Попов Юрий Леонидович,
К.И.Н, доцент, профессор АВН,
ФВУНЦ ВВС «ВВА» в г. Челябинск

Гришаков Роман Константинович,
Курсант 225 учебной группы, 2 факультета,
ФВУНЦ ВВС «ВВА» в г. Челябинск

Кокшаров Александр Сергеевич,
Курсант 225 учебной группы, 2 факультета,
ФВУНЦ ВВС «ВВА» в г. Челябинск

СИСТЕМА РАСПОЗНАВАНИЯ ЛИЦ И БИОМЕТРИИ ЧЕЛОВЕКА ДЛЯ ПРЕДОТВРАЩЕНИЯ ТЕРАКТОВ И ДИВЕРСИЙ

Аннотация: В контексте борьбы с терроризмом, биометрические технологии, в том числе распознавание лиц, применяются для контроля на границах и в национальных системах идентификации, что позволяет предотвращать теракты и диверсии.

Ключевые слова: Распознавание, технологии, система, обнаружение.

1. Введение

1.1. Актуальность проблемы: Угрозы терроризма и диверсий в современном мире

Современный мир характеризуется высокой динамикой геополитических процессов, что, к сожалению, сопровождается ростом террористической активности и увеличением риска диверсий. Согласно данным за 2023 год, было зафиксировано более 5,300 террористических актов по всему миру, повлекших за собой почти 16,000 смертей. Наиболее пострадавшими странами стали Сирия (1,405 атак), Пакистан (695 атак) и Израиль (665 атак).

Рост террористической активности наблюдается не только в традиционных зонах конфликтов, но и в регионах Западной Африки, где конкуренция за ресурсы, такие как золото и уран, подпитывает экстремистские группировки . Нигер, к примеру, столкнулся с 94% увеличением числа жертв терроризма в 2024 году.

Угроза терроризма в 2023 году увеличилась из-за политической нестабильности, технологических изменений и конкуренции за ресурсы.

В этих условиях, разработка и внедрение эффективных систем предотвращения террористических актов и диверсий приобретает первостепенное значение. Одним из перспективных направлений в данной области является использование систем распознавания лиц и биометрии человека, позволяющих автоматизировать процессы идентификации и контроля доступа, значительно повышая уровень безопасности.

Таджикский государственный медицинский университет подчеркивает, что профилактика терроризма требует комплексного подхода со стороны государства и гражданского общества. Разрабатываемые и внедряемые системы распознавания лиц и биометрии человека могут стать важной составляющей этой работы.

В условиях роста технологических возможностей экстремистских организаций, использующих искусственный интеллект и зашифрованные коммуникации, совершенствование и внедрение передовых технологий для противодействия этим угрозам становится необходимостью.

1.2. Цель доклада: Рассмотрение возможностей и ограничений систем распознавания лиц и биометрии для предотвращения терактов

Целью данного доклада является всестороннее рассмотрение потенциала и ограничений современных систем распознавания лиц и биометрических технологий в контексте предотвращения террористических актов и диверсий. Мы исследуем, как эти технологии могут быть использованы для повышения общественной безопасности, а также проанализируем связанные с их применением юридические и технические вызовы.

Современные системы распознавания лиц, такие как Clearview AI, Amazon Rekognition и ESPY – Face Search, значительно расширили возможности правоохранительных органов. Clearview AI, например, использует обширную базу данных изображений из открытых источников, включая социальные сети, что позволяет находить совпадения среди широкой аудитории. Однако, несмотря на потенциальную пользу, необходимо учитывать баланс между эффективностью этих технологий и вопросами конфиденциальности.

В контексте борьбы с терроризмом, биометрические технологии, в том числе распознавание лиц, применяются для контроля на границах и в национальных системах идентификации. Цель – предотвращение и раскрытие преступлений, обеспечение общественной безопасности и привлечение к ответственности виновных. Несмотря на то, что предоставленные данные не содержат конкретных примеров успешного предотвращения терактов с помощью биометрии, правоохранительные органы рассматривают технологии распознавания лиц как инструмент, способствующий предотвращению и раскрытию преступлений.

В докладе будут рассмотрены ограничения и проблемы, связанные с использованием этих технологий, включая вопросы точности, предвзятости, конфиденциальности, безопасности данных, юридические аспекты. Несмотря на улучшения в технологиях распознавания лиц на основе искусственного интеллекта, они все еще не являются безошибочными, и уровни точности могут варьироваться в зависимости от факторов, таких как качество изображения и условия освещения. Ошибки, такие как ложные срабатывания и ложные отрицания, остаются серьезной проблемой, особенно в правоохранительных приложениях, где неверная идентификация может иметь серьезные последствия. Также, использование технологий распознавания лиц вызывает опасения по поводу конфиденциальности, поскольку они позволяют отслеживать и идентифицировать людей без их согласия.

Анализ возможностей и ограничений позволит сформировать сбалансированное представление о перспективах и рисках применения систем распознавания лиц и биометрии в борьбе с терроризмом, а также определить необходимые условия для их эффективного и этичного использования.

1.3. Задачи доклада: Обзор существующих технологий, анализ эффективности.

Обзор существующих технологий: В рамках доклада будет представлен обзор современных биометрических технологий, включая распознавание лиц, анализ радужной оболочки глаза, сканирование отпечатков пальцев, голосовую аутентификацию, а также перспективные направления, такие как поведенческая и мультимодальная биометрия. Особое внимание будет уделено геномной регистрации, как методу повышения возможностей выявления террористов.

Анализ эффективности: Будет проведен анализ эффективности применения данных технологий в целях идентификации, контроля доступа к критически важным объектам и повышения уровня безопасности. Анализ будет включать рассмотрение существующих проблем, таких как возможность обмана систем, технологические ограничения, связанные с внешними факторами, и необходимость разработки дополнительных алгоритмов и программного обеспечения.

2. Теоретические основы распознавания лиц и биометрии

2.1. Принципы работы систем распознавания лиц: Алгоритмы обнаружения, выделения признаков, сравнения

Современные системы распознавания лиц представляют собой сложные комплексы, использующие различные алгоритмы для идентификации и верификации лиц на изображениях и видео.

1. Алгоритмы обнаружения: Основная задача на данном этапе – выявление наличия лица на изображении или видеопотоке, даже при удаленности объекта или слабом освещении. Технология **Visible Light** использует для этого самообучающиеся алгоритмы.

2. Алгоритмы выделения признаков: После обнаружения лица система выделяет уникальные признаки, характеризующие конкретного человека.

