ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«17» августа 2023 г. № 821-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 76286
от "06" декабря 2023 г.

О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Настоящее Положение на основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» устанавливает требования к обеспечению операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, поставщиками платежных приложений, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ защиты информации при осуществлении переводов денежных средств, а также порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

Глава 1. **Общие положения**

1.1. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ в целях реализации требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее – требования к обеспечению защиты информации), применяемых в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается при осуществлении переводов денежных средств операторами по переводу денежных средств (далее – объекты информационной инфраструктуры), должны:

применять меры защиты информации, посредством выполнения которых обеспечивается реализация уровней защиты информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения информации, указанной в абзаце первом пункта 1.3 настоящего Положения, в целях осуществления переводов денежных средств, установленных 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», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст[1] (далее – ГОСТ Р 57580.1-2017);

проводить ежегодное тестирование на предмет наличия возможности проникновения в информационную инфраструктуру и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры, в том числе в соответствии с пунктами 3.8 и 3.9 настоящего Положения;

[1] М., ФГУП «Стандартинформ», 2017.

проводить оценку соответствия уровням защиты информации (далее – оценка соответствия защиты информации) 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», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст[1] (далее – ГОСТ Р 57580.2-2018), и пунктами 2.3, 2.4, 3.6–3.9, 4.4, 4.5, 6.7 и 6.8 настоящего Положения.

Оценка соответствия защиты информации должна осуществляться с привлечением организаций, имеющих 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).

В целях обеспечения защиты информации операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ должны хранить результат оценки соответствия защиты информации, подготовленный проверяющей организацией в виде отчета, не менее пяти лет начиная с даты его выдачи проверяющей организацией.

1.2. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ, указанные в подпункте 1.4.3 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты

[1] М., ФГУП «Стандартинформ», 2018.

информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»[1] (далее – Положение Банка России от 20 апреля 2021 года № 757-П), должны выполнять требования к обеспечению защиты информации, применяемые в отношении прикладного программного обеспечения автоматизированных систем и приложений, в том числе в соответствии с пунктами 2.5, 3.8–3.10, 4.6, 6.9 и 6.10 настоящего Положения.

Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, а также операторы электронных платформ, указанные в абзаце первом настоящего пункта, должны использовать 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 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[2] (далее соответственно – оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения, ГОСТ Р ИСО/МЭК 15408-3-2013), и обрабатывающие информацию, указанную в абзаце первом пункта 1.3 настоящего Положения:

прикладное программное обеспечение автоматизированных систем и приложений, распространяемых клиентам операторов по переводу

[1] Зарегистрировано Минюстом России 15 июня 2021 года, регистрационный № 63880.
[2] М., ФГУП «Стандартинформ», 2014.

денежных средств для совершения действий, непосредственно связанных с осуществлением переводов денежных средств;

программное обеспечение, эксплуатируемое на участках, используемых для приема документов, связанных с осуществлением переводов денежных средств, составленных в электронном виде (далее – электронные сообщения), к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»).

По решению операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов услуг информационного обмена, операторов услуг платежной инфраструктуры, операторов электронных платформ, указанных в подпункте 1.4.3 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 757-П, оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений проводится самостоятельно или с привлечением проверяющей организации.

1.3. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ должны выполнять требования к обеспечению защиты информации, применяемые в отношении технологии обработки информации, подготавливаемой, обрабатываемой и хранимой на участках идентификации, аутентификации и авторизации клиентов операторов по переводу денежных средств при совершении действий в целях осуществления переводов денежных средств; формирования (подготовки), передачи и приема электронных сообщений; удостоверения права клиентов операторов по переводу денежных средств распоряжаться денежными средствами; осуществления переводов денежных средств; учета результатов осуществления переводов денежных средств; хранения электронных сообщений и информации об осуществленных переводах денежных средств (далее соответственно – защищаемая информация, технологические участки).

