].

Обращает на себя внимание тот факт, что упомянутый программный комплекс активно

4 О государственной автоматизированной информационной системе «Сфера» : постановление правительства Москвы от 17.03.2021 № 328-ПП [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс».

5 Не голос, а математика: как развивают биометрию в Ростовской области [Электронный ресурс]. URL: https://rostov.rbc.ru/rostov/26/03/2020/5e7c7b059a79476f613986dd (дата обращения: 03.11.2023).

6 Выступление начальника ГУ МВД России по Ростовской области генерал-лейтенанта полиции О.П. Агаркова на заседании Законодательного собрания Ростовской области 22.02.2022 [Электронный ресурс]. URL: https://media.mvd.ru/files/embed/2358391 (дата обращения: 03.11.2023).

7 Всех накроют куполом: стало известно, что обсуждали главы курортов Кубани в Сочи [Электронный ресурс]. URL: https://sochi1.ru/text/gorod/2023/05/17/72313406 (дата обращения: 03.11.2023).

8 В Краснодарском крае до конца года запустят систему распознавания лиц [Электронный ресурс]. URL: https://ug.tsargrad.tv/news/v-krasnodarskom-krae-do-konca-goda-zapustjat-sistemu-raspoznavanija-lic_820396 (дата обращения: 03.11.2023).

9 В Краснодаре за год раскрыли 250 преступлений благодаря системе «Безопасный город» [Электронный ресурс]. URL: https://ug.tsargrad.tv/news/v-krasnodareza-god-raskryli-250-prestuplenij-blagodarja-sisteme-bezopasnyj-gorod_686318?ysclid=lojzt0hxxh272181827 (дата обращения: 04.11.2023).

внедряется и в других субъектах Российской Федерации. Например, по состоянию на май 2023 г. на территории Волгоградской области установлено 2711 видеокамер, однако только 200 из них имеют возможность детектирования правонарушителей на основе искусственного интеллекта. Дальнейшее развитие будет происходить не только в направлении наращивания количества точек фиксации фото- и видеоизображений, но и добавления функционала биометрической аналитики[10].

В 2021 г. в Севастополе запущен, а позднее введен в эксплуатацию АПК «Безопасный город»[11], среди возможностей которого декларирована функция обнаружения и распознавания лиц в режиме реального времени и с архивной видеозаписи[12]. УМВД России по г. Севастополю с помощью данного комплекса проводится опознание злоумышленников, что подтверждается положительными результатами в части установления местонахождения лиц, объявленных в федеральный розыск, а также причастных к совершению преступлений.

В отличие от Ростовской области и Краснодарского края АПК, развернутый на территории Севастополя, имеет кратно большее соотношение количества камер к площади и численности населения, а также в нем заложен функционал для работы с алгоритмами видеоанализа. Среди иных возможностей разработчики выделяют детектирование массового скопления людей и автоматическое распознавание лиц – сопоставление лиц людей с контрольными списками, загруженными в систему.

Затронув проблематику количества видеокамер, нельзя не упомянуть опыт Москвы. Так, по материалам открытых источников, в составе системы «Безопасный город» только на конец 2020 г. было подключено более 173 000 камер, полностью охватывавших столицу[13]. В рамках проведенного исследования возможностей программно-аппаратных комплексов можно сделать вывод о том, что правоохранительные органы имеют обширный инструментарий для криминалистической идентификации лиц, причастных к противоправной деятельности.

Проблемные вопросы использования аппаратно-программных комплексов «Безопасный город» в оперативной и следственной деятельности и пути их решения

К сожалению, при решении задач борьбы с терроризмом, экстремизмом и иными видами преступности правоохранительные органы сталкиваются с общими проблемами. Таковой является не столько поэтапное внедрение систем видеоконтроля в общественных местах, сколько отсутствие единой базы данных, позволяющей отождествить лицо на фотоизображении или видеозаписи, в силу особенностей функционирования банков данных различных правоохранительных органов и государственных организаций (учреждений).

