



Facial recognition technologies in ensuring public safety: foreign experience and development prospects

Lyudmila YUGAY¹

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

ARTICLE INFO

Article history:

Received December 2021

Received in revised form

15 December 2022

Accepted 20 January 2022

Available online

15 February 2022

Keywords:

artificial intelligence,
machine learning,
face recognition,
computer vision,
public safety,
fundamental human rights.

ABSTRACT

The article discusses the implementation of intelligent video surveillance and monitoring systems for the purpose of crime detection and investigation. In the work is presented a systematic analysis of law enforcement practice, which indicates the relevance of the use of video and photographic materials in ensuring public order and security, their presentation as evidence in the disclosure and investigation of crimes. The advanced foreign experience of using facial recognition technology in anti-crime activities is considered on the example of the People's Republic of China, Great Britain, the EU countries, the Russian Federation, the Republic of Belarus and other countries. Also, the Chinese, European and mixed models of the functioning of "smart cities" based on intelligent video surveillance systems have been identified. The opinions and views of scientists on the introduction of facial recognition technologies based on artificial intelligence technology, machine learning and neural networks are analyzed. The author raises the issue of the need to respect the fundamental rights and freedoms of citizens, to ensure the confidentiality of private life and to ensure the safety of biometric personal data. In this connection, it is proposed to develop and adopt the Concept of the national biometric identification system and the Law of the Republic of Uzbekistan "On State biometric registration".

2181-1415/© 2022 in Science LLC.

DOI: <https://doi.org/10.47689/2181-1415-vol3-iss1/S-pp278-287>

This is an open access article under the Attribution 4.0 International (CC BY 4.0) license (<https://creativecommons.org/licenses/by/4.0/deed.ru>)

¹ Doctor of Philosophy (PhD) in Law, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan. Tashkent, Uzbekistan. E-mail: yugai.lyudmila@mail.ru.

Жамоат хавфсизлигини таъминлашда юз қиёфаси бўйича аниқлаш технологиялари: хорижий тажриба ва ривожланиш истиқболлари

Калит сўзлар:

сунъий интеллект, машина таълими, юз қиёфаларини аниқлаш, компьютерда кўриш, жамоат хавфсизлиги, фундаментал инсон ҳуқуқлари.

АННОТАЦИЯ

Мақолада жиноятларни фош қилиш ва тергов қилиш мақсадида интеллектуал видеокузатув ва мониторинг тизимини жорий қилиш масалалари таҳлил қилинган. Шунингдек, ҳуқуқни қўллаш амалиётининг тизимли таҳлили тақдим этилган бўлиб, унга кўра, жамоат тартиби ва хавфсизлигини таъминлашда видео ва фотоматериаллардан фойдаланиш, уларни жиноятларни фош қилиш ва тергов қилишда далил сифатида тақдим этишнинг долзарблиги исботланади. Шу билан бир қаторда, Хитой Халқ Республикаси, Буюк Британия, Европа Иттифоқи мамлакатлари, Россия Федерацияси, Беларусь Республикаси ва бошқа мамлакатлар мисолида жиноятчиликка қарши курашда юз қиёфасини аниқлаш технологияларини қўллаш бўйича илғор хорижий тажриба ўрганилган. Хусусан, интеллектуал видеокузатув тизимига асосланган “ақлли шаҳарлар” амал қилишининг Хитой, Европа ва аралаш моделлари таҳлил қилинган. Қатор олимларнинг сунъий интеллект, машина таълими ва нейротармоқлар технологияларига асосланган тизимларини жорий қилиш бўйича қарашлар ва фикрлар ўрганилади. Муаллиф томонидан инсон ҳуқуқларининг асосий ҳуқуқ ва эркинликларини таъминлаш, шахсий ҳаёт дахлсизлиги ва шахсий биометрик маълумотларни сақлашни таъминлаш масаласи кўриб чиқилган. Шу муносабат билан шахсни биометрик идентификациялаш миллий тизими Концепцияси ҳамда Ўзбекистон Республикасининг “Давлат биометрик рўйхатга олиш тўғрисида”ги Қонунини қабул қилиш тавсия этилади.

