

Регулирование оборота биометрических персональных данных в РФ

Актуальность материала: **17.04.2026**

Презентация "Регулирование оборота биометрических персональных данных в РФ":

- Понятие и виды биометрии — статические (отпечатки пальцев, радужка, геном, фото) и динамические (голос, подпись, поведенческие паттерны) характеристики в контексте ч. 1 ст. 11 152-ФЗ.
- Позиции ведомств — сравнительная таблица писем Минцифры и Роскомнадзора по вопросу: является ли фотография биометрическими персональными данными? Спойлер: единого ответа до сих пор нет.
- ♾ Судебная практика — два массива дел: когда суды признавали сведения биометрией (фото на пропусках, рисунок вен, видеозаписи с камер в общей собственности) и когда — нет (городские камеры МВД, видео с мобильного телефона, запись спящего сотрудника).
- Прецедент с ФСБ и Росгвардией — разбор реального дела 2022 г.: бизнес-центр «Зеленоград», 170 фотографий детей без согласия родителей, штраф по ч. 2 ст. 13.11 КоАП РФ.
- ЕБС и 572-ФЗ — типы биометрии (упрощённая, стандартная, подтверждённая), транзакционная и векторная модели взаимодействия, требования по аккредитации.
- 7 ограничений при встраивании биометрии в ИТ/ИИ-продукты: закрытый перечень ЕБС, запрет трансграничной передачи, обязательная аккредитация, особый режим согласия, защита несовершеннолетних, пределы точности (FAR/FRR), только векторная модель для аккредитованных.
- ⚠ 7 ключевых рисков: необратимость утечки, штрафы до 500 млн ₽ и уголовная ответственность, дискриминация ИИ-моделей по данным NIST FRVT, deepfake-атаки, function creep, репутационные риски, прокурорские проверки.
- Рекомендации для продуктовых команд — архитектурные (on-device, векторное хранение, liveness-детекция) и процессные (оценка рисков до запуска, журналы согласий, уведомление РКН в 24/72 ч.).

Регулирование оборота биометрических персональных данных в РФ

Разнообразие областей применения биометрии

(ГОСТ Р 54412-2019)

—

Примеры практического применения биометрии

Австралийская полиция будет определять внешность подозреваемых по ДНК

Для поиска преступников полиция нередко использует фоторобот — но австралийские правоохранители намерены применить для этой цели более продвинутое решение. Технология Massively Parallel Sequencing (MPS), по словам её разработчиков, способна прогнозировать пол, цвет глаз и даже страну происхождения подозреваемого на основе образцов ДНК, обнаруженных на месте преступления.

В ближайшее время технология пройдёт модернизацию и предположительно сможет распознавать более детальные характеристики, такие как цвет волос, возраст, индекс массы тела и рост человека. Процесс секвенирования ДНК позволяет декодировать информацию, содержащуюся в длинных цепочках. Современное оборудование и новые технологии могут одновременно считывать свыше 6 триллионов оснований ДНК. Это позволяет значительно расширить возможности для анализа.

Согласно пресс-релизу ведомства, MPS уже была тщательно протестирована на точность перед практическим применением. Такой же метод анализа ДНК будет применяться и в расследовании дел о пропавших без вести. Подобные технологии уже используются и в некоторых других странах.

—
В тюрьму на 13 лет благодаря фотографии в соцсетях: полиция считала с неё отпечатки пальцев

Полиция Мерсисайда определила по странному снимку, на котором автор фото держит в руке кусок голубого сыра, его отпечатки пальцев. Остальное было делом техники. Теперь Карлу Стюарту придётся провести 13,5 лет в тюрьме, так как он признан виновным в передаче наркотических средств.

Sn.fhn поделился этой фотографией в [EncroChat](#), якобы зашифрованной соцсети, которая была взломана властями в марте прошлого года. С тех пор полиция Мерсисайда заявляет, что власти выявили около 10 000 её пользователей в Великобритании, которые «участвуют в координации и планировании поставок и распределения наркотиков и оружия, отмывании денег и другой преступной деятельности». Полиция сообщила, что в общей сложности во всём мире было идентифицировано 60 000 пользователей соцсети.

