НАУЧНЫЙ ОБЗОР

УДК 004.056.55
DOI

АНАЛИЗ МЕТОДОВ FACE ANTI-SPOOFING ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Минкин А.В., Каракеян А.С.

ФГАОУ ВО «Казанский федеральный университет», Елабуга, e-mail: avminkin@kpfu.ru

Статья посвящена вопросам биометрической аутентификации, а конкретно методам Face Anti-Spoofing, направленным на защиту от попыток обмана систем распознавания лиц. Подчеркивается важность этих методов в эпоху цифровой трансформации, когда биометрические данные становятся ключевыми информационными ресурсами в разных сферах жизни. Целью работы является рассмотрение современного состояния технологий защиты биометрических систем и рекомендации по их практическому применению в условиях цифрового общества. Методология исследования основана на анализе и систематизации научной литературы. В ходе исследования был проведен анализ 288 публикаций, из которых отобраны 48, охватывающих современные подходы в Face Anti-Spoofing. Рассмотрены публикации из научных баз данных eLIBRARY.RU, Scopus и Google Scholar за последние 5 лет. Методы FAS классифицированы по уровню риска и требованиям к аппаратуре, выделены три уровня угроз: низкий, средний и высокий риск. Особое внимание уделяется использованию различных аналитических инструментов, таких как LBP, Optical Flow и нейросети типа CNN, RNN и трансформеров. Кроме того, проведен сравнительный анализ правового регулирования сферы обработки биометрических данных между российским Федеральным законом № 152-ФЗ и Европейским регламентом GDPR, выявлены различия в степени детализации и жесткости санкций. В заключение сделан вывод о важности непрерывного улучшения технологий и моделей FAS для эффективной борьбы с новыми видами угроз, такими как распространение Deepfake и усовершенствованные способы обхода защитных механизмов.

Ключевые слова: биометрия, face anti-spoofing, витальность, пассивные методы, идентификация, глубокое обучение, цифровизация

ANALYSIS OF FACE ANTI-SPOOFING METHODS FOR ENSURING THE SECURITY OF BIOMETRIC AUTHENTICATION IN THE CONTEXT OF DIGITALIZATION

Minkin A.V., Karakeyan A.S.

Kazan Federal University, Yelabuga, e-mail: avminkin@kpfu.ru

The article is devoted to the issues of biometric authentication, specifically Face Anti-Spoofing methods aimed at protecting against attempts to deceive facial recognition systems. The importance of these methods is emphasized in the era of digital transformation, when biometric data are becoming key information resources in various spheres of life. The purpose of the work is to consider the current state of biometric system protection technologies and recommendations for their practical application in a digital society. The research methodology is based on the analysis and systematization of scientific literature. The study analyzed 288 publications, of which 48 were selected, covering modern approaches to Face Anti-Spoofing. Publications from scientific databases of eLibrary data are considered.RU, Scopus and Google Scholar for the last 5 years. FAS methods are classified by risk level and hardware requirements, and three threat levels are identified – low, medium, and high risk. Special attention is paid to the use of various analytical tools such as LBP, Optical Flow, and neural networks such as CNN, RNN, and transformers. In addition, a comparative analysis of the legal regulation of biometric data processing between Russian Federal Law No. 152-FZ and the European Regulation GDPR was carried out, revealing differences in the degree of detail and severity of sanctions. In conclusion, it is concluded that it is important to continuously improve FAS technologies and models in order to effectively combat new types of threats, such as the spread of Deepfake and improved ways to circumvent security mechanisms.

Keywords: biometrics, face anti-spoofing, vitality, passive methods, identification, deep learning, digitalization

Введение

В настоящее время главным ресурсом является информация, а среди множества её аспектов превыше всего находится именно тот, который связан с биометрическими данными человека. Биометрия включает в себя набор данных о человеке: особенности внешности, голоса, лица, пальцев, телосложения, роста и поведения, которые уникальны [1; 2]. С принятием федеральной программы «Информационное общество» 2014 года в Российской Федерации была поставлена цель полной цифровизации всех общественно-государственных услуг. В ее рамках произошла глобальная автоматизация всех процессов, охватывающих административные и социальные задачи [3]. Также программа включает в себя и модернизацию системы идентификации и аутентификации личности гражданина. Переход этой системы на электронную платформу обеспечил высокую скорость обработки

данных, предотвращение правонарушений, а значит, и повышение общественного порядка, облегчил процесс совершения мелких бытовых покупок. Однако внедрение автоматизированной системы биометрии привело и к появлению новых вызовов, связанных, в первую очередь, с попытками обмана системы.

Цель исследования – осветить современное состояние технологий защиты биометрических систем и дать рекомендации по их практическому применению в условиях цифрового общества.

Материалы и методы исследования

Проведенное исследование базировалось на анализе специализированной научной литературы и публикаций по протоколу PRISMA, освещающих современные подходы в Face Anti-Spoofing (FAS). Для этого использовались статьи из отечественных и зарубежных научных журналов, а также материалы ведущих международных конференций на русском и английских языках, опубликованные в 2020-2025 гг., из баз данных eLIBRARY.RU, РИНЦ, Scopus и IEEExplore с высоким impact factor. Для поиска использовались такие строки запросов, как biometrics, face anti-spoofing, vitality, passive methods, identification, лицевая биометрия, предотвращение ложной аутентификации по лицу, защита от подделок при распознавании лица, обработка персональных данных, при этом не рассматривались дублирующие исследования, репринты, исследования на иных языках, кроме заявленных (английский и русский), письма и краткие сообщения. При поиске в базах данных eLIBRARY.RU, РИНЦ найдено 205 публикаций. Поиск по другим научным базам проводился аналогично. Всего 288 публикаций включены в поиск и посвящены: биометрической идентификации и аутентификации – 124, развитию технологий распознавания лиц – 86, этическим и правовым аспектам – 57, практическому применению и внедрению технологий – 21. По результатам поиска 48 работ легли в основу данного обзора: 1) обзор классификации методов FAS, 2) обзор направлений развития технологии распознавания лиц, 3) обзор нормативно-правовых требований для обработки персональных данных, 4) обзор практического применения и внедрения технологии. Полученные в результате систематического обзора и метаанализа научные данные могут быть применены при формулировании рекомендаций относительно выбора оптимальной стратегии обеспечения безопасности.