Глубокое обучение: Современные алгоритмы часто используют глубокие нейронные сети, такие как сверточные нейронные сети. **Krizhevsky et al. (2017)** описывают применение глубоких сверточных нейронных сетей для классификации изображений, что стало основой для многих современных систем распознавания лиц. **Deng et al. (2019)** представили метод **ArcFace**, улучшающий точность распознавания лиц за счет добавочной угловой маржинальной потери.

Модели на основе признаков: Используются для извлечения характерных признаков лица. **Gabor Wavelet Transform** может использоваться для извлечения признаков лиц, как указано в диссертации Kepenekci B. “Face recognition using gabor wavelet transform”. **Local Binary Patterns (LBP)** также применяются для распознавания лиц, как описано в работе **Ahonen et al. (2004)**.

Например, технология **Visible Light** оценивает соседние пиксели для формирования уникальных идентификаторов человека.

3. Алгоритмы сравнения: На заключительном этапе выделенные признаки сравниваются с данными, хранящимися в базе данных лиц, для идентификации или верификации. **Visible Light** выявляет углы наклона лица в трехмерном формате для дальнейшего восстановления картинки и более точной идентификации.

Модели глубокого обучения для сложных условий: В сложных условиях, таких как низкая освещенность и частичные окклюзии, модели глубокого обучения показывают улучшенную эффективность. Статья Беркасова, П. Ю. сравнивает **MobileNetV2**, **InceptionV3** и **EfficientNetV2M**, показав, что **EfficientNetV2M** имеет наилучшие показатели потери регрессии (0.0090) при обнаружении лиц в сложных условиях.

4. Дополнительные алгоритмы: Оценка качества изображения для экономии вычислительных мощностей. Выравнивание: Система репозиционирует глаза, нос и рот человека для более точной идентификации.

2.2. Биометрические методы идентификации: Отпечатки пальцев, радужная оболочка глаза, голос, ДНК и другие

В контексте предотвращения террористических актов и диверсий, биометрические методы идентификации представляют собой важный инструмент, позволяющий с высокой точностью идентифицировать личность и контролировать доступ к критически важным объектам и информации. Разнообразие биометрических характеристик, используемых для идентификации, включает в себя как хорошо известные методы, такие как отпечатки пальцев, так и более современные, основанные на анализе радужной оболочки глаза, голоса или даже ДНК.

Отпечатки пальцев:

Традиционный и широко распространенный метод, основанный на уникальном рисунке папиллярных линий на пальцах. Несмотря на зрелость технологии, современные системы

идентификации по отпечаткам пальцев продолжают совершенствоваться в плане скорости и точности сканирования, а также устойчивости к подделкам.

Радужная оболочка глаза:

Уникальный рисунок радужной оболочки глаза является высоконадежным биометрическим идентификатором. Сканирование радужной оболочки бесконтактно и позволяет быстро и точно идентифицировать личность. Технология находит применение в системах контроля доступа высокого уровня безопасности.

Голос:

Анализ характеристик голоса, таких как тембр, частота и интонация, позволяет создать уникальный голосовой профиль. Голосовая биометрия удобна в использовании, особенно в системах удаленной аутентификации, но может быть уязвима к подделкам и влиянию внешних шумов. Массимилиано Тодиско в своих работах подчеркивает важность разработки надежных и устойчивых к атакам систем голосовой биометрии, а также необходимость защиты конфиденциальности данных.

ДНК:

Анализ ДНК является наиболее точным методом идентификации личности, однако требует времени и специального оборудования для проведения анализа. В контексте предотвращения террористических актов и диверсий, анализ ДНК может быть использован для идентификации останков, установления личности подозреваемых или жертв.

Другие биометрические методы:

Помимо перечисленных, существуют и другие биометрические методы идентификации, такие как геометрия лица, рисунок вен на ладони или пальце, походка и другие. Выбор конкретного метода зависит от требований к безопасности, удобству использования и стоимости системы.

Безопасность и уязвимости биометрических методов:

Несмотря на высокую точность и надежность биометрических систем идентификации, они не лишены уязвимостей. Существуют методы обхода биометрических систем, такие как использование поддельных отпечатков пальцев, голосовых имитаций или манипулирование изображениями лица. Поэтому, важно постоянно совершенствовать системы защиты биометрических данных и разрабатывать новые методы противодействия атакам.

Правовые аспекты:

Использование биометрических данных поднимает важные вопросы, связанные с защитой персональных данных и соблюдением прав человека. Необходимо разработать четкие правовые рамки, регулирующие сбор, хранение и использование биометрических данных, а также обеспечить прозрачность и подотчетность систем биометрической идентификации. В Канаде, например, Комиссия по доступу к информации запретила использование технологий распознавания лиц для контроля посещаемости сотрудников, что подчеркивает важность соблюдения законов о конфиденциальности. Несоблюдение таких законов может привести к штрафам до 10 миллионов долларов или 2% от годового оборота .

Сбербанк, как пример безопасной биометрической системы в России: Сбербанк стал первым в России, кто прошел аттестацию Федеральной службы по техническому и экспортному контролю (ФСТЭК), подтвердившую безопасность его биометрической системы. Это подтверждает соответствие системы требованиям безопасности, предъявляемым к государственным информационным системам.

В заключение, биометрические методы идентификации представляют собой мощный инструмент для повышения безопасности и предотвращения террористических актов и диверсий. Однако, для эффективного и безопасного использования биометрических технологий необходимо учитывать технические и правовые аспекты, а также постоянно совершенствовать системы защиты биометрических данных от уязвимостей.

3. Современные технологии распознавания лиц и биометрии

3.1. 2D и 3D распознавание лиц: Сравнение подходов, преимущества и недостатки

Современные системы распознавания лиц активно используют как 2D, так и 3D подходы. Сравнение точности 2D и 3D распознавания лиц показывает значительные различия в их эффективности и надежности, что обусловлено особенностями каждой технологии. В контексте предотвращения террористических актов и диверсий, понимание этих различий критически важно.

2D Распознавание Лиц

Преимущества:

Доступность и экономичность: Алгоритмы 2D распознавания лиц широко распространены и относительно недороги, что делает их экономически привлекательным решением.

Недостатки:

Чувствительность к условиям освещения и позе: 2D-системы полагаются на плоские изображения, что делает их уязвимыми к изменениям освещения и ракурса съемки, потенциально снижая точность идентификации.

Порог ошибок: По данным Faceter, для 2D-систем характерен ложный пропуск (False Acceptance Rate) в 0,1% и ложный отказ (False Rejection Rate) до 2,5%

3D Распознавание Лиц

Преимущества:

Высокая точность: 3D-технологии создают трехмерные модели лиц, что позволяет существенно повысить точность распознавания. Faceter указывает на ложный пропуск всего в 0,0005% и ложный отказ в 0,1%.

