Банки собирают биометрические данные клиентов в единую базу: что это значит и как удалить информацию о себе

Банки уведомляют клиентов, что отправляют биометрические данные в Единую биометрическую систему (ЕБС). Объясняем, что это за данные, как этим способом идентификации пользуются многие, даже не догадываясь об этом, и насколько оправдан страх перед этой технологией.

Что происходит с биометрическими данными в России

Летом этого года многие россияне запаниковали из-за требования государства передать биометрию граждан в единую систему. В МФЦ в разных городах выстраивались очереди из желающих отказаться от сбора и хранения своих данных. Ажиотаж начался после того, как банки начали рассылать клиентам уведомления, что передают биометрические данные россиян. Это они были обязаны сделать до 1 октября, однако по итогу процесс продолжается и далее.

Эксперты считают, что формально банки, возможно, сделали все в срок, однако обнаружили данные, которые ранее не считали биометрией. Например, это могут быть фото с паспортом, которые делают представители кредитного учреждения на первой встрече с клиентом при дистанционном обслуживании.

С 1 декабря 2023 года Россияне смогут воспользоваться новым способом оплаты — по биометрии. Станет доступна плата за проезд в столичном метро, а также за товары и услуги в онлайн- и офлайн-магазинах. Этот способ еще называют биоэквайрингом.

Что такое биометрия

Биометрические данные — уникальные физиологические или поведенческие характеристики человека, которые могут быть измерены и использованы для идентификации или аутентификации личности. Эти данные могут включать в себя отпечатки пальцев, скан

радужки глаза, голосовые отпечатки, геометрию лица, динамику набора текста и множество других параметров.

В сфере финансов биометрические данные приобретают особое значение. Они используются для обеспечения безопасности и аутентификации клиентов в банковских системах, мобильных приложениях для финансовых операций и в других финансовых инструментах. Вот несколько способов, как биометрические данные находят свое применение:

- Аутентификация клиентов. Биометрические данные позволяют банкам и финансовым учреждениям удостовериться, что клиент действительно является тем, за кого себя выдает. Это снижает риски мошенничества и несанкционированных операций.
- Упрощение процессов. С использованием биометрических данных клиенты могут легко и удобно проводить финансовые операции, не запоминая сложные пароли или ПИН-коды. Например, разблокировка смартфона с помощью отпечатка пальца.
- Безопасность данных. Биометрические данные сложнее подделать или украсть, чем пароли или ПИН-коды, что делает их надежным средством защиты финансовой информации.
- Противодействие отмыванию денег и финансовым преступлениям. Биометрическая идентификация помогает выявлять подозрительные финансовые операции, а значит, и бороться с финансовым мошенничеством.
- Повышение уровня обслуживания клиентов. Введение биометрических технологий позволяет финансовым учреждениям предоставлять услуги клиентам быстрее и с бóльшим для них комфортом.

Какие бывают виды биометрических персональных данных

Вот основные виды биометрических данных:

- Отпечатки пальцев. Этот вид биометрии основан на уникальных узорах на кончиках пальцев. Системы считывания отпечатков пальцев широко используются в мобильных устройствах и системах безопасности.
- Сканирование радужки глаза. Радужка глаза имеет сложные узоры, которые могут быть сканированы и использованы для идентификации. Этот метод более точный и надежный.
- Геометрия лица. Системы распознавания лица анализируют уникальные черты лица человека, такие как форма глаз, носа и рта. Этот вид биометрии часто применяется в системах видеонаблюдения и разблокировки устройств.
- Голосовые отпечатки. Голос каждого человека уникален по тону, скорости и интонации. Голосовые системы биометрии используются в голосовых устройствах, таких как системы голосового управления.
- Динамика набора текста. Каждый человек набирает текст на клавиатуре или сенсорном экране уникальным образом. Этот вид биометрии может быть использован для аутентификации при вводе паролей или ПИН-кодов.
- Сканирование ладони. Узоры на ладони также уникальны для каждого человека и могут быть использованы для аутентификации.
- Электрокардиограмма (ЭКГ). Электрическая активность сердца у каждого человека различна и может быть использована в качестве биометрического идентификатора.
- Сосудистый отпечаток. Узоры сосудов внутри ладони или сетчатки глаза также могут служить уникальными биометрическими данными.

ДНК тоже можно использовать как биометрическую идентификацию, но понятно, что в повседневных задачах применять этот способ нельзя. Представьте, что вам нужно перевести

деньги со счета, но перед этим — сдать свой генетический материал и ждать его расшифровки до 30 дней. Это неудобно, поэтому такую сложную биометрию банки и госучреждения не используют. К этой же категории можно отнести ЭКГ, сосудистый отпечаток, радужку глаза и так далее. Сканирование этих данных не создает удобство, а только делает процесс более долгим.