Технологии распознавания лиц в обеспечении общественной безопасности: зарубежный опыт и перспективы развития

Ключевые слова:

искусственный интеллект, машинное обучение, распознавание лиц, компьютерное зрение, общественная безопасность, фундаментальные права человека.

АННОТАЦИЯ

В статье рассматриваются вопросы внедрения системы интеллектуального видеонаблюдения и мониторинга в целях раскрытия и расследования преступлений. Представляется системный анализ правоприменительной практики, которая свидетельствует об актуальности использования видео- и фотоматериалов при обеспечении общественного порядка и безопасности, их представления в качестве доказательств при раскрытии и расследовании

преступлений. Рассматривается передовой зарубежный опыт использования технологии распознавания лиц в деятельности по противодействию преступности на примере Китайской Народной Республики, Великобритании, стран Евросоюза, Российской Федерации, Республики Беларусь и других стран. Определены китайская, европейская и смешанные модели функционирования «умных городов», основанных на системах интеллектуального видеонаблюдения. Анализируются мнения и взгляды учёных относительно внедрения технологий распознавания лиц, основанных на технологии искусственного интеллекта, машинного обучения и нейросетей. Автором поднимается вопрос необходимости соблюдения основополагающих прав и свобод граждан, обеспечения конфиденциальности частной жизни и обеспечения сохранности биометрических персональных данных. В связи с чем, предлагается разработать и принять Концепцию национальной системы биометрической идентификации личности и Закон Республики Узбекистан «О государственной биометрической регистрации».

ВВЕДЕНИЕ

Развитие научно-технического прогресса в обществе расширило возможности по использованию инновационных подходов в деятельности по обеспечению общественного порядка и безопасности. Высокотехнологичные решения позволяют ускорить процессы сбора и анализа поступающей криминалистически значимой информации. Видео- и фотоматериалы могут использоваться для предотвращения, раскрытия и расследования преступлений, что обуславливает активное внедрение в деятельность по противодействию преступности передовых средств видеонаблюдения.

И.А. Шашкова отмечает о тенденции перехода к глобальному информационному сообществу с развитой системой информационных телекоммуникаций (инфокоммуникаций), одним из проявлений которого является повсеместное распространение средств видеонаблюдения. Данные средства включают в себя инфракрасные видеокамеры, оснащенные датчиком движения, стоящие на охране границы; система наблюдения за автодорогами, следящая за скоростным режимом, распознающая и сверяющая номера автомобилей, проверяя их по базам данных угнанных автомобилей, системы видеонаблюдения для обеспечения охраны банков, торговых центров, развлекательных учреждений, промышленных предприятий, других коммерческих и некоммерческих организаций. Также камерами наружного видеонаблюдения оборудуются места массового скопления людей и это, как правило, парки, скверы, площади, рынки и торговые центры [1. С. 236–241].

А.М. Израелян, Г.М. Израелян, Д.Н. Климова справедливо отмечают, что за последние годы компьютерное зрение набрало большую популярность в сфере информационных технологий и выделилось в отдельное направление. Глубина проникновения технологий в разных отраслях настолько велика, что трудно

представить, где она не применяется. Методы распознавания и глубокого обучения нейросетей – это одно из актуальных направлений в развитии информационных технологий, систем безопасности и автоматизации на производстве [2. С. 111–114].

Материалы и методы. Анализ правоприменительной практики органов внутренних дел Республики Узбекистан свидетельствует о том, что за прошедший 2021 г. наблюдается ощутимый рост проведенных портретных идентификаций по сравнению с 2020 г. на 260,5%, из которых идентификация по фотоизображениям возросла за указанный период на 295,2%, а по видеоматериалам – на 392,1% [3].

М.С. Мочалов и М.В. Медведев отмечают, что на сегодняшний день идентификация людей является одной из актуальных задач цифровой обработки изображений и компьютерного зрения в создании интеллектуальных систем обеспечения безопасности [4. С. 64–65].