Результаты исследования и их обсуждение

1. Классификация методов FAS.

FAS – это система, обеспечивающая распознавание настоящего лица от фальшивого, дающая возможность с помощью анализа изображения в видеопотоке определить, используется ли для аутентификации биометрический образец, взятый у живого объекта [4]. Методы FAS можно классифицировать по используемой информации и необходимости специализированного оборудования [5]. Многие авторы используют следующую классификацию этих методов: пассивные, активные и гибридные [6–8]. Однако для эффективной организации и анализа методов FAS предлагается следующая таксономия, основанная на двух ключевых аспектах: рисковый профиль атаки и вычислительные ограничения. Для классификации методов FAS по уровню риска используем два ключевых показателя: ACER (Average Classification Error Rate) – средняя частота ошибок классификации, которая характеризует общее качество метода FAS, оценивая одновременно успешность обнаружения атак и число ложноположительных результатов, и BPCER (Bonafide Presentation Classification Error Rate) – частота ошибок правильной аутентификации настоящих пользователей, т.е. процент случаев, когда настоящие пользователи неверно отвергнуты системой как поддельные. Эти метрики позволяют находить компромисс между безопасностью (минимизировать ошибки принятия атак) и комфортом пользователей (минимизировать необоснованное блокирование).

Рассмотрим три уровня риска и соответствующие им ресурсные требования. Атаки с низким уровнем сложности и вероятности успеха обычно включают использование простых методов, таких как низкокачественные фотографии или примитивные маски (ACER $\leq$ 1%, BPCER $\leq$ 0.5%). Эти атаки легко обнаруживаются современными системами безопасности и требуют минимальных ресурсов для реализации. Атаки среднего уровня сложности используют улучшенные маски, качественные фотографии и простые видеоподделки (Deepfake) (1% < ACER $\leq$ 5%, 0.5% < BPCER $\leq$ 2%). Эти атаки сложнее обнаружить, поскольку они выглядят более убедительно. Сложные атаки (ACER > 5%, BPCER > 2%), включают высококачественные трехмерные маски, реалистичные Deepfake и комбинированные методы обмана [9–11].

Такое деление помогает разработчикам чётко понимать минимальный уровень

защиты, соответствующий каждому типу угроз. Оно также способствует оптимизации ресурсов, позволяя выбирать оптимальное соотношение затрат и уровня безопасности. Простые методы, используемые в атаках низкого риска, требуют минимальных ресурсов. Они подходят для недорогих мобильных устройств и бюджетных серверов. Например, для создания примитивной маски достаточно обычного принтера и бумаги. Среднетяжелые методы, применяемые в атаках среднего риска, требуют средних вычислительных мощностей. Обычные процессоры и стандартные графические карты способны обеспечить достаточные ресурсы для этих целей. Например, создание качественной маски требует использования специализированных программ для моделирования и печати. Мощные методы, характерные для атак высокого риска, нуждаются в высокопроизводительном оборудовании.

Графические ускорители и специализированные чипы позволяют быстро обрабатывать большие объемы данных и создавать сложные подделки. Например, обучение модели Deepfake требует мощных GPU и больших объемов памяти [12-14]. Для борьбы с Deepfake самым доступным методом является анализ свойства изображения/видеопотока с использованием стандартных (RGB) камер, встроенных в оборудование. Система автоматически анализирует видеопоток и определяет витальность человека (витальность означает, что с системой контактирует «живой» человек) [15]. Одними из популярных анализов в этом случае считаются отслеживание моргания глаз, движения губ [16], сравнение модели с лицом в видеопотоке, изменение эмоций и повороты головы. Для этого применяются алгоритмы анализа локальных бинарных паттернов (Local Binary Patterns – LBP), техники вейвлет-анализа и методы оценки пространственных градиентов [17]. Кожа человека обладает уникальными микрохарактеристиками (например, структура пор, рельеф поверхности), отличающимися от характеристик искусственных материалов (экран монитора, бумага) [18; 19]. Алгоритмы оптического потока (Optical Flow) [20–22] и временные ряды позволяют выявить характерные особенности живых лиц, такие как непроизвольная моторика, отсутствующая в статичных изображениях или видеоматериалах низкого разрешения.

Методики обнаружения экранных границ, артефактов компрессии видеосигнала, характерных световых рефлексов (отражения стекла очков, специфическое освещение дисплея) используются для идентификации представленного объекта как искусственно воспроизведённого [23]. Методы глубокого обучения (Convolutional Neural Networks – CNN [24], Recurrent Neural Networks – RNN [25], Transformer Architectures [26]) обеспечивают эффективное распознавание тонких признаков различия между подлинными лицами и искусственными объектами. Применяются также и специальные инфракрасные датчики, которые фиксируют отражение активного инфракрасного излучения (ИК) от кожных покровов субъекта [27]. У живых лиц распределение температуры неоднородно вследствие особенностей кровоснабжения, выраженных тёплыми зонами, соответствующими анатомическим сосудистым структурам [28]. Наконец, существуют так называемые мультимодальные или гибридные методы, которые представляют совмещение программного обеспечения с аппаратными средствами [29; 30].