Операторы по переводу денежных средств, банковские платежные

агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ в целях реализации требований к обеспечению защиты защищаемой информации на технологических участках должны обеспечивать:

конфиденциальность, целостность, доступность и достоверность защищаемой информации;

регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации;

регистрацию результатов совершения действий, связанных с осуществлением доступа к защищаемой информации.

1.4. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ должны регистрировать результаты совершения следующих действий, связанных с осуществлением доступа к защищаемой информации:

идентификации, аутентификации и авторизации клиентов операторов по переводу денежных средств при совершении действий в целях осуществления переводов денежных средств;

приема электронных сообщений от клиентов операторов по переводу денежных средств;

приема (передачи) электронных сообщений при взаимодействии операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов услуг информационного обмена, операторов услуг платежной инфраструктуры, операторов электронных платформ при осуществлении переводов денежных средств, в том числе для удостоверения права клиентов операторов по переводу денежных средств распоряжаться денежными средствами и для учета результатов переводов денежных средств;

реализации мер, установленных подпунктом 1.9 пункта 1 приложения 1 к настоящему Положению;

осуществления доступа работников к защищаемой информации, выполняемого с использованием автоматизированных систем, программного обеспечения;

осуществления действий клиентов операторов по переводу денежных средств с защищаемой информацией, выполняемых с использованием автоматизированных систем, программного обеспечения.

1.4.1. Регистрации подлежат следующие данные о действиях, выполняемых работниками с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) совершения работником действий с защищаемой информацией;

присвоенный работнику идентификатор, позволяющий установить работника в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат совершения работником действия с защищаемой информацией (успешно или неуспешно);

информация, используемая для идентификации устройств, при помощи которых либо в отношении которых осуществлен доступ к автоматизированной системе, программному обеспечению в целях совершения работником действий с защищаемой информацией.

1.4.2. Регистрации подлежат следующие данные о действиях, выполняемых клиентами операторов по переводу денежных средств с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) совершения клиентом оператора по переводу денежных средств действий с защищаемой информацией;

присвоенный клиенту оператора по переводу денежных средств идентификатор, позволяющий установить клиента оператора по переводу денежных средств в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат совершения клиентом оператора по переводу денежных средств действия с защищаемой информацией (успешно или неуспешно);

информация, используемая для идентификации устройств, при помощи которых либо в отношении которых осуществлен доступ к автоматизированной системе, программному обеспечению в целях совершения клиентом оператора по переводу денежных средств действий с защищаемой информацией.

1.5. Операторы по переводу денежных средств, операторы услуг платежной инфраструктуры в целях реализации требований к обеспечению защиты информации, применяемых в отношении информирования Банка России об инцидентах (событиях), связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе включенных в перечень типов инцидентов, согласованный 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» (далее – Федеральный закон от 26 июля 2017 года № 187-ФЗ), и размещаемый Банком России на официальном сайте Банка России в сети «Интернет» (далее соответственно – инциденты защиты информации, перечень типов инцидентов), должны осуществлять информирование Банка России:

о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, принятых мерах и проведенных мероприятиях по реагированию на выявленные оператором по переводу денежных средств, оператором услуг платежной инфраструктуры 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 официальных сайтах в сети «Интернет», выпуск пресс-релизов и проведение пресс-конференций не позднее одного рабочего дня до дня проведения такого мероприятия;

о сайтах в сети «Интернет», которые используются операторами по переводу денежных средств, операторами услуг платежной инфраструктуры для осуществления их деятельности, принадлежащих им и (или) принадлежащих иной организации, но администрируемых в интересах операторов по переводу денежных средств, операторов услуг платежной инфраструктуры на основании договора возмездного оказания услуг.

Информирование операторами по переводу денежных средств, операторами услуг платежной инфраструктуры осуществляется посредством представления в Банк России сведений, указанных в абзацах втором и третьем настоящего пункта. Информация о форме и сроке представления указанных сведений подлежит согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, согласно пункту 6 части 4 статьи 6 Федерального закона от 26 июля 2017 года № 187-ФЗ и размещается на официальном сайте Банка России в сети «Интернет».

