ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«30» января 2025 г. № 851-П

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
г. Москва
Регистрационный № 81462
от "6" марта 2025.

Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента

На основании статьи 57^4 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» настоящее Положение устанавливает обязательные для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента.

1. Требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента (далее – требования к обеспечению защиты информации) применяются для обеспечения защиты информации, подготавливаемой, обрабатываемой и хранимой в автоматизированных системах, входящих в состав объектов информационной инфраструктуры и используемых для осуществления банковских операций, связанных

с осуществлением перевода денежных средств (далее соответственно – защищаемая информация, банковская операция):

информации, в том числе составляющей банковскую тайну, содержащейся в документах, составленных при осуществлении банковских операций в электронном виде (далее – электронные сообщения), формируемых работниками кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы (далее соответственно – работники, филиалы иностранных банков), и (или) клиентами кредитных организаций, филиалов иностранных банков (далее – клиенты);

информации, необходимой для авторизации клиентов при совершении действий в целях осуществления банковских операций и удостоверения права клиентов распоряжаться денежными средствами;

информации об осуществленных банковских операциях;

информации, связанной с приемом к исполнению и исполнением распоряжений пользователя платформы цифрового рубля;

ключевой информации средств криптографической защиты информации (далее – СКЗИ), в том числе средств электронной подписи, используемой при осуществлении банковских операций (далее – криптографические ключи).

В случае если защищаемая информация содержит персональные данные, кредитные организации, филиалы иностранных банков должны применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

2. Требования к обеспечению защиты информации включают в себя:

требования к обеспечению защиты информации, применяемые в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечиваются кредитной

организацией, филиалом иностранного банка для осуществления банковских операций (далее – объекты информационной инфраструктуры);

требования к обеспечению защиты информации, применяемые в отношении прикладного программного обеспечения автоматизированных систем и приложений;

требования к обеспечению защиты информации, применяемые в отношении технологии обработки защищаемой информации;

иные требования к обеспечению защиты информации в соответствии с пунктами 6–13 настоящего Положения.

Кредитные организации, филиалы иностранных банков должны осуществлять планирование применения, применение, контроль применения и совершенствование применения мер, направленных на реализацию требований к обеспечению защиты информации, установленных настоящим пунктом.

3. Кредитные организации, филиалы иностранных банков должны выполнять следующие требования к обеспечению защиты информации, применяемые в отношении объектов информационной инфраструктуры:

3.1. Кредитные организации, филиалы иностранных банков должны применять меры защиты информации, посредством выполнения которых обеспечивается реализация следующих уровней защиты информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения защищаемой информации в целях осуществления банковских операций, предусмотренных пунктом 6.7 раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»[1] (далее – ГОСТ Р 57580.1-2017):

системно значимые кредитные организации, кредитные организации,

[1] Утвержден и введен в действие 1 января 2018 года приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст (М., ФГУП «Стандартинформ», 2017).

выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг, – усиленный уровень защиты информации;

кредитные организации, не относящиеся к кредитным организациям, указанным в абзаце втором настоящего подпункта, – стандартный уровень защиты информации;

филиалы иностранных банков – минимальный уровень защиты информации;

филиалы иностранных банков – стандартный уровень защиты информации.

Кредитные организации, указанные в абзаце третьем настоящего подпункта, ставшие кредитными организациями, указанными в абзаце втором настоящего подпункта, не позднее восемнадцати месяцев после того, как стали кредитными организациями, указанными в абзаце втором настоящего подпункта, должны применять меры защиты информации, посредством выполнения которых обеспечивается реализация усиленного уровня защиты информации.

Кредитные организации, филиалы иностранных банков, совмещающие деятельность с деятельностью некредитной финансовой организации, оператора услуг информационного обмена, оператора услуг платежной инфраструктуры, оператора электронных платформ и формирующие в отношении объектов информационной инфраструктуры один контур безопасности в соответствии с пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, должны применять меры защиты информации, посредством выполнения которых обеспечивается реализация наиболее высокого уровня защиты информации, установленного пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, из предусмотренных настоящим пунктом и нормативными актами Банка России, устанавливающими на основании статьи 76^{4-1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – Федеральный закон «О Центральном банке

Российской Федерации (Банке России)») и части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – Федеральный закон «О национальной платежной системе») требования к обеспечению защиты информации для некредитных финансовых организаций, операторов услуг информационного обмена, операторов услуг платежной инфраструктуры, операторов электронных платформ.

