



**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ
КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

ПРИКАЗ

№ _____

Москва

Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации

В соответствии с пунктом 1 части 13 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2021, № 11, ст. 1708), абзацем шестым пункта 1 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418 (Собрание законодательства Российской Федерации, 2008, № 23, ст. 2708; 2021, № 26, ст. 4967),

ПРИКАЗЫВАЮ:**1. Утвердить:**

порядок обработки, включая сбор и хранение, параметров биометрических персональных данных согласно приложению № 1 к настоящему приказу;

порядок размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, согласно приложению № 2 к настоящему приказу;

требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации, согласно приложению № 3 к настоящему приказу.

2. Признать утратившими силу приказы Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации:

от 25 июня 2018 г. № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» (зарегистрирован Минюстом России 4 июля 2018 г., регистрационный № 51532);

от 4 июля 2019 г. № 369 «О внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25 июня 2018 г. № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» (зарегистрирован Минюстом России 25 сентября 2019 г., регистрационный № 56059).

3. Настоящий приказ вступает в силу с 1 марта 2022 г. и действует до 1 марта 2028 г.

Министр

М.И. Шадаев

ПРИЛОЖЕНИЕ № 1
к приказу Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 10 сентября 2021 г. № 930

ПОРЯДОК
обработки, включая сбор и хранение, параметров биометрических
персональных данных

1. Обработка, включая сбор и хранение, параметров биометрических персональных данных для идентификации реализуется с применением информационных технологий и технических средств, имеющих подтверждение соответствия требованиям, установленным в соответствии со статьей 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2021, № 11, ст. 1708) (далее – Федеральный закон № 149-ФЗ), которое проводится федеральным органом исполнительной власти, осуществляющим регулирование в сфере идентификации физических лиц на основе биометрических персональных данных.

2. В соответствии с настоящим порядком проводится обработка параметров биометрических персональных данных физического лица следующих видов:

данные изображения лица;

данные голоса, собранные текстозависимым методом.

3. Для проведения идентификации сбор параметров биометрических персональных данных субъекта персональных данных производится при его личном присутствии уполномоченным сотрудником государственного органа, банка и иной организации, в случаях, определенных федеральными законами, в целях создания биометрического контрольного шаблона, хранение которого осуществляется в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее соответственно – орган и организация, единая биометрическая система) или уполномоченными сотрудниками организаций, владеющих информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающих услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц, в случаях, определенных частями 18.18, 18.20 статьи 14.1 Федерального закона № 149-ФЗ (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2021, № 1, ст. 18) (далее – организации,

осуществляющие идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц), в целях создания биометрического контрольного шаблона, хранение которого осуществляется в иных информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц.

4. Биометрические контрольные шаблоны используются в процессе проведения идентификации и (или) аутентификации физического лица, в том числе без его личного присутствия.

Уполномоченный сотрудник органа и организации при сборе параметров биометрических персональных данных в единую биометрическую систему, уполномоченный сотрудник организации, осуществляющей идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, при сборе параметров биометрических персональных данных в информационную систему такой организации подписывает собранные биометрические персональные данные своей усиленной электронной подписью.

5. Органы и организации, осуществляющие идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, при сборе параметров биометрических персональных данных для идентификации должны обеспечивать:

определение уполномоченных сотрудников, осуществляющих сбор параметров биометрических персональных данных и их обеспечение сертификатами ключей проверки электронной подписи;

защищенное хранение выданных уполномоченным сотрудникам, осуществляющим сбор параметров биометрических персональных данных, ключей электронной подписи, обеспечивающее их конфиденциальность и исключающее несанкционированное изменение, добавление и удаление в соответствии с законодательством Российской Федерации в области использования электронных подписей;

подписание своей усиленной электронной подписью уполномоченным сотрудником, осуществляющим сбор параметров биометрических персональных данных, информации, содержащей биометрические персональные данные, собранные указанным сотрудником, и иной информации, указанной в пункте 14 настоящего порядка;

обеспечение и регулярную проверку (не реже одного раза в неделю) функционирования информационных технологий и технических средств, иных программно-технических средств, предназначенных для обеспечения процессов сбора и обработки параметров биометрических персональных данных, в том числе автоматизированную передачу результатов проведенной проверки в единую биометрическую систему или иную информационную систему, обеспечивающую идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц соответственно.