1.6. В случае если защищаемая информация содержит персональные данные, операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ 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 от 27 июля 2006 года № 152-ФЗ).

Обеспечение защиты персональных данных операторами по переводу денежных средств, банковскими платежными агентами (субагентами),

операторами услуг информационного обмена, операторами услуг платежной инфраструктуры, операторами электронных платформ осуществляется в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[1].

1.7. Обеспечение защиты информации при осуществлении переводов денежных средств с использованием средств криптографической защиты информации (далее – СКЗИ) операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ осуществляется в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон от 6 апреля 2011 года № 63-ФЗ), 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[2] (далее – Положение ПКЗ-2005), и технической документацией на СКЗИ.

Обеспечение защиты персональных данных с использованием СКЗИ осуществляется в соответствии с 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» и приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

---

[1] Зарегистрирован Минюстом России 14 мая 2013 года, регистрационный № 28375, с изменениями, внесенными приказами ФСТЭК России от 23 марта 2017 года № 49 (зарегистрирован Минюстом России 25 апреля 2017 года, регистрационный № 46487), от 14 мая 2020 года № 68 (зарегистрирован Минюстом России 8 июля 2020 года, регистрационный № 58877).

[2] 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).

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»[1] с применением СКЗИ, 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), и обеспечивающих нейтрализацию угроз безопасности персональных данных, определенных Банком России в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ.

В случае если операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы платежных систем, операторы услуг платежной инфраструктуры, операторы электронных платформ применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

1.8. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ при взаимодействии в целях обеспечения контроля целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом должны использовать усиленную электронную подпись в соответствии с требованиями Федерального закона от 6 апреля 2011 года № 63-ФЗ, созданную с использованием средств электронной подписи и

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

средств удостоверяющего центра, имеющих сертификат соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

1.9. Признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, операторами услуг платежной инфраструктуры, операторами электронных платформ должно осуществляться в соответствии со статьей 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ.

Глава 2. Требования к обеспечению операторами по переводу денежных средств, поставщиками платежных приложений (при их привлечении операторами по переводу денежных средств) защиты информации при осуществлении переводов денежных средств

2.1. Операторы по переводу денежных средств должны выполнять требования к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением переводов денежных средств, в соответствии с Положением 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»[1] (далее – Положение Банка России от 17 апреля 2019 года № 683-П).

2.2. Операторы по переводу денежных средств в целях реализации требований к обеспечению защиты информации должны обеспечить защиту следующей защищаемой информации:

[1] Зарегистрировано Минюстом России 16 мая 2019 года, регистрационный № 54637, с изменениями, внесенными Указанием Банка России от 18 февраля 2022 года № 6071-У (зарегистрировано Минюстом России 20 июня 2022 года, регистрационный № 68919).

указанной в пункте 1 Положения Банка России от 17 апреля 2019 года № 683-П;

об остатках денежных средств на банковских счетах клиентов операторов по переводу денежных средств;

об остатках электронных денежных средств клиентов операторов по переводу денежных средств;

о конфигурации, определяющей параметры работы объектов информационной инфраструктуры, технических средств защиты информации.

2.3. Операторы по переводу денежных средств должны обеспечивать проведение оценки соответствия защиты информации не реже одного раза в два года.

2.4. Операторы по переводу денежных средств должны обеспечивать уровень соответствия защиты информации не ниже четвертого, предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

2.5. Операторы по переводу денежных средств, являющиеся системно значимыми кредитными организациями, кредитными организациями, признанными Банком России значимыми на рынке платежных услуг, 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 приложение, 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[1].

Операторы по переводу денежных средств, не указанные в абзаце первом настоящего пункта, в случае принятия решения о необходимости проведения сертификации прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного

[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).

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.