—
Итальянского мафиози нашли спустя 20 лет благодаря фото на Google Maps

Полиция Италии арестовала 60-летнего босса сицилийской мафии Джоаккино Гаммино спустя 20 лет безуспешных розысков. Его задержание стало возможным благодаря Google Street View.

Джоаккино Гаммино был осуждён за убийство и считался одним из самых разыскиваемых мафиози в Италии. Гаммино тогда перепутал прохожего с членом враждебной мафии «Коза Ностра» и застрелил его.

После бегства из Италии мафиози в течение многих лет жил в городке Галапагар возле Мадрида. Мафиози там женился, сменил имя на Мануэль. Преступник торговал овощами и содержал ресторан «Сицилийский ужин» с меню в стиле «Крёстного отца».

Гаммино раскрыл своё местоположение случайно — его сфотографировала машина Google Maps. После того как кадр появился в сети, полицейские заметили, что мужчина очень похож на находящегося в розыске преступника.

Когда полицейские приехали задерживать итальянца, он был крайне удивлён. По его словам, на протяжении десяти лет он даже не звонил своей семье, чтобы не рисковать.

Более 9 тыс. преступников задержали с помощью системы распознавания лиц в метро Москвы

Умная система видеоаналитики «Сфера», т. е. система распознавания лиц, с момента запуска 1 сентября 2020 года помогла найти в общественном транспорте 1 324 человека, которые числились пропавшими без вести, среди них — 280 детей, сообщает департамент транспорта Москвы.

Также были выявлены 9 007 человек, находящихся в федеральном розыске, в том числе убийцы, насильники, грабители. Они пытались скрыться после совершения тяжких преступлений и представляли угрозу.

Как утверждают в Дептрансе, система преобразовывает лицо человека в уникальный биометрический ключ. Она «узнаёт» только тех людей, которые есть в базах розыска, остальные пассажиры остаются на 100% анонимными — доступ к информации есть исключительно у правоохранительных органов.

О допущенных «умной системой видеоаналитики» ошибках идентификации граждан не сообщается.

—

Clearview AI: новый глаз Саурана, следящий за всеми

Стартап Clearview AI, который разработал систему распознавания лиц, собрал около 30 млрд фотографий из социальных сетей. Кроме того, система обработала около миллиона поисковых запросов для американских полицейских служб. Владельцы фотографий не давали согласие на их использование в системе.

Полиция Майами подтвердила использование Clearview AI для раскрытия преступлений, а представитель отдела сообщил, что система уже помогла раскрыть несколько убийств и используется около 450 раз в год.

Программное обеспечение стартапа считается одним из самых точных в мире. Система позволяет загружать фото лица и искать совпадения в базе данных миллиардов изображений, а затем показывает, где это лицо встречается в интернете.

—

Нейросеть определяет имя человека по фото

В осуществлённую The Mitre Corp (США) разработку технологии, которая длилась 3 года и получила название «эффект Дориана Грея» в честь антигероя романа Оскара Уайльда, инвестировали \$2 млрд.

Основой разработки послужило исследование Еврейского университета в Иерусалиме, где учёные предоставили искусственному интеллекту (ИИ) 13 000 изображений лиц с подписанными именами. В результате нейросеть наделила каждое имя определёнными чертами.

ИИ не требуется сличать лица на фото с базами данных в интернете, и он способен угадывать имя человека с точностью от 72% до 80,5%, выбирая из двух предложенных вариантов.

ИИ будет способен работать и в обратном порядке — если задать имя, то ИИ сможет подобрать под него лицо.

Выявление сексуальной ориентации мужчин по голосу

Учёные из Сиднейского университета провели исследование, которое подтвердило возможность идентификации сексуальной ориентации мужчины по его голосу. Из исследования стало ясно, что определение ориентации гомосексуальных и гетеросексуальных мужчин по голосу является более лёгкой задачей, нежели определение ориентации бисексуальных мужчин.