3.2. Кредитные организации, филиалы иностранных банков должны проводить ежегодное тестирование на предмет наличия возможностей проникновения в информационную инфраструктуру и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

4. Кредитные организации, филиалы иностранных банков должны выполнять следующие требования к обеспечению защиты информации, связанной с осуществлением перевода денежных средств, применяемые в отношении прикладного программного обеспечения автоматизированных систем и приложений:

4.1. Кредитные организации, филиалы иностранных банков должны использовать для осуществления банковских операций прошедшие сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю в соответствии с порядком, установленным постановлением Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации» (далее – сертификация), или прошедшие оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД4, 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»[2] (далее – оценка соответствия прикладного программного

[2] Утвержден и введен в действие 1 сентября 2014 года приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст (М., ФГУП «Стандартинформ», 2014).

обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения), и обрабатывающие защищаемую информацию:

прикладное программное обеспечение автоматизированных систем и приложений, распространяемых клиентам для совершения действий в целях осуществления банковских операций;

программное обеспечение, эксплуатируемое на участках, используемых для приема электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (далее соответственно – отдельное программное обеспечение, сеть «Интернет»).

В отношении прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения, не указанных в абзацах втором и третьем настоящего подпункта, кредитные организации, филиалы иностранных банков должны самостоятельно определять необходимость проведения сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

4.2. По решению кредитной организации, филиала иностранного банка оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения проводится самостоятельно или с привлечением организации, имеющей лицензию на осуществление деятельности по технической защите конфиденциальной информации для проведения 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 года № 79 (далее – проверяющая организация).

4.3. Системно значимые кредитные организации, кредитные организации, значимые на рынке платежных услуг, в случае принятия ими решения

о необходимости проведения сертификации прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения должны обеспечить сертификацию прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения не ниже 4 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76[3].

Кредитные организации, не указанные в абзаце первом настоящего подпункта, филиалы иностранных банков в случае принятия решения о необходимости проведения сертификации прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения должны обеспечить сертификацию прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения не ниже 5 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76.

Кредитные организации, указанные в абзаце втором настоящего подпункта, ставшие кредитными организациями, указанными в абзаце первом настоящего подпункта, не позднее восемнадцати месяцев после того, как стали кредитными организациями, указанными в абзаце первом настоящего подпункта, должны обеспечить сертификацию прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения не ниже 4 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76.

4.4. Кредитные организации, филиалы иностранных банков, которые используют для осуществления банковских операций прошедшие оценку соответствия прикладное программное обеспечение автоматизированных

[3] 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).

систем и приложений, а также отдельное программное обеспечение при внесении изменений в исходный текст указанных прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения, реализующий технологию обработки защищаемой информации в соответствии с подпунктом 5.2 пункта 5 настоящего Положения, должны проводить оценку соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

5. Кредитные организации, филиалы иностранных банков должны выполнять следующие требования к обеспечению защиты информации, применяемые в отношении технологии обработки защищаемой информации:

5.1. Кредитные организации, филиалы иностранных банков должны обеспечить целостность электронных сообщений.

В целях обеспечения целостности электронных сообщений кредитные организации, филиалы иностранных банков должны обеспечивать реализацию мер по использованию любого вида усиленной электронной подписи, предусмотренной частью 1 статьи 5 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон «Об электронной подписи»), или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

При использовании усиленной неквалифицированной электронной подписи в целях обеспечения целостности электронных сообщений кредитные организации, филиалы иностранных банков должны обеспечить использование усиленной неквалифицированной электронной подписи, созданной с использованием средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, при осуществлении регулирования в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности» (далее –

требования, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности).

При осуществлении банковских операций с использованием мобильной версии приложения кредитные организации, являющиеся участниками платформы цифрового рубля, в целях обеспечения целостности электронных сообщений должны обеспечить применение СКЗИ, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, посредством использования которых реализуются двухсторонняя аутентификация, шифрование и имитозащита информации на прикладном уровне и (или) на уровне представления данных в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 государственного стандарта ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»[4] (далее – ГОСТ Р ИСО/МЭК 7498-1-99), в соответствии с требованиями нормативного акта Банка России, принятого на основании статьи 82^{10} Федерального закона «О Центральном банке Российской Федерации (Банке России)», пункта 7 части 1, части 3 статьи 30^{7} Федерального закона «О национальной платежной системе».

5.2. Кредитные организации, филиалы иностранных банков должны осуществлять регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации, указанной в абзацах втором – пятом пункта 1 настоящего Положения, при совершении следующих действий (далее – технологические участки):

идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций, в том числе идентификация клиентов при создании сертификатов ключей проверки

[4] Принят постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78 и введен в действие 1 января 2000 года (М., ИПК «Издательство стандартов», 1999).