6. Уполномоченные сотрудники, осуществляющие сбор параметров биометрических персональных данных, обязаны соблюдать конфиденциальность используемых ими ключей электронной подписи.

7. Кредитные организации, некредитные финансовые организации, которые осуществляют указанные в части первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 24, ст. 4210) виды деятельности, субъекты национальной платежной системы (далее - организации финансового рынка), осуществляющие сбор и обработку используемых для идентификации параметров биометрических персональных данных, должны обеспечивать:

1) информирование Банка России о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при обработке, включая сбор и хранение, параметров биометрических персональных данных (далее соответственно – инциденты безопасности, требования по защите информации), которые привели или могут привести к нарушению или попыткам нарушения целостности, конфиденциальности и (или) доступности защищаемой информации.

Организации, указанные в настоящем пункте, осуществляют информирование Банка России о выявленных инцидентах безопасности не позднее одного рабочего дня со дня их выявления;

2) ежегодное проведение оценки соответствия требований по защите информации с привлечением организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049; 2020, № 49, ст. 7943), и информирование Банка России о результатах такой оценки.

8. Организации, не относящиеся к организациям финансового рынка, осуществляющие сбор и обработку используемых для идентификации параметров биометрических персональных данных, должны обеспечивать:

1) информирование Минцифры России о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при обработке, включая сбор и хранение, параметров биометрических персональных данных (далее соответственно – инциденты безопасности, требования по защите информации), которые привели или могут привести к нарушению или попыткам нарушения целостности, конфиденциальности и (или) доступности защищаемой информации.

Организации, указанные в настоящем пункте, осуществляют информирование Минцифры России о выявленных инцидентах безопасности не позднее одного рабочего дня со дня их выявления;

2) ежегодное проведение оценки соответствия требований по защите информации с привлечением организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации

от 3 февраля 2012 г. № 79, и информирование Минцифры России о результатах такой оценки.

9. Обработка параметров биометрических персональных данных физического лица осуществляется после проведения идентификации физического лица в соответствии с требованиями, утвержденными в соответствии с пунктом 2 части 2 статьи 14.1 Федерального закона № 149-ФЗ, а также получения согласия на обработку персональных данных и биометрических персональных данных в соответствии с частью 5 статьи 14.1 Федерального закона № 149-ФЗ при сборе в единую биометрическую систему, а при сборе в иные информационные системы, обеспечивающие идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц – после получения согласия на обработку персональных и биометрических персональных данных в соответствии с требованиями законодательства Российской Федерации в области персональных данных.

В случае отзыва субъектом персональных данных в соответствии с частью 2 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2017, № 31, ст. 4772) (далее – Федеральный закон № 152-ФЗ) согласия на обработку персональных данных использование его параметров биометрических персональных данных в целях проведения идентификации и (или) аутентификации не осуществляется.

10. В процессе обработки параметров биометрических персональных данных в единой биометрической системе, параметров биометрических персональных данных в иных информационных системах, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, создаются биометрические образцы данных изображения лица (далее – БО изображения лица) и биометрические образцы данных голоса (далее – БО записи голоса) субъекта.

11. Создаваемые для проведения идентификации БО изображения лица должны соответствовать следующим требованиям:

цвета пикселей изображений фронтального типа должны быть представлены в 24-битовом цветовом пространстве RGB, в котором на каждый пиксель приходится по 8 битов на каждый компонент цвета: красный, зеленый и синий;

поворот головы должен быть не более 5° от фронтального положения;

наклон головы должен быть не более 5° от фронтального положения;

отклонение головы должно быть не более 8° от фронтального положения;

расстояние между центрами глаз должно составлять не менее 120 пикселей либо не менее 45 пикселей в соответствии с пунктом 12 порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, утвержденного настоящим приказом (далее – Порядок размещения и обновления);

изображение должно содержать полное изображение головы человека в анфас, включая левое и правое ухо (при их наличии), верхнюю точку лобной области головы и подбородок;

не допускается перекрытие волосами или посторонними предметами изображения лица по всей ширине от бровей до нижней губы;

на изображении должно присутствовать только одно лицо, наличие других лиц, фрагментов других лиц не допускается;

выражение лица должно быть нейтральным, рот закрыт, оба глаза открыты нормально для соответствующего субъекта (с учетом поведенческих факторов и (или) медицинских заболеваний);

лицо должно быть равномерно освещено, чтобы на изображении лица отсутствовали тени и блики;

не допускается использование ретуши и редактирования изображения;

допускается кадрирование изображения;

в случае фотографирования человека в очках не допускается наличие солнцезащитных очков и ярких световых артефактов или отражения вспышки от очков;

изображение лица должно быть сохранено в формате .jpeg или .png; код сжатия: JPEG (0 x 00), PNG (0 x 03);

фотографирование человека должно производиться с помощью средств автоматизации, позволяющих обеспечить расположение изображения головы в кадре в соответствии с требованиями настоящего приказа.

