ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации Банка России по нейтрализации организациями финансового рынка угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой

08.10.2024 № 18-МР

Глава 1. Общие положения

1.1. Настоящие Методические рекомендации разработаны в целях обеспечения единства подходов организаций финансового рынка, указанных в части 1 статьи 3 Федерального закона от 29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее соответственно – организации финансового рынка, Федеральный закон от 29 декабря 2022 года № 572-ФЗ), к нейтрализации угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой, перечень которых определен Указанием Банка России от 25 сентября 2023 года № 6540-У «О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, векторов

единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой»[1] (далее – угрозы безопасности биометрических персональных данных).

1.2. Организациям финансового рынка рекомендуется принимать меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных, на следующих технологических участках:

1.2.1. В процессе сбора биометрических персональных данных и их передачи в целях размещения или обновления биометрических персональных данных в единой биометрической системе:

на технологическом участке сбора биометрических персональных данных в головном офисе, филиалах или внутренних структурных подразделениях организаций финансового рынка, являющихся банками с универсальной лицензией или банками с базовой лицензией, указанными в пункте 5^6 статьи 7 Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – банки), с использованием стационарных средств вычислительной техники и банкоматов, а также работниками банков с использованием планшетов и при передаче собранных биометрических персональных данных между головным офисом, филиалами или внутренними структурными подразделениями банков, между планшетами и информационной инфраструктурой внутренних структурных подразделений банков (далее – сбор биометрических персональных данных);

на технологическом участке взаимодействия информационных систем банков с единой биометрической системой в целях размещения или обновления биометрических персональных данных в единой биометрической системе с использованием единой системы межведомственного электронного взаимодействия (далее – СМЭВ).

---

[1] Зарегистрировано Минюстом России 26 октября 2023 года, регистрационный № 75742.

1.2.2. В процессе обработки (за исключением сбора) биометрических персональных данных, при проверке и передаче информации о степени соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, содержащимся в единой биометрической системе (далее – информация о степени соответствия), при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой в целях идентификации физического лица в соответствии с частью 1 статьи 9 Федерального закона от 29 декабря 2022 года № 572-ФЗ (далее – удаленная (дистанционная) идентификация) и аутентификации физического лица в соответствии с частью 1 статьи 10 Федерального закона от 29 декабря 2022 года № 572-ФЗ (далее – удаленная (дистанционная) аутентификация):

на технологическом участке удаленной (дистанционной) идентификации или удаленной (дистанционной) аутентификации клиента – физического лица;

на технологическом участке проверки и передачи информации о степени соответствия при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой.

1.2.3. На технологическом участке взаимодействия информационных систем организаций финансового рынка с единой биометрической системой при передаче собранных биометрических персональных данных в случае, указанном в части 14 статьи 4 Федерального закона от 29 декабря 2022 года № 572-ФЗ, при получении векторов единой биометрической системы в соответствии с пунктом 2 части 2 статьи 8 Федерального закона от 29 декабря 2022 года № 572-ФЗ и при направлении оператору единой биометрической системы мотивированного запроса и получении информации в соответствии с пунктом 9 части 2 статьи 8, части 3 статьи 15 Федерального закона от 29 декабря 2022 года № 572-ФЗ.

1.2.4. На технологическом участке предоставления организациями финансового рынка в соответствии с частью 5 статьи 10 Федерального закона от 29 декабря 2022 года № 572-ФЗ в единую систему идентификации

и аутентификации сведений о физических лицах, содержащихся в информационных системах организаций финансового рынка, включая идентификаторы таких сведений, перед использованием единой биометрической системы для аутентификации.

1.3. Организациям финансового рынка рекомендуется обеспечивать защиту информации при использовании единой биометрической системы с применением средств криптографической защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (далее – СКЗИ), разработанных и эксплуатируемых в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 года № 66[1] (далее – Положение ПКЗ-2005), и эксплуатационной документацией на СКЗИ.

Глава 2. **Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке сбора биометрических персональных данных**

2.1. Банкам рекомендуется применять меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных, при сборе биометрических персональных данных физических лиц при личном присутствии клиента работниками банков:

в головном офисе, филиалах или внутренних структурных подразделениях банков с использованием стационарных средств вычислительной техники и банкоматов;

с использованием планшетов.

---

[1] Зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382, с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 года № 173 (зарегистрирован Минюстом России 25 мая 2010 года, регистрационный № 17350).