2.6. Операторы по переводу денежных средств должны установить порядок их информирования привлекаемыми ими банковскими платежными агентами (субагентами), операторами услуг информационного обмена о выявленных ими инцидентах защиты информации. Операторы по переводу денежных средств по запросу Банка России должны направлять в Банк России сведения об инцидентах защиты информации, полученные от привлекаемых ими банковских платежных агентов (субагентов), операторов услуг информационного обмена.

2.7. Операторы по переводу денежных средств в случаях, предусмотренных договорами с клиентами, содержащими условия указанного в части 1 статьи 9 Федерального закона от 27 июня 2011 года № 161-ФЗ договора об использовании электронного средства платежа, устанавливают в отношении операций по осуществлению переводов денежных средств, осуществляемых с использованием сети «Интернет», указанные в заявлениях клиентов ограничения по параметрам операций, в том числе ограничения, указанные в пункте 2.10 настоящего Положения.

2.8. При осуществлении переводов денежных средств с использованием сети «Интернет» и размещении программного обеспечения, используемого клиентами операторов по переводу денежных средств при осуществлении переводов денежных средств, на средствах вычислительной техники, для которых операторами по переводу денежных средств не обеспечивается непосредственный контроль защиты информации от воздействия вредоносного кода, операторы по переводу денежных средств должны реализовать технологические меры и (или) реализовать ограничения по параметрам операций по осуществлению переводов денежных средств на основании заявлений клиентов в отношении операций по осуществлению

переводов денежных средств, в том числе в соответствии с частью 9 статьи 20 Федерального закона от 27 июня 2011 года № 161-ФЗ.

2.9. Технологические меры, указанные в пункте 2.8 настоящего Положения, должны предусматривать:

механизмы идентификации и аутентификации клиента оператора по переводу денежных средств при формировании (подготовке) и при подтверждении им электронных сообщений в соответствии с законодательством Российской Федерации;

механизмы двухфакторной аутентификации клиента оператора по переводу денежных средств при совершении им действий в целях осуществления переводов денежных средств;

механизмы и (или) протоколы формирования и обмена электронными сообщениями, обеспечивающих защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации, в том числе аутентификацию входных электронных сообщений;

взаимную (двухстороннюю) аутентификацию участников обмена средствами вычислительной техники операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов услуг информационного обмена, операторов услуг платежной инфраструктуры, операторов электронных платформ, клиентов операторов по переводу денежных средств;

возможность использования клиентом оператора по переводу денежных средств независимых программных сред для формирования (подготовки) и подтверждения электронных сообщений;

возможность контроля клиентом оператора по переводу денежных средств реквизитов распоряжений о переводе денежных средств при формировании (подготовке) электронных сообщений (пакета электронных сообщений) и их подтверждении;

возможность установления временных ограничений на выполнение клиентом оператора по переводу денежных средств подтверждения электронных сообщений;

функции передаваемого клиенту оператора по переводу денежных средств программного обеспечения, используемого при осуществлении переводов денежных средств и предназначенного для установки на мобильные устройства клиента оператора по переводу денежных средств, связанные с выявлением модификации мобильного устройства клиента оператора по переводу денежных средств с использованием недекларируемых возможностей, в том числе деактивации (отключения) механизма разграничения доступа (далее – недекларируемая модификация мобильного устройства клиента), а также уведомлением клиента оператора по переводу денежных средств о случаях недекларируемой модификации мобильного устройства клиента с указанием рисков использования такого устройства (при наличии технической возможности реализации соответствующих функций).

2.10. При реализации ограничений по параметрам операций по осуществлению переводов денежных средств применяются ограничения на:

максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени;

перечень возможных получателей денежных средств;

временной период, в который могут быть совершены переводы денежных средств;

географическое местоположение устройств, с использованием которых может осуществляться формирование (подготовка) и (или) подтверждение клиентом оператора по переводу денежных средств электронных сообщений;

перечень идентификаторов устройств, с использованием которых может осуществляться формирование (подготовка) и (или) подтверждение клиентом оператора по переводу денежных средств электронных сообщений;

перечень предоставляемых услуг, связанных с осуществлением переводов денежных средств.

