Рубрика 2. Методы и системы защиты информации, информационная безопасность

УДК 004.056.5:004.93

А. Г. Уймин[1]

[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ: ВОЗМОЖНОСТИ И УЯЗВИМОСТИ

Аннотация. *Статья посвящена системному анализу возможностей и уязвимостей, возникающих при применении алгоритмов искусственного интеллекта в современных системах биометрической аутентификации. Актуальность исследования обусловлена качественным сдвигом в архитектуре цифровой идентичности к середине 2020-х годов: внедрением стандартов WebAuthn Level 3 и passkeys, ужесточением нормативно-методических требований EU AI Act и NIST SP 800-63B-4, а также стремительным развитием атак на основе морфинга и дипфейков. В статье рассматриваются ключевые биометрические модальности — распознавание лиц, отпечатков пальцев (включая бесконтактные технологии), радужки и сетчатки глаза — в контексте применения нейросетевых архитектур (CNN, ResNet/DRN). Анализируются метрики качества биометрических систем (FPIR, FNIR, APCER, BPCER, IAPMR) и международные бенчмарки FRVT и IREX. Отдельное внимание уделяется угрозам: атакам предъявления (PA), морфингу, дипфейкам, бесконтактному спуфингу, а также методам противодействия (PAD, MAD). Рассматривается архитектура passkeys/WebAuthn L3 как модель разделения биометрической верификации и криптографической аутентификации. Предложена методология оценки и снижения рисков, совместимая с требованиями EU AI Act, ISO/IEC 30107-3 и NIST SP 800-63B-4. Уточнены архитектурные и организационные меры, позволяющие связать технические метрики с требованиями управления рисками. Сделан вывод о том, что дальнейшее развитие биометрических систем определяется не ростом вычислительных мощностей, а способностью объединить интеллектуальную обработку признаков, этические ограничения и инженерную воспроизводимость в рамках подотчётных и верифицируемых архитектур.*

Ключевые слова: *биометрическая аутентификация, искусственный интеллект, атака предъявления, морфинг, дипфейк, WebAuthn, EU AI Act.*

Введение

Биометрическая аутентификация как процедура верификации личности на основе уникальных физиологических или поведенческих характеристик человека к середине 2020-х годов претерпевает качественную трансформацию. В предшествующее десятилетие основным вектором развития отрасли являлось повышение точности распознавания за счёт наращивания вычислительных мощностей и объёмов обучающих данных. К 2025 году актуализированы принципиально иные исследовательские и инженерные задачи: обеспечение регуляторной совместимости биометрических систем, их управляемости и подотчётности в условиях применения алгоритмов искусственного интеллекта (ИИ).

Указанный сдвиг обусловлен совокупностью взаимосвязанных факторов. Первый фактор: принятие Европейским союзом Акта об искусственном интеллекте (EU AI Act) [1] и обновление руководства NIST по цифровой идентичности (SP 800-63B-4) [2] сформировали новые нормативно-методические рамки для биометрических систем, применяемых в критически важных сценариях идентификации и аутентификации. Второй фактор: интенсивное развитие генеративных нейросетевых моделей породило новый класс угроз — морфинг и дипфейки. Указанные типы атак принципиально отличаются от традиционных атак предъявления по векторам реализации и требуют специализированных методов противодействия [3, 4]. Третий фактор: принятие стандарта WebAuthn Level 3 консорциумом W3C и широкое распространение технологии passkeys существенно изменили архитектуру цифровой идентичности. В рамках указанных архитектурных сценариев биометрические данные функционально переориентированы: вместо самостоятельного сетевого фактора аутентификации они приобретают статус локального механизма разблокировки криптографического ключа [5].

Совокупность этих факторов определяет актуальность системного анализа возможностей и уязвимостей ИИ-алгоритмов в биометрических системах аутентификации. Существующие обзорные работы, как правило, сосредоточены либо на технических аспектах

распознавания [6, 7], либо на отдельных видах атак [8, 9], либо на регуляторных вопросах [10]. Комплексного рассмотрения, охватывающего одновременно технические возможности, актуальные угрозы, метрики оценки и регуляторный контекст, в отечественной литературе явно недостаточно.

Цель настоящей статьи — сформулировать и обосновать системное понимание возможностей и уязвимостей, возникающих при применении алгоритмов ИИ в биометрических системах аутентификации, и предложить практически применимую методологию оценки, снижения рисков и обеспечения соответствия регуляторным требованиям.

Для достижения поставленной цели решаются следующие задачи:

- охарактеризовать современное состояние биометрической аутентификации с учётом роли ИИ-алгоритмов;
- систематизировать ключевые биометрические модальности и применяемые нейросетевые архитектуры;
- проанализировать метрики качества и международные бенчмарки оценки биометрических систем;
- классифицировать актуальные угрозы и методы противодействия;
- рассмотреть архитектуру passkeys/WebAuthn L3 как модель разделения биометрической и криптографической составляющих аутентификации;
- предложить методологию оценки рисков, совместимую с действующими регуляторными требованиями.

Материалы и методы

Исследование выполнено методами системного анализа, сравнительного анализа технических стандартов и регуляторных документов, а также обзора актуальной научно-технической литературы. В качестве основных источников использованы: международные стандарты ISO/IEC 30107-3 [11], ANSI/NIST ITL [12], руководство NIST SP 800-63B-4 [2], регламент EU AI Act [1], технические спецификации W3C WebAuthn Level 3 [5], а также результаты бенчмарков FRVT (Face Recognition Vendor Test) и IREX (Iris Exchange), публикуемых Национальным институтом стандартов и технологий США (NIST) [13, 14].

Анализ угроз проводился в соответствии с таксономией атак предъявления, закреплённой в ISO/IEC 30107-3, с учётом расширений для морфинга и дипфейков, предложенных в работах [3, 4, 8]. Архитектурный анализ passkeys/WebAuthn L3 основан на спецификациях FIDO Alliance [15] и W3C [5]. Регуляторный анализ выполнен путём сопоставления требований EU AI Act, NIST SP 800-63B-4 и ISO/IEC 30107-3 применительно к биометрическим системам высокого риска.

Результаты

1. Биометрическая аутентификация в 2025 году: качественный сдвиг

К 2025 году биометрическая аутентификация прошла путь от экспериментальных систем с высоким уровнем ошибок до промышленных решений, обеспечивающих точность распознавания лиц на уровне, превышающем возможности человека-эксперта в контролируемых условиях [6]. Этот прогресс стал возможным благодаря переходу от традиционных алгоритмов обработки изображений к глубоким нейронным сетям — прежде всего свёрточным нейронным сетям (CNN) и архитектурам с остаточными связями (ResNet, DRN) [7].

Вместе с тем качественный сдвиг 2024–2025 годов состоит не в очередном улучшении метрик точности, а в изменении самой парадигмы применения биометрии. Можно выделить пять ключевых тенденций.

Сводная схема взаимосвязи биометрических модальностей, требований и инструментов оценки представлена на рис. 1.