Предлагаемая таксономия (табл. 1) отличается от традиционной классификации («активные / пассивные / гибридные») четкой корреляцией с риск-профилем. Традиционная классификация фокусируется преимущественно на используемых инструментах и технических средствах (камера, датчики и т.п.). Предлагаемый подход основан на уровнях риска и вычисляемых показателях, что обеспечивает четкое понимание требуемой защищенности и затрат.

Таблица 1

Матрица соответствия методов

Категория	Низкий риск	Средний риск	Высокий риск
Минимальные ресурсы	Процедурные анализы (анализ пикселей, простейшие алгоритмы машинного зрения)	Анализ движения (глаза, губы)	Использование легких CNN
Умеренные ресурсы	Легкие CNN, анализ глубинной карты	Глубокие CNN, мультимодальные методы	Анализ теплового отпечатка, комбинация датчиков
Высокие ресурсы	Глубокие CNN с дополнительными датчиками	Трансформеры, многоуровневые нейросети	Специализированные датчики, многослойные защитные механизмы

Источник: составлено авторами на основе полученных данных в ходе исследования.

Таксономия позволяет быстрее подобрать подходящий метод защиты в зависимости от конкретных условий эксплуатации и предполагаемой интенсивности атак. Использование критериев, таких как ACER и BPCER, гарантирует актуальность подхода применительно к последним достижениям в области Face Anti-Spoofing. Таким образом, данная таксономия обеспечивает структурированный подход к обеспечению безопасности биометрической аутентификации, учитывая актуальные технологические реалии и потребности цифровой эпохи.

2. Обзор направлений развития технологии распознавания лиц.

Технология распознавания лиц является быстро развивающейся областью исследований, при этом остается ряд проблем, которые связаны с точностью, безопасностью и устойчивостью к атакам и требуют дальнейшего изучения и разработки инновационных решений [31; 32]. Одним из факторов повышения точности технологий распознавания лиц является расширение тренировочных наборов данных (FaceForensics++, Deepfake Detection, CELEB-A, CELEB-DF, Deepfake Detection Challange, DF-TIMIT, DF-1.0 и др.) [33–35]. Кроме того, исследователи работают над созданием синтетически генерируемых данных с использованием генеративных состязательных сетей (GANs) [36–38]. GAN позволяют создавать реалистичные изображения лиц, которые затем используются для расширения существующих наборов данных. Однако используемые данные представляют ограниченный набор, что приводит к тому, что разработчики сосредотачиваются лишь на заранее определенных видах атак, поэтому в последние годы ученые начали активно исследовать способы повышения устойчивости моделей обнаружения поддельных атак к неизвестным угрозам.

Среди наиболее перспективных подходов выделяются методы zero-shot/few-shot [14; 26]. Суть метода заключается в том, что модель обучается генерировать признаки и обобщенные шаблоны, способные эффективно справляться с новыми видами атак, которые отсутствовали в тренировочном наборе данных [39]. Основная разница между этими двумя подходами состоит именно в наличии или отсутствии доступного количества образцов новых видов атак. При обучении с нулевым числом примеров система учится выявлять новые угрозы исключительно на основе существующих типов атак, без наличия хотя бы минимального числа реальных примеров новой атаки. Этот подход особенно полезен, когда сбор дополнительных данных является дорогостоящим или невозможным процессом. Методы с несколькими примерами, напротив, предполагают наличие небольшого объема новых данных, что позволяет дополнительно повысить точность классификации путем тонкой настройки параметров модели. Использование таких подходов требует тщательной разработки архитектуры нейронных сетей, способных эффективно извлекать и обобщать признаки различных классов подделок, поэтому глубокие нейронные сети также становятся основой для создания FAS [10]. Также разработчики оптимизируют алгоритмы, уменьшая требования к производительности конечного устройства, что делает возможным применение этих технологий на смартфонах и планшетах [15], и используют многомерные данные (голос, частота сердечных сокращений и температура тела).

Как ранее авторами было упомянуто, для оценки эффективности технологий распознавания лиц необходимы надежные и объективные метрики, такие как BPCER, ACER, коэффициент ошибок классификации атаки посредством представления (APCER – Attack Presentation Classification Error Rate), равная ошибка обнаружения (D-EER – Detection Equal Error Rate) [39; 40]. Однако, как правило, в публикациях, посвященных FAS, есть привязка датасета и методов, которые используют исследователи для оценки качества модели, поэтому, как отмечено в работе [5], выбранные методы остаются недостаточно универсальными для широкого применения в различных сценариях реального мира. В результате метрики, при работе с внутренними базами данных, где условия съемки и качество изображений схожи с условиями реальных запросов, показывают лучший результат в сравнении с переходом к кросс-базовым сценариям, где различия между зарегистрированными лицами и предъявляемыми изображениями значительны. Таким образом, разработка надежной системы защиты от подделки лиц требует интеграции современных технологий глубокого обучения, использования многоканальных подходов и постоянного расширения наборов данных. Только комплексное решение сможет обеспечить необходимую защиту в условиях постоянно меняющихся угроз и требований безопасности.

3. Обзор нормативно-правовых требований для обработки персональных данных.

Защита персональных данных является приоритетом как для граждан, так и для бизнеса во всем мире, поэтому Европейский союз (ЕС) принял «Общий регламент по защите данных» (GDPR), который устанавливает строгие правила обработки персональных данных. Российская Федерация также имеет ряд законодательных актов, регулирующих защиту личной информации граждан.