Операторы по переводу денежных средств в случаях, предусмотренных договорами с клиентами, содержащими условия указанного в части 1 статьи 9 Федерального закона от 27 июня 2011 года № 161-ФЗ договора об использовании электронного средства платежа, на основании их заявлений вправе установить иные ограничения по параметрам операций по осуществлению переводов денежных средств.

2.11. Контроль за соблюдением банковскими платежными агентами (субагентами) требований к обеспечению защиты информации при осуществлении переводов денежных средств осуществляется операторами по переводу денежных средств на основании договора, заключенного между операторами по переводу денежных средств и привлекаемыми ими банковскими платежными агентами в соответствии частью 2 статьи 4 Федерального закона от 27 июня 2011 года № 161-ФЗ.

Операторы по переводу денежных средств при привлечении банковских платежных агентов (субагентов) должны на основе системы управления рисками определить для них критерии необходимости и периодичности, тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, проведения оценки соответствия защиты информации, сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

Получение операторами по переводу денежных средств информации о соблюдении операторами услуг информационного обмена, предоставляющими услуги информационного обмена операторам по переводу денежных средств, требований к обеспечению защиты информации при осуществлении переводов денежных средств осуществляется на основании заключенного договора между операторами по переводу денежных средств и операторами услуг информационного обмена в соответствии с пунктом 33 статьи 3 Федерального закона от 27 июня 2011 года № 161-ФЗ.

2.12. При осуществлении операторами по переводу денежных средств подтверждения совершения переводов денежных средств с использованием электронной почты, в том числе при представлении клиентам операторов по переводу денежных средств справок (выписок) по банковским операциям и банковским счетам, операторы по переводу денежных средств должны реализовывать механизмы подтверждения принадлежности клиенту адреса электронной почты, на который оператором по переводу денежных средств направляются уведомления о совершенных переводах денежных средств.

2.13. При привлечении операторами по переводу денежных средств поставщики платежных приложений, предоставляющие платежные приложения для их применения клиентами операторов по переводу денежных средств, должны обеспечить соответствие указанных платежных приложений требованиям к защите информации, установленным в отношении проведения работ по разработке, сертификации и (или) оценке соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения, при наличии указанных требований в договорах, заключенных поставщиками платежных приложений с операторами по переводу денежных средств в соответствии с пунктом 29 статьи 3 Федерального закона от 27 июня 2011 года № 161-ФЗ.

Глава 3. Требования к обеспечению банковскими платежными агентами (субагентами) (при их привлечении для участия в осуществлении переводов денежных средств) защиты информации при осуществлении переводов денежных средств

3.1. Банковские платежные агенты (субагенты), за исключением банковских платежных агентов, осуществляющих операции платежного агрегатора, должны обеспечивать защиту информации при участии в осуществлении переводов денежных средств в отношении следующих операций:

принятие от физического лица наличных денежных средств, в том числе с применением банкоматов;

выдача физическому лицу наличных денежных средств, в том числе с применением банкоматов;

принятие от юридического лица, индивидуального предпринимателя и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года № 161-ФЗ, наличных денежных средств с применением банкоматов в целях зачисления принятых наличных денежных средств на открытые им банковские счета.

3.2. Банковские платежные агенты, осуществляющие операции платежного агрегатора, должны обеспечивать защиту информации в процессе формирования (подготовки) электронных сообщений при приеме электронных средств платежа юридическими лицами, индивидуальными предпринимателями и иными лицами, указанными в части 13 статьи 14^1 Федерального закона от 27 июня 2011 года № 161-ФЗ, при участии в переводе денежных средств в пользу юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 13 статьи 14^1 Федерального закона от 27 июня 2011 года № 161-ФЗ, по операциям с использованием электронных средств платежа.

3.3. Банковские платежные агенты (субагенты), за исключением банковских платежных агентов, осуществляющих операции платежного агрегатора, при совершении операций, указанных в пункте 3.1 настоящего Положения, в целях реализации требований к обеспечению защиты информации должны обеспечить защиту защищаемой информации, указанной в графе 3 строк 1 и 2 приложения 2 к настоящему Положению.