60 голосовых записей, включающих по 20 гомосексуальных мужчин, бисексуалов и гетеросексуалов, были оценены 70 участниками исследования. Участникам было предложено определить, звучит ли голос мужественно или нетрадиционно, и какая у владельца голоса сексуальная ориентация. Результаты показали, что участники с большей точностью могли определить сексуальную ориентацию гомосексуальных и гетеросексуальных мужчин по их голосам. Однако бисексуальные голоса часто воспринимались как наиболее мужественные. Учёные подчёркивают, что этот метод не может быть надёжным для идентификации бисексуальных мужчин по их голосам.

Apple запатентовала технологию, которая позволит [AirPods](#) узнавать человека по уху

Компания Apple подала заявление на регистрацию нового патента для технологии биометрической идентификации. В ней используются наушники [AirPods](#). Суть в том, что технология позволяет определять пользователей по форме ушей.

В описании говорится, что у каждого человека в ушах создаётся уникальное эхо, которое можно использовать для идентификации. Для этого в наушниках планируется разместить ультразвуковые датчики, которые и будут определять эхо. При генерации сигнала возникнет уникальный звуковой «рисунок», который позволит точно идентифицировать пользователя.

Такой подход даст возможность наушникам [AirPods](#) играть только в ушах владельца iPhone. Если их возьмёт другой человек, музыка прекратится.

Автоматическое измерение температуры и распознавание лиц в корпоративной HR-системе

SAP совместно с партнёрами Facemetric, Cisco Systems, Konica Minolta и Skybuffer разработала систему автоматического измерения температуры и распознавания лиц, которая интегрируется с корпоративной HR-системой, почтой и мессенджерами. Сбор биометрических данных и взаимодействие пользователей происходит через чат-бот в Telegram, предусмотрены различные сценарии информирования сотрудников и HR-специалистов, а также формирование статистических отчётов. Проект был реализован экспертами подразделения SAP Services CIS. Система представлена на выставке инноваций в Центре цифрового лидерства SAP.

Цифровые слепки распознанных лиц хранятся в системе в обезличенном виде, а фотографии

проходов удаляются через сутки. Также предусмотрена опция анонимизации реальной температуры сотрудника, в этом случае система будет высылать только информацию о положительном или отрицательном результате замера относительно заданного порога срабатывания. Кроме этого, каждому сотруднику можно задать свой индивидуальный температурный порог, учитывая особенности организма.

—
Легализация биометрии и её оборота в РФ

Определение биометрических данных

ч. 1 ст. 11 152-ФЗ от 27.07.2006 «О персональных данных»

Биометрические персональные данные — это сведения о физиологических и биологических особенностях человека, которые:

1. **Позволяют** установить личность человека; 2. **Используются** для установления личности человека.

Биометрия → строгое регулирование

—
Сведения о физиологических и биологических особенностях человека

Статические сведения

Физиологическая характеристика человека, т. е. уникальное свойство, данное человеку от рождения, например:

- рисунок вен; - папиллярные узоры пальцев; - радужная оболочка и сетчатка глаза; - геномная информация (п. 3 ст. 1 242-ФЗ от 03.12.2008 «О государственной геномной регистрации в РФ»); - фотография или видеоизображение лица.

Динамические сведения

Поведенческая характеристика человека, например:

- голос; - подпись, показывающая физиологическо-поведенческие характеристики (степень нажатия, направление движений, штрих и прочие аспекты); - поведенческие паттерны (например, нажатие клавиш).

—
Сведения позволяют установить личность человека

- □ Оператор должен организовывать и, возможно, осуществлять обработку биометрических данных, т. е. если такие данные обрабатываются исключительно на устройстве пользователя, а оператору сообщаются лишь сведения о результатах идентификации, то нельзя говорить об обработке оператором биометрических данных. - □ В ст. 11 152-ФЗ прямо не указано, что с помощью биометрических персональных данных оператор может не только установить (идентифицировать) личность субъекта данных, но и удостоверить/подтвердить

(аутентифицировать) личность. - В ст. 11 152-ФЗ отсутствует квалифицирующий критерий применения специальных технических средств (средств автоматизации) для получения эталонных образцов биометрических данных физического лица и последующего автоматизированного (автоматического) сопоставления эталонных образцов с получаемыми/предъявляемыми биометрическими данными. - В законодательстве РФ не указывается на достоверную идентификацию субъекта как на необходимый признак биометрических данных, хотя наличие ошибок идентификации неизбежно. Все биометрические технологии характеризуются такими параметрами, как False Accept Rate (процент ошибочного разрешения доступа) и False Reject Rate (процент ошибочного отказа в доступе).