Внедрение интеллектуальных систем видеонаблюдения с применением искусственного интеллекта (далее по тексту – ИИ) и нейросетей является современным мировым трендом. Представляет интерес передовой зарубежный опыт стран, которые являются флагманом в развитии высокотехнологичных инноваций.

Китай является мировым лидером по разработке и внедрению искусственного интеллекта. Развитию проектов, связанных с искусственным интеллектом уделяется особое внимание со стороны руководства страны на самом высоком уровне. Если размер мирового рынка этой сферы в среднем растет на 26,2% в год, то в Китае этот показатель составляет 44,5% в год [5. С. 588–606]. Разработка систем идентификации фото- и видеоизображений включены в «Трехлетний план содействия развитию индустрии искусственного интеллекта (2018–2020 гг.)», включающий конкретные мероприятия и принципы развития ИИ в Китае [6]. Известные китайские IT-гиганты Hikivison, Dahua, iFlyTek, SenseTime и Jiadu занимаются разработкой и реализацией данных инновационных проектов.

Необходимо отметить, что 8 из 10 наиболее «наблюдаемых» мировых городов находятся в Китае. Другие два города – Это Лондон и Атланта [7]. Камеры обеспечивают безопасность территории, в отдельных случаях фиксируют противоправное деяние или лицо, совершившее преступление. Система распознает лицо и передает сигнал: о наличии у лица неоплаченных штрафов, нарушении правил дорожного движения, несвоевременной выплате банковского кредита, уклонении от алиментов или нахождения в розыске.

К примеру, проект «Eyesool» («Острый глаз») включает в себя системы наблюдения в более чем 20 аэропортах и на железнодорожных станциях. Данная система направлена на обнаружение и задержание разыскиваемых лиц. Благодаря данной системе осуществляется ежедневная передача порядка двух миллионов изображений лиц в полицейскую систему по сбору данных под названием Skynet.

Проект «Skynet» был внедрен в 2005 г. и представляет собой национальную систему технико-контролируемого отслеживания (ТКО). Данный проект объединяет около 176 млн видеокамер, в планах до 2020 г. увеличить их число до 626 млн. Для сравнения, национальные системы видеонаблюдения США включают около 50 млн камер, Великобритании – 5–6 млн, России – около 300 тыс. При этом

китайская система ТКО не ограничивается решением задач обеспечения общественной безопасности и противодействия преступности – она становится важной частью для создания системы «социального кредитного рейтинга» («Social Credit System») – национальной базы электронных досье «благонадежности» каждого гражданина [8].

Д. Примшиц и С. Голубев отмечают, что создание интеллектуальных платформ в Китае обеспечивает комплексное воздействие на формирование поведенческих мотивов общества, мониторинг и управление этим процессом, а также противодействие терроризму и криминальной активности. Внедрение ИИ-инструментов в сферу общественной безопасности позволяет осуществлять мониторинг с помощью интеллектуальных систем, в основе которых находятся комплексы различных сенсоров и анализа видеоинформации, новые высокотехнологичные средства идентификации личности, в том числе дистанционного и биометрического распознавания [9. С. 43–50].

Осенью 2017 года на пивном фестивале в Циндао полиция с помощью камер задержала 25 человек, находящихся в розыске [10, С.13]. На четырёх входах на территорию фестиваля установили 18 видеокамер. Техника зафиксировала в толпе лица разыскиваемых и распознала их за секунду. Среди задержанных – лицо, находившееся в розыске 10 лет. Система работает с точностью до 98,1 %. При обнаружении совпадения черт внешности лица с данными криминалистической базы полиции, звучит сигнал тревоги. На выходах стояли шесть офицеров, которые задерживали подозреваемых [11. С. 16].

Данные технологии выявляют нарушителей правил дорожного движения, осуществляют поиск его личности в социальных сетях и базах мобильных операторов, при совпадении полицейские отправляют человеку штраф и сообщение с предупреждением.