3.4. Банковские платежные агенты, осуществляющие операции платежного агрегатора, при совершении операций, указанных в пункте 3.2 настоящего Положения, в целях реализации требований к обеспечению защиты информации должны обеспечить защиту защищаемой информации, указанной в графе 3 строки 3 приложения 2 к настоящему Положению.

3.5. Банковские платежные агенты (субагенты) должны обеспечить реализацию минимального уровня защиты информации для объектов информационной инфраструктуры, предусмотренного пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.

По решению банковских платежных агентов (субагентов) уровень защиты информации для объектов информационной инфраструктуры, предусмотренный пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, может быть повышен на основе анализа рисков.

3.6. Банковские платежные агенты, осуществляющие операции платежного агрегатора, должны проводить оценку соответствия защиты информации не реже одного раза в два года.

3.7. Банковские платежные агенты, осуществляющие операции платежного агрегатора, должны реализовывать уровень соответствия защиты информации не ниже четвертого, предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

3.8. Банковские платежные агенты (субагенты), за исключением банковских платежных агентов, осуществляющих операции платежного агрегатора, должны на основе критериев, установленных операторами по переводу денежных средств, проводить тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры, оценку соответствия защиты информации, сертификацию или оценку соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

3.9. Банковские платежные агенты, осуществляющие операции платежного агрегатора, должны на основе критериев, установленных операторами по переводу денежных средств, проводить тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры, сертификацию или оценку соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

3.10.В случае принятия решения о необходимости проведения сертификации прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения банковские платежные агенты (субагенты) должны обеспечить сертификацию прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения не ниже 6 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76.

3.11. Банковские платежные агенты (субагенты) должны обеспечить при осуществлении операций, указанных в пунктах 3.1 и 3.2 настоящего Положения, реализацию технологических мер по обеспечению защиты информации в соответствии с приложениями 1 и 2 к настоящему Положению.

Глава 4. Требования к обеспечению операторами услуг информационного обмена (при оказании услуг информационного обмена) защиты информации при осуществлении переводов денежных средств

4.1. Операторы услуг информационного обмена должны обеспечивать защиту информации при оказании операторам по переводу денежных средств услуг информационного обмена в отношении следующих операций:

осуществление переводов денежных средств с использованием электронных средств платежа на основании электронных сообщений клиентов операторов по переводу денежных средств;

осуществление переводов денежных средств с использованием электронных средств платежа на основании электронных сообщений иностранных поставщиков платежных услуг.

4.2. Операторы услуг информационного обмена при осуществлении операций, указанных в пункте 4.1 настоящего Положения, в целях реализации требований к обеспечению защиты информации должны обеспечить защиту

защищаемой информации, указанной в графе 3 строк 4 и 5 приложения 2 к настоящему Положению.

4.3. Операторы услуг информационного обмена должны обеспечить реализацию стандартного уровня защиты информации для объектов информационной инфраструктуры, предусмотренного пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.

По решению операторов услуг информационного обмена уровень защиты информации для объектов информационной инфраструктуры, предусмотренный пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, может быть повышен на основе анализа рисков.

4.4. Операторы услуг информационного обмена должны проводить оценку соответствия защиты информации не реже одного раза в два года.

4.5. Операторы услуг информационного обмена должны реализовать уровень соответствия защиты информации не ниже четвертого, предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

4.6. В случае принятия решения о проведении сертификации прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения операторы услуг информационного обмена 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.

4.7. Операторы услуг информационного обмена должны обеспечить при осуществлении операций, указанных в пункте 4.1 настоящего Положения, реализацию технологических мер по обеспечению защиты информации в соответствии с приложениями 1 и 2 к настоящему Положению.