—

Сведения используются для установления личности человека

Биометрическая аутентификация — процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем своего биометрического образа и путём преобразования этого образа в соответствии с заранее определённым протоколом аутентификации.

Не следует путать данные системы с системами биометрической идентификации, каковыми являются, к примеру, системы распознавания лиц водителей и биометрические средства учёта рабочего времени. Биометрические системы аутентификации работают в активном, а не пассивном режиме и почти всегда подразумевают авторизацию. Хотя данные системы не идентичны системам авторизации, они часто используются совместно (например, в дверных замках с проверкой отпечатка пальца).

—

Позиции ведомств по биометрии

Документ / Источник	Ключевая позиция	Фото — БПД?	Условие / Основание
—	—	—	—
Письмо Минцифры № ЛБ-С-074-24059 (28.08.2020)	Перечислены данные, НЕ относящиеся к БПД: копии паспорта, фото в личном деле, подпись, рентген-снимки, видеосъёмка в публичных местах	В перечисленных случаях — нет	Нет цели установления личности
Письмо Минцифры № ОП-П24-070-19433 (17.07.2020)	Фото в СКУД — БПД, т. к. используется для установления личности при пропускном режиме. Обработка БПД несовершеннолетних в школах недопустима	Да (в СКУД)	Используется для установления личности при проходе
Письмо РКН № 08-78032 (29.08.2022)	Фото является БПД только если прямо отнесено к таковым НПА (напр. загранпаспорт по Постановлению Правительства № 125). В иных случаях — основания ст. 6 ФЗ-152	Зависит от НПА	Если прямо указано в законодательном акте РФ

Письмо РКН № 08АП-6782 (10.02.2020)	Практические рекомендации по БПД несовершеннолетних. Квалификация фото не привязана к формату изображения	☐ Зависит от цели	Используется для установления личности
Ответ РКН на обращение № 08-128904 (23.04.2024)	Фото само по себе не биометрично, т. к. не содержит термограммы лица, рисунка радужки, папиллярных узоров	☐ Само по себе — нет	Без индивидуальных параметров установления личности

Судебная практика признания сведений в качестве биометрии

- фотографии на пропусках (Определение Верховного Суда РФ от 05.03.2018 №307-КГ18-101 по делу №А42-342/2017; Постановление Арбитражного суда Северо-Западного округа от 21.11.2017 №Ф07-11732/2017 по делу №А42-342/2017); - ладони учащихся, рисунок вен рук, используемый для идентификации при оплате (Решение Лискинского районного суда Воронежской области от 09.07.2018 №12-35/2018); - информация о здоровье наследодателя, содержащаяся в медицинской организации (Апелляционное определение Московского городского суда от 30.01.2019 по делу №33а-1238/2019); - сведения, содержащиеся в удостоверении моряка (Апелляционное определение Санкт-Петербургского городского суда от 07.07.2020 №33а-13473/2020 по делу №2а-769/2020); - видеоизображения, получаемые с помощью видеокамеры в общей долевой собственности истца и ответчика (Определение Пятого кассационного суда общей юрисдикции от 28.09.2021 по делу №88-7100/2021); - фотографии несовершеннолетних лиц с указанием их фамилий, имён и отчеств (Решение Зеленоградского районного суда города Москвы от 23.06.2022 по делу №12-0531/2022); - фотография работника, опубликованная его бывшим работодателем на рабочем сайте для привлечения внимания соискателей к своим вакансиям (Определение Второго кассационного суда общей юрисдикции от 04.07.2023 по делу №88-13675/2023); - признание недопустимости дактилоскопирования без согласия работника для обеспечения пропускного и внутриобъектового режимов в организации, где хранятся наркотические лекарственные препараты (Определение Второго кассационного суда общей юрисдикции от 01.11.2022 по делу №88-24328/2022).