электронных подписей и выдаче таких сертификатов клиентам в соответствии с требованиями пункта 1 части 1 статьи 13 Федерального закона «Об электронной подписи» в целях осуществления операций с цифровыми рублями;

формирование (подготовка), передача и прием электронных сообщений;

удостоверение права клиентов распоряжаться денежными средствами;

осуществление банковской операции, учет результатов ее осуществления;

хранение электронных сообщений и информации об осуществленных банковских операциях.

5.2.1. Технология обработки защищаемой информации, применяемая на всех технологических участках, указанных в подпункте 5.2 настоящего пункта, должна обеспечивать целостность и достоверность защищаемой информации.

Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце втором подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать идентификацию устройств клиентов при осуществлении банковских операций с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций, филиалов иностранных банков.

В случае если банковская операция осуществляется с использованием мобильной версии приложения, кредитные организации, филиалы иностранных банков должны проверить использование клиентом – физическим лицом абонентского номера подвижной радиотелефонной связи в случае его использования во взаимоотношениях с кредитной организацией, филиалом иностранного банка и использовать полученные сведения при анализе характера, параметров и объема совершаемых их клиентами операций (осуществляемой клиентами деятельности).

В случае если банковская операция осуществляется с использованием мобильной версии приложения, кредитные организации, филиалы иностранных банков должны контролировать изменение идентификационного

модуля, определенного в соответствии с подпунктом 3^2 статьи 2 Федерального закона от 7 июля 2003 года № 126-ФЗ «О связи», используемого в устройстве клиента, идентифицированном в соответствии с абзацем вторым настоящего подпункта (далее – идентификационный модуль устройства клиента).

В случае выявления факта изменения идентификационного модуля устройства клиента кредитные организации, филиалы иностранных банков не вправе осуществлять аутентификацию и авторизацию клиента с использованием абонентского номера подвижной радиотелефонной связи клиента или с использованием информационных систем третьих лиц, обеспечивающих аутентификацию и авторизацию физических лиц посредством указанного абонентского номера подвижной радиотелефонной связи, до момента подтверждения принадлежности клиенту абонентского номера подвижной радиотелефонной связи способом, не связанным с использованием абонентского номера подвижной радиотелефонной связи клиента, или с использованием информационных систем третьих лиц, обеспечивающих аутентификацию и авторизацию физических лиц посредством указанного абонентского номера подвижной радиотелефонной связи.

Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце третьем подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать:

двойной контроль посредством осуществления проверки правильности формирования (подготовки) электронных сообщений;

входной контроль посредством осуществления проверки правильности заполнения полей электронного сообщения и прав владельца электронной подписи;

контроль дублирования электронного сообщения (в случае если проведение такой процедуры дополнительно установлено кредитной организацией в соответствии пунктом 2.2 Положения Банка России от 29 июня 2021 года № 762-П «О правилах осуществления перевода

денежных средств»[5]);

структурный контроль электронных сообщений;

защиту при передаче по каналам связи защищаемой информации.

Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце четвертом подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать:

подписание клиентом электронных сообщений способом, указанным в подпункте 5.1 настоящего пункта;

получение от клиента подтверждения совершаемой банковской операции.

Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце пятом подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать:

проверку соответствия (сверку) выходных электронных сообщений с соответствующими входными электронными сообщениями;

проверку соответствия (сверку) результатов осуществления банковских операций с информацией, содержащейся в электронных сообщениях;

направление клиентам уведомлений об осуществлении банковских операций в случае, когда такое уведомление предусмотрено законодательством Российской Федерации или договором.

Кредитные организации, филиалы иностранных банков должны реализовывать механизмы подтверждения использования клиентом адреса электронной почты в случае его использования во взаимоотношениях с кредитной организацией, филиалом иностранного банка, на который кредитной организацией, филиалом иностранного банка направляются уведомления о совершаемых банковских операциях, справки (выписки) по совершенным банковским операциям.

В случае использования единой системы идентификации и

---

[5] Зарегистрировано Минюстом России 25 августа 2021 года, регистрационный № 64765, с изменениями, внесенными Указаниями Банка России от 25 марта 2022 года № 6104-У (зарегистрировано Минюстом России 25 апреля 2022 года, регистрационный № 68320), от 3 августа 2023 года № 6497-У (зарегистрировано Минюстом России 10 августа 2023 года, регистрационный № 74717).

аутентификации, определенной в соответствии с пунктом 5 статьи 2 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 – единая система идентификации и аутентификации), кредитные организации, филиалы иностранных банков должны соблюдать требования к обеспечению защиты информации в соответствии с Техническими требованиями к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия, утвержденными приказом Министерства связи и массовых коммуникаций Российской Федерации от 23 июня 2015 года № 210 [6], а также требования технической и эксплуатационной документации по подключению к единой системе идентификации и аутентификации.

