ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации 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

14.02.2019 № 4-МР

Глава 1. Общие положения

1.1. В целях нейтрализации 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, определенных Указанием Банка России № 4859-У, Публичного акционерного общества «Ростелеком» № 01/01/782-18 от 9 июля 2018 года «О перечне 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 в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в Единой биометрической системе» (далее - Указание Банка России № 4859-У) Банк России доводит до сведения кредитных организаций (далее – банки) следующие рекомендации по обеспечению информационной безопасности.

1.2. Настоящие рекомендации по обеспечению информационной безопасности банкам рекомендуется применять при использовании ЕБС на следующих технологических участках.

1.2.1. В процессе сбора биометрических персональных данных физических лиц для целей передачи в ЕБС:

на технологическом участке сбора биометрических персональных данных физических лиц;

на технологическом участке передачи собранных биометрических персональных данных физических лиц между структурными подразделениями банка;

на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью передачи в ЕБС с использованием Единой системы межведомственного электронного взаимодействия (далее – СМЭВ);

на технологическом участке передачи биометрических персональных данных физических лиц в ЕБС с использованием СМЭВ.

1.2.2. В процессе обработки запросов физических лиц и их персональных данных, а также информации о степени соответствия в целях проведения идентификации физического лица без его личного присутствия с использованием биометрических персональных данных (далее – удаленная идентификация):

на технологическом участке удаленной идентификации клиента – физического лица;

на технологическом участке проверки результатов удаленной идентификации клиента – физического лица в Единой системе идентификации и аутентификации (далее – ЕСИА) и ЕБС;

на технологическом участке взаимодействия банка с ЕСИА и ЕБС.

1.3. Банкам рекомендуется обеспечивать защиту информации при использовании ЕБС с применением средств криптографической защиты информации, имеющих подтверждение соответствия требованиям,

установленным федеральным органом исполнительной власти 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 Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66, зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года № 6382, 25 мая 2010 года № 17350 (далее – Положение ПКЗ-2005), и технической документацией на СКЗИ.

Глава 2. Обеспечение информационной безопасности в процессе сбора биометрических персональных данных физических лиц для целей передачи в ЕБС

2.1. В целях обеспечения информационной безопасности на технологическом участке сбора биометрических персональных данных физических лиц банкам рекомендуется следующее.

2.1.1. Рекомендуется размещать объекты информационной инфраструктуры, используемые на технологическом участке сбора, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

2.1.2. Для объектов информационной инфраструктуры в пределах сегмента (группы сегментов) вычислительных сетей рекомендуется применять 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 приказом Росстандарта от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП

«Стандартинформ», 2017) (далее – ГОСТ Р 57580.1-2017).

2.1.3. Рекомендуется применять средства защиты информации, сертифицированные по системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, не ниже 5 класса.

К указанным средствам защиты информации относятся:

средства (системы) защиты информации от несанкционированного доступа (далее – СЗИ от НСД);

средства защиты информации от воздействия вредоносного кода (далее – СЗИ от ВВК);

средства межсетевого экранирования;

средства (системы) обнаружения вторжений (компьютерных атак).

2.1.4. Обращаем внимание на необходимость обеспечить реализацию мер, указанных в пунктах 7, 8 Приложения № 1 к Приказу Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25 июня 2018 года № 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», зарегистрированному Министерством юстиции Российской Федерации 4 июля 2018 года № 51532.

В целях усиления информационной безопасности на технологическом участке сбора биометрических персональных данных физических лиц в дополнение к указанным мерам рекомендуется обеспечить для каждого сотрудника, осуществляющего сбор параметров биометрических персональных данных физических лиц (далее – уполномоченный сотрудник), возможность использования персонального квалифицированного сертификата ключа проверки электронной подписи

для подписания электронных сообщений, содержащих биометрические персональные данные, в целях установления факта подписания электронных сообщений этим сотрудником.

2.1.5. Рекомендуется обеспечить информирование уполномоченных сотрудников о регистрации (протоколировании) информации о его 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.

2.1.6. Рекомендуется исключить возможность хранения биометрических персональных данных физических лиц на автоматизированном рабочем месте, предназначенном для сбора и обработки биометрических персональных данных, после завершения регистрации биометрических персональных данных физического лица в ЕБС.