Таблица 2

Сравнение GDPR и Российского ФЗ-152

Критерий	GDPR	Российский ФЗ-152
Требования к сбору	Свободное и осознанное согласие	Добровольное письменное согласие
Локализация данных	Нет обязательного требования	Хранение в РФ
Ответственность	Штрафы до €20 млн	Штрафы до ₽75 тыс.
Цель обработки	Ограниченная	Минимальная
Особенности контроля	Регулятор ICPE	Роскомнадзор

Источник: составлено авторами на основе полученных данных в ходе исследования.

Пожалуй, основным является Федеральный закон № 152-ФЗ «О персональных данных», который применяется исключительно на территории Российской Федерации и касается только российских граждан и компаний, работающих на российском рынке. Этот закон также определяет основные термины и принципы обработки персональных данных, но его требования менее детализированы по сравнению с GDPR [41]. GDPR предоставляет субъектам данных широкие права, эти права являются обязательными для исполнения всеми организациями, работающими с персональными данными [42]. Федеральный закон № 152-ФЗ также предусматривает некоторые права субъектов данных, такие как право на доступ к своим данным и право требовать прекращения обработки данных. Оценка рисков и уведомительные процедуры в случае нарушений данных также менее формализованы и строго определены, чем в GDPR. Нарушение требований GDPR может повлечь серьезные штрафы. В России нарушения законодательства о защите персональных данных наказываются штрафами значительно меньшего размера, обычно исчисляемыми тысячами рублей. Надзорным органом выступает Роскомнадзор, который осуществляет проверки и принимает решения о наложении штрафов. Эти нормативно-правовые акты обеспечивают правовую основу для обработки персональных данных и устанавливают строгие правила для организаций, работающих с такими данными. Таким образом, несмотря на схожесть целей регулирования, GDPR и российские законы существенно различаются по степени детализации, широте предоставляемых прав и суровости санкций (табл. 2). Кроме того, для различных отраслей существуют свои особенности и рекомендации профильных комитетов обеспечения безопасности биометрической аутентификации. Например, в банковском секторе, помимо № 152-ФЗ, банки следуют внутренним правилам и указаниям Центрального банка РФ (№ 6540-У) и международным стандартам (ISO/IEC 27001, PCI DSS). Ассоциация банков России рекомендует использовать FAS совместно с другими способами подтверждения личности. В государственном секторе существуют нормативные документы Федеральной службы безопасности (Приказ 13.02.2023 № 77, от 11.05.2023 № 213, от 18.03.2025 № 117), Министерства связи и массовых коммуникаций (Приказ от 10.09.2021 № 930), Постановление Правительства Российской Федерации (Приказ от 23.10.2021 № 1815), а межведомственная комиссия по защите государственной тайны рекомендует осуществлять проверку исходящих потоков данных и контроль возможных вторжений через вредоносные файлы. В IT-секторе ассоциация профессиональных разработчиков программного обеспечения России рекомендует проводить сертификацию продуктов FAS независимыми лабораториями на предмет устойчивости к новым видам угроз. Руководствуясь рекомендациями профильных комитетов и правилами профильных ведомств, организация сможет обеспечить надежную защиту своей инфраструктуры и минимизировать риски.

4. Применение технологий FAS.

FAS внедряется поэтапно, начиная с пилотного этапа, на котором проверяется совместимость системы с инфраструктурой предприятия, оценивается функциональность и безопасность. Следующий шаг – стадия масштабирования, предусматривающая постепенное увеличение числа пользователей и проведение обучающих мероприятий. Завершающий этап – регулярное обслуживание, направленное на поддержание стабильности и своевременное обновление системы. Критериями успеха каждого этапа являются положительные отзывы, низкий уровень ошибок и готовность инфраструктуры. Мониторинг производительности и постоянная обратная связь обеспечивают плавный переход между стадиями внедрения. Уже сейчас FAS-технология активно применяется в разнообразных сферах, включая коммерческие организации и государственные структуры [43; 44].

Компания Apple использует систему Face ID с защитой от spoofing [45]. Для повышения безопасности она ввела методы детекции живых лиц, используя инфракрасные датчики и алгоритмы машинного обучения. Полиция и спецслужбы также применяют FAS-решения для контроля доступа на режимные объекты и выявления преступников с высокой точностью и минимизацией риска ложных срабатываний [46]. Компании используют FAS-технологии для удалённой верификации работников, особенно при доступе к корпоративным данным и системам управления [47].

Если рассматривать выбор методов FAS в зависимости от сценариев применения, то для мобильных приложений можно рекомендовать простые и энергоэффективные методы, такие как LBP, миниатюрные CNN-модели и анализ оптического потока. Для серверных решений лучше подойдут продвинутые алгоритмы глубокого обучения (глубокие CNN, трансформеры) и многомодальные методы. В корпоративной среде рекомендуется внедрять комплексные меры защиты, включающие многослойные проверки, мониторинг окружающей среды и интегрированную биометрию. Это позволит эффективно применять технологии FAS, балансируя между производительностью, стоимостью и степенью необходимой защиты.

5. Выводы.

Научные исследования в области лицевой биометрии имеют значительный рост в последние годы. Используя только одно ключевое слово DeepFake в поисковой системе Mendeley и ограничившись только англоязычной литературой, имеем следующий результат (рис. 1). На рисунке 1 построены график по годам и диаграмма по типам публикации, которые показывают линейный рост публикаций и почти 50%-ное присутствие журнальных статей.