12. Создаваемые для проведения идентификации БО записи голоса должны соответствовать следующим требованиям:

отношение сигнал-шум для звука не менее 15 дБ;

глубина квантования не менее 16 бит;

частота дискретизации не менее 16 кГц;

запись голоса должна быть сохранена в формате RIFF (WAV);

код сжатия: PCM/uncompressed (0 x 0001);

количество каналов в записи голоса: 1 (монорежим) канал;

не допускается использовать шумоподавление;

на записи должен присутствовать голос одного человека;

произнесенное субъектом сообщение должно соответствовать последовательности букв и (или) цифр, сгенерированной программным обеспечением информационной системы органа или организации;

запись голоса должна содержать указанную последовательность полностью и не должна прерываться;

при осуществлении записи голоса эмоционально-психологическое состояние и состояние субъекта должно быть нормальным, не возбужденным, без явных признаков заболеваний, препятствующих произнесению сообщения, указанного в абзаце двенадцатом настоящего пункта, или способных нарушить тембр и (или) звучание голоса;

сообщение, указанное в абзаце одиннадцатом настоящего пункта, должно быть произнесено субъектом на русском языке.

Запрещено получение БО записи голоса путем перекодирования фонограмм, записанных с помощью технических средств телефонной сети общего пользования.

13. Проверка биометрических образцов, собранных уполномоченными сотрудниками органов и организаций, биометрических образцов, собранных уполномоченными сотрудниками организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, на соответствие требованиям, установленным пунктами 10, 11 настоящего порядка (далее – контроль качества), осуществляется в автоматизированном режиме с использованием программного обеспечения, предоставляемого оператором единой биометрической системы.

14. В случае если в процессе прохождения контроля качества установлено соответствие биометрических образцов требованиям, указанным в пунктах 10, 11 настоящего порядка, такие образцы, содержащие в том числе метку даты, времени и места, информацию о технических средствах, с использованием которых осуществлялся процесс сбора и обработки параметров биометрических персональных данных, и о их состоянии, а также информацию о способе сбора параметров биометрических персональных данных в единую биометрическую систему, передаются органами и организациями в единую биометрическую систему в автоматизированном режиме с использованием средств криптографической защиты информации, позволяющих обеспечить безопасность персональных данных от угроз, определенных для организаций финансового рынка в соответствии с частью 14 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», для иных органов и организаций – в соответствии с пунктом 4 части 13 указанной статьи, в том числе с использованием единой системы межведомственного электронного взаимодействия.

15. В единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, биометрические образцы проходят контроль качества с использованием программного обеспечения единой биометрической системы.

В случае если в процессе прохождения контроля качества, осуществляемого в соответствии с абзацем первым настоящего пункта, установлено несоответствие биометрических образцов требованиям, указанным в пунктах 10, 11 настоящего порядка, создание биометрического контрольного шаблона не осуществляется.

В случае если в процессе прохождения контроля качества, осуществляемого в соответствии с абзацем первым настоящего пункта, установлено несоответствие биометрических образцов требованиям, указанным в пунктах 10, 11 настоящего порядка, органы и организации, осуществляющие размещение в единой биометрической системе биометрических персональных данных субъекта, обязаны направить информацию об указанных событиях в единую биометрическую систему в автоматизированном режиме с использованием в том числе единой системы межведомственного электронного взаимодействия, а также принять организационно-технические меры по повышению качества сбора параметров биометрических персональных данных.

16. Хранение параметров биометрических персональных данных, размещенных в единой биометрической системе, осуществляется в соответствии с требованиями, установленными в соответствии со статьей 19 Федерального закона № 152-ФЗ и статьей 14.1 Федерального закона № 149-ФЗ, в течение не менее чем 50 лет со дня их размещения в указанной системе.

Хранение параметров биометрических персональных данных в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, собранных для проведения идентификации, не допускается.