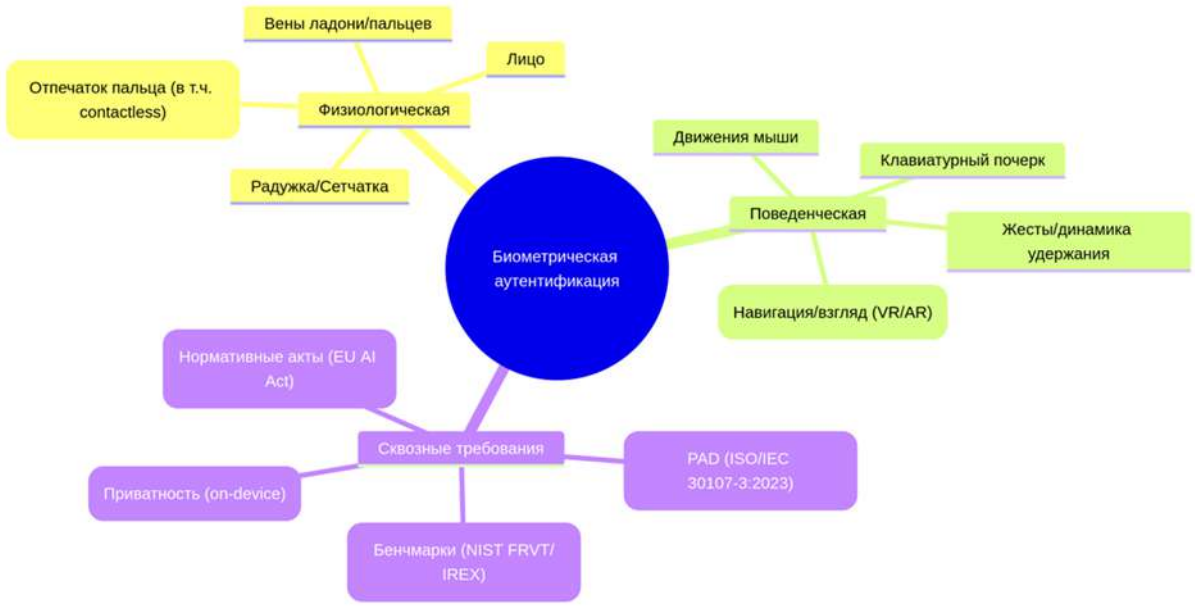

Рис. 1. Биометрическая аутентификация в 2025 году: модальности, требования и инструменты оценки

Тенденция 1: переход к passkeys и WebAuthn L3. Широкое внедрение технологии passkeys, основанной на стандарте WebAuthn Level 3 консорциума W3C, принципиально изменило роль биометрии в архитектуре аутентификации. В модели passkeys биометрическая верификация (например, сканирование отпечатка пальца или лица) выполняется локально на устройстве пользователя и служит исключительно для разблокировки криптографического ключа, хранящегося в защищённом хранилище устройства (platform authenticator). Сервер (Relying Party) не получает биометрические данные: при входе он проверяет криптографическое подтверждение владения приватным ключом, а сведения о свойствах аутентификатора могут дополнительно подтверждаться механизмом аттестации [5, 15]. Это принципиально отличается от традиционных схем, в которых биометрический шаблон передавался на сервер для сопоставления.

Тенденция 2: ужесточение регуляторных и нормативно-методических требований. Вступление в силу EU AI Act [1] и обновление NIST SP 800-63B-4 [2] сформировали новые требования к биометрическим системам, применяемым в сценариях высокого риска. EU AI Act относит отдельные сценарии удалённой биометрической идентификации и биометрической категоризации к запрещённым или строго ограниченным практикам, а биометрическую верификацию в критически важных инфраструктурах — к высокорисковым сценариям, требующим оценки соответствия, ведения документации и обеспечения человеческого надзора [1].

Хронология ключевых нормативных изменений и стандартов, влияющих на проектирование биометрических систем, приведена на рис. 2.

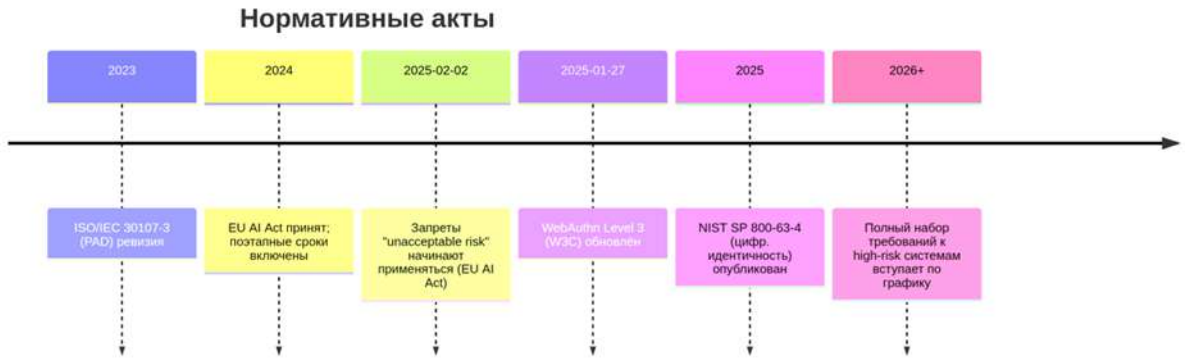

Рис. 2. Нормативный контекст развития биометрических систем и ИИ-компонентов

Тенденция 3: развитие технологий PAD/MAD. Стремительное развитие генеративных нейросетей сделало создание высококачественных синтетических биометрических данных (морфинг, дипфейки) доступным для широкого круга злоумышленников. В ответ активно развиваются технологии обнаружения атак предъявления (PAD — Presentation Attack Detection) и обнаружения морфинга (MAD — Morphing Attack Detection) [3, 8].

Тенденция 4: распространение бесконтактных и мультимодальных решений. Пандемия COVID-19 ускорила переход к бесконтактным технологиям захвата биометрических данных, прежде всего к бесконтактному сканированию отпечатков пальцев с помощью обычных камер. Мультимодальные системы, объединяющие несколько биометрических модальностей, обеспечивают более высокую устойчивость к атакам и более низкий уровень ошибок [6].

Тенденция 5: воспроизводимость и сопоставимость через бенчмарки. Критически важной становится возможность объективного сравнения биометрических систем разных производителей. Бенчмарки FRVT (для систем распознавания лиц) и IREX (для систем распознавания радужки), проводимые NIST, стали де-факто стандартом оценки производительности [13, 14].

2. Биометрические модальности и нейросетевые архитектуры

2.1. Распознавание лиц

Распознавание лиц является наиболее широко применяемой биометрической модальностью. Современные системы распознавания лиц основаны на глубоких нейронных сетях, обученных на больших наборах изображений. Архитектуры ResNet и их производные (DRN — Deep Residual Networks) позволяют извлекать высокоуровневые признаки лица, относительно устойчивые к изменению освещения, ракурса и возрастным изменениям [7].

Процесс работы системы распознавания лиц включает несколько этапов: обнаружение лица на изображении, нормализацию (выравнивание по ключевым точкам), извлечение признаков (embedding) с помощью нейронной сети и сопоставление полученного вектора признаков с шаблоном (template), хранящимся в базе данных. В режиме верификации (1:1) система сравнивает два вектора признаков и принимает решение о совпадении на основе порогового значения. В режиме идентификации (1:N) система ищет наиболее близкое совпадение в базе данных шаблонов.