Для более детального анализа в данной статье использовался трехэтапный протокол проведения систематического обзора: формулировка исследовательских вопросов, поиск в базах данных и критерии включения и исключения исследовательских статей (рис. 2). Исследовательские вопросы: таксономия FAS, направление развития, нормативно-правовые требования и применение, определили содержание данного обзора. Поиск осуществлялся по ключевым словам, указанным в разделе «Материалы и методы исследования» данного обзора с использованием оператора «ИЛИ». Авторы использовали следующие шаги для выбора подходящих статей для этого исследования: идентификация, скрининг, включение. Критериями включения статей были: оригинальные исследовательские статьи, обзорные статьи, опубликованные в период с 2020 по 2025 г., которые содержат ключевые слова для поиска в названии, аннотации или полном тексте научных статей, статьи, которые дают положительный ответ хотя бы на один исследовательский вопрос, в которых разработанное решение должно быть направлено на устранение проблем с обнаружением атак с использованием распознавания лиц. Критериями исключения являются: дублирующие исследовательские статьи, статьи с отсутствием полного текста и не имеющие отношения к обнаружению живых лиц.

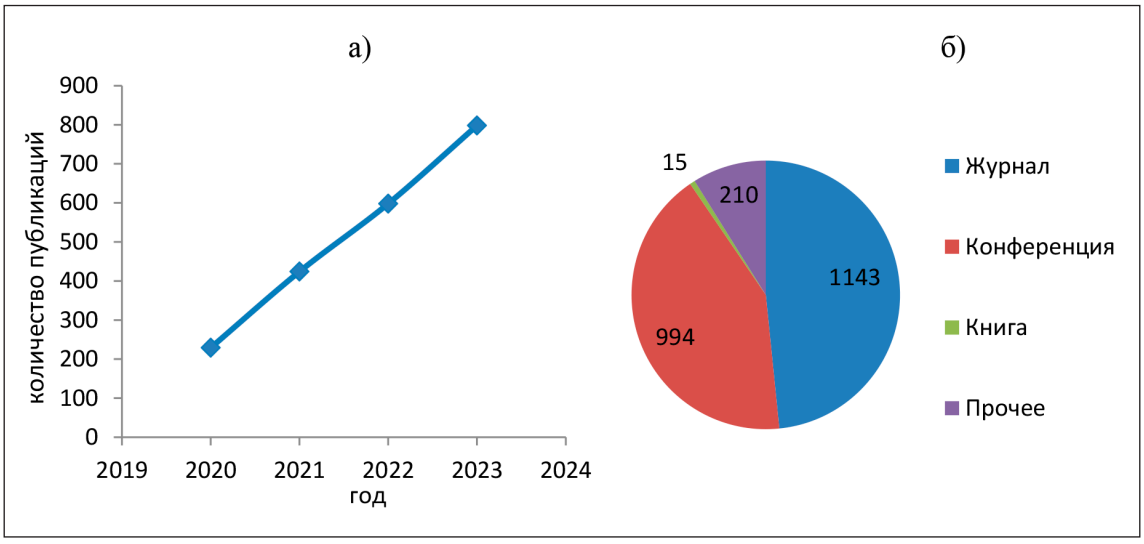

Рис. 1. Распределение научных статей по (а) году публикации, (б) типу публикации
Источник: составлено авторами на основе полученных данных в ходе исследования

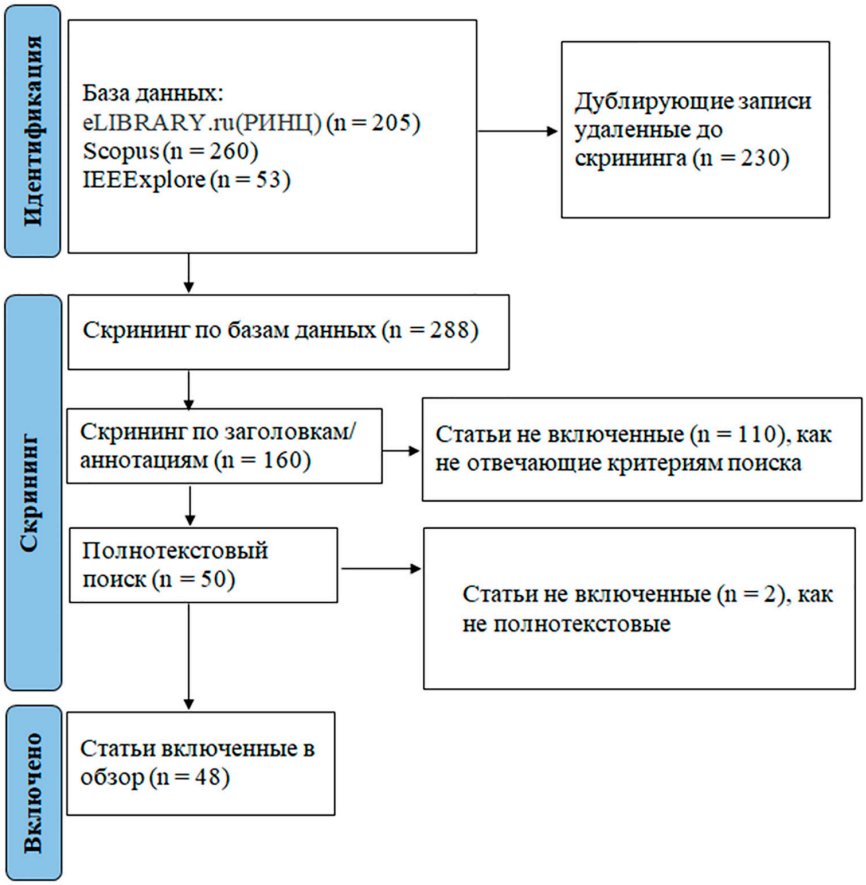

Рис. 2. Диаграмма потока PRISMA
Источник: составлено авторами на основе полученных данных в ходе исследования