2.1.7. Рекомендуется осуществлять контроль целостности и подтверждение подлинности 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 КС2 в случае применения средств защиты информации от несанкционированного доступа не ниже 4-ого класса защищенности, сертифицированных по системе сертификации ФСТЭК России, или путем их подписания УКЭП, реализуемой средствами электронной подписи класса не ниже КС3 в иных случаях.

2.1.8. Рекомендуется обеспечить регистрацию действий, связанных с:

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

доступом указанных сотрудников к объектам информационной инфраструктуры банка, используемым для сбора биометрических персональных данных физических лиц;

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

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

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

2.2. В целях обеспечения информационной безопасности на технологическом участке передачи биометрических персональных данных физических лиц между структурными подразделениями банка банкам рекомендуется следующее.

2.2.1. Рекомендуется[1] обеспечивать конфиденциальность передаваемой информации, содержащей биометрические персональные данные физических лиц, на технологическом участке передачи собранных биометрических персональных данных физических лиц между структурными подразделениями банка с применением СКЗИ класса не ниже КС2 в случае применения средств защиты информации от несанкционированного доступа не ниже 4-ого класса защищенности, сертифицированных по системе сертификации ФСТЭК России, или с применением СКЗИ класса не ниже КС3 в иных случаях.

2.2.2. Рекомендуется обеспечить регистрацию действий, связанных с передачей электронных сообщений, содержащих собранные биометрические персональные данные.

---

[1] Во исполнение требований пункта 1.2 Указания Банка России № 4859-У, пунктов 11 и 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 № 378 (далее - приказ ФСБ России № 378).

2.3. В целях обеспечения информационной безопасности на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью передачи в ЕБС с использованием СМЭВ банкам рекомендуется следующее.

2.3.1. Рекомендуется размещать объекты информационной инфраструктуры, используемые на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью передачи в ЕБС с использованием СМЭВ, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

2.3.2. Банкам для объектов информационной инфраструктуры в пределах сегмента (группы сегментов) вычислительных сетей, предусмотренных подпунктом 2.3.1 настоящего пункта, рекомендуется применять меры защиты информации, реализующие стандартный уровень (уровень 2) защиты информации, определенный ГОСТ Р 57580.1-2017.

2.3.3. Банкам – системно значимым кредитным организациям для объектов информационной инфраструктуры в пределах сегмента (группы сегментов) вычислительных сетей, предусмотренных подпунктом 2.3.1 настоящего пункта, рекомендуется применять меры защиты информации, реализующие усиленный уровень (уровень 1) защиты информации, определенный ГОСТ Р 57580.1-2017.

2.3.4. Банкам – системно значимым кредитным организациям для объектов информационной инфраструктуры в пределах сегмента (группы сегментов) вычислительных сетей, предусмотренных подпунктом 2.3.1 настоящего пункта, рекомендуется реализовывать мероприятия по обеспечению непрерывности и восстановления деятельности, исключающие приостановление обработки, а также передачи биометрических персональных данных физических лиц на продолжительный (более двух часов) период времени.

2.3.5. Рекомендуется применять средства защиты информации, сертифицированные по системе сертификации ФСТЭК России на

соответствие требованиям по безопасности информации, не ниже 5 класса.

К указанным средствам защиты информации относятся:

СЗИ от НСД;

СЗИ от ВВК;

средства межсетевого экранирования;

средства (системы) обнаружения вторжений (компьютерных атак).

2.3.6. Банкам – системно значимым кредитным организациям рекомендуется применять средства защиты информации, сертифицированные по системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, не ниже 4 класса.

К указанным средствам защиты информации относятся:

СЗИ от НСД;

СЗИ от ВВК;

средства межсетевого экранирования;

средства (системы) обнаружения вторжений (компьютерных атак).

2.3.7. Рекомендуется[2] осуществлять контроль целостности и подтверждение подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью передачи в ЕБС с использованием СМЭВ, путем их подписания УКЭП банка, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2).

2.3.8. Рекомендуется обеспечивать функционирование объектов информационной инфраструктуры для выполнения действий, указанных в подпункте 2.3.7 настоящего пункта, любым из следующих способов:

с использованием собственного решения;

с использованием типового решения;

---

[2] Во исполнение требований пункта 1.3.1 Указания Банка России № 4859-У, пункта 13 приложения к приказу ФСБ России № 378.

с использованием решения поставщика услуг (облачного решения), при наличии такого решения на рынке информационных технологий.