Глава 5. Требования к обеспечению операторами платежных систем защиты информации при осуществлении переводов денежных средств

5.1. Операторы платежных систем в целях реализации требований к обеспечению защиты информации должны определить порядок обеспечения защиты информации в платежной системе в соответствии с пунктом 11 части 3 статьи 28 Федерального закона от 27 июня 2011 года № 161-ФЗ, при определении которого участники платежной системы должны реализовать следующие мероприятия:

установление состава и пороговых значений показателей уровня риска информационной безопасности участника платежной системы;

реализация операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры механизмов, направленных на соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств, и контроль их соблюдения операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры;

реализация операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры процессов выявления и идентификации риска информационной безопасности участника платежной системы, а также его оценки;

реализация операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры процессов реагирования на инциденты защиты информации и восстановления штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации;

реализация операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной

инфраструктуры взаимодействия при обмене информацией об инцидентах защиты информации;

реализация операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента, определенных пунктами 3.2 и 3.4 Указания Банка России от 9 января 2023 года № 6354-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, форме и порядке получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента»[1].

5.2. Операторы платежных систем должны определить мероприятия по контролю за соблюдением установленных пороговых значений показателей уровня риска информационной безопасности участника платежной системы и реализации процессов применения в отношении операторов по переводу денежных средств, являющихся участниками платежной системы, и операторов услуг платежной инфраструктуры ограничений по параметрам операций по осуществлению переводов денежных средств в случае выявления факта превышения пороговых значений показателей уровня риска информационной безопасности участника платежной системы, в том числе условий снятия таких ограничений.

5.3. Операторы платежных систем в целях снижения риска информационной безопасности участника платежной системы должны

[1] Зарегистрировано Минюстом России 25 мая 2023 года, регистрационный № 73472.

совершенствовать механизмы реализации требований, указанных в пункте 5.5 настоящего Положения, предусматривающих в том числе накопление и учет опыта реагирования на инциденты защиты информации и восстановления функционирования платежной системы после их реализации.

5.4. Операторы платежных систем должны установить требования к содержанию, форме и периодичности направления операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры оператору платежной системы информации для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств.

Операторы национально значимых платежных систем должны уведомлять федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, в соответствии с требованиями, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, об установленных ими требованиях к содержанию, форме и периодичности направления указанной в абзаце первом настоящего пункта информации в части применения СКЗИ.

5.5. Операторы платежных систем должны обеспечить учет и доступность для операторов по переводу денежных средств, являющихся участниками платежной системы, и операторов услуг платежной инфраструктуры информации:

о выявленных в платежной системе инцидентах защиты информации;

о способах реагирования на инциденты защиты информации.

5.6. Операторы значимых платежных систем должны обеспечить использование:

в аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих криптографические алгоритмы, не определенные национальными стандартами Российской Федерации (далее – иностранные криптографические алгоритмы), имеющих подтверждение соответствия требованиям, установленным федеральным

органом исполнительной власти, уполномоченным в области обеспечения безопасности;

в аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы, определенные национальными стандартами Российской Федерации (далее – криптографические алгоритмы Российской Федерации), имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности;

СКЗИ, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы Российской Федерации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности».

В целях обеспечения бесперебойности функционирования информационной инфраструктуры платежной системы и ее устойчивости к внешним воздействиям операторам национально значимых платежных систем необходимо определять долю технических средств информационной инфраструктуры национально значимой платежной системы, в которых обеспечивается использование СКЗИ, указанных в абзаце четвертом настоящего пункта, на основании требований, устанавливаемых Указанием Банка России от 25 июля 2014 года № 3342-У «О требованиях к информационным технологиям, используемым операторами услуг платежной

инфраструктуры, для целей признания платежной системы национально значимой платежной системой»[1].

Операторы по переводу денежных средств, операторы услуг информационного обмена, операторы услуг платежной инфраструктуры для обеспечения защиты информации при осуществлении переводов денежных средств вправе использовать СКЗИ иностранного производства в случаях, не противоречащих требованиям, установленным в абзацах втором – четвертом настоящего пункта.