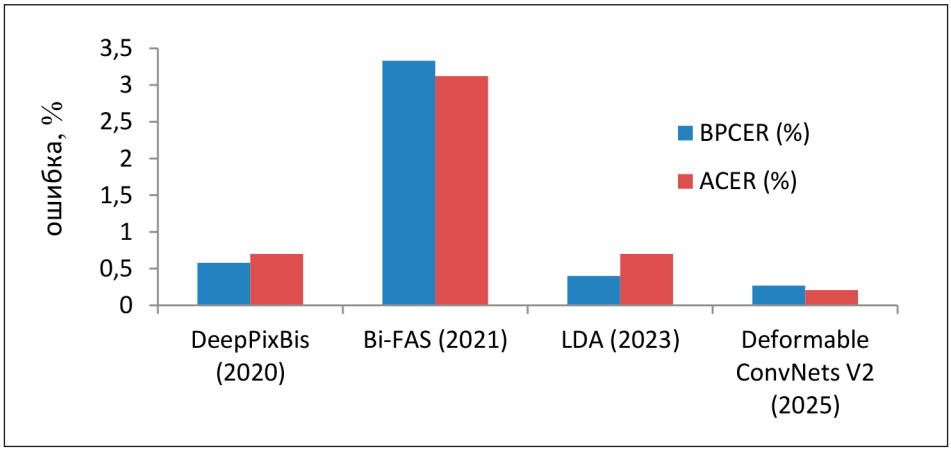

Рис. 3. Сравнения BPCER, ACER для датасета OULU-NPU
Источник: составлено авторами на основе полученных данных в ходе исследования

В обзоре авторы указывали, что в публикациях по данной теме используются различные методы и базы данных, поэтому для примера приведем измерение показателей ACER и BPCER на датасете OULU-NPU (рис. 3) [48].

На рисунке 3 видно, что наблюдается снижение измеренных показателей с 2021 по 2025 г. благодаря разработке новых методов. Отметим, что в статьях по данной теме, несмотря на отмеченные ранее проблемы и перспективы исследования, наблюдается

улучшение показателей основных метрик, методов и алгоритмов исследования.

Заключение

Проведенный обзор позволяет сделать следующие важные выводы относительно современного состояния и перспектив развития технологий FAS. Биометрия становится ключевым элементом безопасности в цифровом обществе, особенно в свете ускоренной цифровизации различных сфер жизни. Автоматизированные системы распознавания сталкиваются с новыми рисками, такими как технологии Deepfake, создающими серьезные угрозы безопасности. Исследованы основные тенденции в развитии методов противодействия спуфингу, среди которых выделяется потенциал глубоких нейронных сетей (CNN, RNN, трансформеры). Несмотря на активное внедрение биометрических технологий, нормативно-правовая база остается недостаточно проработанной, требуя дальнейшей гармонизации с международными стандартами (GDPR). Таким образом, обзор выявил острую потребность в дальнейшем совершенствовании существующих методов защиты, повышении надежности систем и выработке адекватных правовых механизмов регулирования обращения с персональными данными. Результаты указанного обзора и комплексный подход позволяют выбрать оптимальный метод FAS, исходя из рискового профиля атаки и вычислительных ограничений.

Список литературы

1. Карцан И.Н. Биометрические данные: новые возможности и риски // Современные инновации, системы и технологии. 2023. № 3. С. 0201-0211. URL: https://cyberleninka.ru/article/n/biometricheskie-dannye-novye-vozmozhnosti-i-riski (дата обращения: 09.06.2025).

2. Жуков Я.В., Лысенко Р.Ю., Протас Н.Г., Тарасова Г.М. Биометрия. Как работает и какие риски несет? // Modern Economy Success. 2020. № 3. С. 13-19. EDN: RCPMFQ.

3. Храмов Е.Н., Вершинина О.В. Биометрические технологии как фактор повышения безопасности и конкурентоспособности в финансовой инфраструктуре России // Фундаментальные исследования. 2025. № 4. С. 69-79. URL: https://fundamental-research.ru/ru/article/view?id=43814 (дата обращения: 10.06.2025).

4. Ming Z., Visani M., Luqman M.M., Burie J.C. A survey on anti-spoofing methods for facial recognition with rgb cameras of generic consumer devices // Journal of imaging. 2020. Vol. 6. № 12. DOI: 10.3390/jimaging6120139.

5. Anthony P.B. Ay and G. Aydin, A Review of Face Anti-spoofing Methods for Face Recognition Systems // 2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA), Kocaeli, Turkey. 2021. P. 1-9. DOI: 10.1109/INISTA52262.2021.9548404.

6. Золотарев В.В., Поважнюк А.О., Маро Е.А. Методы усиления процедуры идентификации пользователей на основе технологии liveness detection // Известия ЮФУ. Технические науки. 2022. № 2 (226). С. 212-225 . DOI: 10.18522/2311-3103-2022-2-212-225.

7. Yu Z., Qin Y., Li X., Zhao C., Lei Z., Zhao G. Deep Learning for Face Anti-Spoofing: A Survey // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023. Vol. 45. № 5. P. 5609-5631. DOI: 10.1109/TPAMI.2022.3215850.

8. Heidari A., Jafari Navimipour N., Dag H., Unal M. Deepfake detectionusing deep learning methods: A systematic and comprehensive review. // WIREs Data Mining and Knowledge Discovery. 2024. Vol. 14. DOI: 10.1002/widm.1520.

9. Malik A., Kuribayashi M., Abdullahi S.M., Khan A.N. DeepFake Detection for Human Face Images and Videos: A Survey // IEEE Access. 2022. Vol. 10. P. 18757-18775. DOI: 10.1109/ACCESS.2022.3151186.