Устойчивость к изменениям: 3D-распознавание менее подвержено влиянию освещения и ракурса, так как анализируется геометрия лица.

Недостатки:

Сложность оборудования: 3D-системы требуют дорогостоящего оборудования, такого как лазерные сканеры и специализированные камеры.

Ограниченные базы данных: Существует дефицит обширных баз данных 3D-моделей лиц, что затрудняет анализ в реальном времени.

Сложность идентификации близнецов: Минимальные различия между близнецами могут привести к ошибкам идентификации.

3.2 Использование глубокого обучения в распознавании лиц: Сверточные нейронные сети

Глубокое обучение совершило революцию в области распознавания лиц, и ключевую роль в этом сыграли свёрточные нейронные сети (CNN). CNN являются специализированным классом нейронных сетей, разработанных для обработки данных с выраженной пространственной структурой, что идеально подходит для анализа изображений.

Сверточные нейронные сети (CNN): Архитектура и принципы работы

Архитектура CNN вдохновлена строением зрительной коры головного мозга, где нейроны реагируют на локальные области изображения. Это позволяет CNN эффективно извлекать

иерархические признаки, начиная от простых краёв и текстур до сложных паттернов, характерных для человеческих лиц. Типичная CNN состоит из нескольких слоев:

Свёрточные слои: Выполняют операцию свёртки, применяя фильтры к входному изображению для извлечения признаков.

Слои подвыборки (pooling layers): Уменьшают размерность представления, делая сеть более устойчивой к небольшим изменениям положения и масштаба лица.

Полносвязные слои: Используются для классификации извлеченных признаков и принятия решения об идентификации лица.

В последние годы были разработаны различные архитектуры CNN, которые значительно улучшили точность распознавания лиц, такие как LeNet-5, AlexNet, VGG, GoogleNet (Inception), ResNet.

Современные тенденции

Исследования в области распознавания лиц с использованием глубокого обучения продолжают активно развиваться. Одной из перспективных тенденций является учет позы лица при распознавании выражений. Так, техника, использующая метод ближайших соседей для определения позы и нейронную сеть на основе расширенной модели ансамбля, достигла 90% точности.

В 2023 году наблюдается активное развитие технологий глубокого обучения, включая применение глубоких нейронных сетей, таких как сверточные нейронные сети (CNN), которые остаются основным инструментом для задач компьютерного зрения, включая распознавание лиц.

3.3. Биометрические системы на основе поведенческих характеристик: Анализ походки, клавиатурный почерк

Поведенческая биометрия использует уникальные особенности поведения человека для идентификации. Два перспективных направления – анализ походки и клавиатурный почерк – демонстрируют потенциал в повышении безопасности и предотвращении угроз.

Анализ походки:

Несмотря на отсутствие свежих исследований за 2023 год в предоставленных данных, важно отметить общий тренд развития биометрических технологий. Интегрированные биометрические системы, объединяющие несколько методов идентификации, могут включать и анализ походки в будущем. Развитие технологий машинного обучения и компьютерного зрения открывает новые возможности для создания надежных систем распознавания походки.

Клавиатурный почерк:

Клавиатурный почерк представляет собой уникальный стиль набора текста, который может быть использован для биометрической идентификации. В 2023 году в РТУ МИРЭА была разработана система идентификации пользователей по клавиатурному почерку, направленная на повышение безопасности доступа к информационным системам. Эта система анализирует скорость набора, динамику печати и частоту ошибок, создавая уникальный вектор характеристик для каждого пользователя.

Эффективность системы: Система анализирует несколько ключевых характеристик набора текста, включая:

Скорость набора: как быстро пользователь вводит текст.

Динамика печати: изменения в скорости и ритме набора.

Частота ошибок: количество опечаток и их типы.

На основе этих данных модуль создает уникальный вектор характеристик для каждого пользователя, который затем сравнивается с шаблоном в базе данных. Система также

автоматически обновляет шаблоны, адаптируясь к изменениям в поведении пользователя, что делает её более точной и надежной.

Преимущества и применение: Клавиатурный почерк представляет собой альтернативу традиционным методам аутентификации, таким как пароли. Новый модуль предлагает надежную защиту без необходимости в дополнительном оборудовании. Исследования влияния физического состояния на клавиатурный почерк могут дополнительно повысить точность системы. Данная технология может применяться в информационной безопасности, финансовых технологиях и корпоративных системах.

Точность и безопасность поведенческих биометрических систем

Высокая точность распознавания: Поведенческие биометрические системы стремятся к высокой точности, однако возможны ошибки распознавания. Это подчеркивает необходимость использования многофакторной идентификации.

Динамическая биометрия: Современные подходы к поведенческой биометрии включают динамическую идентификацию, при которой биометрические шаблоны не хранятся постоянно, а формируются и используются только в момент запроса. Это повышает уровень безопасности.

Уязвимость к утечкам данных: Одним из основных рисков является невозможность замены биометрических данных в случае их утечки. Поэтому важно использовать децентрализованную архитектуру хранения данных.

Ошибочная идентификация: Несмотря на высокую точность, ошибки распознавания могут привести к временной потере доступа к сервисам. Это подчеркивает необходимость внедрения антиспуфинг-технологий.

Формирование цифровой зависимости: Полная зависимость от биометрических механизмов может создать уязвимость. Поэтому важно сохранять возможность альтернативной авторизации.

4. Применение систем распознавания лиц и биометрии для предотвращения терактов и диверсий

4.1. Контроль доступа на критически важные объекты: Аэропорты, вокзалы, электростанции

Системы распознавания лиц и другие биометрические технологии играют ключевую роль в усилении безопасности на критически важных объектах, таких как аэропорты, вокзалы и электростанции, обеспечивая надежный контроль доступа и предотвращая потенциальные террористические акты и диверсии.

Аэропорты и вокзалы:

Улучшение безопасности и удобства пассажиров: В аэропортах биометрические технологии, такие как распознавание лиц и отпечатков пальцев, значительно повышают уровень безопасности, исключая возможность использования поддельных документов и облегчая идентификацию личности. Пассажиры могут связывать свои биометрические данные с билетами для более безопасного и удобного процесса регистрации и посадки. “Введение биометрической технологии в аэропортах преобразует клиентский опыт и усиливает безопасность”.