Огромный массив собираемых биометрических данных обуславливает необходимость правового регулирования. Биометрические данные, собранные с помощью систем видеонаблюдения по распознаванию лиц в Китае, защищены Документом технических требований к личной информационной безопасности (Personal Information Security Specifications), который вступил в силу 1 мая 2018 г. Данный документ определяет, что сбор персональных данных должен осуществляться по согласию владельца для «законных, обоснованных, необходимых и конкретных целей».

Кроме того, полиция с 2018 г. применяет разработанные китайской компанией LLVision Technology Co солнцезащитные «умные» очки со встроенной камерой, которые подключены к криминалистической базе данных и позволяют выявить лиц, находящихся в розыске [12].

В Китае внедрена система оплаты проезда в метро, на железнодорожном вокзале при помощи технологии распознавания лиц. Данная процедура позволяет снизить нагрузку на транспорте, повысить скорость пассажиропотока, а также усилить меры безопасности. Кроме того, отдельные туристические автобусы оборудованы данной технологией. При повторном входе в автобус после посещения достопримечательностей туристов, система распознает их внешность и не требует повторного предъявления билетов. Данная процедура позволяет повысить туристический сервис и способствовать обеспечению общественного порядка.

Практика внедрения данных систем в Великобритании показывает о несколько ином пути их развития. Ежедневно житель Лондона попадает в объектив видеокамер в среднем до трехсот раз в сутки. Еще по состоянию на 2013 г. в Великобритании число установленных видеокамер приближалось к четырем миллионам. В Лондоне установлено более 420 тысяч видеокамер, что составляет около 20% всех уличных видеокамер в мире. Часть из них способны отслеживать, нет ли на теле проходящего человека каких-либо подозрительных предметов, а также распознавать лица людей, находящихся в розыске [13].

В Великобритании с 2012 года внедрены камеры наружного наблюдения, хранение видеоматериалов и доступ к информации регулирует специальное законодательство. Кодекс (Руководство) по применению камер наблюдения обеспечивает пропорциональное применение средств наблюдения, т.е. меры видеоконтроля, применяемые на объекте, должны соотноситься с ожидаемыми рисками и угрозами.

В 2016 г. в Великобритании поэтапно были внедрены системы распознавания лиц. Полицейскими службами Лондона начала использоваться технология распознавания лиц в режиме реального времени (LFR – Live Facial Recognition). Данная технология направлена на борьбу с тяжкими насильственными преступлениями, сопряженными с использованием оружия и др.

Специалисты отмечают имеющийся значительный процент ошибок по отношению к лицам африканского происхождения и других представителей этнических меньшинств в связи с тем, что система обучается преимущественно на лицах светлокожих людей. Кроме того, наблюдается тенденция, что краеугольным камнем на сегодняшний день становится вопрос соблюдения прав и свобод отдельного гражданина, неприкосновенности частной жизни, и тем более представителей этнических меньшинств.

Несмотря на то, что полиция уверена в эффективности системы LFR, правозащитные организации считают её недостаточно надежной и даже противозаконной. Представители научного сообщества из Университета Эссекса в 2019 г. обосновали, что уровень погрешности системы может достигать 81% [14].

Общим трендом в странах Евросоюза является особый акцент на неприкосновенности частной жизни, минимизации рисков и угроз, связанных со злоупотреблениями в сфере распознавания лиц. На повестке дня остро стоит вопрос о введении моратория в странах Евросоюза на распознавания лиц в общественных местах до решения правовых аспектов их использования в целях обеспечения личных прав граждан и обеспечения конфиденциальности частной жизни [15].

Еврокомиссией предлагается ввести механизм, который позволял бы блокировать и те технологии, которые уже используются, но в процессе эксплуатации стали опасными. Например, системы распознавания лиц, которые изначально создавались для обеспечения безопасности, а теперь используются для политического преследования. Исключение сделают для ИИ-решений, которые применяют в вооруженных силах, для обеспечения безопасности, предотвращения терактов, а также поиска пропавших детей и преступников [16].