2.2. В целях нейтрализации угроз безопасности биометрических персональных данных на технологическом участке сбора биометрических персональных данных физических лиц банкам рекомендуется:

2.2.1. Размещать объекты информационной инфраструктуры, используемые на технологическом участке сбора биометрических персональных данных, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

2.2.2. Для объектов информационной инфраструктуры в пределах сегмента (группы сегментов) вычислительных сетей, в отношении которых применяются меры защиты информации, реализующие стандартный уровень (уровень 2) защиты информации, определенный национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным и введенным в действие приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст[1] (далее – ГОСТ Р 57580.1-2017), рекомендуется обеспечивать уровень соответствия не ниже четвертого в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденным и введенным в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст[2] (далее – ГОСТ Р 57580.2-2018).

2.2.3. Применять средства защиты информации, прошедшие сертификацию в системе сертификации ФСТЭК России, на соответствие требованиям по безопасности информации не ниже 5-го класса защиты.

2.2.4. Применять СКЗИ, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

---

[1] М., ФГУП «Стандартинформ», 2017.
[2] М., ФГУП «Стандартинформ», 2018.

2.2.5. Обеспечить информирование сотрудников, осуществляющих сбор биометрических персональных данных физических лиц (далее – уполномоченный сотрудник), о регистрации (протоколировании) информации об их действиях при сборе и обработке биометрических персональных данных физических лиц и о последствиях нарушения правил обработки персональных данных физических лиц в соответствии с законодательством Российской Федерации.

2.2.6. В целях реализации запретов на хранение используемых в целях идентификации и (или) аутентификации биометрических персональных данных, установленных пунктами 1 и 2 части 1 статьи 15 Федерального закона от 29 декабря 2022 года № 572-ФЗ, исключить возможность хранения биометрических персональных данных физических лиц на устройствах, предназначенных для сбора биометрических персональных данных, после размещения биометрических персональных данных физического лица в единой биометрической системе.

2.2.7. Обеспечить контроль физической безопасности устройств сбора биометрических персональных данных для ограничения несанкционированного физического доступа к содержимому устройства и предотвращения несанкционированного использования или модификации устройства (включая замену всего устройства) на всех этапах жизненного цикла устройства.

2.3. При сборе биометрических персональных данных физических лиц в головном офисе, филиалах или внутренних структурных подразделениях банков с использованием стационарных средств вычислительной техники и банкоматов, а также при передаче собранных биометрических персональных данных между головным офисом, филиалами или внутренними структурными подразделениями банков банкам рекомендуется:

обеспечивать целостность электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, путем их подписания усиленной квалифицированной электронной подписью (далее – УКЭП), реализуемой средствами электронной подписи класса не ниже КС3, предусмотренными пунктом 12 Состава и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10 июля 2014 года № 378[1] (далее – Состав и содержание организационных и технических мер), а также пунктом 15 Требований к средствам электронной подписи, утвержденных приказом ФСБ России от 27 декабря 2011 года № 796[2] (далее – Требования к средствам электронной подписи);

обеспечивать конфиденциальность электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, путем применения СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер.

2.4. При сборе биометрических персональных данных физических лиц работниками банков с использованием планшетов и при передаче собранных биометрических персональных данных между планшетами и информационной инфраструктурой внутренних структурных подразделений банков банкам рекомендуется:

обеспечивать целостность электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, путем их подписания УКЭП, реализуемой средствами электронной подписи класса не ниже КС1, предусмотренными пунктом 10 Состава и содержания организационных и технических мер, а также пунктом 13 Требований к средствам электронной подписи, в случае применения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации не ниже 4-го уровня доверия в соответствии с Требованиями по безопасности информации,

---

[1] Зарегистрирован Минюстом России 18 августа 2014 года, регистрационный № 33620.

[2] Зарегистрирован Минюстом России 9 февраля 2012 года регистрационный № 23191, с изменениями, внесенными приказом ФСБ России от 4 декабря 2020 года № 555 (зарегистрирован Минюстом России 30 декабря 2020 года, регистрационный № 61972), приказом ФСБ России от 13 апреля 2021 года № 142 (зарегистрирован Минюстом России 20 мая 2021 года, регистрационный № 63528), приказом ФСБ России от 13 апреля 2022 года № 179 (зарегистрирован Минюстом России 11 мая 2022 года, регистрационный № 68446).

устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76[1] (далее – Требования по безопасности информации, устанавливающие уровни доверия), или путем их подписания УКЭП, реализуемой средствами электронной подписи класса не ниже КС2, предусмотренными пунктом 11 Состава и содержания организационных и технических мер, в иных случаях, а также пунктом 14 Требований к средствам электронной подписи;

обеспечивать конфиденциальность электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, путем применения СКЗИ класса не ниже КС1, предусмотренных пунктом 10 Состава и содержания организационных и технических мер, в случае применения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации не ниже 4-го уровня доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия, или путем применения СКЗИ класса не ниже КС2, предусмотренных пунктом 11 Состава и содержания организационных и технических мер, в иных случаях.

2.5. Банкам рекомендуется обеспечить регистрацию действий, связанных с:

назначением и изменением прав доступа уполномоченных сотрудников к объектам информационной инфраструктуры банка, используемым для сбора биометрических персональных данных физических лиц;

выполнением процедур идентификации, аутентификации, авторизации уполномоченных сотрудников при доступе к объектам информационной инфраструктуры банка, используемым для сбора биометрических персональных данных физических лиц;

---

[1] Зарегистрирован Минюстом России 11 сентября 2020 года, регистрационный № 59772, с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 года № 68 (зарегистрирован Минюстом России 20 июля 2022 года, регистрационный № 69318).

формированием электронного сообщения, содержащего собранные биометрические персональные данные физических лиц, для передачи;

подписанием электронных сообщений, содержащих собранные биометрические персональные данные физических лиц;

передачей электронных сообщений, содержащих собранные биометрические персональные данные физических лиц в целях размещения или обновления биометрических персональных данных в единой биометрической системе;

уничтожением (удалением) биометрических персональных данных физических лиц на объектах информационной инфраструктуры банка.

2.6. Банкам рекомендуется обеспечить хранение информации о регистрируемых действиях, указанных в пункте 2.5 настоящих Методических рекомендаций, не менее 5 лет.

Глава 3. Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке взаимодействия информационных систем банков с единой биометрической системой в целях размещения или обновления биометрических персональных данных в единой биометрической системе с использованием СМЭВ

3.1. Банкам рекомендуется размещать объекты информационной инфраструктуры банков, используемые на технологическом участке взаимодействия информационных систем банков с единой биометрической системой в целях размещения или обновления биометрических персональных данных в единой биометрической системе с использованием СМЭВ, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

3.2. Банкам для объектов информационной инфраструктуры в пределах сегмента (группы сегментов) вычислительных сетей, предусмотренных пунктом 3.1 настоящих Методических рекомендаций, для которых применяются меры защиты информации, реализующие стандартный уровень (уровень 2) защиты информации, определенный

ГОСТ Р 57580.1-2017, рекомендуется обеспечивать уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018.

3.3. Банкам рекомендуется применять средства защиты информации, прошедшие сертификацию в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, не ниже 5-го класса защиты.

3.4. Банкам, являющимся системно значимыми кредитными организациями, рекомендуется применять средства защиты информации, прошедшие сертификацию в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, не ниже 4-го класса защиты.

3.5. Банкам рекомендуется обеспечивать целостность электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке взаимодействия информационных систем банков с единой биометрической системой в целях размещения или обновления биометрических персональных данных в единой биометрической системе с использованием СМЭВ путем их подписания УКЭП, реализуемыми средствами электронной подписи класса не ниже КВ2, предусмотренными пунктом 13 Состава и содержания организационных и технических мер, а также пунктом 17 Требований к средствам электронной подписи, любым из следующих способов:

с использованием собственного решения;

с использованием типового решения по информационной безопасности;

с использованием решения поставщика услуг (облачного решения).