2.3.8.1. В случае функционирования объектов информационной инфраструктуры с использованием собственного решения для выполнения действий, указанных в подпункте 2.3.7 настоящего пункта, рекомендуется обеспечить:

получение квалифицированного сертификата ключа проверки электронной подписи банка, созданного аккредитованным Минкомсвязью России удостоверяющим центром (ФГБУ НИИ «Восход») с применением средств удостоверяющего центра класса не ниже КВ2;

встраивание программно-аппаратного модуля криптографической защиты (HSM), сертифицированного в качестве СКЗИ по классу не ниже КВ (средства электронной подписи по классу не ниже КВ2), в подсистему обработки биометрических персональных данных физических лиц в соответствии с требованиями, изложенными в эксплуатационной документации на программно-аппаратный модуль криптографической защиты (HSM), собственными силами, при наличии соответствующей лицензии ФСБ России, либо силами сторонних организаций, имеющих соответствующую лицензию ФСБ России;

создание и использование доверенной среды функционирования информационной системы, взаимодействующей (формирующей вызовы) с программно-аппаратным модулем криптографической защиты (HSM), сертифицированным по классу не ниже КВ, в процессе подписания электронных сообщений, содержащих биометрические персональные данные физических лиц, УКЭП, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2), которая обеспечивается следующим:

исполнением на операционной системе, которая соответствует либо требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели

защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 3-ему классу защищенности и «Защита от несанкционированного доступа к информации. Часть I. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 2-ому уровню контроля, либо требованиям ФСБ России по защите конфиденциальной информации от несанкционированного доступа в автоматизированных информационных системах по классу АК3;

применением средств межсетевого экранирования, сертифицированных ФСТЭК России на соответствие требованиям к устройствам типа межсетевой экран не менее чем 3-его класса защищённости, применением СЗИ от ВВК, предназначенных для применения на серверах информационных систем (тип «Б») и сертифицированных ФСТЭК России на соответствие требованиям к антивирусным средствам не менее чем 2-ого класса защищенности;

применением 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 3-его класса защищенности;

применением в информационной системе, взаимодействующей (формирующей вызовы) с программно-аппаратным модулем криптографической защиты (HSM), аппаратно-программных модулей доверенной загрузки (АПМДЗ) уровня платы расширения, сертифицированных ФСТЭК России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ по 2-ому классу защиты;

использованием прикладного программного обеспечения, применяемого в доверенной среде, прошедшего проверку на отсутствие недекларированных возможностей и соответствующего 4-ому уровню

контроля отсутствия недекларированных возможностей согласно Руководящему документу «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», утвержденному приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114, или сертифицированного в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Росстандарта от 8 ноября 2013 года № 1340-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014) (далее – ГОСТ Р ИСО/МЭК 15408-3-2013);

проведением тематических исследований по оценке влияния подсистемы обработки биометрических персональных данных физических лиц, совместно с которой предполагается штатное функционирование программно-аппаратного модуля криптографической защиты (HSM), на выполнение предъявленных к HSM требований по классу КВ, с привлечением аккредитованной ФСБ России специализированной организации в соответствии с пунктом 35 Положения ПКЗ-2005;

разработкой эксплуатационной документации на объекты информационной инфраструктуры и эксплуатацией в соответствии с

указанной документацией.

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.

2.3.8.2. В случае функционирования объектов информационной инфраструктуры с использованием типового решения для выполнения действий, указанных в подпункте 2.3.7 настоящего пункта, рекомендуется обеспечить:

применение типового решения, разработанного на основе системного проекта, согласованного с ФСБ России, имеющего положительное заключение ФСБ России о соответствии типового решения требованиям по безопасности информации и включающего комплект разрешительной документации, утвержденный и (или) согласованный ФСБ России;

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

эксплуатацию в соответствии с документацией на типовое решение.