5.2.2. Кредитные организации, филиалы иностранных банков должны регистрировать результаты выполнения действий, связанных с осуществлением доступа к защищаемой информации, на всех технологических участках, указанных в подпункте 5.2 настоящего пункта, включая регистрацию действий работников, а также регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения.

5.2.3. Регистрации подлежат данные о действиях работников, выполняемых с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) осуществления банковской операции;

присвоенный работнику идентификатор, позволяющий установить

---

[6] Зарегистрирован Минюстом России 25 августа 2015 года, регистрационный № 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).

работника в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат осуществления банковской операции (успешная или неуспешная);

идентификационная информация, используемая для адресации устройства, с использованием и в отношении которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (адрес компьютера и (или) коммуникационного устройства (маршрутизатора) на сетевом уровне).

5.2.4. Регистрации подлежат данные о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) совершения действий клиентом в целях осуществления банковской операции;

присвоенный клиенту идентификатор, позволяющий установить клиента в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат совершения клиентом действия в целях осуществления банковской операции (успешная или неуспешная);

идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (адрес компьютера и (или) коммуникационного устройства (маршрутизатора) на сетевом уровне, международный идентификатор абонента (индивидуальный номер абонента клиента – физического лица), международный идентификатор пользовательского оборудования (оконечного оборудования) клиента – физического лица, абонентский номер подвижной радиотелефонной связи и (или) иной идентификатор устройства).

Регистрации дополнительно подлежат данные о действиях клиентов, выполняемых с использованием автоматизированных систем, программного

обеспечения на технологическом участке, указанном в абзаце втором подпункта 5.2 настоящего пункта:

дата (день, месяц, год) и время (часы, минуты, секунды) начала соединения и окончания соединения сессии на транспортном уровне в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 ГОСТ Р ИСО/МЭК 7498-1-99, при авторизации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций;

идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (адрес на сетевом уровне и адрес на транспортном уровне (порт) компьютера и (или) коммуникационного устройства (маршрутизатора), предусмотренные разделом 11 государственного стандарта Российской Федерации ГОСТ Р ИСО 7498-3-97 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 3. Присвоение имен и адресация»[7] (далее – ГОСТ Р ИСО 7498-3-97);

идентификационная информация, используемая для адресации автоматизированной системы, программного обеспечения, к которым осуществлен доступ с целью осуществления банковских операций (адрес на сетевом уровне и адрес на транспортном уровне (порт) автоматизированной системы, программного обеспечения, предусмотренные разделом 11 ГОСТ Р ИСО 7498-3-97);

географическое местоположение устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (при наличии).

---

[7] Принят и введен в действие с 1 июля 1998 года постановлением Комитета Российской Федерации по стандартизации, метрологии и сертификации от 19 августа 1997 года № 286 (М., ИПК «Издательство стандартов», 1997).

5.2.5. Кредитные организации, филиалы иностранных банков должны хранить информацию, указанную в абзацах втором, четвертом пункта 1, подпунктах 5.2.3 и 5.2.4 настоящего пункта, абзацах четвертом и пятом пункта 12 настоящего Положения, а также обеспечивать ее целостность и доступность не менее пяти лет начиная с даты ее формирования (поступления).

5.2.6. При выполнении клиентами действий с использованием автоматизированных систем, программного обеспечения на технологических участках, предусмотренных абзацами вторым, четвертым подпункта 5.2 настоящего пункта, кредитные организации, филиалы иностранных банков должны убедиться в том, что действия в целях осуществления банковской операции совершаются тем клиентом – физическим лицом либо тем представителем клиента, которые были идентифицированы в соответствии с требованиями Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

5.3. Кредитные организации, филиалы иностранных банков должны обеспечить подтверждение составления электронных сообщений уполномоченным на это лицом.

Кредитные организации, филиалы иностранных банков в целях подтверждения составления электронных сообщений уполномоченным на это лицом должны:

обеспечить использование электронной подписи в соответствии с Федеральным законом «Об электронной подписи»;

осуществлять признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, в соответствии со статьей 6 Федерального закона «Об электронной подписи».

При использовании усиленной неквалифицированной электронной подписи в целях подтверждения составления электронных сообщений уполномоченным на это лицом кредитные организации, филиалы иностранных банков должны обеспечить использование усиленной неквалифицированной электронной подписи, созданной с использованием

средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

В целях обеспечения целостности электронных сообщений кредитные организации, филиалы иностранных банков должны обеспечивать реализацию мер по использованию любого вида усиленной электронной подписи, предусмотренной частью 1 статьи 5 Федерального закона «Об электронной подписи»), или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

6. Обеспечение защиты информации с помощью СКЗИ при осуществлении банковских операций осуществляется в соответствии с Федеральным законом «Об электронной подписи», Федеральным законом «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», 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 [8] (далее – Положение ПКЗ-2005), приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении 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» [9] и технической документацией на СКЗИ.