3.5.1. В случае использования собственного решения рекомендуется обеспечить:

получение квалифицированного сертификата ключа проверки электронной подписи банка, созданного в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» удостоверяющим центром, с применением средств удостоверяющего центра класса не ниже КВ2, предусмотренных пунктом 13 Состава и содержания организационных и технических мер, а также пунктом 13 Требований

к средствам удостоверяющего центра, утвержденных приказом ФСБ России от 27 декабря 2011 года № 796;

встраивание программно-аппаратного модуля криптографической защиты (HSM), прошедшего оценку соответствия требованиям по безопасности информации к СКЗИ по классу не ниже КВ, предусмотренным пунктом 13 Состава и содержания организационных и технических мер, и средствам электронной подписи по классу не ниже КВ2, предусмотренным пунктом 17 Требований к средствам электронной подписи, в подсистему обработки биометрических персональных данных физических лиц в соответствии с требованиями, изложенными в эксплуатационной документации на программно-аппаратный модуль криптографической защиты (HSM), в соответствии с пунктом 35 Положения ПКЗ-2005;

создание в соответствии с пунктом 3.6 настоящей главы и использование доверенной среды функционирования информационной системы, взаимодействующей (формирующей вызовы) с программно-аппаратным модулем криптографической защиты (HSM), прошедшего оценку соответствия требованиям по безопасности информации к СКЗИ по классу не ниже КВ, предусмотренного пунктом 13 Состава и содержания организационных и технических мер, в процессе подписания электронных сообщений, содержащих биометрические персональные данные физических лиц, УКЭП, реализуемой средствами электронной подписи класса не ниже КВ2, предусмотренными пунктом 13 Состава и содержания организационных и технических мер, а также пунктом 17 Требований к средствам электронной подписи.

3.5.2. В случае использования согласованного с ФСБ России типового решения по информационной безопасности рекомендуется обеспечить:

взаимодействие между информационными системами банка и типовым решением по информационной безопасности по прикладным программным интерфейсам (API) в соответствии с документацией на типовое решение;

эксплуатацию типового решения по информационной безопасности в соответствии с документацией на него.

3.5.3. В случае использования решения поставщика услуг (облачного решения) рекомендуется обеспечить:

применение решения поставщика услуг (облачного решения), имеющего положительное заключение ФСБ России о соответствии решения поставщика услуг (облачного решения) требованиям по безопасности информации и включающего комплект эксплуатационной документации, согласованной ФСБ России;

криптографическую аутентификацию процессов при осуществлении доступа к информационной инфраструктуре решения поставщика услуг (облачного решения) с применением СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер;

криптографическую аутентификацию уполномоченных сотрудников банка, а также криптографическое подтверждение достоверности и целостности электронного сообщения, содержащего биометрические персональные данные физического лица, с применением средств электронной подписи класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер, а также пунктом 15 Требований к средствам электронной подписи;

использование решений поставщика услуг (облачного решения) в соответствии с эксплуатационной документацией, согласованной ФСБ России.

3.6. В случае применения банками решения, указанного в подпункте 3.5.1 пункта 3.5 настоящих Методических рекомендаций, банкам рекомендуется создавать доверенную среду функционирования информационной системы с использованием:

операционной системы, имеющей подтверждение соответствия Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19 августа 2016 года № 119[1], либо требованиям к средствам защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну,

[1] Зарегистрирован Минюстом России 19 сентября 2016 года, регистрационный № 43691.

от несанкционированного доступа, установленным ФСБ России, по классу АК3;

антивирусных средств, сертифицированных ФСТЭК России на соответствие требованиям к антивирусным средствам не менее чем 4-го класса защиты согласно Требованиям к средствам антивирусной защиты, утвержденным приказом ФСТЭК России от 20 марта 2012 года № 28[1];

средств межсетевого экранирования, сертифицированного ФСТЭК России на соответствие требованиям к устройствам типа межсетевой экран не менее чем 4-го класса защиты, с применением средства защиты информации от воздействий вредоносного кода, предназначенных для применения на серверах информационных систем (тип «А»), согласно Требованиям к межсетевым экранам, утвержденным приказом ФСТЭК России от 9 февраля 2016 года № 9[2], а также средств защиты от компьютерных атак, сертифицированных ФСТЭК России на соответствие требованиям к программным, программно-аппаратным или аппаратным средствам типа «системы обнаружения вторжений» не менее чем 4-го класса защищенности согласно Требованиям к системам обнаружения вторжений, утвержденным приказом ФСТЭК России от 6 декабря 2011 года № 638[3], либо средств, совмещающих в себе межсетевой экран и систему обнаружения вторжения (NGFW) не ниже 4-го класса защищенности, сертифицированных согласно Требованиям по безопасности информации к многофункциональным межсетевым экранам уровня сети, утвержденным приказом ФСТЭК России от 7 марта 2023 года № 44[4];