Бенчмарк FRVT, проводимый NIST, позволяет объективно сравнивать системы распознавания лиц разных производителей по стандартизированным метрикам на стандартизированных наборах данных [13]. Результаты FRVT показывают, что лучшие современные системы достигают показателя FNIR (False Negative Identification Rate — доля пропущенных совпадений) менее 0,3% при FPIR (False Positive Identification Rate — доля ложных совпадений) 0,01% на отдельных наборах данных высокого качества.

Обобщённая матрица практических преимуществ и ограничений систем распознавания лиц представлена на рис. 3.

Рис. 3. Матрица преимуществ и ограничений распознавания лиц в условиях актуальных атак

2.2. Бесконтактное сканирование отпечатков пальцев

Традиционное контактное сканирование отпечатков пальцев (с использованием ёмкостных или оптических сенсоров) дополняется бесконтактными технологиями (contactless fingerprint), основанными на захвате изображения пальца обычной камерой. Это открывает новые возможности для применения биометрии в гигиенически чувствительных средах и при удалённой аутентификации.

Основная техническая сложность бесконтактного сканирования состоит в необходимости компенсации перспективных искажений, неравномерного освещения и деформаций кожи. Современные нейросетевые подходы позволяют решить эти задачи, однако интероперабельность (совместимость) шаблонов, полученных бесконтактным способом, с шаблонами, полученными контактным способом, остаётся открытой проблемой [6].

Типовая последовательность обработки при бесконтактном захвате отпечатка пальца показана на рис. 4.

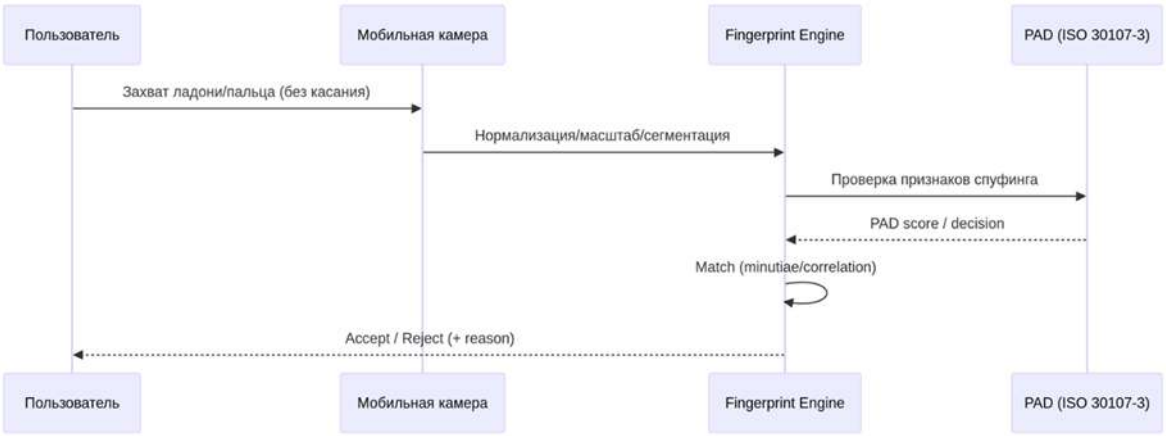

Рис. 4. Переход к бесконтактному сканированию отпечатка пальца: захват, нормализация и PAD-проверка

2.3. Распознавание радужки и сетчатки

Радужная оболочка глаза уникальна для каждого человека и сохраняет свою структуру на протяжении всей жизни — эти свойства позволяют относить её к числу наиболее надёжных биометрических модальностей. Современные системы распознавания радужки работают в ближнем инфракрасном диапазоне (NIR), который обеспечивает чёткое изображение текстуры вне зависимости от цвета глаз и условий освещения [18].

Бенчмарк IREX, проводимый NIST, оценивает производительность систем распознавания радужки по метрикам FNIR и FPIR [14]. Распознавание сетчатки может обеспечивать очень высокую точность, но требует специализированного оборудования и тесного контакта с ним. Из-за этого сетчатку используют преимущественно на высокозащищённых объектах.

Укрупнённая схема обработки данных радужки и сетчатки в биометрической системе приведена на рис. 5.

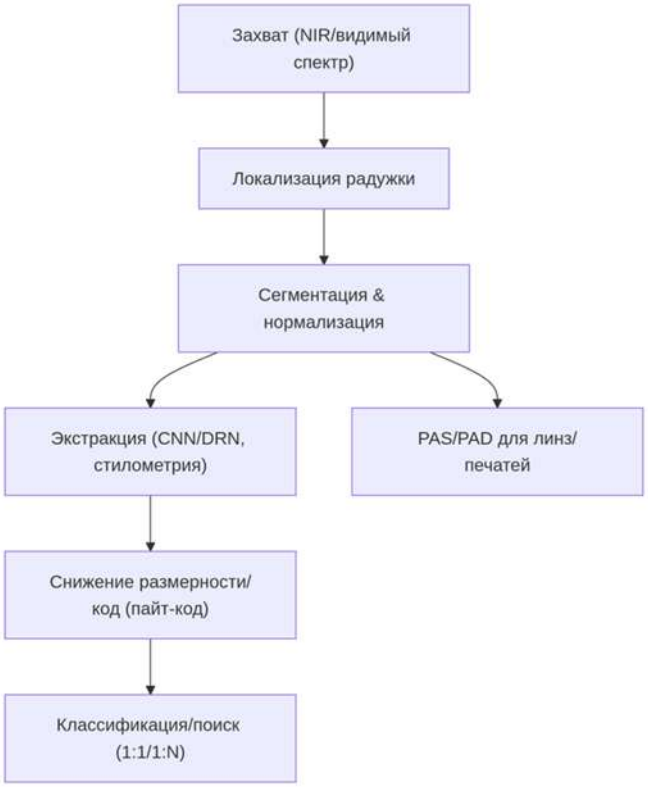

Рис. 5. Обработка данных радужки и сетчатки: захват, локализация, сегментация и сопоставление

3. Метрики качества биометрических систем

Оценка качества биометрических систем требует применения специализированных метрик, учитывающих специфику задачи верификации или идентификации личности. Стандартизация метрик, закреплённая в ISO/IEC 30107-3 [11] и стандартах ANSI/NIST ITL [12], обеспечивает возможность объективного сравнения систем разных производителей.

3.1. Метрики верификации и идентификации

В задаче верификации (1:1) используются три основные метрики:

- FAR (False Acceptance Rate) — доля случаев, когда система принимает самозванца за легитимного пользователя;
- FRR (False Rejection Rate) — доля случаев, когда система отвергает легитимного пользователя;
- EER (Equal Error Rate) — точка, в которой FAR = FRR; служит интегральной характеристикой системы.
- В задаче идентификации (1:N) применяются:
- FPIR (False Positive Identification Rate) — доля случаев, когда система ошибочно идентифицирует самозванца как одного из зарегистрированных пользователей;

– FNIR (False Negative Identification Rate) — доля случаев, когда система не находит совпадения для легитимного пользователя.

3.2. Метрики оценки устойчивости к атакам

В рамках стандарта ISO/IEC 30107-3 [11] установлена номенклатура количественных метрик для оценки устойчивости биометрических систем к атакам предъявления. Базовый набор показателей включает следующие величины.

APCER (Attack Presentation Classification Error Rate) определяется как доля атак предъявления, ошибочно классифицированных биометрической системой в качестве подлинных предъявлений (bona fide).