Ускорение процедур: Биометрические терминалы позволяют пассажирам проходить регистрацию без вмешательства человека, сопоставляя их лица с сохраненной биометрической информацией в системе, что значительно ускоряет процесс. “Пассажиры, прошедшие биометрическую проверку, также испытывают более качественный процесс досмотра”. На этапе

посадки в самолёт используются терминалы распознавания лиц, которые проверяют идентичность пассажиров, предотвращая посадку лиц с поддельными документами.

Сокращение времени ожидания: Внедрение биометрических технологий сокращает время ожидания на всех этапах путешествия. В России наблюдается тенденция к “бесшовным путешествиям”, где пассажиры, прошедшие все проверки, могут быстрее получить свой багаж по прибытии.

Глобальное распространение: 98% авиакомпаний уже внедрили или планируют внедрить биометрические системы в своих терминалах. Ожидается, что 60% авиакомпаний интегрируют биометрию в ключевые точки взаимодействия с пассажирами в течение следующих пяти лет.

Пример США: Управление таможенного и пограничного контроля США (CBP) внедрило 32 технологии сравнения лиц для входа в 32 аэропортах, идентифицировав более 2 миллионов пассажиров.

Общественное мнение: Несмотря на опасения по поводу конфиденциальности, 43% людей одобряют использование технологий распознавания лиц в аэропортах.

Электростанции:

Хотя конкретные примеры применения биометрических систем на электростанциях в предоставленной информации отсутствуют, аналогичные технологии контроля доступа и идентификации могут быть использованы для:

Предотвращения несанкционированного доступа: Биометрическая идентификация сотрудников и посетителей может исключить проникновение посторонних на территорию электростанции, тем самым предотвращая диверсии и теракты.

Контроля доступа к критически важным зонам: Ограничение доступа к определенным зонам электростанции на основе биометрической идентификации сотрудников, имеющих соответствующие права доступа.

Учета рабочего времени и контроля доступа: Мониторинг присутствия персонала на объекте и контроль за соблюдением рабочего графика, что повышает общую безопасность объекта.

Нормативное регулирование аспекты:

GDPR (ЕС): Биометрические данные считаются особой категорией, требующей явного согласия на сбор и обработку. Нарушение требований GDPR влечет за собой значительные штрафы.

CCPA (США): Пользователи имеют право на уведомление о сборе биометрических данных и отказ от их обработки.

Федеральный закон «О персональных данных» (Россия): Требует согласия пользователя на сбор и обработку биометрических данных, а также хранения их на территории РФ.

4.2. Системы видеонаблюдения с функцией распознавания лиц в общественных местах: Обнаружение лиц, находящихся в розыске

Системы видеонаблюдения (СВН) с функцией распознавания лиц (СРЛ) активно интегрируются в общественные пространства с целью повышения безопасности и оперативного обнаружения лиц, находящихся в розыске. Эти системы позволяют в режиме реального времени идентифицировать людей, сопоставляя их биометрические данные с базами данных правоохранительных органов. Такая возможность способствует оперативному реагированию на потенциальные угрозы и задержанию преступников.

Примеры внедрения и эффективность:

Внедрение СРЛ в различных городах мира демонстрирует их потенциал в борьбе с преступностью. Например, в Лондоне, СВН с функцией распознавания лиц используются для

повышения безопасности в общественных местах. Ожидается, что к 2025 году точность этих систем достигнет 99.9%, даже в сложных условиях освещения или при ношении масок, благодаря использованию 3D-карт лиц и алгоритмов на базе искусственного интеллекта (ИИ) .

В Нью-Йорке СРЛ применяются для контроля доступа в здания и на транспортных узлах. Системы анализируют данные в реальном времени и отправляют предупреждения о подозрительном поведении, например, если человек несколько дней подряд находится в определенном месте в нерабочее время.

В России технологии распознавания лиц, разработанные компанией NTechLab, привели к задержанию более 180 нарушителей во время Чемпионата мира по футболу в 2018 году и помогли задержать 11 преступников в Татарстане в 2019 году.

Технологические аспекты:

Современные СРЛ используют искусственный интеллект и машинное обучение для повышения точности идентификации. Облачные решения для хранения и анализа данных обеспечивают доступ к информации из любой точки и снижают затраты на локальное хранение.

Заключение: Системы видеонаблюдения с функцией распознавания лиц представляют собой эффективный инструмент в борьбе с преступностью и терроризмом.

4.3. Идентификация личности в онлайн-пространстве: Предотвращение финансирования терроризма, выявление экстремистской пропаганды

Системы распознавания лиц и биометрии играют важную роль в предотвращении террористических актов и диверсий, особенно в контексте идентификации личности в онлайн-пространстве. Две ключевые задачи, решаемые с помощью этих технологий – это предотвращение финансирования терроризма и выявление экстремистской пропаганды.

Предотвращение финансирования терроризма:

В 2023 году борьба с финансированием терроризма в России была значительно активизирована, что подтверждается данными Росфинмониторинга о блокировке операций в отношении около 1,5 тыс. лиц. Использование биометрических данных и систем распознавания лиц может существенно повысить эффективность отслеживания и пресечения финансовых потоков, связанных с террористической деятельностью.

Усиление идентификации пользователей онлайн-платформ: Системы распознавания лиц могут быть интегрированы в процессы верификации личности на финансовых платформах, в социальных сетях и других онлайн-сервисах, что позволит предотвратить использование поддельных или украденных документов для осуществления финансовых операций в пользу террористических организаций.

Мониторинг транзакций: Биометрические данные могут использоваться для мониторинга транзакций и выявления подозрительных операций, которые могут быть связаны с финансированием терроризма. Например, системы могут автоматически уведомлять о крупных переводах средств лицам, находящимся в списках подозреваемых в террористической деятельности.

Анализ поведения пользователей: Комбинация биометрических данных и поведенческой аналитики позволяет выявлять пользователей, чья активность в онлайн-пространстве может указывать на причастность к финансированию терроризма. Это может включать анализ частоты и объема транзакций, характера коммуникаций и посещаемых веб-сайтов.

Международное сотрудничество: Эффективное предотвращение финансирования терроризма требует активного международного сотрудничества. Россия активно взаимодействует с международными партнерами в этой области, отвечая на 100% запросов из других стран. Использование унифицированных биометрических стандартов и систем обмена

данными может значительно упростить и ускорить процесс выявления и пресечения трансграничных финансовых операций, связанных с терроризмом.

В 2023 году в российское законодательство были внесены изменения, направленные на ужесточение мер ответственности за финансирование терроризма, включая новую редакцию статьи 205 УК РФ. Также рассматривается вопрос об отмене наличных денежных средств в стране, что позволит эффективнее отслеживать финансовые потоки.

Выявление экстремистской пропаганды:

Системы распознавания лиц и биометрии могут быть использованы для выявления и блокировки распространения экстремистской пропаганды в онлайн-пространстве.