аппаратно-программных модулей доверенной загрузки уровня платы расширения, сертифицированных ФСТЭК России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ не ниже 4-го класса защиты согласно Требованиям к средствам доверенной загрузки, утвержденным приказом ФСТЭК России от 27 сентября 2013 года № 119[5], в информационной системе, взаимодействующей

---

[1] Зарегистрирован Минюстом России 3 мая 2012 года, регистрационный № 24045.
[2] Зарегистрирован Минюстом России 25 марта 2016 года, регистрационный № 41564.
[3] Зарегистрирован Минюстом России 1 февраля 2012 года, регистрационный № 23088.
[4] Зарегистрирован Минюстом России 14 июня 2023 года, регистрационный № 73832.
[5] Зарегистрирован Минюстом России 16 декабря 2013 года, регистрационный № 30604.

(формирующей вызовы) с программно-аппаратным модулем криптографической защиты (HSM);

прикладного программного обеспечения, применяемого в доверенной среде, которое сертифицировано в системе сертификации ФСТЭК России в соответствии с порядком, установленным Положением о сертификации средств защиты информации, утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации», или прошло оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД 4, предусмотренного пунктом 7.6 раздела 7 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст[1] (далее – ГОСТ Р ИСО/МЭК 15408-3-2013);

результатов тематических исследований по оценке влияния, проводимых в соответствии с пунктом 35 Положения ПКЗ-2005, подсистемы обработки биометрических персональных данных физических лиц, совместно с которой предполагается штатное функционирование программно-аппаратного модуля криптографической защиты (HSM), на выполнение предъявленных к программно-аппаратному модулю криптографической защиты (HSM) требований по безопасности информации к СКЗИ по классу не ниже КВ, предусмотренного пунктом 13 Состава и содержания организационных и технических мер.

Доверенная среда функционирования информационной системы может быть создана с использованием специализированного программно-аппаратного средства (адаптера), обеспечивающего информационно-технологическое взаимодействие объектов информационной инфраструктуры банка с программно-аппаратным модулем криптографической защиты (HSM) и соответствующего описанию, приведенному в настоящем пункте.

---

[1] М., ФГУП «Стандартинформ», 2014.

3.7. В случае применения банками решения, указанного в подпункте 3.5.1 пункта 3.5 настоящих Методических рекомендаций, рекомендуется обеспечивать целостность биометрических персональных данных путем сверки электронных сообщений, содержащих биометрические персональные данные, входящих в сегмент вычислительной сети банков, в котором осуществляется их обработка, с исходящими из указанного сегмента вычислительной сети электронными сообщениями, содержащими биометрические персональные данные, в информационной инфраструктуре банка до их передачи в единую биометрическую систему с использованием СМЭВ.

3.8. В целях обеспечения конфиденциальности передаваемых электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке взаимодействия информационных систем банков с единой биометрической системой в целях размещения или обновления биометрических персональных данных в единой биометрической системе с использованием СМЭВ банкам рекомендуется применять СКЗИ класса не ниже КС3, предусмотренные пунктом 12 Состава и содержания организационных и технических мер.

3.9. Банкам рекомендуется обеспечивать направление электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, в единую биометрическую систему с использованием СМЭВ[1] с учетом рекомендаций по работе со СМЭВ, размещенных в информационно-телекоммуникационной сети «Интернет» по адресу https://info.gosuslugi.ru/new/smev.

3.10. Банкам рекомендуется обеспечить регистрацию действий, связанных с:

---

[1] Обращаем внимание на необходимость соблюдения Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия, утвержденных приказом Министерства связи и массовых коммуникаций Российской Федерации от 23 июня 2015 года № 210 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия» (зарегистрирован Минюстом России 25 августа 2015 года № 38668, с изменениями, внесенными приказом Министерства связи и массовых коммуникаций Российской Федерации от 22 февраля 2017 года № 71 (зарегистрирован Минюстом России 2 июня 2017 года, регистрационный № 46934).

выполнением процедур сверки электронных сообщений, содержащих биометрические персональные данные, входящих в сегмент вычислительной сети банков, в котором осуществляется их обработка, с исходящими из указанного сегмента вычислительной сети электронными сообщениями, содержащими биометрические персональные данные;

подписанием УКЭП банка, реализуемой средствами электронной подписи класса не ниже КВ2, предусмотренными пунктом 13 Состава и содержания организационных и технических мер, а также пунктом 17 Требований к средствам электронной подписи, электронных сообщений, содержащих биометрические персональные данные физических лиц;

передачей электронных сообщений, содержащих биометрические персональные данные физических лиц, при направлении в единую биометрическую систему.