Судебная практика непризнания сведений в качестве биометрии

- видеоизображения на городских камерах видеонаблюдения, используемое ГУ МВД РФ по г. Москве для целей, связанных с общественной безопасностью (Кассационное определение Второго кассационного суда общей юрисдикции от 31.07.2020 г. №88а-17020/2020; Апелляционное определение Московского городского суда от 30.01.2020 по делу №33а707/2020, №2а-577/2019); - видеоизображения на частных камерах видеонаблюдения при том, что земельный участок истцов не охватывается камерой, а качество съёмки не позволяет достоверно идентифицировать полученные при съёмке изображения с конкретными лицами (Апелляционное определение Верховного суда Республики Коми от 04.02.2019 по делу №33-640/2019); - видеоизображение, полученное посредством съёмки на камеру мобильного телефона (по причине того, что видеозапись не содержит сведений, позволяющих идентифицировать физическое лицо как конкретного субъекта данных) (Постановление Четвёртого кассационного суда общей юрисдикции от 16.10.2020 по делу №16-894/2020); - видеозапись с камер наблюдения медицинской организации, продемонстрированная

посетителю с целью помощи в установлении обстоятельств пропажи телефона посетителя (Определение Восьмого кассационного суда общей юрисдикции от 19.12.2019 по делу №88-1005/2019); - информация, потенциально собираемая с камеры видеонаблюдения в доме при том, что она не направлена на квартиру истца и используется для охраны и безопасности владельца (Решение Кировского районного суда города Саратова от 01.06.2021 по делу №2-2354/2021); - информация с камер видеонаблюдения в государственном органе до передачи в целях идентификации (Апелляционное определение Нижегородского областного суда от 19.12.2018 по делу №33а-15421/2018); - изображение спящего работника до того момента, как оно будет передано для установления личности (Решение Кинешемского городского суда Ивановской области от 27.05.2021 по делу №2-873/2021); - проверка уполномоченным/должностным лицом благонадёжности («живости») владельца учётной записи (профиля) на интернет-ресурсе по видеоизображению владельца указанного профиля (Решение Рязанского областного суда от 11.03.2026 по делу №33-342/2026); - признание допустимости дактилоскопирования работников для обеспечения пропускного и внутриобъектового режимов объекта ТЭК (Определение Седьмого кассационного суда общей юрисдикции от 06.09.2022 по делу №88-13416/2022).

Прокурорская проверка обработки биометрических данных при поддержке ФСБ и Росгвардии

- ООО «Савёлкинский проезд, д. 4» осуществлял пропускной режим в здание управления бизнес-центром «Зеленоград». 20.01.2022 года прокуратурой Зеленоградского административного округа г. Москвы, в связи с обращением гражданки, была проведена проверка исполнения законодательства о персональных данных указанным юридическим лицом. К проведению проверки в качестве специалистов были привлечены сотрудники территориального отдела ФСБ и Отдела лицензионно-разрешительной работы Росгвардии по Зеленоградскому АО. - В ходе проверки был установлен факт хранения с 02.10.2021 года на компьютерах, используемых администраторами ООО «Савёлкинский проезд, д. 4», 170 фотографий учащихся ООО «*» **(Центр Компьютерного Обучения и дополнительного образования) с указанием фамилий, имён и отчеств каждого ребёнка (биометрические персональные данные — исходя из Определения ВС РФ от 05.03.2018 №307-КГ18-101 и письма Минцифры России от 17.07.2020 №ОП-П24-070-19433). Через несколько минут после осмотра компьютеров обнаруженные файлы были удалены из компьютеров кем-то из сотрудников ООО «Савёлкинский проезд, д. 4». - Должностное лицо — старший администратор ООО «Савёлкинский проезд, д. 4» — на основании приказа руководителя организации является лицом, ответственным за обработку персональных данных субъектов при оформлении электронных карт доступа. Таким образом, старший администратор ООО «Савёлкинский проезд, д. 4» осуществлял незаконную обработку персональных данных 170 учащихся ООО «*», то есть совершил административное правонарушение, предусмотренное ч. 2 ст. 13.11 КоАП РФ, так как письменные согласия родителей на обработку персональных данных их детей в управляющей компании и ООО «***» отсутствовали. - Решением мирового судьи судебного участка №2 района Савёлки г. Москвы 18.04.2022 старшему администратору ООО «Савёлкинский проезд, д. 4» был назначен административный штраф в 20 000 ₽ по ч. 2 ст. 13.11 КоАП РФ. Зеленоградский районный суд Москвы 23.06.2022 оставил указанное решение в силе.**