Идентификация распространителей: Системы распознавания лиц могут использоваться для идентификации лиц, распространяющих экстремистские материалы в социальных сетях, на форумах и других онлайн-платформах. Интеграция с базами данных правоохранительных органов позволит быстро идентифицировать известных экстремистов и заблокировать их аккаунты.

Анализ контента: Хотя в предоставленном контексте нет конкретных примеров успешного выявления экстремистской пропаганды с использованием технологий распознавания лиц, возможности, такие как TRASSIR Face Recognition 2.0, позволяют обнаруживать и идентифицировать лица на изображениях, распознавать атрибуты внешности и проводить поиск лиц в базе данных, что может быть полезно для мониторинга контента и выявления подозрительных лиц.

Обнаружение “фейков”: Технология определения “живости” лица предотвращает использование изображений для обмана систем распознавания, что важно для обеспечения надежности системы при мониторинге потенциальных угроз.

Автоматическое удаление контента: Системы могут настраивать реакции на события, что позволяет автоматизировать процесс реагирования на выявление подозрительных лиц или поведения.

Вывод: Системы распознавания лиц и биометрии представляют собой мощный инструмент для предотвращения террористических актов и диверсий в онлайн-пространстве. Однако для эффективного использования этих технологий необходимо обеспечить соблюдение этических и правовых норм, а также активное международное сотрудничество.

4.4. Интеграция с базами данных правоохранительных органов: Поиск и задержание подозреваемых

Интеграция систем распознавания лиц с базами данных правоохранительных органов представляет собой мощный инструмент для оперативного поиска и задержания подозреваемых в совершении преступлений, включая террористические акты и диверсии. Хотя прямые примеры интеграции систем распознавания лиц не упоминаются в предоставленной информации, аналогия с системами автоматического распознавания номерных знаков (ALPR) позволяет понять принципы и возможности такого взаимодействия.

Принцип работы и аналогия с ALPR:

Подобно тому, как ALPR-системы интегрируются с базами данных для выявления угнанных автомобилей или транспортных средств, связанных с преступной деятельностью, системы распознавания лиц могут быть подключены к базам данных разыскиваемых лиц, террористов и других представляющих интерес для правоохранительных органов. При обнаружении лица, соответствующего записям в базе данных, система немедленно уведомляет соответствующие службы, что позволяет оперативно реагировать и задерживать подозреваемого.

Практическое применение:

В сценарии предотвращения терактов и диверсий, интеграция с базами данных позволяет:

Выявлять лиц, находящихся в розыске: Система распознавания лиц, установленная в общественных местах, таких как аэропорты, вокзалы, торговые центры, может идентифицировать лиц, находящихся в федеральном или международном розыске за терроризм или другие тяжкие преступления.

Контролировать соблюдение ограничений: Система может контролировать соблюдение запретов на посещение определенных мест лицами, представляющими угрозу безопасности.

Связывать подозреваемых с местами преступлений: Анализируя данные распознавания лиц, можно выявлять закономерности в перемещениях подозреваемых и связывать их с местами, где были совершены преступления или планировались диверсии. По аналогии с тем, как ALPR помогла связать движения подозреваемых с местами преступлений, предоставив критически важные доказательства.

Заключение:

Интеграция систем распознавания лиц с базами данных правоохранительных органов представляет собой перспективное направление в области обеспечения безопасности и борьбы с терроризмом. Правильное применение этих технологий, в сочетании с соблюдением этических и правовых норм, может значительно повысить эффективность работы правоохранительных органов и предотвратить совершение тяжких преступлений.

5. Анализ эффективности и ограничений

5.1. Факторы, влияющие на точность распознавания лиц: Освещение, ракурс, возрастные изменения

Точность систем распознавания лиц критически зависит от ряда факторов, среди которых ключевыми являются условия освещения, ракурс лица и возрастные изменения биометрических признаков. Неучет этих факторов может существенно снизить эффективность системы, особенно в контексте предотвращения террористических актов и диверсий.

Освещение:

Недостаточное или неравномерное освещение может серьезно затруднить процесс распознавания. Системы распознавания лиц в условиях низкой освещенности сталкиваются с вызовами, включающими слабую видимость, частичные препятствия (например, очки, маски). Современные решения, такие как технология **Visible Light**, используют самообучающиеся алгоритмы для оптимизации распознавания в сложных условиях. Эта технология включает этапы обнаружения лица, определения его положения в 3D-формате, оценки качества изображения, выравнивания и извлечения признаков, что позволяет эффективно идентифицировать людей даже в полумраке. Кроме того, модели глубокого обучения, такие как **MobileNetV2**, **InceptionV3** и **EfficientNetV2M**, демонстрируют улучшенную точность и эффективность в сложных условиях освещения. Например, **EfficientNetV2M** показала наилучшее значение потери регрессии (0.0090) при тестировании на фотографиях лиц, снятых в сложных условиях.

Ракурс:

Угол обзора и ракурс лица оказывают существенное влияние на восприятие и распознавание лиц. Исследования показывают, что ракурс может изменять восприятие и оценку изображаемых объектов, что критично для систем распознавания. Важность угла обзора в восприятии изображений подчёркивается в исследованиях, изучавших влияние ракурса камеры на восприятие людей в новостях. Современные исследования также рассматривают влияние угла

обзора на восприятие цифровой презентации продуктов, что может быть применимо и к распознаванию лиц. Кроме того, вертикальный угол камеры влияет на невербальную коммуникацию в селфи, что связано с восприятием лиц.

Возрастные изменения:

Возрастные изменения биометрических признаков – это необратимый физиологический процесс, влияющий на характеристики, используемые для биометрической идентификации. Изменения в текстуре кожи, появление морщин и другие физические изменения могут затруднить идентификацию, особенно в системах распознавания лиц и отпечатков пальцев. Важно учитывать этот фактор при разработке биометрических систем, стремясь к созданию более надежных и эффективных решений, устойчивых к возрастным изменениям.

Вывод:

Для повышения эффективности и надежности систем распознавания лиц в целях предотвращения террористических актов и диверсий необходимо учитывать и минимизировать влияние указанных факторов. Это требует применения современных алгоритмов, устойчивых к изменениям освещения и ракурса, а также разработки методов, компенсирующих влияние возрастных изменений биометрических признаков.

5.2. Устойчивость к обману: Использование масок, грима, пластической хирургии

Системы распознавания лиц (СРЛ) подвержены уязвимостям при попытках обмана с использованием масок, грима и пластической хирургии, что создает существенные проблемы для их применения в целях предотвращения терактов и диверсий.