В случае наличия в технической документации на СКЗИ требований к оценке влияния аппаратных, программно-аппаратных и программных

---

[8] 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).

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

средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований такая оценка должна проводиться в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности при осуществлении регулирования в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности».

6.1. В случае если кредитная организация, филиал иностранного банка применяют СКЗИ российского производства, СКЗИ должны иметь подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, при осуществлении регулирования в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности».

6.2. Криптографические ключи должны изготавливаться клиентом (самостоятельно) и (или) кредитной организацией, филиалом иностранного банка.

6.3. Безопасность процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ, используемые для изготовления криптографических ключей.

7. Кредитные организации, филиалы иностранных банков должны формировать для клиентов рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее – вредоносный код), в целях противодействия осуществлению переводов денежных средств без согласия клиента.

Кредитные организации, филиалы иностранных банков должны доводить до клиентов информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью совершения действий в целях осуществления банковских операций лицами, не обладающими правом на их совершение, и мерах по снижению указанных рисков:

мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом совершались действия в целях осуществления банковской операции;

мерах по контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления банковской операции, и своевременному обнаружению воздействия вредоносного кода.

8. В целях противодействия осуществлению переводов денежных средств без согласия клиента кредитные организации в случаях, предусмотренных договорами с клиентами, содержащими условия указанного в части 1 статьи 9 Федерального закона «О национальной платежной системе» договора об использовании электронного средства платежа (далее – договор об использовании электронного средства платежа), на основании их заявлений устанавливают в отношении операций, осуществляемых с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций через сеть «Интернет», ограничения на осуществление операций клиентами либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени. Ограничения по операциям могут быть установлены как на все операции клиентов, так и в разрезе типов (параметров) операций.

9. В целях противодействия осуществлению переводов денежных средств без согласия клиента кредитные организации в рамках реализуемой ими на основании части четвертой статьи 24 Федерального закона «О банках и банковской деятельности» (в редакции Федерального закона от 3 февраля

1996 года № 17-ФЗ) (далее – Федеральный закон «О банках и банковской деятельности») системы управления рисками, в том числе на основании сведений, полученных от операторов услуг платежной инфраструктуры, в случаях, предусмотренных договором об использовании электронного средства платежа, устанавливают ограничения по параметрам (на сумму одной операции, общую сумму, период времени) операций по приему наличных денежных средств с использованием преобразованных данных платежной карты посредством банкоматов или иных технических устройств.

10. В целях противодействия осуществлению переводов денежных средств без согласия клиента системно значимые кредитные организации, кредитные организации, значимые на рынке платежных услуг, должны обеспечить возможность использования мобильной версии приложения для приема заявлений клиентов – физических лиц о каждом случае совершения операций без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием, для формирования на основании указанного заявления справки о каждой указанной операции, содержащей информацию, указанную в приложении 1 к настоящему Положению, а также для подтверждения клиентом – физическим лицом того, что операция, в отношении которой кредитной организацией получен от Банка России запрос в соответствии с порядком, установленным Банком России на основании части 6 статьи 27 Федерального закона «О национальной платежной системе», является операцией без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием.

Кредитные организации, не указанные в абзаце первом настоящего пункта, ставшие кредитными организациями, указанными в абзаце первом настоящего пункта, не позднее восемнадцати месяцев после того, как стали кредитными организациями, указанными в абзаце первом настоящего пункта, должны реализовать требование абзаца первого настоящего пункта.

Кредитные организации должны обеспечить возможность приема заявлений физических лиц о случаях зачисления наличных денежных средств на банковские счета третьих лиц с использованием преобразованных данных платежной карты посредством банкоматов или иных технических устройств, осуществленного под влиянием обмана или при злоупотреблении доверием.

Кредитные организации должны регистрировать заявления, указанные в абзацах первом и третьем настоящего пункта, с указанием даты регистрации и регистрационного номера заявления.

11. В целях противодействия осуществлению переводов денежных средств без согласия клиента кредитные организации в случаях, предусмотренных договором об использовании электронного средства платежа, должны уведомлять законных представителей (родителей, усыновителей или попечителя) несовершеннолетних клиентов в возрасте от четырнадцати до восемнадцати лет о предоставлении указанным несовершеннолетним клиентам электронных средств платежа, о совершаемых указанными несовершеннолетними клиентами операциях с использованием электронных средств платежа.