Рассмотрим одну из типичных следственных ситуаций: лицо, совершившее преступление, не установлено, правоохранительные органы располагают лишь его фотоизображением. Следователь направляет поручение органу, осуществляющему оперативно-розыскную деятельность, на установление лица. Оперативный сотрудник проводит идентификацию по всем имеющимся ведомственным учетам, однако при использовании городских систем распознавания лиц по камерам видеонаблюдения идентифицировать злоумышленника не представляется возможным ввиду отсутствия базы данных, позволяющей сопоставить имеющееся изображение с референсом в ведомственных базах данных. Кроме того, качество самих фотоизображений лиц зачастую не позволяет проводить идентификацию. Передача же массива

10 Региональная система видеонаблюдения способствует безопасности жителей Волгоградской области [Электронный ресурс]. URL: https://kit.volgograd.ru/current-activity/cooperation/news/463350/?sphrase_id=875225 (дата обращения: 03.11.2023).

11 Опытная эксплуатация АПК «Безопасный город» начнется в мае [Электронный ресурс]. URL: https://sev.gov.ru/info/news/145240/?sphrase_id=3250201 (дата обращения: 03.11.2023).

12 Внедрение аппаратно-программного комплекса «Безопасный город» в Севастополе [Электронный ресурс]. URL: https://dcr.sev.gov.ru/files/iblock/b51/BezopGor.pdf (дата обращения: 03.11.2023).

13 Единое хранилище данных [Электронный ресурс]. URL: https://ehd.moscow/index.php?id_src=441&id_ind=900&id_tab=1&action=show_details_90open&show=inds&show_full=1&exist=1&source=-9997&id_root[0]=441_441&id_root[1]=441_900 (дата обращения: 03.11.2023).

фотоизображений от различных органов государственной власти требует наличия законодательно урегулированных оснований, а также технической возможности хранения, обработки и пополнения данных, в том числе с учетом возможности обновления. Вынуждены констатировать, что данная проблематика имеет место во многих регионах и в каждом случае решается индивидуально.

В данном контексте резонно возникает вопрос о потенциальном нарушении прав человека и гражданина при сборе информации о нем, надежности хранения и обработки персональных данных. В эпоху производства так называемых дипфейков и возможностей подделки любой информации отождествление личности при помощи камер наружного видеонаблюдения, установленных не в рамках систем «Безопасный город» и подобных, требует более тщательного подхода к верификации исходных сведений. При наличии сомнений у любой из заинтересованных сторон полученные фото- и видеоматериалы могут быть проверены в рамках проведения комплекса оперативно-розыскных мероприятий или соответствующих следственных действий.

Считаем, что урегулировать описанные правоотношения возможно путем формирования централизованных учетов хранения информации. ПАО «Ростелеком» является оператором и разработчиком Единой биометрической системы (далее – ЕБС), созданной в соответствии с распоряжением Правительства РФ от 22 февраля 2018 г.[14], функционирующей в интересах банковского сектора. Оператор системы осуществляет не только обработку биометрических данных конкретных лиц, но и сбор и хранение таких данных в целях осуществления удаленной финансовой деятельности (открытие счетов, проведение денежных операций).

К особенностям формирования ЕБС относится процедура сбора данных, фотографирование человека согласно правилам фотосъемки, а также срок хранения информации – 50 лет. При этом идентификация возможна не позднее 3 лет после отбора персональных данных или отказа клиента от обработки данных. Таким образом, система, в отличие от фотоизображений, используемых правоохранительными органами, обладает не только полной, но и релевантной информацией. Безусловно, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[15] регламентирует обязанность оператора ЕБС передавать сведения правоохранительным органам, однако это не решает фундаментальной задачи – опознания лица в режиме реального времени в превентивных целях или в целях раскрытия преступлений по горячим следам. Одним из потенциальных прообразов такой системы может стать упомянутая государственная автоматизированная система «Сфера».