В России системы распознавания лиц на основе искусственных нейросетей внедряют в аэропорта, метрополитен, банки для удобства и безопасности граждан. Аппаратно-программные комплексы «Безопасный город» функционируют в

городах России в целях мониторинга и предупреждения различных угроз общественной безопасности и правопорядку. Камеры самостоятельно сопоставляют лица из видеопотока с базой данных людей, находящихся в розыске, и в случае совпадений сообщают находящемуся рядом сотруднику полиции [17. С. 201–212].

Технология FindFace SDK для распознавания лиц, разработанная компанией NTechLab (Россия), идентифицирует каждого, находящегося в любом месте, при большом скоплении народа. FindFace SDK идентифицирует лицо на фото или видео, затем составляет шаблон и сравнивает его с содержимым баз данных. При помощи данной технологии в 2018 году во время проведения Чемпионата мира по футболу было задержано более 180 нарушителей. А в 2019 году система поспособствовала задержанию 11 преступников в Татарстане. FindFace SDK используется пока не на всей территории Российской Федерации, а лишь в крупных городах – Москве, Санкт-Петербурге, Рязани и на территории Татарстана [18. С. 62–65].

До 2023 г. МВД России в рамках реализации стратегии национальной безопасности планирует внедрить Федеральную информационную систему биометрических учетов (далее по тексту – ФИСБУ) для поиска преступников и подозреваемых с помощью городских камер видеонаблюдения. ФИСБУ в перспективе объединит ресурсы дактилоскопической и фоноскопической информации, лабораторий ДНК-анализа, биометрических комплексов, а также систем проверки по оперативно-справочным, розыскным и криминалистическим учётам.

Использование систем искусственного интеллекта в Южной Корее при обеспечении общественной безопасности в «Умном городе» показывает высокую эффективность. Так, в городе Сонго к сети подключен каждый объект, с помощью внедрения сенсоров в улицы, здания и дороги; датчики отправляют данные в главный пункт управления для проведения анализа общей обстановки и т.п. [19. С. 314–316].

В Республике Беларусь функционирует достаточно большое количество баз данных, содержащих как персональные, так и иные данные в отношении каждого человека. Функционирует государственная централизованная автоматизированная информационная система «Регистр населения», основу которой составляет база персональных данных граждан, иностранных граждан и лиц без гражданства, постоянно проживающих в Республике Беларусь. В связи с этим применение систем искусственного интеллекта позволяет не только распознать лицо человека, но и получить всю информацию о нем путем выборки, которая содержится во всех базах данных страны [20. С. 84–92].

Е.Г. Бершадская, Е.И. Игоревич, А.И. Мартышкин отмечают, что, несмотря на многолетние исследования идентификации человека по лицу и разработку подобных систем, вопрос получения наиболее результативного метода идентификации человека по его лицу остается открытым. Главной задачей большинства современных систем автоматической идентификации человека по лицу является сравнение вида определенного выбранного лица с базой изображений остальных лиц. Сравнительными характеристиками подобных систем являются вероятность ошибочного распознавания и вероятность ошибочного отказа в распознавании [21. С. 49–53].

На сегодняшний день в Республике Узбекистан наряду с дактилоскопическими системами эффективно используются габитоскопические базы данных. Внедрен аппаратно-программный комплекс «Безопасный город», который обеспечивает видеонаблюдение на стадионах, вокзалах, аэропортах, крупных рынках и других местах массового скопления людей. Благодаря системам видеонаблюдения фиксируются правонарушения, устанавливаются лица, совершившие их, свидетели и очевидцы преступлений и т.д.

В соответствии с Постановлением Президента Республики Узбекистан «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта» от 17 февраля 2021 г. [22] ведется работа по разработке Стратегии развития искусственного интеллекта, определяющей проекты по внедрению биометрических технологий. Таких, как системы распознавания лиц (Face-ID) и голосовой верификации личности, внедрение Единой биометрической системы, удаленной цифровой идентификации лиц при получении банковских и государственных услуг.