Поэтому в качестве основных биометрических данных используется три их вида: отпечаток пальца, геометрия лица и голос. Их просто скопировать и сопоставлять с эталонами из базы данных.

Иногда различные виды биометрии комбинируют. Это требуется, чтобы обеспечить высокую степень защиты.

Кто и как собирает биометрические данные

Биометрические данные собирают разные организации и учреждения в зависимости от их целей и потребностей.

Банки и другие финансовые учреждения собирают геометрию лица и отпечаток голоса для аутентификации клиентов при проведении финансовых операций через мобильные приложения или банковские терминалы.

Таможенные и пограничные службы. Чтобы идентифицировать путешественников, многие страны собирают сканы отпечатков пальцев и фотографии. В медицинской сфере биометрические данные используют для идентификации пациентов и доступа к медицинской истории.

Технологические компании собирают биометрические данные через датчики, такие как сканеры отпечатков пальцев или камеры для распознавания лиц, чтобы обеспечить дополнительную защиту и удобство для пользователей. По сути, когда вы разблокируете свой телефон с помощью своего лица или отпечатка пальца, вы пользуетесь биометрией.

Важно помнить, что собирать и хранить биометрические данные можно только с согласия человека. Более того, согласно действующему законодательству, любой гражданин может отозвать свои данные. Правда, это правило не касается биометрии, которая хранится в органах внутренних дел.

Биометрические данные обладают особым статусом в силу своей уникальности и чувствительности, и их хранение требует дополнительных мер безопасности. Обычно они хранятся и обрабатываются следующими способами:

- Хранение в зашифрованном виде. Биометрические данные часто хранятся в зашифрованной форме, что делает их труднопонимаемыми для несанкционированного доступа. Только авторизованные системы и лица могут расшифровать их.
- Хэширование. Вся биометрия, которая хранится в цифровом виде, захэширована. На сервере хранится не запись вашего голоса, фотография лица или отпечатки, а уникальные характеристики, преобразованные в уникальный код. При этом процессе нельзя восстановить исходные записи.
- Сохранение на безопасных серверах. Организации, собирающие биометрические данные, обычно хранят их на высокозащищенных серверах или в облаке с применением передовых мер безопасности.
- Строгие права доступа. Только авторизованные сотрудники с определенными правами могут получить доступ к этим данным.
- Удаление неиспользуемых данных. Если биометрические данные больше не требуются или срок их хранения истек, они должны быть удалены без возможности восстановления.
- Строгое законодательство. Организации, собирающие и хранящие биометрические данные, должны строго соблюдать законы о защите данных и приватности.

Что такое Единая биометрическая система (ЕБС)

ЕБС — единая государственная цифровая платформа для работы с биометрией. Система начала развиваться в России с 2018 года по инициативе Центрального банка и Минцифры. ЕБС хранит лишь слепки лица и голоса — в ней нет такой информации, как ФИО, адрес, паспортные данные и др. Поэтому, даже если злоумышленник попытается получить доступ к данным, определить, кому они принадлежат, будет невозможно, уверяют в ЦБТ.

Эта система была одной из многих. Банки и частные компании могли собирать свои данные, госорганы — другие. Однако до 30 сентября 2023 года все организации были обязаны передать все хранящиеся у них биометрические данные в ЕБС. Таким образом, вся биометрия россиян с 1 октября хранится у одного оператора. Это по-прежнему не касается данных, которые собирают для своей деятельности органы внутренних дел.

При этом за 30 дней до срока передачи данных компании были обязаны сообщить своим клиентам, что их биометрия будет передана в единую государственную платформу.

Если человек не против передачи информации, то данные переносят в ЕБС по защищенному каналу в автоматическом режиме. От передачи данных можно отказаться, причем сделать в любой момент.

Это важно запомнить. С июля 2023 года в Рунете появилось паническое сообщение, которое пользователи отправляют друг другу. Кратко его суть: если не отказаться от передачи биометрии до 1 сентября, то государство и банки навсегда завладеют этими данными, даже если вы этого не захотите.

Это не так. Во-первых, отказаться можно в любой момент. Во-вторых, принудительно собирать биометрию запрещено, а отказ от ее сдачи не может влиять на оказание государственных и муниципальных услуг.

Как удалить биометрические данные и проверить, сдавали ли вы биометрию

Если ваша биометрия уже есть в ЕБС, ее можно удалить в любой момент. Для этого нужно зайти в свой профиль на «Госуслугах». В настройках «Профиль» найти раздел «Биометрия». Вы увидите список хранящихся данных, дату сдачи и организацию, которая их зарегистрировала. Там же есть соответствующая кнопка, с помощью которой биометрию можно удалить.