3.11. Банкам рекомендуется обеспечить хранение информации о регистрируемых действиях, указанных в пункте 3.10 настоящих Методических рекомендаций, не менее 5 лет.

Глава 4. Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке удаленной (дистанционной) идентификации или удаленной (дистанционной) аутентификации клиента – физического лица

4.1. Организациям финансового рынка рекомендуется обеспечить использование прикладного программного обеспечения автоматизированных систем и приложений, распространяемых организациями финансового рынка клиентам, для совершения действий в целях осуществления удаленной (дистанционной) идентификации или удаленной (дистанционной) аутентификации с использованием биометрических персональных данных, которые сертифицированы в системе сертификации ФСТЭК России в соответствии с порядком, установленным Положением о сертификации средств защиты информации, утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации», или прошли оценку соответствия по требованиям

к ОУД не ниже чем ОУД 4, предусмотренного пунктом 7.6 раздела 7 ГОСТ Р ИСО/МЭК 15408-3-2013.

4.2. Организациям финансового рынка рекомендуется разработать памятку для клиента, описывающую особенности работы программного обеспечения для удаленной (дистанционной) идентификации или удаленной (дистанционной) аутентификации физического лица с использованием биометрических персональных данных на устройстве клиента и возможные действия клиента в случае компрометации ключей аутентификации. В памятку рекомендуется включить основные положения эксплуатационной документации используемых для взаимодействия программных и (или) программно-аппаратных средств на устройстве клиента.

4.3. Для обеспечения целостности и конфиденциальности передаваемой информации при проведении удаленной (дистанционной) идентификации или удаленной (дистанционной) аутентификации при взаимодействии с использованием устройства физического лица, а также оконечных устройств информационных систем, обеспечивающих функционирование контрольно-пропускных пунктов, организациям финансового рынка рекомендуется на стороне клиента применять СКЗИ не ниже класса КС1, предусмотренные пунктом 10 Состава и содержания организационных и технических мер.

4.4. Для обеспечения целостности и конфиденциальности передаваемой информации при осуществлении удаленной (дистанционной) аутентификации с использованием мобильных (переносных) устройств вычислительной техники (в том числе планшетов и электронных терминалов), принадлежащих организациям финансового рынка, организациям финансового рынка рекомендуется:

применять СКЗИ класса не ниже КС1, предусмотренные пунктом 10 Состава и содержания организационных и технических мер, в случае применения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации не ниже 4-го уровня доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия;

применять СКЗИ класса не ниже КС2, предусмотренные пунктом 11 Состава и содержания организационных и технических мер, в иных случаях.

4.5. Для обеспечения целостности и конфиденциальности передаваемой информации при осуществлении удаленной (дистанционной) аутентификации с использованием стационарных средств вычислительной техники и банкоматов организациям финансового рынка рекомендуется применять СКЗИ класса не ниже КС2, предусмотренные пунктом 11 Состава и содержания организационных и технических мер.

Глава 5. Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке проверки и передачи информации о степени соответствия при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой

5.1. Организациям финансового рынка рекомендуется обеспечивать целостность и конфиденциальность электронных сообщений при передаче информации о степени соответствия в организациях финансового рынка путем применения СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер.

5.2. Организациям финансового рынка рекомендуется обеспечивать контроль целостности электронных сообщений при обработке информации о степени соответствия в целях удаленной (дистанционной) идентификации физического лица путем проверки УКЭП, которой подписано электронное сообщение, реализуемой средствами электронной подписи класса не ниже КВ2, предусмотренными пунктом 13 Состава и содержания организационных и технических мер, а также пунктом 17 Требований к средствам электронной подписи.

5.3. Организациям финансового рынка рекомендуется обеспечивать контроль целостности электронных сообщений при обработке информации о степени соответствия в целях удаленной (дистанционной) аутентификации

физического лица путем проверки УКЭП, которой подписано электронное сообщение, реализуемой средствами электронной подписи класса не ниже КС3, предусмотренными пунктом 12 Состава и содержания организационных и технических мер, а также пунктом 15 Требований к средствам электронной подписи.