BPCER (Bona Fide Presentation Classification Error Rate) определяется как доля подлинных предъявлений, ошибочно классифицированных биометрической системой в качестве атак предъявления.

IAPMR (Impostor Attack Presentation Match Rate) определяется как доля атак предъявления, при реализации которых биометрическая система одновременно принимает предъявление в качестве подлинного и осуществляет успешное сопоставление полученного биометрического образца с шаблоном целевого пользователя.Среди указанных метрик

IAPMR обладает наибольшей значимостью с позиции обеспечения информационной безопасности биометрической системы. Численное значение IAPMR количественно характеризует вероятность того, что предпринятая атака предъявления приведёт к успешному преодолению процедуры биометрической аутентификации.

3.3. Компромисс между безопасностью и удобством использования

При настройке биометрических систем неизбежно возникает противоречие: снижение APCER обычно достигается за счёт роста BPCER. Чем выше чувствительность системы PAD, тем больше легитимных пользователей она может ошибочно отвергать. Оптимальный порог определяется сценарием применения, моделью угроз и требованиями регулятора [11].

4. Угрозы и атаки на биометрические системы

4.1. Классификация атак предъявления

Атака предъявления (Presentation Attack, PA) — это попытка злоумышленника обмануть биометрическую систему путём предъявления артефакта (Presentation Attack Instrument, PAI), имитирующего биометрические характеристики легитимного пользователя. Стандарт ISO/IEC 30107-3 [11] классифицирует PAI по типу: фотографии, видеозаписи, маски (2D и 3D), силиконовые накладки, контактные линзы с нанесённым рисунком радужки и т.д.

Традиционные атаки предъявления (распечатанные фотографии, воспроизведение видео) относительно легко обнаруживаются современными системами PAD. Значительно более сложную угрозу представляют атаки с использованием высококачественных 3D-масок и, особенно, атаки на основе синтетических данных, генерируемых нейросетями.

4.2. Морфинг

Морфинг (morphing) — это синтез изображения, сочетающего биометрические черты нескольких людей таким образом, что полученное изображение успешно сопоставляется с шаблонами каждого из них. Морфинг-атаки представляют особую угрозу для систем верификации документов, удостоверяющих личность: злоумышленник может получить паспорт с морфированным изображением, которое будет успешно верифицировано как его лицо, так и лицо сообщника [3, 19].

Современные алгоритмы морфинга основаны на генеративно-состязательных сетях (GAN) и диффузионных моделях, что позволяет создавать морфированные изображения высокого качества, практически неотличимые от подлинных фотографий. Обнаружение морфинга (MAD — Morphing Attack Detection) является активной областью исследований; существующие методы MAD делятся на одноизображенческие (single-image MAD, применяемые при пограничном контроле) и дифференциальные (differential MAD, требующие сравнения с доверенным изображением) [3].

Процессная логика выявления морфинга и дипфейков при регистрации и проверке документов показана на рис. 6.

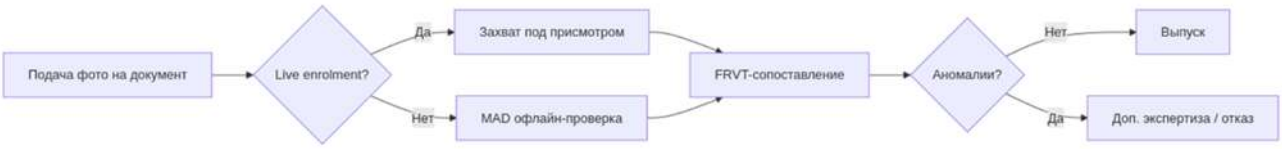

Рис. 6. Процессная схема противодействия морфингу и дипфейкам при регистрации и проверке

4.3. Дипфейки

Дипфейк (deepfake) определяется как синтетическое изображение, видеозапись или аудиосигнал, сгенерированные нейросетевой моделью с целью имитации визуальных или голосовых характеристик конкретного человека. В контексте задач биометрической аутентификации дипфейки формируют угрозу преимущественно для систем удалённой верификации лица, функционирующих в режиме реального времени с применением механизмов обнаружения признаков жизни (liveness detection) [4].

Современные системы liveness detection реализуют различные методы обнаружения синтетических данных: анализ микродвижений лицевой мускулатуры, реакция на случайно генерируемые запросы (challenge-response), спектральный анализ текстуры кожного покрова в нескольких диапазонах излучения, оценка физиологических микропризнаков. Гонка вооружений между системами генерации синтетических данных и системами их обнаружения сохраняется в активной фазе: совершенствование детекторов сопровождается соответствующим совершенствованием генеративных моделей [4, 8].

4.4. Бесконтактный спуфинг

Бесконтактный спуфинг (contactless spoof) определяется как атака на системы бесконтактного сканирования отпечатков пальцев, реализуемая с применением печатных, экранных или синтетически сгенерированных изображений папиллярного узора. Переход индустрии биометрических технологий к бесконтактным методам захвата отпечатков пальцев сопровождается формированием принципиально новых векторов атак. Традиционные методы обнаружения атак предъявления (PAD), разработанные для контактных сенсорных систем, не во всех случаях применимы к бесконтактным архитектурам захвата изображений [6].

4.5. Атаки на процесс регистрации

Самостоятельную категорию угроз биометрическим системам составляют атаки на процедуру первичной регистрации (enrollment). При успешной регистрации злоумышленником поддельного биометрического шаблона в системе — например, посредством компрометации процедуры верификации клиента KYC (Know Your Customer) — последующие операции аутентификации будут устойчиво проходить для атакующего субъекта. Повышенную опасность формирует регистрация морфированного шаблона: указанный тип атаки обеспечивает возможность использования единой учётной записи несколькими физическими лицами одновременно [3, 19].

5. Методы противодействия угрозам

5.1. Обнаружение атак предъявления (PAD)

Технологии обнаружения атак предъявления PAD (Presentation Attack Detection) ориентированы на выявление попыток компрометации биометрической системы посредством использования синтетических артефактов. Современные методы PAD группируются по нескольким категориям в зависимости от информативного признака, лежащего в основе детекции.

Текстурный анализ. Метод базируется на выявлении различий в микротекстуре живого кожного покрова и поверхности артефакта (силиконовых масок, фотографических отпечатков). Нейросетевые алгоритмы анализа обеспечивают обнаружение тонких текстурных различий, недоступных для регистрации традиционными алгоритмическими методами на основе ручной экстракции признаков.

Мультиспектральный анализ. Метод реализует одновременную регистрацию изображений в нескольких спектральных диапазонах: видимом свете, ближнем инфракрасном,

тепловом инфракрасном. Живой кожный покров обладает характерным спектральным профилем отражения и поглощения излучения, который трудно воспроизвести в материалах артефактов.

Анализ микродвижений. Метод обеспечивает обнаружение характерных для живого человека физиологических микродвижений: моргание, пульсация кожи под действием сердечного цикла, спонтанные микродвижения головы, саккадические движения глазных яблок. Системы типа challenge-response запрашивают у пользователя выполнение случайно генерируемых действий — поворот головы, мимическая реакция, — что существенно затрудняет применение статических артефактов в атаках предъявления.