Биометрическая идентификация и аутентификация в ЕБС

Разграничение сферы регулирования 152-ФЗ и 572-ФЗ

(см. <https://ebs.ru/documents/>)

Изменение регулирования с 2023 г.

(см. <https://ebs.ru/documents/>)

Типы биометрии в ЕБС: упрощённая, стандартная, подтверждённая

(см. <https://ebs.ru/citizens/>)

Организация работы СКУД по требованиям 572-ФЗ

(см. <https://ebs.ru/documents/>)

Модели взаимодействия с ЕБС: транзакционная и векторная

(см. <https://ebs.ru/documents/>)

Транзакционная модель [идентификация/аутентификация в ЕБС]

(см. <https://ebs.ru/documents/>)

Векторная модель [аутентификация в КБС]

(см. <https://ebs.ru/documents/>)

Требования по аккредитации

(см. <https://ebs.ru/documents/>)

—

Особенности, ограничения, риски и рекомендации при встраивании биометрии в ИТ/ИИ-продукты

Снятие и преобразование в цифровую форму (биометрический вектор) отличительной характеристики

(Компоненты биометрической системы общего вида — ГОСТ Р 54412-2019)

—

Проблемы терминологии

Установление личности субъекта данных (ст. 11 152-ФЗ):

1. Биометрическая идентификация (572-ФЗ) — установление личности путём установления сведений о лице (1-to-n, «кто это?») **2. Биометрическая аутентификация** (572-ФЗ) — установление личности путём установления лица (1-to-1, «ты ли это?»)

—

Использование фотографии для управления физическим доступом

Правила обработки биометрии для контроля и управления доступом на территорию →

—

Сценарии обработки биометрических ПД

Квалификация по двум критериям: наличие биометрического распознавания × факт установления личности

Без распознавания и установления личности

- □ Видеонаблюдение для охраны объекта (имущество, безопасность посетителей) - □ Видеофиксация производственного процесса (технологический контроль) - □ Фотофиксация полок для анализа покупательского поведения - □ Видеоотслеживание меток (спецсостав) на форме/оборудовании вместо личности - ✖ Обработка ПД отсутствует или БПД не обрабатываются

Небиометрическое установление личности

- □ Охранник вручную сличает фото на пропуске с лицом посетителя - □ Видеозапись рабочих мест для контроля трудовой дисциплины - □ Проверка «живости» владельца аккаунта без хранения БПД - □ Авто-сличение фото посетителя с паспортом (разовый/постоянный) - □ Liveness-проверка при ВКС: живой ли человек, без установления личности - ✖ Личность устанавливается, но биометрическая система не задействована

Биометрическое установление личности

- □ Авто-аутентификация клиента по лицу/голосу в колл-центре [572-ФЗ] - □ Бесконтактная оплата проезда по лицу — [FacePay](#) [572-ФЗ] - □ Автоматическое создание учётки каршеринга через ЕБС + ЕСИА [572-ФЗ] - □ Сверка лица/голоса с базой мошенников [ст. 11 152-ФЗ / 572-ФЗ] - □ Аутентификация по отпечаткам пальцев в СКУД [ст. 11 152-ФЗ] - ✖ Строгий режим — ст. 11 152-ФЗ и/или 572-ФЗ, требуется ЕБС

Биораспознавание без установления личности

- □ Подсчёт уникальных посетителей без идентификации (охрана объекта) - □ Распознавание отсутствия СИЗ на производственной площадке - □ Обнаружение угроз в толпе (оружие, паника, оставленные предметы) - □ Транскрибация ВКС с разделением голосов без привязки к личности - □ Анализ усталости водителя по датчикам ТС (без ID водителя) - ✖ Биораспознавание есть, но ст. 11 152-ФЗ не применяется

—

Ограничения при встраивании биометрии в ИТ/ИИ-продукты

01 — Закрытый перечень биометрии в ЕБС

В рамках 572-ФЗ для автоматизированной идентификации/аутентификации допускаются только изображение лица и запись голоса. Геномная информация, отпечатки пальцев, рисунок вен, радужка в ЕБС не размещаются.