Заключение

На наш взгляд, именно синергия всей биометрической информации о физических лицах, имеющейся у государственных органов, учреждений и организаций, позволит наиболее эффективно проводить идентификацию лиц в интересах правоохранительных органов. Отсутствие действенной интеграции единой централизованной системы хранения всех данных о физических особенностях граждан Российской Федерации и иностранных гражданах в определенной мере усложняет процесс опознания лиц, что негативно сказывается на эффективности использования передовых методов и способов установления личности злоумышленников.

Представляется необходимым в первую очередь законодательно урегулировать вопросы взаимодействия различных ведомств. Например, искомое лицо находится в ином субъекте Российской Федерации, где фиксируется на камерах видеонаблюдения, однако его данные неизвестны ввиду наличия нерелевантного фотоизображения в базе данных или оно идентифицируется, однако отсутствуют сведения о его потенциальной причастности к противоправной деятельности. В настоящее

14 Распоряжение Правительства РФ от 22.02.2018 № 293-р // Доступ из справ.-правовой системы «КонсультантПлюс».

15 Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

время правоохранительные органы ограничены в возможностях обмена сведениями, а для проверки фотоизображения по системам видеоаналитики необходимо направлять соответствующие запросы в органы местного самоуправления или территориальные органы внутренних дел. Данный порядок отрицательно влияет на скорость и качество проведения оперативно-розыскных мероприятий и следственных действий.

Считаем, что рассмотренная проблематика обладает значительным потенциалом в использовании правоохранительными органами. Местные власти в тесном сотрудничестве с силовыми структурами и заинтересованными ведомствами проводят комплекс мероприятий по увеличению количества наружных камер видеонаблюдения, устанавливаемых в наиболее посещаемых общественных местах. Принимая во внимание особую террористическую угрозу в приграничных регионах, имеются основания полагать о скорой активизации работы в данном направлении.

Список источников

1. Куликов А.В. Личность террориста: современные методики определения / А.В. Куликов, О.А. Шелег // Известия ТулГУ. Экономические и юридические науки. – 2022. – № 4. – С. 27–33.
2. Эксархопуло А.А. К вопросу о сущности криминалистической идентификации / А.А. Эксархопуло, И.А. Макаренко // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. – 2019. – № 2. – С. 12–19.
3. Кривогин М.С. Особенности правового регулирования биометрических персональных данных / М.С. Кривогин // Право. Журнал Высшей школы экономики. – 2017. – № 2. – С. 80–89.
4. Методы обработки и распознавания изображений лиц в задачах биометрии / Г.А. Кухарев, Е.И. Каменская, Ю.Н. Матвеев и др. ; под ред. М.В. Хитрова. – Санкт-Петербург : Политехника, 2013. – 388 с.
5. Частикова В.А. Аналитический обзор методов идентификации личности на основе биометрических характеристик / В.А. Частикова, А.А. Титова, Д.О. Войлова // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. – 2022. – № 1 (296). – С. 92–112.
6. Фролова Е.Ю. Идентификация человека по биометрическим данным: обзор современных технологий / Е.Ю. Фролова, Ю.А. Кошлыкова // Северо-Кавказский юридический вестник. – 2022. – № 3. – С. 167–174.
7. Шатов Д.В. Лицевая биометрия и нейронные сети в криминалистике: современные возможности и проблемы применения / Д.В. Шатов, С.С. Барсуков, И.Н. Шипанов // Юрист-правоведъ. – 2023. – № 1 (104). – С. 155–163.
8. Щеголева Н.Л. Применение методов лицевой биометрии в криминалистике / Н.Л. Щеголева // Криминалистика и судебная экспертиза: прошлое, настоящее, взгляд в будущее : материалы ежегодной международной научно-практической конференции. – Санкт-Петербург, 2017. – С. 331–335.
9. Булгаков Д.Ю. Особенности организации распределенных вычислений в облачной инфраструктуре ИСОМ МВД России / Д.Ю. Булгаков // Академическая мысль. – 2021. – № 1 (14). – С. 13–15.

