Обзор
Минцифры установило правила работы с биометрическими данными

С 15 октября 2021 года, согласно данным Правительства Москвы, пассажиры метро оплатили при помощи Face Pay более 160 тыс. поездок. Кроме того, Верховный суд разрешил штрафовать нарушителей масочного режима без проведения расследования и экспертизы, теперь достаточно протокола и фотофиксации. Все это говорит о том, что все чаще различные решения о доступе куда-либо, о назначении штрафа и т.п. будут приниматься на основе данных биометрии, изображений. А это значит, что вопрос обеспечения конфиденциальности и целостности биометрических данных граждан становится все более значимым.

В целях обеспечения безопасности биометрических данных за последнее время было выпущено несколько документов: **приказы Министерства цифрового развития, связи и массовых коммуникаций** Российской Федерации № 902 от 01.09.2021 и № 930 от 10.09.2021 г. (зарегистрированы в Министерстве юстиции РФ), а также **постановление Правительства РФ** № 1815 от 23.10.2021 г.

В октябре 2021 года Министерство цифрового развития взамен устаревшего приказа № 321 от 25.06.2018 г. опубликовало новый приказ № 930 от 10.09.2021 г. об утверждении **порядка обработки, размещения и обновления биометрических персональных данных (ПДн)**. В этом приказе утверждены:
- порядок обработки параметров биометрических данных физических лиц, включая данные изображения лица и данные голоса;
- порядок размещения и обновления биометрических персональных данных;
- требования к информационным системах и техническим средствам, предназначенным для обработки биометрических персональных данных.

Подписанный приказ вступает в силу с 1 марта 2022 года и действует до 1 марта 2028 года, а пока обработка биометрических персональных данных должна осуществляться в соответствии с предыдущим приказом № 321.

Новый документ направлен на регулирование деятельности организаций, проводящих идентификацию и/или аутентификацию с использованием биометрических ПДн физических лиц, а также обеспечение исполнения требований к качеству биометрических образцов, размещаемых в Единой Биометрической Системе (ЕБС). Целью издания нового приказа является унификация параметров образцов биометрических данных, собираемых в различные коммерческие биометрические системы.

Согласно приказу, сбор биометрических данных физического лица с целью создания **биометрического контрольного шаблона**[1] и его хранения в ЕБС может

[1] Биометрический контрольный шаблон - биометрический образец или комбинация биометрических образцов, пригодные для хранения в качестве контрольных для дальнейшего сравнения)

осуществляться только при личном присутствии этого лица следующими категориями лиц:

1. Уполномоченные сотрудники государственных органов, банков и иных организаций, осуществляющих обработку (сбор, хранение и передачу информацию о степени их соответствия предоставленным биометрическим данным);
2. Уполномоченные лица организаций, владеющих информационными системами, обеспечивающими идентификацию и/или аутентификацию и оказывающих услуги по идентификации и/или аутентификацию с использованием биометрических персональных данных.

Затем биометрические контрольные шаблоны могут применяться для идентификации/аутентификации физического лица без его присутствия. При этом уполномоченный сотрудник осуществляющей обработку ПДн организации подписывает собранные с целью идентификации/аутентификации биометрические ПДн своей усиленной электронной подписью и обязуется соблюдать конфиденциальность используемых ими ключей электронных подписей.

Перед сбором биометрии государственные органы и другие организации обязаны:

- определить уполномоченных сотрудников,
- обеспечить защищенное хранение ключей электронной подписи,
- обеспечить подписание уполномоченными сотрудниками собранных биометрических ПДн своей усиленной ЭП,
- не реже 1 раза в неделю проверять функционирование информационных систем и технических средств, задействованных в работе с биометрическими ПДн.

Приказ также обязует организации, осуществляющие обработку биометрических персональных данных, **информировать вышестоящие органы** о произошедших инцидентах информационной безопасности и регламентирует сроки этого информирования. Банки и финансовые организации, в том числе кредитные, обязаны сообщить Банку России об инцидентах информационной безопасности не позднее 1 рабочего дня с момента его выявления. Нефинансовые организации в свою очередь должны оповестить об инцидентах в такой же срок свой надзорный орган – Минцифры РФ. Кроме того, организации ежегодно с привлечением лицензированных организаций должны проводить оценку соответствия требований к защите информации и информировать контролирующие органы о результатах оценки.

Обрабатывать биометрические ПДн в соответствии с требованиями 149-ФЗ и другими законами в области персональных данных можно только после проведения идентификации физического лица и получения **согласия на обработку ПДн и биометрических ПДн**. В случае отзыва субъектом ПДн своего согласия обработка биометрических ПДн должна быть прекращена.

Но есть ряд случаев, когда закон о защите персональных данных позволяет не получать у гражданина на биометрию согласие в письменном виде, если:

- исполняется судебное решение,
- осуществляется разбирательство по уголовному, административному, гражданскому делу,
- производится регистрация в рамках обязательной государственной процедуры (получение заграничного или российского паспорта),
- проводятся действия в рамках международных соглашений о реадмиссии,
- речь идет о выполнении задач по обороне государства, предупреждению террористических актов, поддержанию транспортной безопасности и т.п.

При каждом обращении физического лица в организации, осуществляющие идентификацию или аутентификацию с использованием биометрических данных, в информационных системах этих организаций создаются **биометрические образцы данных изображения лица и голоса**, которые затем сравниваются с биометрическим контрольным шаблоном. Требования к образцам изображения лица и голоса зафиксированы в п.11 и 12, соответственно, Приказа Минцифры №930 от 10.09.2021 г. Контроль качества этих образцов производится в автоматизированном режиме с использованием специализированного программного обеспечения, предоставляемого оператором ЕБС. При прохождении контроля каждый образец отмечается датой, временем и местом создания, информацией о технических средствах, использованных для сбора и обработки биометрических персональных данных.