12. Кредитные организации, филиалы иностранных банков к инцидентам (событиям), связанным с нарушением требований к обеспечению защиты информации, должны относить события, которые привели или могут привести к осуществлению банковских операций без согласия клиента, неоказанию услуг, связанных с осуществлением банковских операций, в том числе включенные в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации в соответствии с пунктом 5 части 4 статьи 6 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», и

размещаемый Банком России на официальном сайте Банка России в сети «Интернет» (далее соответственно – инцидент защиты информации, перечень типов инцидентов).

Кредитные организации определяют порядок фиксации инцидентов защиты информации в базе событий в соответствии с пунктами 7.3 и 7.5 Положения Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» [10] и порядок информационного обмена со службой управления рисками, создаваемой в соответствии с пунктом 3.6 Указания Банка России от 15 апреля 2015 года № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы»[11].

Кредитные организации, филиалы иностранных банков должны регистрировать инциденты защиты информации с указанием:

защищаемой информации, обрабатываемой на технологическом участке (участках), на котором (которых) произошел несанкционированный доступ к защищаемой информации;

результата реагирования на инцидент защиты информации, в том числе действий по возврату денежных средств.

Кредитные организации, филиалы иностранных банков в целях реализации требований к обеспечению защиты информации должны осуществлять информирование Банка России, в том числе на основании запросов Банка России:

---

[10] Зарегистрировано Минюстом России 3 июня 2020 года, регистрационный № 58577, с изменениями, внесенными Указаниями Банка России от 25 марта 2022 года № 6103-У (зарегистрировано Минюстом России 30 августа 2022 года, регистрационный № 69846).

[11] Зарегистрировано Минюстом России 26 мая 2015 года, регистрационный № 37388, с изменениями, внесенными Указаниями Банка России от 3 декабря 2015 года № 3878-У (зарегистрировано Минюстом России 28 декабря 2015 года, регистрационный № 40325), от 16 ноября 2017 года № 4606-У (зарегистрировано Минюстом России 7 декабря 2017 года, регистрационный № 49156), от 27 июня 2018 года № 4838-У (зарегистрировано Минюстом России 5 сентября 2018 года, регистрационный № 52084), от 8 апреля 2020 года № 5431-У (зарегистрировано Минюстом России 3 июня 2020 года, регистрационный № 58576), от 10 января 2023 года № 6356-У (зарегистрировано Минюстом России 14 июня 2023 года, регистрационный № 73833), от 6 октября 2023 года № 6569-У (зарегистрировано Минюстом России 25 декабря 2023 года, регистрационный № 76594).

о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, принятых мерах и проведенных мероприятиях по реагированию на выявленные кредитной организацией, филиалом иностранного банка или Банком России инциденты защиты информации, включенные в перечень типов инцидентов, а также о планируемых мероприятиях по раскрытию информации об инцидентах защиты информации, включая размещение информации на своих официальных сайтах в сети «Интернет», выпуск пресс-релизов и проведение пресс-конференций не позднее одного рабочего дня до дня проведения мероприятия;

о сайтах в сети «Интернет», которые используются кредитной организацией, филиалом иностранного банка для осуществления их деятельности, принадлежащих им и (или) принадлежащих иной организации, но администрируемых в интересах кредитной организации, филиала иностранного банка на основании договора возмездного оказания услуг.

Информация о данных, направляемых кредитными организациями, филиалами иностранных банков в Банк России в целях предоставления сведений, указанных в абзацах седьмом и восьмом настоящего пункта, размещается Банком России на официальном сайте Банка России в сети «Интернет».

Кредитные организации, филиалы иностранных банков направляют в Банк России сведения, указанные в абзацах седьмом и восьмом настоящего пункта, с использованием технической инфраструктуры (автоматизированной системы) Банка России или резервного способа взаимодействия (при технической невозможности использования технической инфраструктуры (автоматизированной системы) Банка России), информация о которых размещается на официальном сайте Банка России в сети «Интернет».

Предоставление кредитными организациями, филиалами иностранных банков в Банк России сведений, указанных в абзаце седьмом настоящего пункта, осуществляется в сроки, определенные приложением 2 к настоящему Положению.

13. Кредитные организации, филиалы иностранных банков должны

проводить оценку соответствия уровням защиты информации, предусмотренным пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017 и определенным в подпункте 3.1 пункта 3 настоящего Положения (далее – оценка соответствия защиты информации), и оценку выполнения требований к обеспечению защиты информации, применяемых с использованием технологических мер защиты информации и применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений, с соблюдением следующих требований:

13.1. Оценка соответствия защиты информации должна осуществляться в соответствии с положениями раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»[12] (далее – ГОСТ Р 57580.2-2018).

13.2. Оценка соответствия защиты информации должна осуществляться с привлечением проверяющих организаций.

