

Квалификация некоторых сценариев обработки биометрических персональных данных

Актуальность материала: **13.04.2026**

В последние годы во многих юрисдикциях, включая Россию, вопросы обработки биометрии приобретают критическое значение — это обусловлено:

- широким распространением технологий распознавания лица, голоса, отпечатков и т. п. в частном и государственном секторах;
- усиленной правовой регламентацией обработки таких данных (в т.ч. в связи с Федеральным законом № 152-ФЗ о ПД и Федеральным законом от 29.12.2022 г. № 572-ФЗ о ЕБС);
- высокой чувствительностью биометрической информации, поскольку она позволяет установить личность человека в уникальной форме, что делает её особым объектом правовой охраны.

В такой ситуации точная квалификация конкретных сценариев обработки — не абстрактная теоретическая задача, а фундамент для правильного применения норм, исключения юридических рисков и защиты прав субъектов данных.

Аналитический материал посвящен классификации и квалификации сценариев обработки биометрических персональных данных (БПД) — то есть, рассмотрению различных ситуаций, в которых данные, характеризующие физиологические и поведенческие особенности человека, могут обрабатываться и какие именно действия по обработке подпадают под регулируемые нормы. В материале перечислены практические примеры, систематизированные по категориям, включая потоковую видеозапись, автоматические проверки личности, биометрическую аутентификацию и др.

Это позволяет сформировать чёткое представление о том, какие повседневные процессы юридически считаются обработкой биометрических данных и как они квалифицируются в правовом контексте. Одних только общих определений в нормативных актах часто недостаточно, чтобы ответить на вопросы практики.

Материал помогает:

- понять, когда действие является обработкой БПД, а когда — нет;
- отличить автоматизированное и неавтоматизированное установление личности;
- соотнести бизнес-процессы с правовыми требованиями.

Для компаний, юристов и разработчиков важно иметь ориентиры, которые позволяют согласовать собственные процессы с законом и избежать штрафов, предписаний или блокировок. Систематизация сценариев служит таким ориентиром.

Обработка БПД ¹⁾	Неприменение биометрического распознавания ²⁾	Применение биометрического распознавания
Отсутствие установления личности	1.1. Потокковая видеозапись на объектах недвижимости организации для обеспечения защиты посетителей и имущества от противоправных деяний (посягательств) 1.2. Потокковая видеозапись на объектах недвижимости организации для фиксации и контроля производственного процесса 1.3. Фотофиксация полок с выложенными товарами в магазине для анализа покупательского поведения и оптимизации обслуживания в ритейле 1.4. Фото/видео фиксация визуальной маркировки, т.е. нанесенных с помощью специального состава меток на одежду (рабочую форму) персонала, оборудование или инвентарь для мониторинга логистических процессов на складах и в промышленности, для управления пассажиропотоками, для рационального использования рабочих пространств и автоматизации клининга	2.1. Потокковая видеозапись территории для подсчета уникальных посетителей территории организации для принятия решения о надлежащих мерах охраны 2.2. Потокковая видеозапись территории для сигнализации о несоблюдении на производственной площадке требований по использованию средств индивидуальной защиты 2.3. Потокковая видеозапись территории для обнаружения угроз в местах массового скопления людей (применения оружия, насилия, поиска оставленных предметов, лежащих людей и признаков паники в толпе) 2.4. Автоматическая запись, анализ и транскрибация (расшифровка) содержания общения между несколькими участниками ВКС - с разделением голосов участников 2.5. Создание и использование для общения по ВКС реалистичных цифровых-аватаров/двойников на основе фото/видео пользователя 2.6. Автоматический сбор и анализ сведений о признаках усталости водителя как с помощью специальных датчиков транспортного средства, так и при фиксации неоднократного выезда транспортного средства с полосы движения 2.7. Речевая аналитика для офлайн-разговоров, позволяющая транскрибировать и анализировать диалоги с клиентами в точках продаж, в т.ч. отвечать на вопросы о клиентах в свободном формате, например: «Почему клиент отказался?» или «О каких товарах спрашивал клиент, которых не было в наличии?»³⁾