М.С. Абламейко, Н.В. Шакель, Р.П. Богуш выделяют китайскую, европейскую и смешанную модели функционирования «умных городов», основанных на системах интеллектуального видеонаблюдения [20. С. 84–92]. Каждая из моделей имеет свои особенности и механизмы реализации. На наш взгляд, Республике Узбекистан целесообразно придерживаться смешанной модели использования систем видеонаблюдения, рационального использования видеонаблюдения, минимизируя риски злоупотреблений и фальсификаций материалов, необходимо разработать соответствующую правовую базу, регламентирующую сбор, обработку, хранение биометрической информации.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЯ

Необходимо отметить, что при использовании в доказывании камер с функцией распознавания лиц должны безоговорочно соблюдаться нормы Конституции, Уголовного кодекса, Уголовно-процессуального кодекса, Закона Республики Узбекистан «О персональных данных» и другие нормы, охраняющие частную жизнь граждан. Запрет на вмешательство в частную жизнь, а также право на защиту от такого вмешательства закреплены в статье 12 Всемирной декларации прав человека (1948 г.). В статье 17 Международного пакта о гражданских и политических правах (1966 г.) установлен запрет на произвольное или незаконное вмешательство в личную и семейную жизнь.

Можно принципиально отказаться от внедрения систем распознавания лиц и иных биометрических технологий в стране, закрыть тему правовой регламентации по причине нарушения фундаментальных прав личности, несогласия общества и т.д. Однако вышеуказанное не остановит развитие научно-технического прогресса, а отсутствие соответствующей правовой базы только создаст возможности безответственного отношения к биометрическим персональным данным, злоупотреблениям, повлечет дополнительные риски и угрозы при сборе и обработке информации.

В связи с перспективой развития технологии распознавания лиц, ID-карт, внедрением Единой биометрической системы, возникает необходимость разработки Концепции национальной системы биометрической идентификации личности. Данная Концепция определит принципы Национальной системы

идентификации личности, основные положения обеспечения защиты прав и свобод личности. Зарубежный опыт показывает целесообразность разработки и принятия Закона Республики Узбекистан «О государственной биометрической регистрации».

ВЫВОДЫ

При внедрении данных технологий необходимо принять во внимание комплекс мер: технических, организационных, методических и самое главное правовых. Современные системы распознавания лиц, несомненно, затрагивают вопросы, связанные с защитой прав и законных интересов граждан от произвольного и несанкционированного контроля за их жизнью и поведением и иных угроз, связанных с незаконным вмешательством в личную жизнь. В связи с этим необходимо соблюдать баланс интересов государства в части обеспечения общественной безопасности государства и общества в целом, и интересов личности – с точки зрения недопущения злоупотребления вмешательством в свою жизнь со стороны государства.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Шашкова И.А. Пределы допустимого вмешательства в частную жизнь посредством использования камер видеонаблюдения в целях раскрытия преступлений // Уголовно-процессуальный кодекс Российской Федерации: достижения и проблемы применения: Сборник научных статей V Международной студенческой научно-практической конференции. Юго-Западный государственный университет. – 2019. – С. 236–241.
2. Исраелян А.М., Исраелян Г.М., Климова Д.Н. Нейросетевые методы идентификации человека по изображению лица // Актуальные научные исследования в современном мире. – 2021. – № 11-12 (79). – С. 111–114.
3. Статистические данные ГЭК МВД Республики Узбекистан за 2021 г.
4. Мочалов М.С., Медведев М.В. Идентификация человека в системах видеонаблюдения // Юность и Знания – Гарантия Успеха – 2015: Сборник научных трудов 2-й Международной научно-практической конференции. Отв. Ред. Горохов А.А., 2015. – 2 том. – С. 64–65.
5. Струкова П.Э. Искусственный интеллект в Китае: современное состояние отрасли и тенденции развития // Вестник Санкт-Петербургского университета. – 2020. – Т. 12. – Вып. 4. – С. 588–606.
6. 促进新一代人工智能产业发展三年行动计划 (2018-2020年). 工业和信息化部. 2018 [Трехлетний план содействия развитию индустрии искусственного интеллекта (2018–2020 гг.). Гунъе хэ синьсихуа бу, – 2018. – С. 15.
7. Ширяева П. 168 камер наблюдения на 1000 человек. Как живет в «безопасном» Чунцине? URL: <https://ekd.me/2019/10/168-kamer-nablyudeniya-na-1000-chelovek-kak-zhivetsya-v-bezopasnom-chuncine/> (дата обращения: 25.02.2022)
8. Видеонаблюдение с функцией распознавания лиц будет внедрено в метро до 1 сентября. URL: https://www.m24.ru/news/mehr-Moskvy/23012020/104711?utm_source=CopуBuf (дата обращения: 20.02.2022.).
9. Примшиц Д., Голубев С. Китайский подход к ускоренному освоению технологий искусственного интеллекта // Наука и инновации. – 2019. – №4 (194). – С. 43–50.