В целях обеспечения защиты информации кредитные организации, филиалы иностранных банков должны хранить результат оценки соответствия защиты информации, подготовленный проверяющей организацией в виде отчета, не менее пяти лет начиная с даты его выдачи проверяющей организацией.

13.3. Кредитные организации должны обеспечивать уровень соответствия защиты информации не ниже четвертого, предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

Филиалы иностранных банков должны обеспечивать уровень соответствия защиты информации не ниже третьего, предусмотренного подпунктом «г» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

Филиалы иностранных банков должны обеспечивать уровень соответствия защиты информации не ниже четвертого, предусмотренного

[12] Утвержден и введен в действие 1 сентября 2018 года приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст (М., ФГУП «Стандартинформ», 2018).

подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

13.4. Оценка соответствия защиты информации и оценка выполнения требований к обеспечению защиты информации, применяемых с использованием технологических мер защиты информации и применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений, кредитными организациями, филиалами иностранных банков должны осуществляться не реже одного раза в два года.

13.5. Кредитные организации при проведении оценки выполнения требований к обеспечению защиты информации, применяемых с использованием технологических мер защиты информации и применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений, должны осуществлять расчет значений указанной оценки в отношении видов оценки выполнения требований к обеспечению защиты информации, указанных в пунктах 4.3 и 5.3 Порядка составления и представления отчетности по форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации», установленного Указанием Банка России от 10 апреля 2023 года № 6406-У «О формах, сроках, порядке составления и представления отчетности кредитных организаций (банковских групп) в Центральный банк Российской Федерации, а также о перечне информации о деятельности кредитных организаций (банковских групп)»[13].

14. При обеспечении безопасности объектов информационной инфраструктуры, которые являются объектами критической информационной инфраструктуры Российской Федерации, применяются в том числе требования и порядок, установленные органами государственной власти Российской Федерации в области обеспечения безопасности критической

[13] Зарегистрировано Минюстом России 16 августа 2023 года, регистрационный № 74823, с изменениями, внесенными Указаниями Банка России от 8 декабря 2023 года № 6621-У (зарегистрировано Минюстом России 22 января 2024 года, регистрационный № 76927), от 12 марта 2024 года № 6688-У (зарегистрировано Минюстом России 29 мая 2024 года, регистрационный № 78345), от 10 июля 2024 года № 6800-У (зарегистрировано Минюстом России 25 октября 2024 года, регистрационный № 79916), от 4 сентября 2024 года № 6840-У (зарегистрировано Минюстом России 10 октября 2024 года, регистрационный № 79758), от 16 декабря 2024 года № 6961-У (зарегистрировано Минюстом России 19 декабря 2024 года, регистрационный № 80633).

информационной инфраструктуры Российской Федерации в соответствии со статьей 6 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

15. Настоящее Положение в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 13 декабря 2024 года № ПСД-44) вступает в силу по истечении 10 дней после дня его официального опубликования, за исключением положений, для которых настоящим пунктом установлены иные сроки вступления их в силу.

Абзацы третий и четвертый подпункта 5.1, абзацы седьмой – одиннадцатый подпункта 5.2.4, абзац пятый подпункта 5.3 пункта 5, пункт 10 настоящего Положения вступают в силу с 1 октября 2025 года.

Абзац пятый подпункта 3.1 пункта 3, абзац третий подпункта 13.3 пункта 13 настоящего Положения вступают в силу с 1 января 2027 года.

Абзац четвертый подпункта 3.1 пункта 3, абзац второй подпункта 13.3 пункта 13 настоящего Положения действуют по 31 декабря 2026 года.

16. Со дня вступления в силу настоящего Положения признать утратившими силу:

Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»[14];

Указание Банка России от 18 февраля 2022 года № 6071-У «О внесении изменений в Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской

[14] Зарегистрировано Минюстом России 16 мая 2019 года, регистрационный № 54637.

деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»[15];

Указание Банка России от 6 декабря 2023 года № 6620-У «О внесении изменений в Положение Банка России от 17 апреля 2019 года № 683-П»[16].

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

[15] Зарегистрировано Минюстом России 20 июня 2022 года, регистрационный № 68919.
[16] Зарегистрировано Минюстом России 22 декабря 2023 года, регистрационный № 76546.

Приложение 1
к Положению Банка России
от 30 января 2026 года № 851-П
«Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

Перечень информации для формирования справки о случаях совершения операций без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием

1. Полное фирменное наименование кредитной организации.

2. Информация о заявителе (плательщике):

2.1. Фамилия, имя, отчество (при наличии), дата рождения, реквизиты документа, удостоверяющего личность.