2.3.8.3. В случае функционирования объектов информационной инфраструктуры с использованием поставщика услуг (облачного решения) для выполнения действий, указанных в подпункте 2.3.7 настоящего пункта, рекомендуется обеспечить:

применение решения поставщика услуг (облачного решения), разработанного на основе системного проекта, согласованного с ФСБ России, имеющего положительное заключение ФСБ России о соответствии решения поставщика услуг (облачного решения) требованиям по безопасности информации и включающего комплект разрешительной

документации, утвержденный и (или) согласованный ФСБ России;

криптографическую аутентификацию банка при осуществлении доступа к информационной инфраструктуре решения поставщика услуг (облачного решения) с применением СКЗИ класса не ниже КС3;

криптографическую аутентификацию уполномоченных сотрудников банка, а также криптографическое подтверждение подлинности и целостности электронного сообщения, содержащего биометрические персональные данные физического лица, с применением средств электронной подписи класса не ниже КС2;

эксплуатацию в соответствии с документацией на решение поставщика услуг (облачное решение).

2.3.9. В случае применения решения, указанного в подпункте 2.3.8.1 настоящего пункта, рекомендуется обеспечивать целостность биометрических персональных данных, путем сверки входящих электронных сообщений, содержащих биометрические персональные данные, с исходящими электронными сообщениями, содержащими биометрические персональные данные, в информационной инфраструктуре банка до их передачи в ЕБС с использованием СМЭВ.

2.3.10. Банкам рекомендуется обеспечить регистрацию действий, связанных с:

выполнением процедур сверки информации, содержащейся во входящих электронных сообщениях, с информацией, содержащейся в исходящих электронных сообщениях, указанных в подпункте 2.3.9 настоящего пункта;

подписанием УКЭП банка электронных сообщений, содержащих биометрические персональные данные физических лиц.

2.4. В целях обеспечения информационной безопасности на технологическом участке передачи биометрических персональных данных физических лиц в ЕБС с использованием СМЭВ банкам рекомендуется следующее.

2.4.1. Рекомендуется[3] обеспечивать конфиденциальность передаваемой информации, содержащей биометрические персональные данные физических лиц, на технологическом участке передачи биометрических персональных данных физических лиц в ЕБС с использованием СМЭВ, с применением СКЗИ класса не ниже КС3.

2.4.2. Банкам рекомендуется обеспечивать направление электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, в ЕБС с использованием СМЭВ в соответствии с требованиями, указанными в приказе 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», а также с учетом Методических рекомендаций по работе с Единой системой межведомственного электронного взаимодействия (размещены по адресу https://smev3.gosuslugi.ru/portal/ в разделе «Технологические стандарты и рекомендации») и Регламентов и инструкций для подключения к СМЭВ (размещены по адресу https://smev3.gosuslugi.ru/portal/ в разделе «Регламенты, инструкции, шаблоны документов»).

2.4.3. Банкам рекомендуется обеспечить регистрацию действий, связанных с передачей электронных сообщений, содержащих собранные биометрических персональных данных физических лиц, при направлении в ЕБС.

Глава 3. Обеспечение информационной безопасности в процессе обработки запросов физических лиц и их персональных данных, а

[3] Во исполнение требований пункта 1.3.2 Указания Банка России № 4859-У, пункта 12 приложения к приказу ФСБ России № 378.

также информации о степени соответствия в целях проведения удаленной идентификации физического лица

3.1. В целях обеспечения информационной безопасности на технологическом участке удаленной идентификации клиента – физического лица банкам рекомендуется следующее.

3.1.1. Рекомендуется обеспечить использование прикладного программного обеспечения автоматизированных систем и приложений, распространяемых банками клиентам, для совершения действий в целях осуществления удаленной идентификации с использованием биометрических персональных данных, прошедшего проверку на отсутствие недекларированных возможностей и соответствующего 4-ому уровню контроля отсутствия недекларированных возможностей согласно Руководящему документу «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», введенному в действие приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114, или сертифицированных в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации или в отношении которых проведен анализ уязвимостей по требованиям к ОУД не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013.

3.1.2. Банкам рекомендуется разработать памятку для клиента, описывающую особенности работы программного обеспечения для удаленной идентификации физического лица с использованием биометрических персональных данных на мобильном устройстве клиента и описание возможных действий клиента в случае компрометации ключей

аутентификации.

3.1.3. Для обеспечения конфиденциальности передаваемой информации при взаимодействии с клиентом рекомендуется[4] применять СКЗИ класса не ниже КС1 на стороне клиента и рекомендуется применять СКЗИ класса не ниже КС3 на стороне банка.