10. Можова Е. Отследить за 3 секунды // Полиция. – 2019. – №4 (2738). – С. 13.
11. Приманкой послужило пиво // Щит и меч. – 2017. – №37 (1581). – С. 16.
12. Kinling Lo. In China, these facial-recognition glasses are helping police to catch criminals. URL: <https://www.scmp.com/news/china/society/article/2132395/chinese-police-scan-suspects-using-facial-recognition-glasses> (дата обращения 20.02.2022).
13. Шарафиев И. Лондон использует рекордное количество камер наружного наблюдения. URL: <https://hightech.fm/2019/08/01/cctv>. (дата обращения: 20.10.2021.).
14. В Лондоне установили камеры с системой распознавания лиц. URL: <https://hi-tech.ua/v-londone-ustanovili-kamery-s-sistemoj-raspoznavaniya-licz/> – (дата обращения: 20.10.2021.).
15. Детинич Г. ЕС может запретить технологии распознавания лиц в общественных местах. URL: <https://3dnews.ru/1001694>. (дата обращения: 20.10.2021.).
16. Зуйкова А. Зачем в ЕС хотят ограничить использование искусственного интеллекта. URL: <https://trends.rbc.ru/trends/industry/609c20f29a794735c39c530c>. (дата обращения: 20.10.2021.).
17. Андреева О.И., Иванов В.В., Нестеров А.Ю., Трубникова Т.В. Технологии распознавания лиц в уголовном судопроизводстве: проблема оснований правового регулирования использования искусственного интеллекта // Вестник Томского государственного университета. – 2019. – № 449. – С. 201–212.
18. Пучкова Д.В. Возможность использования габитоскопического модуля и иных современных технологий, при расследовании преступлений // Тенденции развития науки и образования. – 2020. – №68-7. – С. 62–65.
19. Шрейнер И.Ю., Пашкова И.С. Внедрение системы «Умный город» для повышения безопасности городской среды // Безопасность городской среды: материалы IV Междунар. научно-практ. конф., Омск, 16–18 нояб. 2016 г. – Омск: Омский гос. техн. ун-т, 2017. – С. 314–316.
20. Абламейко М.С., Шакель Н.В., Богуш Р.П. Использование систем искусственного интеллекта при обеспечении общественной безопасности в «Умном городе»: юридические аспекты // Вестник Полоцкого государственного университета. – 2021. – № 2021. – С. 84–92.
21. Бершадская Е.Г., Маркин Е.И., Мартышкин А.И. Методы идентификации личности по изображению лица // XXI век: итоги прошлого и проблемы настоящего плюс. – 2020. – Т. 9. – № 1 (49). – С. 49–53.
22. Постановление Президента Республики Узбекистан № ПП–4996 «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта» от 17.02.2021 г. // Национальная база данных законодательства, 18.02.2021 г., № 07/21/4996/0127, 29.07.2021 г., № 07/21/5199/0721.