5.4. Организациям финансового рынка рекомендуется обеспечивать функционирование объектов информационной инфраструктуры для выполнения действий, указанных в пунктах 5.1−5.3 настоящих Методических рекомендаций, с применением протокола на базе OpenID Connect, предусмотренного Методическими рекомендациями по использованию единой системы идентификации и аутентификации, размещенных в информационно-телекоммуникационной сети «Интернет» по адресу https://digital.gov.ru/ru/documents/ (далее – протокол на базе OpenID Connect), безопасная реализация которого в составе подсистемы обработки биометрических персональных данных подтверждена заключением ФСБ России о соответствии требованиям по безопасности информации.

Глава 6. Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке взаимодействия информационных систем организаций финансового рынка с единой биометрической системой при передаче собранных биометрических персональных данных в случае, указанном в части 14 статьи 4 Федерального закона от 29 декабря 2022 года № 572-ФЗ, при получении векторов единой биометрической системы в соответствии с пунктом 2 части 2 статьи 8 Федерального закона от 29 декабря 2022 года № 572-ФЗ и при направлении оператору единой биометрической системы мотивированного запроса и получении информации в соответствии с пунктом 9 части 2 статьи 8, частью 3 статьи 15 Федерального закона от 29 декабря 2022 года № 572-ФЗ

6.1. Организациям финансового рынка рекомендуется обеспечивать целостность электронных сообщений при взаимодействии информационных систем с единой биометрической системой при передаче собранных биометрических персональных данных между осуществлявшими обработку биометрических персональных данных информационными системами

организаций финансового рынка и единой биометрической системой в случае, указанном в части 14 статьи 4 Федерального закона от 29 декабря 2022 года № 572-ФЗ, путем их подписания УКЭП, реализуемой средствами электронной подписи класса не ниже КВ2, предусмотренными пунктом 13 Состава и содержания организационных и технических мер, а также пунктом 17 Требований к средствам электронной подписи.

6.2. Организациям финансового рынка рекомендуется обеспечивать контроль целостности электронных сообщений при получении организациями финансового рынка в соответствии с пунктом 2 части 2 статьи 8 Федерального закона от 29 декабря 2022 года № 572-ФЗ векторов единой биометрической системы в целях аутентификации физического лица путем проверки УКЭП, которой подписано электронное сообщение, реализуемой средствами электронной подписи класса не ниже КВ2, предусмотренными пунктом 13 Состава и содержания организационных и технических мер, а также пунктом 17 Требований к средствам электронной подписи.

6.3. Организациям финансового рынка рекомендуется обеспечивать конфиденциальность электронных сообщений при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой при передаче собранных биометрических персональных данных между осуществлявшими обработку биометрических персональных данных информационными системами организаций финансового рынка и единой биометрической системой в случае, указанном в части 14 статьи 4 Федерального закона от 29 декабря 2022 года № 572-ФЗ, а также при получении организациями финансового рынка в соответствии с пунктом 2 части 2 статьи 8 Федерального закона от 29 декабря 2022 года № 572-ФЗ векторов единой биометрической системы в целях аутентификации физического лица путем применения СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер.

6.4. Организациям финансового рынка рекомендуется обеспечивать целостность и конфиденциальность электронных сообщений при направлении оператору единой биометрической системы в соответствии с пунктом 9

части 2 статьи 8, частью 3 статьи 15 Федерального закона от 29 декабря 2022 года № 572-ФЗ мотивированного запроса о предоставлении информации о результатах проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой биометрической системе, основанного на обращении субъекта персональных данных, предполагающего неправомерную обработку его биометрических персональных данных при проведении аутентификации и (или) оспаривающего результаты проведения аутентификации (далее – информация о результате проверки соответствия), а также при получении от оператора единой биометрической системы в соответствии с пунктом 9 части 2 статьи 8, частью 3 статьи 15 Федерального закона от 29 декабря 2022 года № 572-ФЗ информации о результате проверки соответствия путем применения СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер.

6.5. Организациям финансового рынка рекомендуется при взаимодействии с единой биометрической системой использовать СМЭВ с учетом рекомендаций, предусмотренных пунктом 3.9 настоящих Методических рекомендаций.

6.6. Организациям финансового рынка рекомендуется обеспечить регистрацию действий по передаче электронных сообщений, содержащих биометрические персональные данные физических лиц, при направлении в единую биометрическую систему.