Обработка БПД ¹⁾	Неприменение биометрического распознавания ²⁾	Применение биометрического распознавания
Небиометрическое установление личности⁴⁾	3.1. Сличение уполномоченным лицом (охранником) фотографии человека на пропуске с лицом человека, предъявившего пропуск, для обеспечения внутриобъектового и пропускного режимов⁵⁾ 3.2. Поточная видеозапись на рабочих местах и в рабочих помещениях для контроля трудовой дисциплины (в т.ч. мониторинга и фиксации дисциплинарных проступков) по изображениям работников 3.3. Проверка уполномоченным/должностным лицом благонадежности («живости») владельца учетной записи (профиля) на Интернет-ресурсе по видеоизображению владельца указанного профиля⁶⁾	4.1. Автоматическое сличение фотографии разового посетителя на селфи с фотографией в паспорте/пропуске для определения тождества между обеими фотографиями 4.2. Автоматическое сличение фотографии постоянного посетителя, сделанной при онбординге, с фотографий в паспорте/пропуске для определения тождества между обеими фотографиями 4.3. Автоматическая проверка на liveness («живость», отсутствие подмены лица) и (или) проверка возраста/совершеннолетия при общении с клиентом по аудио- или видеосвязи, то есть на предмет того, что общение производится с живым человеком, не использующим маски или технологию дипфейк 4.4. Автоматический анализ эмоционального фона аудио- или видеозаписи разговоров между клиентом и службой поддержки банка для определения, что клиент находится в состоянии волнения или под давлением, и блокирования банковской операции, даже если личность клиента была ранее формально подтверждена 4.5. Обеспечение входа пользователя на ресурсы организации с использованием результатов работы FaceID, TouchID и иных биометрических сенсоров на пользовательском устройстве (без задействования ИТ-инфраструктуры какой-либо организации) 4.6. Использование фотоизображения работника для генерирования уникального ID (биометрического вектора), которое кодируется в размещаемом на служебном пропуске QR-код для считывания при обеспечении внутриобъектового и пропускного режимов 4.7. Использование голоса человека для оценки возможного наличия у него кардиометаболических заболеваний⁷⁾

Обработка БПД ¹⁾	Неприменение биометрического распознавания ²⁾	Применение биометрического распознавания
Биометрическое установление личности⁸⁾	5.1. Поиск злоумышленников (личность которых требует установления) уполномоченным/должностным лицом по изображениям, полученным на объектах недвижимости организации посредством видеонаблюдения или камеры на устройстве самообслуживания (банкомате, терминале оплаты и т.п.) по имеющимся в распоряжении самой организации, правоохранительных органов или иных уполномоченных лиц образцам для сравнения ^[ст.11 152-ФЗ] 5.2. Проверка уполномоченным/должностным лицом личности владельца учетной записи (профиля) на Интернет-ресурсе по видеоизображению владельца указанного профиля с совокупности с фотографией/сканом паспорта или водительских прав проверяемого лица ⁹⁾ ^[ст.11 152-ФЗ]	6.1. Автоматическая аутентификация клиента по изображению лица и/или записи голоса при его аудио- или видеозвонке в колл-центр организации, при входе на территорию организации, при использовании устройства самообслуживания организации или при подтверждении перевода или иной банковской операции ^[572-ФЗ] 6.2. Осуществление бесконтактной оплаты с помощью биометрии, позволяющая совершать платежи без карты или телефона (биоэквайринг), например, бесконтактная оплата проезда (система FacePay) ^[572-ФЗ] 6.3. Автоматическая идентификация клиента по изображению лица и/или записи голоса с помощью ЕБС для заполнения создаваемой учетной записи каршеринга данными из ЕСИА (портала «Госуслуги») ^[572-ФЗ] 6.4. Автоматическое сравнение изображения лица и/или записи голоса человека, обращающегося в организацию по телефону или офлайн, с содержащимися БПД в базе мошенников ^[ст.11 152-ФЗ/572-ФЗ] 6.5. Выявление потенциальных мошенников посредством анализа поведения субъектов, не являющихся клиентами организации, но регулярно посещающих территорию организации без цели обслуживания, посредством формирования базы БПД таких субъектов ^[ст.11 152-ФЗ/572-ФЗ] 6.6. Автоматическая аутентификация посетителя при проходе в помещение или на территорию организации путем сравнения отпечатков пальцев посетителя (папиллярные узоры пальцев и (или) ладоней рук человека) с контрольными шаблонами отпечатков, хранящимся в системе контроля и управления доступом организации ^[ст.11 152-ФЗ] 6.7. Автоматическая проверка благонадежности ¹⁰⁾ владельца учетной записи (профиля) на Интернет-ресурсе по видеоизображению с поворотом головы владельца указанного профиля, фотографии паспорта и фотографии водительских прав ¹¹⁾ ^[572-ФЗ]

NB: При подготовке материала использовался [практический комментарий Fintech Club RPPA "Обработка биометрических данных и антифрод в деятельности финансовых организаций"](#), с которым рекомендуется дополнительно ознакомиться.