Анализ пространственной геометрии. Методы структурированного освещения и стереоскопической съёмки обеспечивают получение трёхмерной информации о геометрии лица. Реализация указанного подхода делает плоские артефакты (фотографические изображения, экраны мобильных устройств) детектируемыми по геометрическому признаку, поскольку объёмная модель живого лица принципиально отличается от плоского изображения по топологии поверхности.

Стандарт ISO/IEC 30107-3 [11] устанавливает методологические основания тестирования систем PAD и требования к формату представления результатов. Унифицированная методология испытаний обеспечивает возможность объективного сравнительного анализа эффективности систем разных производителей.

5.2. Обнаружение морфинга (MAD)

Методы MAD (Morphing Attack Detection) направлены на выявление морфированных изображений в документах, удостоверяющих личность.

Одноизображенческие методы анализируют артефакты морфинга непосредственно в предъявляемом изображении: следы обработки, аномалии текстуры, несоответствия в деталях лица. Дифференциальные методы сравнивают предъявляемое изображение с доверенным, например с фотографией, сделанной при пограничном контроле, и выявляют признаки морфинга по расхождениям между ними [3].

Нейросетевые методы MAD, как правило, точнее традиционных алгоритмов, однако их устойчивость к новым алгоритмам морфинга, особенно основанным на диффузионных моделях, остаётся предметом активных исследований.

5.3. Непрерывная аутентификация и оценка риска

Традиционная модель аутентификации реализует однократную верификацию личности пользователя в момент входа в информационную систему. Технология непрерывной аутентификации (continuous authentication) обеспечивает мониторинг биометрических и поведенческих признаков субъекта на протяжении всего пользовательского сеанса и направлена на выявление попыток несанкционированного перехвата сессии.

Контекстно-зависимая аутентификация на основе динамической оценки рисков (risk-based authentication) обеспечивает адаптацию требований к процедуре аутентификации в зависимости от текущего контекста доступа. При фиксации аномальных характеристик поведенческого профиля — нетипичных географических координат сессии, отклонений временно́го паттерна входа, нехарактерной последовательности пользовательских действий — система инициирует процедуру запроса дополнительного фактора аутентификации [2].

5.4. Red teaming и тестирование на проникновение

Red teaming — имитация атак на биометрическую систему силами специально подготовленной команды — позволяет выявлять уязвимости, которые стандартное тестирование может не обнаружить. Регулярное проведение таких учений даёт возможность оценить реальную устойчивость системы к актуальным угрозам [9].

6. Архитектура passkeys/WebAuthn L3

6.1. Принципы архитектуры

Технология passkeys, основанная на стандарте WebAuthn Level 3 [5] и спецификациях FIDO Alliance [15], реализует принципиально иную модель аутентификации по сравнению с

традиционными парольными схемами и классическими серверными биометрическими системами.

В архитектуре passkeys каждый пользователь имеет пару криптографических ключей: приватный ключ (private key), хранящийся в защищённом хранилище устройства (platform authenticator), и публичный ключ (public key), зарегистрированный на сервере (Relying Party). При аутентификации сервер отправляет случайный запрос (challenge), который устройство подписывает приватным ключом. Биометрическая верификация (сканирование отпечатка пальца, лица и т.д.) выполняется локально на устройстве и служит исключительно для разблокировки приватного ключа — биометрические данные никогда не покидают устройство [5, 15].

Укрупнённая архитектура разделения локальной биометрической проверки и криптографической аутентификации представлена на рис. 7.

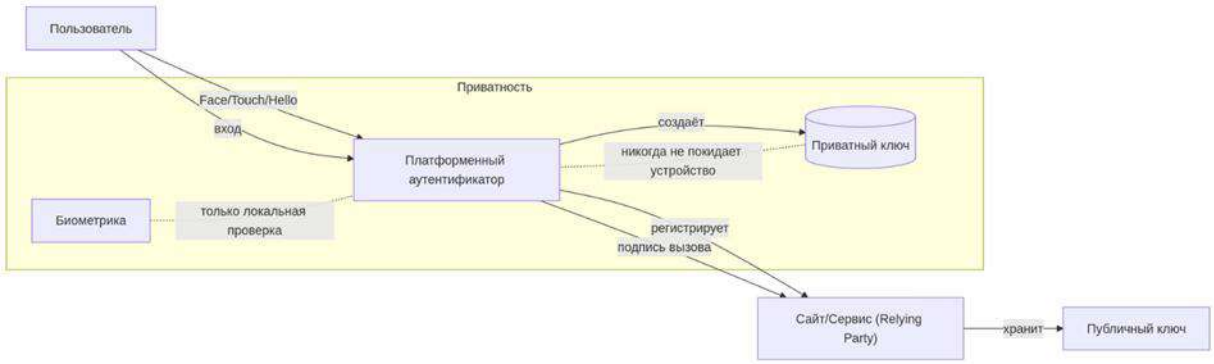

Рис. 7. Архитектура passkeys/WebAuthn L3: локальная биометрия и серверная криптографическая проверка

Такая архитектура обеспечивает несколько ключевых преимуществ с точки зрения безопасности:

– устойчивость к фишингу: приватный ключ привязан к конкретному домену (Relying Party), что делает невозможным его использование на поддельном сайте;
– защита биометрических данных: биометрические данные не передаются на сервер и не хранятся централизованно, что исключает их компрометацию при взломе сервера;
– устойчивость к перехвату: даже при перехвате трафика злоумышленник получает лишь подписанный запрос, который не может быть использован повторно.

6.2. Аттестация и доверие к аутентификатору

Механизм аттестации (attestation) в WebAuthn при регистрации или привязке аутентификатора даёт серверу криптографическое подтверждение его свойств: производителя, модели, уровня сертификации и поддерживаемых функций безопасности. За счёт этого сервер принимает решение о доверии к аутентификатору на основе объективных данных, а не только заявлений пользователя [5]. В корпоративных сценариях аттестация позволяет допускать к работе только сертифицированные аутентификаторы, что снижает риск появления в инфраструктуре скомпрометированных или ненадёжных устройств.

6.3. Ограничения и резервные сценарии

Архитектура passkeys имеет ряд ограничений. Первое — требование совместимого устройства с поддержкой platform authenticator: устаревшие устройства или корпоративные среды с жёсткими требованиями к управлению устройствами могут оказаться несовместимы. Второе — потеря или кража устройства требует механизма восстановления доступа (fallback), который сам по себе становится потенциальным вектором атаки.

Стандарт WebAuthn L3 предусматривает синхронизацию passkeys между устройствами одного пользователя через облачные хранилища производителей. Проблема потери устройства таким образом решается, но возникают новые вопросы — в части безопасности и конфиденциальности [5].

7. Регуляторный контекст и методология оценки рисков

7.1. EU AI Act и биометрические системы

EU AI Act [1] вводит дифференцированный подход к регулированию систем ИИ в зависимости от уровня риска. Применительно к биометрическим системам можно выделить следующие категории и ограничения.

Запрещённые и строго ограниченные практики: биометрическая категоризация по чувствительным признакам, а также отдельные сценарии дистанционной биометрической идентификации в публичных пространствах, прежде всего в режиме реального времени. Для правоохранительных целей предусмотрены специальные исключения и процедурные ограничения.