10. Rana M.S., Nobi M.N., Murali B., Sung A.H. Deepfake Detection: A Systematic Literature Review // IEEE Access. 2022. Vol. 10. P. 25494-25513. DOI: 10.1109/ACCESS.2022.3154404.

11. Tolosana R., Vera-Rodriguez R., Fierrez J., Morales A., Ortega-Garcia J. DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection // Information Fusion. 2020. DOI: 10.1016/j.inffus.2020.06.014.

12. Rostami M., Spinoulas L., Hussein M., Mathai J., Abd-Almageed W. Detection and Continual Learning of Novel Face Presentation Attacks // IEEE/CVF International Conference on Computer Vision (ICCV), Montreal, QC, Canada. 2021. P. 14831-14840. DOI: 10.1109/ICCV48922.2021.01458.

13. Moon Y., Ryoo I., Kim S. (2021). Face Antispoofing Method Using Color Texture Segmentation on FPGA. Security and Communication Networks. 2021. P. 1-11. DOI: 10.1155/2021/9939232.

14. Qin Y., Zhao C., Zhu X., Wang Z., Yu Z., Fu T., Zhou F., Shi J., Lei Z. Learning Meta Model for Zero- and Few-Shot Face Anti-Spoofing // Proceedings of the AAAI Conference on Artificial Intelligence. 2020. Vol. 34. P. 11916-11923. DOI: 10.1609/aaai.v34i07.6866.

15. Surantha N., Sugijakko B. Lightweight face recognition-based portable attendance system with liveness detection // Internet of Things. 2024. Vol. 25. P. 101089. DOI: 10.1016/j.iot.2024.101089.

16. Yang C.-Z., Ma J., Wang S., Liew, A.W.-C. Preventing DeepFake Attacks on Speaker Authentication by Dynamic Lip Movement Analysis // IEEE Transactions on Information Forensics and Security. 2021. Vol. 16. P. 1841-1854. DOI: 10.1109/TIFS.2020.3045937.

17. Jose J., Kumar C.S. Genus and Species-Level Classification of Wrasse Fishes Using Multidomain Features and Extreme Learning Machine Classifier // International Journal of Pattern Recognition and Artificial Intelligence. 2020. Vol. 34. DOI: 10.1142/S0218001420500287.

18. Sharma D., Selwal A. A survey on face presentation attack detection mechanisms: hitherto and future perspectives // Multimedia Systems. 2023. Vol. 29. P. 1527–1577. DOI: 10.1007/s00530-023-01070-5.

19. Zhang B., Tondi B., Barni M. Adversarial examples for replay attacks against CNN-based face recognition with anti-spoofing capability // Computer Vision and Image Understanding. 2020. P. 197-198. DOI: 10.1016/j.cviu.2020.102988.

20. Budiarto R. Face Anti-Spoofing Method with Blinking Eye and HSV Texture Analysis // IOP Conference Series: Materials Science and Engineering. 2020. Vol. 1007. DOI: 10.1088/1757-899X/1007/1/012034.

21. Mittal C., Debnath S. Prabakeran S. Smart Visage: A Face Recognition and Anti-Spoofing System // 2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE), Shivamogga, India. 2024. P. 1-9. DOI: 10.1109/AMATHE61652.2024.10582086.

22. Polok M.Y., Hossain Alvee M.K., Moni F.R., Shopon M., Alam T., Karim M. A. Face Anti-Spoofing Framework Based on Optical Flow Field Texture Analysis // 2024 IEEE 6th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS), Tainan, Taiwan. 2024. P. 374-377. DOI: 10.1109/ECBIOS61468.2024.10885503.

23. Фаворская М.Н., Пахирка А.И. Построение карт глубины при обнаружении презентационных атак в систе-

мах распознавания лиц // Информационные и математические технологии в науке и управлении. 2022. № 3 (27). С. 40-48. DOI: 10.38028/ESI.2022.27.3.005.

24. Muhammad U., Yu Z., Komulainen J. Self-supervised 2D face presentation attack detection via temporal sequence sampling // Pattern Recognition Letters. 2022. DOI: 10.1016/j.patrec.2022.03.001.

25. Li Y, Wang Y., Zhao Z. Face anti-spoofing methods based on physical technology and deep learning // Proc. SPIE 12155, International Conference on Computer Vision, Application, and Design (CVAD 2021). 2021. Vol. 12155. P. 173-184. DOI: 10.1117/12.2626584.

26. George A., Marcel S. On the Effectiveness of Vision Transformers for Zero-shot Face Anti-Spoofing // 2021 IEEE International Joint Conference on Biometrics (IJCB), Shenzhen, China. 2021. P. 1-8. DOI: 10.1109/IJCB52358.2021.9484333.

27. Policepatil S, Hatture SM. Face Liveness Detection: An Overview // International Journal of Scientific Research in Science and Technology. 2021. URL: https://ijsrst.com/paper/8266.pdf (дата обращения: 12.06.2025).

28. Liu X., Wang R., Liu W., Zhang L., Wang X. Quality Matters: Boosting Face Presentation Attack Detection With Image Quality Metrics // IEEE Access. 2024. P. 1-1. DOI: 10.1109/ACCESS.2024.3421345.

29. George A., Marcel S. Cross Modal Focal Loss for RGBD Face Anti-Spoofing // IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA. 2021. P. 7878-7887. DOI: 10.1109/CVPR46437.2021.00779.

30. Yu Z., Wan J., Qin Y., Li X., Li S.Z., Zhao G. NAS-FAS: Static-Dynamic Central Difference Network Search for Face Anti-Spoofing // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2021. Vol. 43. № 9. P. 3005-3023. DOI: 10.1109/TPAMI.2020.3036338.