Биометрические персональные данные, собранные в соответствии с настоящим Порядком, размещенные в единой биометрической системе или в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также обрабатываемые в указанных информационных системах, используются в целях идентификации и (или) аутентификации не более 5 лет с даты сбора, а в случаях, установленных в соответствии с пунктом 12 Порядка размещения и обновления, – не более 3 лет с даты сбора.

По истечении срока, указанного в абзаце третьем настоящего пункта, использование биометрических персональных данных, размещенных в единой биометрической системе или в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, в целях идентификации и (или) аутентификации не допускается.

17. При обработке, включая сбор и хранение, параметров биометрических персональных данных должны применяться средства защиты информации (в том числе средства криптографической защиты информации), обеспечивающие нейтрализацию актуальных угроз безопасности, определенных в соответствии с пунктами 4, 6 части 13 и частями 14, 14.1 статьи 14.1 Федерального закона № 149-ФЗ.

ПРИЛОЖЕНИЕ № 2
к приказу Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 10 сентября 2021 г. №930

ПОРЯДОК
размещения и обновления биометрических персональных данных
в единой биометрической системе и в иных информационных системах,
обеспечивающих идентификацию и (или) аутентификацию
с использованием биометрических персональных данных физических лиц

1. Размещение и обновление в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее – единая биометрическая система) сведений, определенных частью 8 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2021, № 11, ст. 1708) (далее – Федеральный закон № 149-ФЗ) осуществляются банками с универсальной лицензией и банками с базовой лицензией, соответствующими критериям, установленным абзацами вторым – четвертым пункта 5.7 статьи 7 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (Собрание законодательства Российской Федерации, 2001, № 33, ст. 3418; 2021, № 27, ст. 5183), государственными органами и иными организациями в случаях, определенных федеральными законами, с согласия физического лица и на безвозмездной основе.

Размещение и обновление в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, сведений, определенных частью 8 статьи 14.1 Федерального закона № 149-ФЗ, осуществляется организациями, в том числе организациями финансового рынка, владеющими указанными иными информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающими услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц (далее - организации, осуществляющие идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц), с согласия физического лица и на безвозмездной основе при соблюдении условий, установленных федеральными законами.

2. Размещение и обновление в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или)

аутентификацию с использованием биометрических персональных данных физических лиц, биометрических персональных данных осуществляются в соответствии с законодательством Российской Федерации в области персональных данных и настоящим Порядком.

3. Размещение и обновление биометрических персональных данных в единой биометрической системе осуществляется с использованием, в том числе единой системы межведомственного электронного взаимодействия.

4. Обновление сведений в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, осуществляется в соответствии с порядком обработки, включая сбор и хранение, параметров биометрических персональных данных, утверждаемым настоящим приказом (далее – Порядок обработки).

5. При размещении и обновлении сведений в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, кредитные организации, некредитные финансовые организации, которые осуществляют указанные в части первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 24, ст. 4210) виды деятельности, субъекты национальной платежной системы, осуществляющие сбор и обработку используемых для идентификации биометрических персональных, должны осуществлять информирование Банка России о выявленных инцидентах безопасности в соответствии с подпунктом 1 пункта 7 Порядка обработки.

При размещении и обновлении сведений в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, организации, не относящиеся к организациям финансового рынка, осуществляющие сбор и обработку используемых для идентификации параметров биометрических персональных данных, должны осуществлять информирование Минцифры России о выявленных инцидентах безопасности в соответствии с подпунктом 1 пункта 8 Порядка обработки.

6. Размещение и обновление сведений в единой биометрической системе осуществляется в соответствии с требованиями к фиксации действий в соответствии с пунктом 1 части 2 статьи 14.1 Федерального закона № 149-ФЗ.

7. Биометрические персональные данные, а также иная информация, указанная в пункте 13 Порядка обработки, размещаются и обновляются в единой биометрической системе уполномоченным сотрудником органа или организации и подписываются усиленной квалифицированной электронной подписью государственного органа или организации.

8. Размещение биометрических персональных данных физического лица в единой биометрической системе осуществляется, если физическое лицо прошло процедуру регистрации в единой системе идентификации и аутентификации в соответствии с Положением о федеральной государственной информационной

системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», утвержденным приказом Министерства связи и массовых коммуникаций Российской Федерации от 13 апреля 2012 г. № 107 (далее – Положение)¹.