Системы высокого риска: биометрические системы, применяемые в критически важных инфраструктурах, при принятии решений о доступе к образованию, занятости, кредитованию и т.д., а также ряд систем дистанционной биометрической идентификации, не подпадающих под прямой запрет. Для таких систем EU AI Act требует проведения оценки соответствия, ведения технической документации, обеспечения прозрачности, реализации механизмов человеческого надзора и регистрации в базе данных ЕС.

Системы ограниченного риска: системы, взаимодействующие с людьми (например, чат-боты с биометрической верификацией), обязаны информировать пользователей о том, что они взаимодействуют с системой ИИ.

7.2. NIST SP 800-63B-4 и уровни доверия к аутентификации

Руководство NIST SP 800-63B-4 [2] рассматривает биометрию в контексте многофакторной аутентификации и уровней доверия к аутентификатору (Authenticator Assurance Levels, AAL). Биометрическая характеристика не признаётся самостоятельным аутентификатором: она может использоваться вместе с физическим аутентификатором либо как локальный фактор активации многофакторного аутентификатора.

NIST SP 800-63B-4 устанавливает требования к применению биометрии в государственных сценариях: система должна обеспечивать FMR (False Match Rate) не хуже 1:10000 для всех релевантных демографических групп и, как правило, демонстрировать FNMR (False Non-Match Rate) менее 5%. Для распознавания лиц PAD является обязательным, а для радужки и отпечатков пальцев — рекомендованным; также задаются требования к ограничению числа неудачных попыток и контролю инъекционных атак [2].

7.3. ISO/IEC 30107-3 и тестирование PAD

Стандарт ISO/IEC 30107-3 [11] определяет методологию тестирования систем PAD, включая классификацию PAI по типу и уровню сложности, порядок проведения тестов, метрики оценки (APCER, BPCER, IAPMR) и требования к отчётности. Соответствие ISO/IEC 30107-3 может использоваться как один из элементов доказательной базы при сертификации и оценке соответствия биометрических систем.

7.4. Предлагаемая методология оценки рисков

На основе анализа регуляторных требований и актуальных угроз предлагается следующая методология оценки рисков для биометрических систем, основанных на алгоритмах ИИ.

Шаг 1: классификация системы по EU AI Act. Определить, к какой категории риска относится система (запрещённая, высокого риска, ограниченного риска, минимального риска). Для систем высокого риска последующие шаги становятся обязательной частью управления соответствием и безопасностью.

Шаг 2: оценка угроз. Провести систематическую оценку актуальных угроз с учётом типа биометрической модальности, сценария применения (верификация/идентификация, контролируемая/неконтролируемая среда, удалённая/локальная аутентификация) и доступности инструментов атаки для потенциальных злоумышленников.

Шаг 3: тестирование PAD. Провести тестирование системы PAD в соответствии с ISO/IEC 30107-3 с использованием актуального набора PAI, включая синтетические данные (морфинг, дипфейки). Зафиксировать значения APCER, BPCER, IAPMR.

Шаг 4: верификация на бенчмарках. Для систем распознавания лиц — сопоставить результаты с FRVT или принять участие в тестировании; для систем распознавания радужки — использовать IREX. Результаты бенчмарков обеспечивают независимую верификацию заявленных производителем характеристик.

Шаг 5: оценка архитектурных рисков. Проанализировать архитектуру системы с точки зрения защиты биометрических шаблонов (шифрование, хранение в защищённом хранилище), защиты канала передачи данных, устойчивости процедуры регистрации к атакам, а также наличия и безопасности механизмов fallback.

Шаг 6: red teaming. Провести имитацию атак с использованием актуальных инструментов (морфинг, дипфейки, 3D-маски, бесконтактный спуфинг). Зафиксировать выявленные уязвимости и разработать меры по их устранению.

Шаг 7: документирование и мониторинг. Для систем высокого риска по EU AI Act — обеспечить ведение технической документации, журналов аудита и механизмов человеческого надзора. Установить процедуры регулярного пересмотра оценки рисков с учётом появления новых угроз.

8. Ключевые риски и меры противодействия в 2025 году

На основе проведённого анализа можно выделить ключевые риски для биометрических систем аутентификации в 2025 году и соответствующие меры противодействия.

Итоговая приоритизация рисков представлена на рис. 8.

Рис. 8. Приоритизация ключевых рисков биометрической аутентификации в 2025 году

Риск 1. Морфинг-атаки на документы, удостоверяющие личность. Уровень угрозы оценивается как высокий, поскольку инструменты морфинга широко доступны, а качество морфированных изображений продолжает расти. Основные меры противодействия включают внедрение дифференциальных методов MAD при пограничном контроле, использование цифровых подписей для защиты фотографий в документах и обязательную live enrolment для документов высокого уровня доверия.

Риск 2. Дипфейк-атаки на системы удалённой верификации. Уровень угрозы оценивается как высокий, поскольку удалённая верификация широко применяется в KYC-процедурах и онлайн-банкинге. Мерами противодействия выступают многоуровневые системы liveness detection, challenge-response-протоколы и интеграция с аттестованными platform authenticators на базе passkeys/WebAuthn.

Риск 3. Атаки на процедуру регистрации. Уровень угрозы оценивается как средний, так как успешная атака обычно требует физического присутствия или компрометации оператора.

Снижение риска обеспечивается обязательной live enrolment для систем высокого уровня доверия, многоуровневой верификацией при регистрации и аудитом процедур регистрации.

Риск 4. Компрометация централизованных баз биометрических шаблонов. Уровень угрозы является высоким, поскольку утечка биометрических данных необратима: в отличие от пароля, биометрический признак нельзя полноценно заменить. Мерами защиты являются переход к on-device-хранению, применение биометрических криптосистем и шифрование шаблонов, включая перспективные схемы гомоморфного шифрования.

Риск 5. Несоответствие регуляторным требованиям. Уровень угрозы оценивается как высокий из-за возможных санкций и репутационных последствий. Для смягчения риска необходимы оценка соответствия EU AI Act, внедрение процессов управления жизненным циклом ИИ-систем и регулярный аудит соответствия.

Риск 6. Деградация точности при изменении условий эксплуатации. Уровень угрозы оценивается как средний, поскольку нейросетевые модели могут снижать точность при изменении освещения, ракурса, качества сенсора или возрастных характеристик пользователя. Основные меры — регулярное re-enrolment, мониторинг метрик качества в промышленной эксплуатации и использование адаптивных моделей с контролируемыми механизмами обновления.

Риск 7. Предвзятость алгоритмов (algorithmic bias). Уровень угрозы является высоким с точки зрения регуляторного и репутационного риска, поскольку EU AI Act прямо требует оценки и устранения предвзятости. Необходимы тестирование на репрезентативных наборах данных, мониторинг качества по демографическим группам и регулярный аудит моделей.

Обсуждение

Проведённый анализ позволяет сформулировать принципиальные выводы о природе современных вызовов в области биометрической аутентификации.

Первое положение касается фундаментального противоречия между показателями точности и обеспечения безопасности. Нейросетевые алгоритмы обеспечили достижение рекордных показателей точности биометрического распознавания. Одновременно сформировался новый класс уязвимостей: те же нейросетевые технологии, обеспечивающие высокую точность распознавания, применяются злоумышленниками для генерации высококачественных синтетических атак (морфинг, дипфейки). Дальнейшее повышение точности распознавания само по себе не обеспечивает решения проблемы безопасности — необходимо параллельное развитие методов обнаружения синтетических атак [8, 17].