Маски и грим:

Маски значительно снижают эффективность СРЛ, увеличивая частоту ошибок. Исследования показывают, что маскирование лица может увеличить процент ложных совпадений в 10-100 раз по сравнению с ситуациями, когда лицо открыто. Тип маски также влияет на точность распознавания: широкие маски, закрывающие щеки, создают больше ошибок, чем маски, закрывающие только рот и нос.

Пластическая хирургия:

Пластическая хирургия, изменяя форму и текстуру лица, также представляет серьезный вызов для СРЛ . Исследования показывают, что хирургические вмешательства могут затруднить идентификацию личности . Различают локальную (изменяет одну часть лица) и глобальную хирургию (изменяет всю структуру лица). В частности, изменения лицевых ориентиров после пластической хирургии затрудняют распознавание.

Проблемы и решения:

Для повышения устойчивости к обману разрабатываются бимодальные системы, использующие одновременно данные изображения лица и голоса. Также проводятся исследования по разработке моделей распознавания лиц, устойчивых к изменениям, вызванным пластической хирургией, например, на основе нейронных сетей с мета-обучением.

5.3. Возможности обхода биометрических систем: Подделка отпечатков пальцев, имитация голоса

Биометрические системы, несмотря на свою продвинутость, не являются абсолютно неуязвимыми. Злоумышленники постоянно разрабатывают новые методы обхода этих систем, и два наиболее распространенных способа – это подделка отпечатков пальцев и имитация голоса.

Подделка отпечатков пальцев:

Хотя конкретной статистики по подделке отпечатков пальцев в 2023 году не представлено в исходных данных, следует отметить, что современные антиспуффинг-технологии активно

развиваются для противодействия таким атакам. Эти технологии направлены на обнаружение и блокировку попыток использования поддельных биометрических данных. Современные алгоритмы распознавания, используемые в биометрических системах, учитывают множество параметров, таких как текстура кожи и форма отпечатка, что значительно затрудняет подделку.

Имитация голоса:

Имитация голоса представляет собой серьезную угрозу для систем голосовой аутентификации, особенно с развитием технологий глубоких фейков. Глубокие фейки позволяют создавать AI-аватары, имитирующие естественный голос пользователя, что может быть использовано для обхода систем безопасности.

- **Эффективность имитации:** Для успешной атаки злоумышленнику необходим доступ к генератору голоса с соответствующей фонетикой и аудиоустройства для записи и воспроизведения. Важно проводить тестирование биометрических систем на уязвимости к использованию записанных голосов или синтетической речи .
- **Проблемы и вызовы:** Злоумышленники могут использовать записанные образцы голоса для имитации пользователей. Факторы окружающей среды, такие как фоновый шум, могут влиять на точность распознавания голоса. Сбор и хранение голосовых данных поднимают вопросы конфиденциальности и безопасности данных.

Противодействие угрозам:

Для защиты от этих угроз необходимо:

Разрабатывать и внедрять эффективные антиспуфинг-меры, анализирующие динамические характеристики речи и использующие технологии глубоких фейков.

Использовать мультимодальную биометрию, комбинирующую несколько биометрических признаков для повышения безопасности.

Рассмотреть поведенческую биометрию, анализирующую уникальные паттерны поведения пользователей для непрерывной аутентификации.

Постоянно обновлять системы безопасности и следить за последними достижениями в области технологий голосовой аутентификации.

Вывод:

Несмотря на существующие методы обхода, биометрические системы продолжают развиваться и совершенствоваться. Современные технологии защиты направлены на повышение надежности и безопасности биометрических систем, что крайне важно в условиях растущих угроз и вызовов в области кибербезопасности

6. Перспективы развития

6.1. Разработка более устойчивых и точных алгоритмов распознавания лиц

Разработка более устойчивых и точных алгоритмов распознавания лиц является критически важным направлением для повышения эффективности систем безопасности и предотвращения террористических актов. В этой области ключевую роль играют свёрточные нейронные сети (CNN) и новые подходы в машинном обучении.

6.1.1. Эволюция архитектур CNN

Архитектуры CNN продолжают развиваться, предлагая всё более эффективные решения для задач распознавания лиц. От классических моделей, таких как LeNet-5 и AlexNet, до более сложных, таких как VGG, GoogleNet (Inception) и ResNet, каждая архитектура вносила свой вклад в повышение точности и скорости распознавания. ResNet, в частности, решила проблему затухания градиента, позволив создавать очень глубокие сети, что критично для сложных задач.

6.1.2. Современные подходы и технологии

Помимо традиционных CNN, активно развиваются новые подходы, такие как Vision Transformers, которые показывают конкурентоспособные результаты в задачах распознавания изображений. Интеграция этих технологий с CNN может привести к созданию гибридных моделей, обладающих повышенной точностью и устойчивостью к различным условиям. В 2023-2024 годах компании, такие как OpenAI и Anthropic, продолжили развивать свои модели, что может привести к улучшению результатов в различных задачах, включая распознавание лиц.

6.1.3. Распознавание лиц с учетом позы

Одним из перспективных направлений является разработка алгоритмов, устойчивых к изменениям позы лица. Техника, предложенная Altaf в 2025 году, использует метод ближайших соседей для определения позы и нейронную сеть на основе расширенной модели ансамбля для распознавания выражений лиц, достигая 90% точности. Учёт различных поз лиц при распознавании выражений, является значительным шагом вперед в этой области.

6.1.4 Федеративное обучение и мультимодальность Технология федеративного машинного обучения, успешно примененная в России в 2024 году, предоставляет возможность обучения моделей без передачи конфиденциальных данных, что особенно важно для задач распознавания лиц, где защита личных данных является приоритетом. Кроме того, отмечается рост интереса к мультимодальным моделям, интегрирующим различные типы данных (изображения, текст, аудио), что может повысить точность и надежность систем распознавания лиц.

6.2. Интеграция с другими технологиями: Искусственный интеллект, интернет вещей, блокчейн

Перспективы развития систем распознавания лиц и биометрии тесно связаны с интеграцией с другими передовыми технологиями, такими как искусственный интеллект (ИИ), интернет вещей (IoT) и блокчейн. Эта интеграция открывает новые возможности для повышения эффективности, надежности и безопасности в сфере предотвращения терактов и диверсий.

Искусственный интеллект (ИИ):

Интеграция ИИ с системами распознавания лиц позволяет значительно повысить точность и скорость идентификации. Современные алгоритмы глубокого обучения обучаются на огромных массивах данных, что снижает количество ошибок даже в сложных условиях, таких как плохое освещение или частичное закрытие лица. Развитие трехмерного распознавания, использующего глубину и контуры лица, также способствует повышению точности идентификации. Ожидается дальнейшая интеграция ИИ с моделями управления доступом, такими как Zero Trust, что повысит адаптивность и автоматизацию контроля доступа.