6.7. Организациям финансового рынка рекомендуется обеспечить хранение информации о регистрируемых действиях, указанных в пункте 6.6 настоящих Методических рекомендаций, не менее 5 лет.

Глава 7. **Меры, направленные на нейтрализацию угроз безопасности биометрических персональных данных на технологическом участке предоставления организациями финансового рынка в соответствии с частью 5 статьи 10 Федерального закона от 29 декабря 2022 года № 572-ФЗ в единую систему идентификации и аутентификации сведений о физических лицах, содержащихся в информационных системах организаций финансового рынка, включая идентификаторы таких сведений,**

перед использованием единой биометрической системы для аутентификации

7.1. Организациям финансового рынка рекомендуется обеспечивать целостность и конфиденциальность электронных сообщений при предоставлении в соответствии с частью 5 статьи 10 Федерального закона от 29 декабря 2022 года № 572-ФЗ в единую систему идентификации и аутентификации сведений о физических лицах, содержащихся в информационных системах организаций финансового рынка, включая идентификаторы таких сведений, перед использованием единой биометрической системы для аутентификации путем применения СКЗИ класса не ниже КС3, предусмотренных пунктом 12 Состава и содержания организационных и технических мер, и протокола на базе OpenID Connect, безопасная реализация которого в составе подсистемы обработки биометрических персональных данных подтверждена заключением ФСБ России о соответствии требованиям по безопасности информации, любым из следующих способов:

с использованием собственного решения;

с использованием типового решения по информационной безопасности;

с использованием решения поставщика услуг (облачного решения).

7.2. Организациям финансового рынка рекомендуется учитывать Методические рекомендации по работе с единой системой идентификации и аутентификации, размещенные в информационно-телекоммуникационной сети «Интернет» по адресу https://digital.gov.ru/ru/documents/, и Методические рекомендации по работе с единой биометрической системой, размещенные в информационно-телекоммуникационной сети «Интернет» по адресу https://ebs.ru/business/.

7.3. Организациям финансового рынка рекомендуется обеспечить регистрацию действий по:

взаимодействию с единой системой идентификации и аутентификации и единой биометрической системой, реализуемым в том числе с применением протокола на базе OpenID Connect;

проверке сведений о физических лицах, содержащихся в информационных системах организаций финансового рынка, включая идентификаторы таких сведений.

7.4. Организациям финансового рынка рекомендуется обеспечить хранение информации о регистрируемых действиях, указанных в пункте 7.3 настоящих Методических рекомендаций, не менее 5 лет.

Глава 8. **Информирование Банка России об инцидентах при использовании единой биометрической системы**

8.1. Организациям финансового рынка рекомендуется осуществлять регистрацию инцидентов защиты информации и инцидентов операционной надежности при обработке, включая сбор и передачу, биометрических персональных данных в целях удаленной (дистанционной) идентификации и (или) удаленной (дистанционной) аутентификации, а также при осуществлении удаленной (дистанционной) идентификации или удаленной (дистанционной) аутентификации (далее – инциденты защиты информации и инциденты операционной надежности).

8.2. Организациям финансового рынка рекомендуется информировать Банк России о выявленных инцидентах защиты информации и инцидентах операционной надежности, включенных в перечень типов инцидентов, определенный стандартом Банка России СТО БР БФБО-1.5-2023 «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности», который принят и введен в действие приказом Банка России от 8 февраля 2023 года № ОД-215 и размещен на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» по адресу http://www.cbr.ru/information_security/ (далее – стандарт Банка России СТО БР БФБО-1.5-2023), а также о причинах возникновения инцидента

защиты информации или инцидента операционной надежности, принятых мерах и проведенных мероприятиях по реагированию на инцидент защиты информации или инцидент операционной надежности.

8.3. Организациям финансового рынка в целях информирования Банка России о выявленных инцидентах защиты информации и инцидентах операционной надежности рекомендуется руководствоваться порядком, а также сроками и формами взаимодействия организаций финансового рынка с Банком России, которые определены стандартом Банка России СТО БР БФБО-1.5-2023.

Глава 9. **Заключительные положения**

9.1. С даты издания настоящих Методических рекомендаций отменяются Методические рекомендации Банка России по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, от 14 февраля 2019 года № 4-МР.

9.2. Настоящие Методические рекомендации подлежат опубликованию в «Вестнике Банка России» и размещению на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Заместитель
Председателя Банка России Г.А. Зубарев