Второе положение касается роли архитектурных решений в построении биометрических систем. Переход к архитектуре passkeys/WebAuthn L3 демонстрирует возможность устранения значительной части рисков биометрической аутентификации на уровне системной архитектуры, а не на уровне совершенствования алгоритмов распознавания. Разделение биометрической верификации, локально выполняемой на пользовательском устройстве, и криптографической аутентификации, реализуемой на серверной стороне, устраняет целый класс угроз, связанных с компрометацией централизованных хранилищ биометрических данных [5, 15].

Третье положение касается роли нормативно-правового регулирования. Принятие EU AI Act и обновление NIST SP 800-63B-4 формируют отраслевой переход от экспериментальных подходов к разработке ИИ-систем к подотчётным и верифицируемым архитектурам. Соответствие нормативным требованиям приобретает характер не только юридического обязательства, но и инженерного требования, определяющего архитектурные решения на этапе проектирования [1, 2].

Четвёртое положение касается воспроизводимости и сопоставимости результатов испытаний биометрических систем. Бенчмарки FRVT и IREX, проводимые NIST, выполняют системообразующую функцию в обеспечении объективной оценки эффективности биометрических систем. Участие в указанных бенчмарках и публикация полученных результатов приобретают статус необходимого условия формирования доверия к биометрической системе со стороны регуляторов и заказчиков [13, 14].

Ограничения исследования. Применительно к настоящему обзору необходимо учитывать ряд ограничений. Первое ограничение определяется высокой динамикой развития предметной области: конкретные количественные метрики и технические характеристики систем, приведённые в статье, могут утратить актуальность в течение нескольких лет. Второе ограничение связано с источниковой базой: анализ опирается на публично доступные данные, тогда как реальные характеристики коммерческих систем могут существенно отличаться от публикуемых. Третье ограничение определяется незавершённостью формирования регуляторного ландшафта: правоприменительная практика EU AI Act находится на начальной стадии формирования.

Заключение

Проведённый анализ позволяет сформулировать следующие выводы.

К 2025 году алгоритмы искусственного интеллекта приобрели статус определяющего фактора точности, адаптивности и масштабируемости биометрических систем аутентификации. Одновременно указанные алгоритмы стали источником формирования новых классов рисков. Современные нейросетевые модели демонстрируют рекордные показатели на бенчмарках FRVT/IREX. Применение этих моделей формирует уязвимость биометрических систем перед атаками морфинга, дипфейками и синтетическими спуфами. Проблематика доверия и управляемости подобных решений приобретает первоочередную значимость в исследовательской и инженерной повестке.

Международные стандарты и регуляторные рамки — EU AI Act, ISO/IEC 30107-3, NIST SP 800-63B-4, ISO/IEC 24745 — формируют отраслевой переход от экспериментальных подходов к разработке ИИ-систем к подотчётным и верифицируемым архитектурам. Применительно к сценариям использования высокого уровня риска соответствие нормативным требованиям приобретает обязательный характер вместо рекомендательного.

Архитектурное решение passkeys/WebAuthn L3 обеспечивает функциональное разделение процедуры биометрической верификации и процедуры криптографической аутентификации. Указанное разделение устраняет целый класс угроз информационной безопасности, формируемых централизованным хранением биометрических данных.

Предложенная в работе методология оценки рисков обеспечивает интеграцию системы классификации по EU AI Act, процедуры тестирования PAD по ISO/IEC 30107-3, верификации на бенчмарках FRVT/IREX и регулярного red teaming. Совокупность указанных компонентов формирует практически применимый инструментарий для разработчиков и операторов биометрических систем.

Дальнейшее развитие биометрических технологий определяется не количественным ростом вычислительных мощностей. Решающим фактором становится способность к интеграции интеллектуальной обработки признаков, этических ограничений и принципов инженерной воспроизводимости в рамках подотчётных системных архитектур.

Библиографический список

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. — 2024. — L 1689. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (дата обращения: 31.03.2025).
2. Temoshok D., Fenton J., Lefkovitz N., Regenscheid A., Richer J. Digital Identity Guidelines: Authentication and Authenticator Management: NIST Special Publication 800-63B. — Gaithersburg, MD: National Institute of Standards and Technology, 2025. — DOI: 10.6028/NIST.SP.800-63B-4.
3. Scherhag U., Rathgeb C., Merkle J., Breithaupt R., Busch C. Face Recognition Systems Under Morphing Attacks: A Survey // IEEE Access. — 2019. — Vol. 7. — P. 23012–23026. — DOI: 10.1109/ACCESS.2019.2899367.
4. 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. — Vol. 64. — P. 131–148. — DOI: 10.1016/j.inffus.2020.06.014.

5. Balfanz D., Czeskis A., Hodges J., Jones J. C., Jones M. B., Kumar A., Lindemann R., Powers A., Verrept J. Web Authentication: An API for accessing Public Key Credentials Level 3: W3C Recommendation. — 2023. — URL: https://www.w3.org/TR/webauthn-3/ (дата обращения: 31.03.2025).
6. Maltoni D., Maio D., Jain A. K., Feng J. Handbook of Fingerprint Recognition. — 3rd ed. — Cham: Springer, 2022. — 512 p. — DOI: 10.1007/978-3-030-83624-5.
7. Guo Y., Zhang L., Hu Y., He X., Gao J. MS-Celeb-1M: A Dataset and Benchmark for Large-Scale Face Recognition // Lecture Notes in Computer Science. — 2016. — Vol. 9907. — P. 87–102. — DOI: 10.1007/978-3-319-46487-9_6.
8. Ramachandra R., Busch C. Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey // ACM Computing Surveys. — 2017. — Vol. 50, No. 1. — Art. 8. — DOI: 10.1145/3038924.
9. Biggio B., Roli F. Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning // Pattern Recognition. — 2018. — Vol. 84. — P. 317–331. — DOI: 10.1016/j.patcog.2018.07.023.
10. Regan P. M., Jesse J. Ethical Challenges of Edtech, Big Data and Personalized Learning: Twenty-First Century Student Sorting and Tracking // Ethics and Information Technology. — 2019. — Vol. 21, No. 3. — P. 167–179. — DOI: 10.1007/s10676-018-9492-2.
11. ISO/IEC 30107-3:2023. Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. — Geneva: International Organization for Standardization, 2023.
12. NIST Special Publication 500-290. Biometric Specifications for Personal Identity Verification. — Gaithersburg, MD: National Institute of Standards and Technology, 2020.
13. Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects: NIST Interagency Report 8280. — Gaithersburg, MD: National Institute of Standards and Technology, 2019. — DOI: 10.6028/NIST.IR.8280.
14. Grother P., Ngan M. Iris Exchange (IREX) 10: Performance of Iris Recognition Algorithms: NIST Interagency Report 8247. — Gaithersburg, MD: National Institute of Standards and Technology, 2018. — DOI: 10.6028/NIST.IR.8247.
15. FIDO Alliance. FIDO2: WebAuthn & CTAP. Technical Overview. — 2023. — URL: https://fidoalliance.org/fido2/ (дата обращения: 31.03.2025).
16. Jain A. K., Nandakumar K., Ross A. 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities // Pattern Recognition Letters. — 2016. — Vol. 79. — P. 80–105. — DOI: 10.1016/j.patrec.2015.12.013.
17. Marcel S., Nixon M. S., Fierrez J., Evans N. (Eds.) Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Liveness Detection. — 3rd ed. — Cham: Springer, 2023. — 650 p. — DOI: 10.1007/978-3-031-48349-6.
18. Daugman J. How Iris Recognition Works // IEEE Transactions on Circuits and Systems for Video Technology. — 2004. — Vol. 14, No. 1. — P. 21–30. — DOI: 10.1109/TCSVT.2003.818350.
19. Ferrara M., Franco A., Maltoni D. The Magic Passport // Proceedings of the IEEE International Joint Conference on Biometrics (IJCB). — 2014. — P. 1–7. — DOI: 10.1109/BTAS.2014.6996240.
20. Уймин А. Г. Применение технологий цифрового двойника в подготовке специалистов по сетевому и системному администрированию // Современные наукоёмкие технологии. — 2023. — № 5. — С. 112–118.