Размещение биометрических персональных данных физического лица в единой биометрической системе осуществляется при условии, что личность физического лица установлена в соответствии с подпунктом «з» пункта 6.1 Положения.

9. В случае если физическое лицо не зарегистрировано в единой системе идентификации и аутентификации, уполномоченный сотрудник после проведения идентификации физического лица осуществляет с его согласия процедуру регистрации в единой системе идентификации и аутентификации в соответствии с Положением.

10. Если сведения, необходимые для регистрации физического лица в единой системе идентификации и аутентификации, внесены в указанную систему, но процесс регистрации в соответствии с пунктом 8 настоящего порядка не завершен, уполномоченное лицо перед сбором параметров биометрических персональных данных с согласия физического лица размещает или обновляет в электронной форме в единой системе идентификации и аутентификации сведения, необходимые для регистрации в ней, а также устанавливает личность соответствующего физического лица и вносит в единую систему идентификации и аутентификации сведения о способе установления его личности в соответствии с Положением.

11. При наличии у физического лица учетной записи в единой системе идентификации и аутентификации уполномоченный сотрудник осуществляет сбор биометрических персональных данных и размещение их в единой биометрической системе.

12. В случае если при размещении при личном присутствии и обработке указанными в абзаце втором пункта 1 настоящего порядка организациями биометрических персональных данных в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, собраны биометрические персональные данные, соответствующие видам, параметрам и порядку обработки биометрических персональных данных, установленных в соответствии с настоящим приказом, размещаемым в единой биометрической системе биометрическим персональным данным, такие собираемые указанными организациями биометрические персональные данные могут быть размещены в единой биометрической системе до истечения срока, указанного в подпункте 1 пункта 14 настоящего порядка, со дня их размещения в указанных иных информационных системах.

¹ Зарегистрирован Минюстом России 26.04.2012 г., регистрационный № 23952), с изменениями, внесенными приказами Минюста России от 31.08.2012 г. № 218 (зарегистрирован Минюстом России 27.09.2012 г., регистрационный № 25546), от 23.07.2015 г. № 278 (зарегистрирован Минюстом России 26.10.2015 г., регистрационный № 39470) и от 7.07.2016 г. № 307 (зарегистрирован Минюстом России 21.11.2016 г., регистрационный № 44379)

В случае если расстояние между центрами глаз биометрических персональных данных изображения лица, содержащихся в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, составляет менее допустимого значения, указанного в абзаце шестом пункта 11 Порядка обработки, но не менее 45 пикселей, такие собираемые указанными в абзаце втором пункта 1 настоящего порядка организациями биометрические персональные данные размещаются в единой биометрической системе до истечения срока, указанного в подпункте 1 пункта 14 настоящего порядка, со дня их размещения в указанных иных информационных системах, в целях использования для:

а) аутентификации на едином портале государственных и муниципальных услуг;

б) аутентификации в целях получения банковских услуг при личном посещении отделений банковских организаций, клиентами которых они являются.

Размещение биометрических персональных данных в единой биометрической системе в соответствии с настоящим пунктом осуществляется на безвозмездной основе при соблюдении условия, установленного пунктом 8 настоящего порядка, а также при соблюдении положений пунктов 3 и 7 настоящего порядка.

13. Размещенные в единой биометрической системе биометрические персональные данные физического лица используются в целях идентификации и (или) аутентификации физического лица, в случае завершения регистрации соответствующего физического лица в единой системе идентификации и аутентификации при условии, что личность физического лица удостоверена в соответствии с подпунктом «з» пункта 6.1 Положения.

14. Обновление биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, осуществляется физическим лицом добровольно в следующих случаях:

1) по истечении 5 лет со дня их размещения в указанных системах, а в случаях, установленных в соответствии с пунктом 12 настоящего порядка, – по истечении 3-х лет со дня их размещения в указанных системах;

2) по инициативе физического лица.

15. При размещении и обновлении биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, должны применяться средства защиты информации (в том числе средства криптографической защиты информации), обеспечивающие нейтрализацию актуальных угроз безопасности, определенных в соответствии с пунктами 4, 6 части 13 и частями 14, 14.1 статьи 14.1 Федерального закона № 149-ФЗ.