31. Khairnar S., Gite Sh., Kotecha K., Thepade S. Face liveness detection using artificial intelligence techniques: A systematic literature review and future directions // Big Data Cogn. Comput. 2023. P. 37. DOI: 10.3390/bdcc7010037.

32. Shaheed K., Szczuko P., Kumar M., Qureshi I., Abbas Q., Ullah I. Deep learning techniques for biometric security: A systematic review of presentation attack detection systems // Engineering Applications of Artificial Intelligence. 2024. Vol. 129. DOI: 10.1016/j.engappai.2023.107569.

33. Qu Z., Xi Z., Lu W., Luo X., Wang Q., Li B. DF-RAP: A Robust Adversarial Perturbation for Defending Against Deepfakes in Real-World Social Network Scenarios // IEEE Transactions on Information Forensics and Security. 2024. Vol. 19. P. 3943-3957. DOI: 10.1109/TIFS.2024.3372803.

34. Nirkin Y., Wolf L., Keller Y., Hassner T. DeepFake Detection Based on Discrepancies Between Faces and Their Context // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2022. Vol. 44. № 10. P. 6111-6121. DOI: 10.1109/TPAMI.2021.3093446.

35. Yang J., Xiao S., Li A., Lu W., Gao X., Li Y. MSTA-Net: Forgery Detection by Generating Manipulation Trace Based on Multi-Scale Self-Texture Attention // IEEE Transactions on Circuits and Systems for Video Technology. 2022. Vol. 32. № 7. P. 4854-4866. DOI: 10.1109/TCSVT.2021.3133859.

36. Huang Y., Juefei-Xu F., Guo Q., Liu Y., Pu G. FakeLocator: Robust Localization of GAN-Based Face Manipulations // IEEE Transactions on Information Forensics and Security. 2022. Vol. 17. P. 2657-2672. DOI: 10.1109/TIFS.2022.3141262.

37. Ding F., Zhu G., Li Y., Zhang X., Atrey P.K., Lyu S. Anti-Forensics for Face Swapping Videos via Adversarial Training // IEEE Transactions on Multimedia. 2022. Vol. 24. P. 3429-3441. DOI: 10.1109/TMM.2021.3098422.

38. Guarnera L., Giudice O., Battiato S. Fighting Deepfake by Exposing the Convolutional Traces on Images // IEEE Access. 2022. Vol. 8. P. 165085-165098. DOI: 10.1109/ACCESS.2020.3023037.

39. Xing H., Tan S.Y., Qamar F., Jiao Y. Face Anti-Spoofing Based on Deep Learning: A Comprehensive Survey // Appl. Sci. 2025. Vol. 15. P. 6891. DOI: 10.3390/app15126891.

40. Li Y., Yang X., Sun P., Qi H., Lyu S. Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics // IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA. 2020. P. 3204-3213. DOI: 10.1109/CVPR42600.2020.00327.

41. Белая О.В., Кицай Ю.А. Биометрические данные как средство идентификации и аутентификации человека: российский и международный опыт // Право и практика. 2020. № 1. URL: https://cyberleninka.ru/article/n/biometricheskie-dannye-kak-sredstvo-identifikatsii-i-autentifikatsii-cheloveka-rossiyskiy-i-mezhdunarodnyy-opyt (дата обращения: 21.06.2025).

42. Ларионова С.Л. Методика защиты персональных данных с учетом требований регламента ЕС General data protection Regulation // Инновации и инвестиции. 2020. № 6. URL: https://cyberleninka.ru/article/n/metodika-zaschity-personalnyh-dannyh-s-uchetom-trebovaniy-reglamenta-es-general-data-protection-regulation (дата обращения: 21.06.2025).

43. Романец И.И., Тришкин Е.А. Внедрение биометрических технолгий как драйвер развития цифровой экономики // Инновационная экономика: перспективы развития и совершенствования. 2021. № 7 (57). URL: https://cyberleninka.ru/article/n/vnedrenie-biometricheskih-tehnologiy-kak-drayver-razvitiya-tsifrovoy-ekonomiki (дата обращения: 21.06.2025).

44. Шаманина Е.И., Захаренко Ю.С. Биометрические технологии как перспективное направление совершенствования дистанционного банковского обслуживания // Вестник ГУУ. 2020. № 5. URL: https://cyberleninka.ru/article/n/biometricheskie-tehnologii-kak-perspektivnoe-napravlenie-sovershenstvovaniya-distantsionnogo-bankovskogo-obsluzhivaniya (дата обращения: 21.06.2025).

45. Baeza Argüello S., Wakkary R., Andersen K., Tomico O. Exploring the Potential of Apple Face ID as a Drag // Queer and Trans Technology Design Tool. 2021. P. 1654-1667. DOI: 10.1145/3461778.3461999.

46. Канокова Л.Ю. Зарубежный опыт развития технологии распознавания лиц в обеспечении общественной безопасности // Право и управление. 2023. № 1. С. 178-182. EDN: MPPXNS.

47. Katti A.G., Chidananda Murthy M.V. Developments in Face Recognition: A Review of Methods, Algorithms and Real – World Applications, From Classical Methods to Deep Learning // 2025 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Chickballapur, India. 2025. P. 1-7. DOI: 10.1109/ICKECS65700.2025.11035558.

48. Muhammad Ibrahim S., Sohail Ibrahim M., Khan S., Y.-W. Ko, J.-G. Lee. Improving Face Presentation Attack Detection Through Deformable Convolution and Transfer Learning // IEEE Access. 2025. Vol. 13. P. 31228-31238. DOI: 10.1109/ACCESS.2025.3541546.