References

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024, L 1689. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (accessed 31.03.2025).

2. Temoshok D., Fenton J., Lefkovitz N., Regenscheid A., Richer J. Digital Identity Guidelines: Authentication and Authenticator Management. NIST Special Publication 800-63B. Gaithersburg, MD: National Institute of Standards and Technology, 2025. DOI: 10.6028/NIST.SP.800-63B-4.
3. Scherhag U., Rathgeb C., Merkle J., Breithaupt R., Busch C. Face Recognition Systems Under Morphing Attacks: A Survey. IEEE Access, 2019, vol. 7, pp. 23012–23026. DOI: 10.1109/ACCESS.2019.2899367.
4. 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, vol. 64, pp. 131–148. DOI: 10.1016/j.inffus.2020.06.014.
5. Balfanz D., Czeskis A., Hodges J., Jones J. C., Jones M. B., Kumar A., Lindemann R., Powers A., Verrept J. Web Authentication: An API for accessing Public Key Credentials Level 3. W3C Recommendation, 2023. Available at: https://www.w3.org/TR/webauthn-3/ (accessed 31.03.2025).
6. Maltoni D., Maio D., Jain A. K., Feng J. Handbook of Fingerprint Recognition. 3rd ed. Cham: Springer, 2022. 512 p. DOI: 10.1007/978-3-030-83624-5.
7. Guo Y., Zhang L., Hu Y., He X., Gao J. MS-Celeb-1M: A Dataset and Benchmark for Large-Scale Face Recognition. Lecture Notes in Computer Science, 2016, vol. 9907, pp. 87–102. DOI: 10.1007/978-3-319-46487-9_6.
8. Ramachandra R., Busch C. Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. ACM Computing Surveys, 2017, vol. 50, no. 1, art. 8. DOI: 10.1145/3038924.
9. Biggio B., Roli F. Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning. Pattern Recognition, 2018, vol. 84, pp. 317–331. DOI: 10.1016/j.patcog.2018.07.023.
10. Regan P. M., Jesse J. Ethical Challenges of Edtech, Big Data and Personalized Learning: Twenty-First Century Student Sorting and Tracking. Ethics and Information Technology, 2019, vol. 21, no. 3, pp. 167–179. DOI: 10.1007/s10676-018-9492-2.
11. ISO/IEC 30107-3:2023. Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. Geneva: International Organization for Standardization, 2023.
12. NIST Special Publication 500-290. Biometric Specifications for Personal Identity Verification. Gaithersburg, MD: National Institute of Standards and Technology, 2020.
13. Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects. NIST Interagency Report 8280. Gaithersburg, MD: National Institute of Standards and Technology, 2019. DOI: 10.6028/NIST.IR.8280.
14. Grother P., Ngan M. Iris Exchange (IREX) 10: Performance of Iris Recognition Algorithms. NIST Interagency Report 8247. Gaithersburg, MD: National Institute of Standards and Technology, 2018. DOI: 10.6028/NIST.IR.8247.
15. FIDO Alliance. FIDO2: WebAuthn & CTAP. Technical Overview, 2023. Available at: https://fidoalliance.org/fido2/ (accessed 31.03.2025).
16. Jain A. K., Nandakumar K., Ross A. 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. Pattern Recognition Letters, 2016, vol. 79, pp. 80–105. DOI: 10.1016/j.patrec.2015.12.013.
17. Marcel S., Nixon M. S., Fierrez J., Evans N. (Eds.) Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Liveness Detection. 3rd ed. Cham: Springer, 2023. 650 p. DOI: 10.1007/978-3-031-48349-6.
18. Daugman J. How Iris Recognition Works. IEEE Transactions on Circuits and Systems for Video Technology, 2004, vol. 14, no. 1, pp. 21–30. DOI: 10.1109/TCSVT.2003.818350.
19. Ferrara M., Franco A., Maltoni D. The Magic Passport. Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), 2014, pp. 1–7. DOI: 10.1109/BTAS.2014.6996240.
20. Uymin A. G. Primenenie tekhnologiy tsifrovogo dvoynika v podgotovke spetsialistov po setevomu i sistemnomu administrirovaniyu [Application of digital twin technologies in

training specialists in network and system administration]. Sovremennye naukoemkie tekhnologii [Modern High Technologies], 2023, no. 5, pp. 112–118. (In Russian).

Информация об авторах

Уймин Антон Григорьевич — аспирант 2 курса, кафедра безопасности информационных технологий, факультет комплексной безопасности ТЭК, Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина, Москва, Россия. E-mail: uymin.ag@gubkin.ru

THE USE OF ARTIFICIAL INTELLIGENCE ALGORITHMS IN BIOMETRIC AUTHENTICATION SYSTEMS: CAPABILITIES AND VULNERABILITIES

***Uymin A. G.*[1]**

[1]National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. *The article presents a systematic analysis of the capabilities and vulnerabilities arising from the application of artificial intelligence algorithms in modern biometric authentication systems. The relevance of the study is driven by a qualitative shift in digital identity architecture by the mid-2020s: the adoption of WebAuthn Level 3 and passkeys standards, tightening regulatory and methodological requirements of the EU AI Act and NIST SP 800-63B-4, and the rapid development of morphing and deepfake attacks. The article examines key biometric modalities — face recognition, fingerprint recognition (including contactless technologies), iris and retina — in the context of neural network architectures (CNN, ResNet/DRN). Quality metrics of biometric systems (FPIR, FNIR, APCER, BPCER, IAPMR) and international benchmarks FRVT and IREX are analyzed. Special attention is paid to threats: presentation attacks (PA), morphing, deepfakes, and contactless spoofing, as well as countermeasures (PAD, MAD). The passkeys/WebAuthn L3 architecture is examined as a model for separating biometric verification and cryptographic authentication. A risk assessment and mitigation methodology compatible with EU AI Act, ISO/IEC 30107-3 and NIST SP 800-63B-4 requirements is proposed. Architectural and organizational measures linking technical metrics with risk management requirements are specified. The conclusion is drawn that the further development of biometric systems is determined not by the growth of computing power, but by the ability to combine intelligent feature processing, ethical constraints and engineering reproducibility within accountable and verifiable architectures.*

Keywords: *biometric authentication, artificial intelligence, presentation attack, morphing, deepfake, WebAuthn, EU AI Act.*

Information about the authors

Anton G. Uymin — 2nd year postgraduate student, Department of Information Technology Security, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia. E-mail: uymin.ag@gubkin.ru