Хранение биометрических ПДн обязательно в течение не менее 50 лет с даты размещения, кроме случаев, когда субъект ПДн отозвал их. Обновление биометрических ПДн в ЕБС и других информационных системах осуществляется физическим лицом добровольно по истечении 5 лет со дня их размещения или по истечении 3 лет – если расстояние между центрами глаз биометрических ПДн составляет менее допустимого значения в 120 пикселей, но не менее 45 пикселей. Также обновление возможно по инициативе субъекта ПДн в любой момент.

Также документом установлены **требования к информационным технологиям и техническим средствам**, предназначенным для обработки биометрических ПД в целях проведения идентификации и прописана допустимая вероятность ложного совпадения предоставленных государственными органами, финансовыми и другими организациями: для изображения лица этот показатель должен составлять не более 0,0001, для голоса — не более 0,1. Организации финансового рынка должны использовать информационные технологии и технические средства, которые соответствуют 2 уровню защиты информации, установленному национальным стандартом РФ ГОСТ Р 57580.1-2017.
Кроме того, определены требования к средствам защиты информации (в т.ч. средствам криптографической защиты информации) – согласно п. 17 Приказа Минцифры РФ №930, они должны соответствовать п. 4, 6 части 13 и частям 14, 14.1 статьи 14.1 Федерального закона № 149-ФЗ.

В октябре 2021 года Правительство РФ постановлением № 1815 от 23.10.2021 г. утвердило новый **перечень случаев осуществления сбора и обработки биометрических ПДн** для идентификации и аутентификации физического лица. В него вошли: использование биометрических данных для идентификации водителей легкового такси, каршеринга, при проходе на территорию организаций, при участии в собраниях участников гражданско-правового сообщества.

В ноябре 2021 года был опубликован приказ Минцифры РФ № 902 от 01.09.2021 г., который утвердил согласованный с ФСБ России, ФСТЭК России и ПАО Ростелеком **перечень угроз безопасности**, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия биометрическим данным, хранящимся в информационных системах.

Потенциальные угрозы, приведенные в документе, разделены на 7 видов по сценариям использования биометрических персональных данных:

1. При автоматизированной обработке на пользовательском оборудовании, имеющем в составе идентификационный модуль;
2. При сборе биометрических ПДн в центральном (головном) офисе, филиалах или внутренних структурных подразделениях, осуществляющих идентификацию/аутентификацию с использованием стационарных компьютерных средств и при передаче ПДн между филиалами или подразделениями и центральным (головным) офисом;
3. При сборе биометрических ПДн работниками организаций с использованием переносных компьютерных устройств и при передаче собранных данных между переносными устройствами и информационной инфраструктурой структурных подразделений организаций для обработки ПДн;
4. При обработке (за исключения сбора), в том числе хранении, биометрических ПДн и информации о степени их соответствия биометрическим данным физического лица в осуществляющих обработку информационных системах организаций в целях аутентификации;
5. При обработке (за исключения сбора) биометрических ПДн и информации о степени их соответствия при взаимодействии с собственными информационными системами организаций в целях аутентификации с использованием стационарных компьютерных устройств, мобильных устройств и планшетов;
6. При обработке (за исключением сбора) биометрических ПДн и информации о степени их соответствия в осуществляющих их обработку ИС в целях идентификации либо идентификации и аутентификации;
7. При обработке (за исключением сбора) биометрических ПДн и информации о степени их соответствия при взаимодействии с собственными ИС организаций в целях идентификации либо идентификации и аутентификации с использование стационарных компьютерных устройств, мобильных устройств и планшетов.

По виду воздействия на персональные данные угрозы делятся на 4 категории:

1. Угрозы нарушения целостности (подмены, удаления), нарушения достоверности (внесения фиктивных ПДн);
2. Угрозы нарушения конфиденциальности (компрометации) биометрических ПДн (утечка, перехват);
3. Угрозы несанкционированного доступа к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данные, в том числе путем использования уязвимостей кода, архитектуры, конфигурации систем и сетей, внедрения вредоносного программного обеспечения/программно-аппаратных средств;
4. Угрозы нарушения доступности, в том числе отказа в обслуживании компонентов, нарушения функционирования программно-аппаратных средств обработки, передачи и хранения биометрических ПДн, в том числе путем использования различных уязвимостей внедрения вредоносного ПО, использования недекларированных возможностей.

В России основными документами, регулирующими обработку биометрических ПДн являются:

- статья 23 Конституции Российской Федерации,
- статьи 272 и 137 Уголовного Кодекса РФ,
- Федеральный закон «О защите персональных данных» ФЗ-152,
- Кодекс РФ об административных правонарушениях,
- Конвенция Совета Европы № 108 о защите частных лиц в отношении автоматизированной обработки данных личного характера, ратифицированная РФ,
- приведенные в данном обзоре приказы Минцифры РФ и постановление Правительства РФ.

Несмотря на активное законотворчество в направлении обеспечения безопасности биометрических персональных данных на федеральном и на международном уровне, требуется дальнейшая работа непосредственно с операторами персональных данных с целью обеспечения безопасности биометрических данных как в случае вторжения злоумышленников, так и от внутренних угроз.