Интернет вещей (IoT):

IoT предоставляет широкие возможности для создания распределенных систем безопасности и мониторинга. В контексте предотвращения терактов и диверсий, интеграция с IoT может быть реализована через:

Умные камеры и датчики: IoT-устройства, такие как умные камеры с функцией распознавания лиц и датчики движения, могут обеспечивать непрерывный мониторинг критически важных объектов и территорий. Эти системы способны немедленно уведомлять о подозрительной активности, позволяя оперативно реагировать на потенциальные угрозы.

Контроль доступа: IoT-системы могут быть использованы для контроля доступа к охраняемым объектам, интегрируя биометрическую идентификацию с автоматизированными системами управления доступом.

Мониторинг окружающей среды: IoT-датчики могут контролировать условия в местах массового скопления людей, включая уровень влажности и температуры, что особенно важно для выявления аномалий, которые могут свидетельствовать о подготовке к диверсии.

Блокчейн:

Блокчейн технология предлагает решения для защиты биометрических данных от несанкционированного доступа и манипуляций. Ключевые аспекты интеграции блокчейна:

Децентрализованное хранение данных: Использование блокчейна для хранения биометрических данных позволяет создать децентрализованную систему, где данные пользователей хранятся локально, а не в централизованном хранилище, что повышает уровень защиты личной информации.

Неизменность и прослеживаемость данных: Блокчейн обеспечивает неизменность и прослеживаемость данных, делая их невосприимчивыми к изменениям и манипуляциям [[https://scienceforum.ru/2025/article/2018037850]]. Это особенно важно для биометрических данных, используемых в системах безопасности.

Шифрование и управление доступом: Блокчейн можно использовать для управления ключами шифрования и обеспечения безопасного доступа к биометрическим данным.

В целом, интеграция систем распознавания лиц и биометрии с ИИ, IoT и блокчейном создает мощную платформу для повышения эффективности и надежности систем безопасности, способствуя предотвращению терактов и диверсий. Важно отметить, что внедрение этих технологий требует учета этических и правовых аспектов, а также разработки соответствующих стандартов и нормативных актов для защиты личной информации граждан.

6.2. Создание комплексных систем безопасности: Объединение биометрии, видеонаблюдения и аналитики данных

Перспективы развития систем распознавания лиц и биометрии для предотвращения террористических актов и диверсий неразрывно связаны с созданием комплексных систем безопасности, интегрирующих биометрические технологии, видеонаблюдение и аналитику данных. Успешная интеграция этих технологий позволяет значительно повысить уровень безопасности, улучшить операционную эффективность и обеспечить соответствие нормативным требованиям.

Интеграция подразумевает использование многофакторной аутентификации, которая значительно снижает риск несанкционированного доступа. Например, интегрированная биометрическая система может комбинировать биометрическую аутентификацию с ключевыми картами или PIN-кодами для обеспечения многослойной безопасности.

Современные системы видеонаблюдения активно используют технологии искусственного интеллекта (ИИ) для обработки и анализа больших объемов видеоданных в реальном времени. Это позволяет не только быстро находить необходимые фрагменты видео, но и предотвращать потенциальные угрозы. Компании, такие как Hikvision и Dahua Technology, внедряют алгоритмы глубокого обучения, которые улучшают точность распознавания объектов и минимизируют ложные срабатывания.

Умная видеоаналитика позволяет интегрировать видеонаблюдение с другими корпоративными системами, что дает возможность реализовывать сложные сценарии детектирования нарушений и повышает эффективность управления безопасностью. Например, VizorLabs предлагает более 100 предобученных детекторов для различных задач.

В контексте международного сотрудничества, важно отметить, что эффективность комплексных систем безопасности в предотвращении террористических актов зависит от уровня

сотрудничества между государствами, разработки и реализации совместных программ и концепций, а также от постоянного обновления нормативно-правовой базы. В условиях современных угроз, таких как терроризм и экстремизм, важно, чтобы страны-участницы объединяли свои усилия и ресурсы для более эффективного противодействия этим вызовам.

6.3. Развитие нормативно-правовой базы: Регулирование использования технологий распознавания лиц и биометрии

Поскольку технологии распознавания лиц и биометрии становятся все более распространенными в контексте предотвращения террористических актов и диверсий, крайне важно создать надежную нормативно-правовую базу, регулирующую их применение.

На сегодняшний день, 27 марта 2025 года, существуют следующие ключевые направления, требующие законодательного урегулирования:

Ограничение сбора и хранения биометрических данных. Необходимо четко определить цели, для которых может осуществляться сбор биометрических данных, а также установить максимальные сроки их хранения. Должны быть прописаны строгие требования к защите этих данных от несанкционированного доступа, утечек и злоупотреблений.

Прозрачность и осведомленность. Граждане должны быть информированы о том, где и как используются системы распознавания лиц, а также иметь возможность получить информацию о собранных о них данных и оспорить их достоверность. Следует разработать механизмы для обеспечения прозрачности алгоритмов распознавания и исключения дискриминации.

Ответственность за ошибки. Необходимо установить юридическую ответственность за ошибки систем распознавания лиц, приводящие к необоснованным задержаниям, обвинениям или другим негативным последствиям для граждан. Следует определить порядок компенсации ущерба, причиненного такими ошибками.

Контроль и надзор. Важно создать независимый орган, осуществляющий контроль и надзор за соблюдением законодательства в сфере использования биометрических технологий. Этот орган должен иметь полномочия по проведению проверок, расследованию нарушений и применению санкций.

Международное сотрудничество. Необходимо развивать международное сотрудничество в области нормативно-правового регулирования технологий распознавания лиц и биометрии, в том числе путем обмена опытом и разработки общих стандартов. Это особенно важно в контексте борьбы с трансграничным терроризмом и диверсиями.

Использование данных только в заявленных целях. Использование собранных биометрических данных должно быть строго ограничено целями предотвращения террористических актов и диверсий. Запрещено использование этих данных в иных целях, например, для коммерческой рекламы или профилирования граждан. Необходимо предусмотреть санкции за нарушение этого принципа.

Разработка и принятие четкой и всеобъемлющей нормативно-правовой базы позволит обеспечить эффективное использование технологий распознавания лиц и биометрии для защиты общества от террористических угроз и диверсий, одновременно гарантируя соблюдение прав и свобод граждан. Отсутствие такого регулирования может привести к злоупотреблениям, нарушениям прав человека и подрыву доверия к этим технологиям.