ПРИЛОЖЕНИЕ № 3
к приказу Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 10 сентября 2021 г. № 930

ТРЕБОВАНИЯ
к информационным технологиям и техническим средствам,
предназначенным для обработки биометрических персональных данных
в целях проведения идентификации

1. Требования к информационным технологиям и техническим средствам, предназначенным для обработки изображения лица в целях проведения идентификации:

а) для регистрации изображения лица необходимо использовать фото- или видеокамеру (далее – камера), эквивалентное фокусное расстояние которой должно составлять от 26,7 до 100 мм при расположении субъекта на расстоянии 0,3 – 1,0 м от камеры;

б) в целях обеспечения выполнения требований пункта 11 порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, определяемым федеральным органом исполнительной власти, осуществляющим регулирование в сфере идентификации физических лиц на основе биометрических персональных данных, утвержденного настоящим приказом (далее – Порядок обработки), используются камеры со следующими характеристиками:

разрешение получаемого изображения: не менее 1280 x 720 пикселей;

наличие режима автоматической корректировки баланса белого цвета;

в) используемые источники освещения должны создавать в области лица освещенность:

для фото-, видеокамер без автоматической коррекции освещенности – не менее 300 лк;

для фото-, видеокамер с автоматической коррекцией освещенности – не менее 100 лк.

2. Требования к информационным технологиям и техническим средствам, предназначенным для обработки данных голоса в целях проведения идентификации:

а) для регистрации записи голоса необходимо использовать микрофон со следующими характеристиками:

тип: конденсаторный, без автоматической регулировки усиления;

отсутствие шумоподавления;

диапазон частот: не уже чем от 100 до 10000 Гц;

б) в целях обеспечения выполнения требований пункта 12 Порядка обработки используются микрофоны со следующими характеристиками:

соотношение сигнал/шум: не менее 58 дБ;

чувствительность: не менее 30 дБ или не менее 60 дБ при отсутствии нелинейных искажений амплитудно-частотных характеристик микрофона в диапазоне от 100 до 5000 Гц, превышающих отклонение более чем на 7 дБ;

форма диаграммы направленности: суперкардиоида или гиперкардиоида.

3. Вероятность ложного совпадения предоставленных государственным органом, органом местного самоуправления, кредитной организацией, некредитной финансовой организацией, которые осуществляют указанные в части первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 24, ст. 4210) виды деятельности, субъектом национальной платежной системы (далее - организации финансового рынка), иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных изображения лица указанным биометрическим персональным данным физического лица, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных при сравнении один к одному, достаточная для проведения идентификации физического лица, должна составлять не более 0,0001.

Вероятность ложного совпадения предоставленных государственным органом, органом местного самоуправления, организацией финансового рынка, иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных голоса указанным биометрическим персональным данным физического лица, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных при сравнении один к одному, достаточная для проведения идентификации физического лица, должна составлять не более 0,1.

Вероятность ложноположительной биометрической идентификации предоставленных государственным органом, органом местного самоуправления, организацией финансового рынка, иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных изображения лица указанным биометрическим персональным данным физического лица, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных при сравнении один ко многим, достаточная для проведения идентификации физического лица, должна составлять не более 0,0001.

Вероятность ложноположительной биометрической идентификации предоставленных государственным органом, органом местного самоуправления, организацией финансового рынка, иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных голоса указанным биометрическим персональным данным физического лица, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных при сравнении один ко многим, достаточная для проведения идентификации физического лица, должна составлять не более 0,1.

Вероятность ошибки классификации предоставленных государственным органом, органом местного самоуправления, организацией финансового рынка, иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных при атаке на информационные системы, обеспечивающие идентификацию и (или) аутентификацию с использованием биометрических персональных данных, достаточная для проведения идентификации физического лица, должна составлять не более 0,01.

Проверка предоставляемых государственным органом, органом местного самоуправления, организацией финансового рынка, иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных на наличие атаки на биометрическое предъявление осуществляется в автоматизированном режиме с использованием соответствующего программного обеспечения, обеспечивающего мультиалгоритмическое обнаружение атак на биометрическое предъявление с использованием не менее двух однотипных алгоритмов обнаружения атаки на биометрическое предъявление.

Количество однотипных алгоритмов обнаружения атаки на биометрическое предъявление, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, в рамках каждой попытки идентификации должно быть не менее двух.

4. Организации финансового рынка при обработке, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации должны использовать информационные технологии и технические средства, которые соответствуют 2-му уровню защиты информации (стандартный), установленному национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденном приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. 882-ст (Москва, ФГУП «Стандартинформ», 2017).