3.1.4. Для осуществления контроля целостности и подтверждения подлинности электронных сообщений, содержащих результат идентификации физического лица (степени соответствия), на технологическом участке удаленной идентификации клиента – физического лица рекомендуется:

осуществлять обработку электронных сообщений, получаемых от ЕБС, содержащих результат идентификации физического лица (степени соответствия), с применением протокола на базе OpenID Connect, безопасная реализация которого в составе подсистемы обработки биометрических персональных данных подтверждена положительным заключением ФСБ России о соответствии требованиям по безопасности информации, с использованием СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2);

организовать работу по оценке влияния прикладного программного обеспечения и приложений, распространяемых банками клиентам для совершения действий в целях осуществления удаленной идентификации физического лица с использованием биометрических персональных данных, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к СКЗИ требований по классу не ниже КС1, в соответствии с пунктом 35 Положения ПКЗ-2005.

3.2. В целях обеспечения информационной безопасности на технологическом участке проверки результатов удаленной идентификации клиента – физического лица в ЕСИА и ЕБС банкам рекомендуется

[4] Во исполнение требований пункта 1.1 Указания Банка России № 4859-У, пункта 10 приложения к приказу ФСБ России № 378.

следующее.

3.2.1. Рекомендуется[5] осуществлять контроль целостности и подтверждения подлинности электронных сообщений, содержащих результаты идентификации физического лица (степени соответствия), путем их подписания УКЭП банка, реализуемой СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2).

3.2.2. Банкам рекомендуется обеспечивать функционирование объектов информационной инфраструктуры для выполнения действий, указанных в подпункте 3.2.1 настоящего пункта любым из способов, указанных в пункте 2.3.8 главы 2 настоящих методических рекомендаций, с применением протокола на базе OpenID Connect, безопасная реализация которого в составе подсистемы обработки биометрических персональных данных подтверждена положительным заключением ФСБ России о соответствии требованиям по безопасности информации.

3.2.3. Банкам рекомендуется обеспечить регистрацию действий связанных с:

процессом взаимодействия с ЕСИА и ЕБС, реализуемого с применением протокола на базе OpenID Connect;

процессом проверки результатов удаленной идентификации клиента на основании информации о степени соответствия.

3.3. В целях обеспечения информационной безопасности на технологическом участке взаимодействия банка с ЕСИА и ЕБС банкам рекомендуется следующее.

3.3.1. Рекомендуется[6] обеспечивать конфиденциальность получаемой из ЕСИА и ЕБС информации, содержащей результаты идентификации физического лица (степени соответствия) на технологическом участке взаимодействиия банка с ЕСИА и ЕБС, с применением СКЗИ класса не ниже

---

[5] Во исполнение требований пункта 1.4 Указания Банка России № 4859-У, пункта 13 приложения к приказу ФСБ России № 378.

[6] Во исполнение требований пункта 1.5.2 Указания Банка России № 4859-У, пункта 12 приложения к приказу ФСБ России № 378.

КСЗ;

3.3.2. Банкам рекомендуется учитывать Методические рекомендации по работе с ЕСИА (размещены по адресу http://minsvyaz.ru/ru/documents/) и Методические рекомендации по работе с ЕБС (размещены по адресу https://bio.rt.ru/business/).

Глава 4. Информирование Банка России об инцидентах при использовании ЕБС

4.1. Банкам рекомендуется обеспечивать регистрацию инцидентов, связанных с нарушениями требований к обеспечению защиты информации при обработке, включая сбор, а также передаче биометрических персональных данных в целях удаленной идентификации.

4.2. Банкам рекомендуется информировать Банк России о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при обработке, включая сбор, а также передаче биометрических персональных данных в целях удаленной идентификации.

4.2.1. Рекомендуется направлять в Банк России сведения о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при обработке, включая сбор, а также передаче биометрических персональных данных в целях удаленной идентификации с использованием технической инфраструктуры (автоматизированной системы) Банка России.

4.2.2. Банкам рекомендуется направлять информацию о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при обработке, включая сбор, а также передаче биометрических персональных данных в целях удаленной идентификации, по формам предоставления, размещенным на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

4.3. Информирование Банка России о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при обработке, включая сбор, а также передаче биометрических персональных данных в целях удаленной идентификации рекомендуется осуществлять в максимально короткие сроки, по возможности, не превышающие одного рабочего дня с момента выявления инцидента.

Глава 5. Заключительные положения

Настоящие Методические рекомендации подлежат официальному опубликованию.

Заместитель
Председателя Банка России Д.Г. Скобелкин