2.2. Информация об идентификаторах операции и (или) способе ее проведения:

2.2.1. Платежная карта:

номер платежной карты;

полное фирменное наименование кредитной организации, выпустившей платежную карту.

2.2.2. Банковский счет:

банковский идентификационный код (далее – БИК) кредитной организации;

номер банковского счета;

полное фирменное наименование кредитной организации, в которой открыт банковский счет.

2.2.3. Электронное средство платежа (за исключением предоплаченных карт), использованное в системах (средствах) дистанционного обслуживания в целях совершения операций по переводу электронных денежных средств (далее – электронный кошелек):

номер электронного кошелька;

наименование платежной системы.

2.2.4. Сервис быстрых платежей платежной системы Банка России:

БИК кредитной организации;

абонентский номер подвижной радиотелефонной связи.

2.2.5. Банкомат или иное техническое устройство:

полное фирменное наименование кредитной организации и (или) банковского платежного агента (субагента), обслуживающих банкомат или иное техническое устройство;

номер банкомата или иного технического устройства;

адрес нахождения банкомата или иного технического устройства.

3. Информация о получателе средств (при наличии):

3.1. Полное (фирменное) наименование, идентификационный номер налогоплательщика (далее – ИНН) юридического лица.

3.2. Информация об идентификаторах операции и (или) способе ее проведения:

3.2.1. Платежная карта:

номер платежной карты (в формате, установленном правилами платежной системы, в соответствии с требованиями по защите номера платежной карты);

полное фирменное наименование кредитной организации, выпустившей платежную карту.

3.2.2. Электронный кошелек:

номер электронного кошелька;

наименование платежной системы.

3.2.3. Сервис быстрых платежей платежной системы Банка России (в случае осуществления переводов денежных средств между физическими лицами):

абонентский номер подвижной радиотелефонной связи.

3.2.4. Банковский счет:

БИК кредитной организации;

номер банковского счета;

полное фирменное наименование кредитной организации, в которой открыт банковский счет.

3.2.5. Сервис быстрых платежей платежной системы Банка России (в случае зачисления денежных средств на банковские счета получателя средств, являющегося торгово-сервисным предприятием (далее – ТСП):

абонентский номер подвижной радиотелефонной связи;

ИНН ТСП;

идентификатор ТСП;

БИК кредитной организации;

номер банковского счета, открытого в кредитной организации;

полное фирменное наименование кредитной организации, обслуживающей ТСП;

номер операции в сервисе быстрых платежей платежной системы Банка России.

3.2.6. Зачисление денежных средств на банковские счета получателя средств, являющегося ТСП:

банковский идентификационный номер (далее – БИН) участника платежной системы, обслуживающего получателя средств, являющегося ТСП;

ИНН ТСП;

идентификатор ТСП;

БИК кредитной организации;

номер банковского счета, открытого в кредитной организации;

полное фирменное наименование кредитной организации, обслуживающей ТСП.

3.2.7. Банкомат или иное техническое устройство:

полное фирменное наименование кредитной организации и (или) банковского платежного агента (субагента), обслуживающих банкомат или иное техническое устройство;

номер банкомата или иного технического устройства;

адрес нахождения банкомата.

4. Сумма операции.

5. Валюта операции.

6. Дата и время совершения операции (с указанием часовой зоны (часового пояса).

Приложение 2
к Положению Банка России
от 30 января 2015 года № 851-П
«Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

Сроки предоставления кредитными организациями, филиалами иностранных банков Банку России сведений о выявленных инцидентах защиты информации, о принятых мерах и проведенных мероприятиях по реагированию на выявленный инцидент защиты информации

№ п/п	Вид сведений	Срок предоставления
1	2	3
1	Сведения о выявлении инцидента защиты информации	В течение 3 часов с момента выявления инцидента защиты информации, и (или) незаконного раскрытия банковской тайны, и (или) иной защищаемой информации, указанной в пункте 1 настоящего Положения
2	Сведения о выявлении незаконного раскрытия банковской тайны и (или) иной защищаемой информации, указанной в пункте 1 настоящего Положения	
3	Сведения о результатах расследования инцидента защиты информации или незаконного раскрытия банковской тайны	В течение 30 дней со дня направления в Банк России сведений о выявлении инцидента защиты

1	2	3
	и (или) иной защищаемой информации, указанной в пункте 1 настоящего Положения	информации, или незаконного раскрытия банковской тайны, и (или) иной защищаемой информации, указанной в пункте 1 настоящего Положения
4	Сведения о компьютерных инцидентах (в соответствии с частью 5 статьи 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»)	В течение 3 часов с момента выявления компьютерного инцидента в случае его связи с функционированием значимого объекта критической информационной инфраструктуры. В течение 24 часов с момента выявления компьютерного инцидента во всех иных случаях