Заключение

В заключение, системы распознавания лиц и биометрия представляют собой мощные инструменты для повышения безопасности и предотвращения террористических актов и диверсий. Однако их применение требует комплексного подхода, учитывающего технические аспекты.

Актуальность проблемы терроризма и диверсий в современном мире подчеркивает необходимость разработки и внедрения эффективных технологий для обеспечения общественной безопасности. Системы распознавания лиц и биометрии могут значительно повысить уровень защиты, однако их использование должно быть строго регламентировано.

Ключевыми задачами остаются создание надежной нормативно-правовой базы, которая обеспечит защиту персональных данных, прозрачность алгоритмов и возможность обжалования решений, принятых на основе биометрических данных. Также важно учитывать риски дискриминации и нарушения приватности, которые могут возникнуть при использовании этих технологий.

Интеграция биометрических систем с другими передовыми технологиями, такими как искусственный интеллект, интернет вещей и блокчейн, открывает новые горизонты для повышения эффективности и надежности систем безопасности. Однако для успешной реализации этих технологий необходимо обеспечить соблюдение прав и свобод граждан, а также активное участие общества в обсуждении вопросов, связанных с их использованием.

Таким образом, будущее систем распознавания лиц и биометрии зависит от их этичного применения, соблюдения правовых норм и постоянного совершенствования технологий, что позволит эффективно противостоять современным угрозам безопасности.

Список литературы:

1. Statista - Number of terrorist attacks in 2023, by country [Электронный ресурс] // www.statista.com - Режим доступа: https://www.statista.com/statistics/236983/terrorist-attacks-by-country/, свободный. - Загл. с экрана.

2. Global Terrorism Index 2025 [Электронный ресурс] // reliefweb.int - Режим доступа: https://reliefweb.int/report/world/global-terrorism-index-2025, свободный. - Загл. с экрана.

3. Таджикский государственный медицинский университет [Электронный ресурс] // tajmedun.tj - Режим доступа: https://tajmedun.tj/ru/novosti/universitet/terrorizm-i-ekstremizm-ugroza-obshchestvennoy-bezopasnosti204/, свободный. - Загл. с экрана.

4. IEEE Biometrics Council Newsletter [Электронный ресурс] // newsletter.radensa.ru - Режим доступа: https://newsletter.radensa.ru/archives/8893, свободный. - Загл. с экрана.

5. Некоторые вопросы использования биометрических технологий в борьбе с терроризмом [Электронный ресурс] // cyberleninka.ru - Режим доступа: https://cyberleninka.ru/article/n/nekotorye-voprosy-ispolzovaniya-biometricheskih-tehnologiy-v-borbe-s-terrorizmom, свободный. - Загл. с экрана.

6. Аналитический доклад о биометрии и терроризме от ООН [Электронный ресурс] // www.un.org - Режим доступа: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_analytical_brief_biometrics_ru.pdf, свободный. - Загл. с экрана.

7. zkteco-store.ru [Электронный ресурс] // zkteco-store.ru - Режим доступа: https://zkteco-store.ru/gotovye-resheniia/innovacionnye-tehnologii-visiblelight/, свободный. - Загл. с экрана.

8. Krizhevsky et al., 2017 [Электронный ресурс] // link.springer.com - Режим доступа: https://link.springer.com/article/10.1007/s11042-020-09850-1, свободный. - Загл. с экрана.

9. Беркасов, П. Ю., 2023 [Электронный ресурс] // moluch.ru - Режим доступа: https://moluch.ru/archive/482/105735/, свободный. - Загл. с экрана.

10. EURECOM [Электронный ресурс] // www.eurecom.fr - Режим доступа: https://www.eurecom.fr/en/publication/8102, свободный. - Загл. с экрана.

11. InfoWatch [Электронный ресурс] // www.infowatch.ru - Режим доступа: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/biometricheskaya-identifikatsiya-voprosy-regulirovaniya, свободный. - Загл. с экрана.
12. Газета. Ru [Электронный ресурс] // www.gazeta.ru - Режим доступа: https://www.gazeta.ru/tech/news/2025/02/25/25177478.shtml, свободный. - Загл. с экрана.
13. Sigma IS [Электронный ресурс] // www.sigma-is.ru - Режим доступа: https://www.sigma-is.ru/files/article/art_ab_nic_5_2015.pdf, свободный. - Загл. с экрана.
14. Habr, 2023 [Электронный ресурс] // habr.com - Режим доступа: https://habr.com/ru/articles/887268/, свободный. - Загл. с экрана.
15. Altaf et al., 2025 [Электронный ресурс] // journals.plos.org - Режим доступа: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0316562, свободный. - Загл. с экрана.
16. TAdviser [Электронный ресурс] // www.tadviser.ru - Режим доступа: https://www.tadviser.ru/index.php/Статья:LLM_(Большие_языковые_модели), свободный. - Загл. с экрана.
17. [Электронный ресурс] // incode.com - Режим доступа: https://incode.com/blog/innovations-in-biometrics-whats-new-and-whats-on-the-horizon/, свободный. - Загл. с экрана.
18. [Электронный ресурс] // rb.ru - Режим доступа: https://rb.ru/opinion/unified-biometric-system-future/, свободный. - Загл. с экрана.
19. Bioqube, 2024 [Электронный ресурс] // bioqube.ai - Режим доступа: https://bioqube.ai/blog/how-biometrics-enhance-airport-security/, свободный. - Загл. с экрана.
20. Авиапорт, 2025 [Электронный ресурс] // www.aviaport.ru - Режим доступа: https://www.aviaport.ru/news/621891/, свободный. - Загл. с экрана.
21. International Airport Review, 2024 [Электронный ресурс] // www.internationalairportreview.com - Режим доступа: https://www.internationalairportreview.com/article/225603/how-biometrics-is-driving-innovation-in-airports-despite-legislative-restrictions/, свободный. - Загл. с экрана.
22. [Электронный ресурс] // gdpr.eu - Режим доступа: https://gdpr.eu/, свободный. - Загл. с экрана.
23. [Электронный ресурс] // oag.ca.gov - Режим доступа: https://oag.ca.gov/privacy/ccpa, свободный. - Загл. с экрана.
24. http://www.consultant.ru/document/cons_doc_LAW_61801/
25. KompUnity [Электронный ресурс] // kompunity.by - Режим доступа: https://kompunity.by/top-5-tehnologij-videonablyudeniya-2025-ii-raspoznavanie-lits-i-oblachnye-sistemy/, свободный. - Загл. с экрана.