биометрия

1)

Биометрические персональные данные (БПД) – ПД, обладающие биометрическим потенциалом (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность). В некоторых ситуациях квалификация ПД в качестве БПД может быть прямо установлена соответствующими НПА и (или) зависеть от соответствия параметров (характеристик) ПД требованиям применимых стандартов (например, ГОСТ Р ИСО/МЭК 19794-5-2013), а также факта обработки данных в биометрической системе (ИСПД).

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 помощью биометрической системы [ГОСТ ISO/IEC 2382-37-2016 п.37.01.03, ГОСТ Р 54412-2019 п.4.2].

3)

[Т-банк запустил ИИ-анализатор офлайн-разговоров с клиентами](#)

4)

Небиометрическое установление личности – установление сведений о человеке (идентификация) и/или установление самого человека (аутентификация) было произведено без использования БПД - с использованием иных факторов, в т.ч. когда установление личности было произведено предварительно (до начала обработки БПД) или постфактум (после окончания обработки БПД).

5)

Фото в пропуске необходимо не для установления личности, а лишь для удостоверения его прав на владение определенным документом – пропуском, который содержит в себе данные куда разрешен проход. Когда охранник смотрит на пропуск ему совершенно не важно как Вас зовут, и какого года Вы рождения. Главное что пропуск принадлежит Вам.

6)

Видеоизображение человека является биометрией лишь тогда, когда оно используется для установления личности. Если цель — проверить «живость» пользователя без привязки к конкретному лицу, это не подпадает под ст.11 152-ФЗ. Если видео обрабатывается в реальном времени и немедленно удаляется, отсутствует сам субстрат для обработки биометрических данных в правовом смысле. Это обстоятельство существенно отличает ситуацию от случаев, когда оператор накапливает и хранит биометрическую базу. См. [решение Рязанского областного суда от 11.03.2026 по делу №33-342/2026](#)

7)

Логика технологии такая: во время речи в организме человека одновременно «работают» дыхательная система, мышцы гортани, артикуляционного аппарата и механизмы нервной регуляции. И в случае воспаления, нарушения обмена веществ или повышенной нагрузки на сердечнососудистую систему голосовые параметры могут меняться. На слух эти перемены почти неразличимы. Но цифровая обработка голоса с помощью машинного обучения способна зафиксировать малейшие отличия.

8)

Биометрическое установление личности – установление сведений о человеке (идентификация) и/или установление самого человека (аутентификация) с использованием БПД. Автоматизированный способ обработки БПД не является безусловным доказательством факта автоматизации биометрического установления личности, если оно осуществляется с участием уполномоченного/должностного лица, осуществляющего эффективный контроль (в т.ч. возможность прервать автоматизированный процесс и/или изменить решение до его утверждения) в отношении принятия решения о соответствии и/или несоответствии предоставленных БПД «эталонным» БПД. Участие уполномоченного/должностного лица в биометрическом установлении личности выводит данный процесс из области действия

Федерального закона от 29.12.2022 г. № 572-ФЗ. Автоматизированное установление личности с использованием некоторых видов (модальностей) БПД регулируется нормами 572-ФЗ и может осуществляться исключительно с использованием ресурсов Единой биометрической системе биометрических персональных данных (ЕБС). Параметры собираемых для размещения в ЕБС видов БПД (полученное с помощью фотовидеоустройств изображение лица человека, полученная с помощью звукозаписывающих устройств запись голоса человека) установлены приказом Минцифры России от 12.05.2023 № 453.

⁹⁾

(Видео)проверку (с использованием видео- или фотоизображения лица + фото документа, удостоверяющего личность) могут интерпретировать как повторное установление личности, проводимое в случае появления сомнений в отношении достоверности результатов ранее проведенного (не)биометрического установления личности - см. [решение Московского районного суда от 04.12.2025 по делу № 2-2087/2025 ~ М-1409/2025](#)

¹⁰⁾

(Видео)проверку с использованием видео- или фотоизображения лица + фото документа, удостоверяющего личность благонадежности могут интерпретировать как повторное установление личности, проводимое в случае появления сомнений в отношении достоверности результатов ранее проведенного (не)биометрического установления личности.

¹¹⁾

См. [решение Московского районного суда от 04.12.2025 по делу № 2-2087/2025 ~ М-1409/2025](#)

From:

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

Permanent link:

https://www.wiki.privacy-advocates.ru/bpd_scenarii

Last update: 2026/04/16 16:29