02 — Запрет трансграничной передачи БПД

Хранение и обработка — только на территории России. Облачные ИИ-сервисы на зарубежной

инфраструктуре (AWS Rekognition, Azure Face и др.) для задач биометрической идентификации использовать нельзя.

03 — Обязательная аккредитация

Право самостоятельно проводить биометрическую идентификацию вне ЕБС отсутствует. Для аутентификации требуется аккредитация: российское ПО, средства защиты класса КС/КВ, соответствие требованиям ФСТЭК и ФСБ.

04 — Особый режим согласия

Только письменная форма (в т. ч. через УКЭП), добровольно, с правом отзыва в любой момент. Отказ от сдачи БПД не может быть основанием для отказа в услуге или ухудшения её условий.

05 — Особые категории субъектов

Обработка БПД несовершеннолетних в СКУД и образовательных учреждениях прямо не разрешена (письмо Минцифры №ОП-П24-070-19433). Согласие законного представителя не заменяет письменное согласие самого субъекта.

06 — Технологические пределы точности

FAR и FRR всегда больше нуля: 100% точность недостижима. Качество падает с возрастом, из-за травм, условий съёмки, освещения, макияжа. Ошибки идентификации неизбежны и должны быть заложены в продуктовую логику.

07 — Только векторная модель для аккредитованных

Доступ к «сырой» биометрии из ЕБС закрыт: организация получает только биометрический вектор. Это ограничивает возможности дообучения собственных ИИ-моделей на реальных данных пользователей.

—

Ключевые риски при использовании биометрии в ИТ/ИИ-продуктах

01 — Необратимость при утечке

Биометрию нельзя «перевыпустить» как пароль или токен. Скомпрометированный шаблон (голос, лицо) остаётся уязвимостью пожизненно — и для всех систем, где он используется.

02 — Административная и уголовная ответственность

Утечка БПД в любом объёме — штраф до 20 млн ₽ (повтор — 1–3% годовой выручки, т. е. 25–500 млн ₽), нарушение правил работы с ЕБС — штраф до 1,5 млн ₽. Уголовная ответственность по ст. 137, 272, 272.1 УК РФ для должностных лиц.

03 — Смещение и дискриминация ИИ-моделей

По данным NIST FRVT, алгоритмы распознавания лиц показывают разную точность для разных демографических групп. Это источник репутационных претензий и поводов для жалоб в Роскомнадзор и прокуратуру.

04 — Атаки на биометрические системы

Deepfake и синтезированный голос, presentation attacks (маски, фото, 3D-модели), adversarial-воздействие на ИИ. Требуется сертифицированная liveness-проверка и регулярное обновление моделей противодействия.

05 — Function creep и избыточность сбора

Например, биометрическая СКУД начинает использоваться для оценки производительности или поведения сотрудников без надлежащей легализации. Это нарушение принципов целевого характера и минимизации обработки (ст. 5 152-ФЗ).

06 — Репутационные риски и общественное противодействие

Прецеденты с системой распознавания лиц в московском метро и с биометрией в школах показывают: любая биометрическая инициатива попадает под медийный микроскоп. Негативное освещение способно заблокировать запуск продукта.

07 — Предписания РКН и прокурорские проверки

Проверки совместно с ФСБ и Росгвардией могут привести к штрафам, обязанности удалить данные и приостановке обработки (пример: дело ООО «Савёлкинский проезд, д. 4», 2022 г.).