References

1. Kulikov A.V., Sheleg O.A. The identity of a terrorist: modern methods of determining. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = News of the Tula State University. Economic and Legal Sciences*, 2022, no. 4, pp. 27–33. (In Russian).
2. Eskarhpulo A.A., Makarenko I.A. On the essence of forensic identification. *Vestnik Baltijskogo federal'nogo universiteta im. I. Kanta. Seriya: Gumanitarnye i obshchestvennye nauki = Vestnik of Immanuel Kant Baltic Federal University. Series: Humanities and Social Science*, 2019, no. 2, pp. 12–19. (In Russian).
3. Krivogin M.S. Peculiarities of legal regulating biometric personal data. *Pravo. Zhurnal Vysshey shkoly ekonomiki = Law. Journal of the Higher School of Economics*, 2017, no. 2, pp. 80–89. (In Russian).
4. Kukharev G.A., Kamenskaya E.I., Matveev Yu.N. et al.; M.V. Khitrov (ed.). Methods of processing and recognition of facial images in biometric tasks. Saint Petersburg, Politekhnika Publ., 2013. 388 p.
5. Chastikova V.A., Titova A.A., Voylova D.O. Analytical review of personal identification methods based on biometric characteristics. *Vestnik Adygejskogo gosudarstvennogo universiteta. Seriya: Estestvenno-matematicheskie i tekhnicheskie nauki = Bulletin of the Adyghe State University. Series: Natural-Mathematical and Technical Sciences*, 2022, no. 1 (296), pp. 92–112. (In Russian).
6. Frolova E.Yu., Koshlykova Yu.A. Human identification based on biometric data: a review of modern technologies. *Severo-Kavkazskij yuridicheskij vestnik = North Caucasus Legal Vestnik*, 2022, no. 3, pp. 167–174. (In Russian).
7. Shatov D.V., Barsukov S.S., Shipanov I.N. Facial biometry and neural networks in forensic science: modern opportunities and problems of application. *Jurist-Pravoved = Lawyer-Jurist*, 2023, no. 1 (104), pp. 155–163. (In Russian).
8. Shchegoleva N.L. Application of facial biometrics methods in forensic science. *Forensic science and forensic examination: past, present, look into the future. Materials of the annual international scientific and practical conference.* Saint Petersburg, 2017, pp. 331–335. (In Russian).

10. Кузьмин Н.А. О некоторых возможностях использования искусственного интеллекта в системе АПК «Безопасный город» при раскрытии преступлений в г. Москве / Н.А. Кузьмин, А.Ю. Половинка // Вестник Московского университета МВД России. – 2021. – № 5. – С. 177–180.

9. Bulgakov D.Yu. Features of the distributed computing organization in the cloud Infrastructure of ISOD of the MIA of Russia. *Akademicheskaya mysl' = Academic Thought*, 2021, no. 1 (14), pp. 13–15. (In Russian).

10. Kuzmin N.A., Polovinka A.Yu. About some possibilities of using artificial intelligence in the agro-industrial complex «Safe city» in solving crimes in Moscow. *Vestnik Moskovskogo universiteta MVD Rossii = Vestnik of Moscow University of the Ministry of Internal Affairs of Russia*, 2021, no. 5, pp. 177–180. (In Russian).

Информация об авторе

Кутузов Алексей Владимирович – кандидат юридических наук, доцент базовой кафедры «Цифровая и традиционная криминалистика» Юридического института.

Information about the Author

Kutuzov Alexei Vladimirovich – Candidate of Sciences (Law), Assistant Professor of the Basic Department «Digital and Traditional Criminalistics» of the Law Institute.

Статья поступила в редакцию 24.12.2023; одобрена после рецензирования 28.01.2024; принята к публикации 29.01.2024.
The article was submitted 24.12.2023; approved after reviewing 28.01.2024; accepted for publication 29.01.2024.