Если данных в ЕБС нет, то появится сообщение «Биометрия не зарегистрирована». Это не значит, что в ближайшее время она не появится: у организаций есть время до 30 сентября передать данные.

Поэтому уточнить, регистрировали ли вы данные или нет, можно через банк. Это можно сделать через поддержку — по телефону или в чате приложения.

Каждый человек может отказаться от сбора и размещения биометрии, такое право закреплено в законе. Для этого потребуется подать заявления в МФЦ: их принимают с 1 июня 2023 года. С собой нужно взять только паспорт.

Как сдать биометрические данные

У ЕБС есть два вида биометрии — стандартная и подтвержденная. Первую гражданин регистрирует сам с помощью телефона или планшета. Для регистрации потребуется:

- смартфон с NFC-чипом;
- загранпаспорт нового образца;
- подтвержденная учетная запись на «Госуслугах».

Нужно скачать приложение «Госуслуги биометрия». Там есть подробная инструкция по регистрации.

С помощью стандартной биометрии можно дистанционно оформить карту болельщика, оплатить проезд в метро, авторизоваться на «Госуслугах», бесконтактно пройти в офис или на стадион, удаленно заключить договор на оказание услуг связи.

Подтвержденная биометрия сдается только очно в центрах обслуживания. Это, как правило, банки. Редко — МФЦ или отделение почты. Операционист подтвердит вашу учетную запись на «Госуслугах», сделает фотографию и запись голоса. Активация биометрии займет до пяти дней.

С собой понадобится взять паспорт и СНИЛС.

Подтвержденная биометрия дает доступ ко всем видам услуг. Например, можно открыть банковские счета, оформить потребительский кредит, получить усиленную электронную подпись физлица.

Обратите внимание: сдать данные может только гражданин России старше 18 лет. Несовершеннолетние, даже с разрешения родителей, биометрию зарегистрировать не могут.

Плюсы и минусы биометрии

Преимущества биометрических данных:

- Уникальность и надежность. Биометрические данные основаны на уникальных физиологических или поведенческих характеристиках, что делает их надежным средством идентификации.
- Удобство и быстрота. Биометрическая аутентификация быстро и удобно позволяет подтвердить личность без необходимости запоминать сложные пароли или коды.
- Снижение риска мошенничества. Благодаря сложности подделки биометрических данных они помогают снизить риск финансовых мошенничеств и несанкционированных действий.
- Внедрение биометрии усиливает безопасность финансовых операций и доступа к личным данным.
- Улучшение клиентского опыта.

Минусы биометрических данных:

- Возможность утечки данных. Несмотря на высокий уровень безопасности, биометрические данные могут подвергаться угрозам, особенно при атаках на серверы с данными.
- Приватность и беспокойство о данных. Некоторые пользователи опасаются, что их биометрические данные могут использовать без их согласия.
- Сложность восстановления при потере. Если биометрию скомпрометируют, то восстановить надежность — задача сложная из-за неизменяемости. В отличие от классического пароля нельзя просто так изменить свой голос или геометрию лица.
- Технические проблемы. Представьте, у вас сломалась веб-камера на ноутбуке. Как в этом случае войти на те же «Госуслуги», если биометрия — единственный способ входа?
-

Что такое биометрия и как отказаться от ее сбора: кратко

- Биометрические данные — уникальные физиологические или поведенческие характеристики человека, которые могут быть измерены и использованы для идентификации или аутентификации личности.

- Видов биометрии много — от голоса и геометрии лица до ДНК и манеры набора текста. Однако не все из них подходят для бытовых и финансовых операций. Поэтому самыми популярными сейчас являются голос, фотография и отпечатки пальцев.
- До сентября 2023 года биометрические данные собирали разные организации — от банков до нотариусов. Однако до 30 сентября все организации обязаны передать собранные данные в государственную ЕБС.
- Если вы не сдавали биометрические данные ранее, то и передавать нечего: в ЕБС они не появятся.
- Если биометрией все-таки пользовались, но теперь хотите ее отозвать, вы можете сделать это в любой момент.
- Удалить данные можно как онлайн через «Госуслуги» в настройках профиля, так и очно через МФЦ. В последнем случае понадобится паспорт.
- Чтобы, напротив, сдать биометрию, сначала определитесь с целями этого. Если вы хотите дистанционно оформлять договоры с операторами связи, оплачивать поездки в метро и пользоваться картой болельщика, то достаточно стандартной биометрии. Ее можно зарегистрировать через приложение «Госуслуги биометрия».
- Чтобы пользоваться банковскими, а в будущем и страховыми услугами, понадобится зарегистрировать подтвержденную биометрию. Это можно сделать только очно в банках.

Подробнее на сайте https://www.banki.ru/news/daytheme/?id=10992698