Рекомендации по снижению рисков для продуктовых команд

Архитектура и данные

- Отказаться от биометрии, если цель достижима альтернативой (карта, PIN, OTP). Биометрия не должна быть выбором «по умолчанию». - Реализовать обработку на устройстве (on-device): биометрия не покидает смартфон/терминал, оператор получает только результат «да/нет». - Хранить биометрические векторы вместо исходных изображений/записей. Шифрование, ротация ключей, минимальные сроки хранения. - Выбрать путь работы с ЕБС: собственная аккредитация или интеграция через уже аккредитованные организации (Ростелеком, АО «ЦБТ»). - Использовать сертифицированные алгоритмы и liveness-детекцию. Регулярно тестировать на FAR/FRR и устойчивость к deepfake.

Процессы и комплаенс

- Провести до запуска продукта оценку необходимости, пропорциональности, альтернатив и рисков обработки БПД для субъектов данных. - Оформлять явное письменное согласие. Всегда предусматривать безбиометрическую альтернативу без ухудшения условий обслуживания. - Вести журналы согласий и отзывов. Настроить процедуру уведомления Роскомнадзора об утечке в течение 24 часов и о результатах расследования — 72 часов. - Зафиксировать и ограничить цели обработки. Избегать function creep: каждое новое применение биометрии требует предварительной оценки и отдельного согласия. - Прозрачная коммуникация с пользователями: понятное объяснение, какие данные собираются, зачем, где хранятся и как их удалить.

Биометрические идентификация и аутентификация в РФ

Идентификация [ID]

[Суть: установление личности путем установления сведений о лице [152-ФЗ ст.11 ч.1; 572-ФЗ ст.2 п.6; письмо Минцифры от 28.12.2023 № П24-2-04-070-257558]

Алгоритм: получение сведений о лице из ЕСИА/ЕБС [транзакционная модель]

Дефиниции

- идентификатор - уникальное обозначение сведений о лице, необходимое для определения такого лица [572-ФЗ ст.2 п.6]

- идентификация - совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с идентификатором [572-ФЗ ст.2 п.7]

Биометрическое распознавание: автоматизированное (автоматическое) распознавание человека, основанное на его биологических и/или поведенческих (физиологических) характеристиках, производимое путем биометрической идентификации и/или биометрической верификации с использованием биометрической системы [ГОСТ ISO/IEC 2382-37-2016 п.37.01.03, ГОСТ Р 54412-2019 п.4.2]

Биометрическая идентификация: процесс поиска по базе данных биометрических регистраций, направленный на поиск и возврат идентификатора(ов) биометрического контрольного шаблона, связанного с одним индивидом [ГОСТ ISO/IEC 2382-37-2016 п.37.08.02]

Аутентификация [АТ]

Суть: установление личности путем установления лица [152-ФЗ ст.11 ч.1; 572-ФЗ ст.2 п.2; письмо Минцифры от 28.12.2023 № П24-2-04-070-257558]

Алгоритм: поиск [«1-к-п»] или проверка [«1-к-1»] сведений о лице в ЕСИА/ЕБС

[транзакционная модель] или КБС [векторная модель]

Дефиниции

- аутентификация - совокупность мероприятий по проверке лица на принадлежность ему идентификаторов посредством сопоставления их со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификаторами посредством использования аутентифицирующих признаков в рамках процедуры аутентификации, в результате чего лицо считается установленным [572-ФЗ ст.2 п.2]

Биометрическое распознавание: автоматизированное (автоматическое) распознавание человека, основанное на его биологических и/или поведенческих (физиологических) характеристиках, производимое путем биометрической идентификации и/или биометрической верификации с использованием биометрической системы [ГОСТ ISO/IEC 2382-37-2016 п.37.01.03, ГОСТ Р 54412-2019 п.4.2]

Биометрическая верификация: процесс подтверждения биометрического заявления при сравнении [ГОСТ ISO/IEC 2382-37-2016 п.37.08.03]

[биометрия](#)

From:

<https://wiki.privacy-advocates.ru/> - **Privacy Advocates | Альманах**

Permanent link:

https://wiki.privacy-advocates.ru/regulirovanie_oborota_bpd

Last update: **2026/04/29 21:15**