Разработка и эксплуатация СКЗИ, указанных в абзацах втором – четвертом настоящего пункта, должны проводиться в соответствии с Положением ПКЗ-2005.

5.7. Операторы платежных систем в составе требований к обеспечению защиты информации в платежной системе должны определять порядок проведения работ по разработке, сертификации и (или) оценке соответствия в отношении прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения, в том числе платежных приложений, предоставляемых поставщиками платежных приложений клиентам операторов по переводу денежных средств, являющихся участниками данной платежной системы.

Глава 6. Требования к обеспечению операторами услуг платежной инфраструктуры (при осуществлении деятельности операционного центра, платежного клирингового центра и расчетного центра) защиты информации при осуществлении переводов денежных средств

6.1. Операторы услуг платежной инфраструктуры, осуществляющие деятельность операционных центров (далее – ОЦ), при предоставлении операционных услуг должны обеспечивать защиту информации при обмене электронными сообщениями между операторами по переводу денежных средств, между операторами по переводу денежных средств и их клиентами,

[1] Зарегистрировано Минюстом России 9 октября 2014 года, регистрационный № 34269.

операторами услуг платежной инфраструктуры, осуществляющими деятельность платежных клиринговых центров (далее – ПКЦ), операторами услуг платежной инфраструктуры, осуществляющими деятельность расчетных центров (далее – РЦ), между ПКЦ и РЦ.

6.2. ПКЦ при предоставлении услуг платежного клиринга должен обеспечивать защиту информации при осуществлении следующих операций:

выполнение процедур приема к исполнению электронных сообщений операторов по переводу денежных средств, включая проверку соответствия электронных сообщений операторов по переводу денежных средств, определение достаточности денежных средств для исполнения электронных сообщений операторов по переводу денежных средств и определение платежных клиринговых позиций;

передача РЦ для исполнения электронных сообщений ПКЦ, принятых электронных сообщений операторов по переводу денежных средств;

направление операторам по переводу денежных средств извещений (подтверждений), касающихся приема к исполнению электронных сообщений операторов по переводу денежных средств, а также передача извещений (подтверждений), касающихся исполнения электронных сообщений операторов по переводу денежных средств.

6.3. РЦ должен обеспечивать защиту информации при исполнении поступивших от ПКЦ электронных сообщений ПКЦ, операторов по переводу денежных средств посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств.

6.4. Операторы услуг платежной инфраструктуры при осуществлении операций, указанных в пунктах 6.1–6.3 настоящего Положения, в целях реализации требований к обеспечению защиты информации должны обеспечить защиту защищаемой информации, указанной в графе 3 строк 6–10 приложения 2 к настоящему Положению.

6.5. Операторы услуг платежной инфраструктуры в целях реализации требований к обеспечению защиты информации должны принять меры

защиты информации, посредством выполнения которых обеспечивается реализация следующих уровней защиты информации для объектов информационной инфраструктуры, предусмотренных пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017:

операторы услуг платежной инфраструктуры, оказывающие услуги платежной инфраструктуры в рамках системно значимых платежных систем – усиленный уровень защиты информации;

операторы услуг платежной инфраструктуры, не указанные в абзаце втором настоящего пункта – стандартный уровень защиты информации.

6.6. Операторы услуг платежной инфраструктуры, указанные в абзаце третьем пункта 6.5 настоящего Положения, ставшие операторами услуг платежной инфраструктуры, указанными в абзаце втором пункта 6.5 настоящего Положения, не позднее восемнадцати месяцев после того, как стали операторами услуг платежной инфраструктуры, указанными в абзаце втором пункта 6.5 настоящего Положения, должны применять меры защиты информации, посредством выполнения которых обеспечивается реализация усиленного уровня защиты информации.

6.7. Операторы услуг платежной инфраструктуры должны проводить оценку соответствия защиты информации не реже одного раза в два года.

6.8. Операторы услуг платежной инфраструктуры должны реализовать уровень соответствия защиты информации не ниже четвертого, предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

6.9. Операторы услуг платежной инфраструктуры, указанные в абзаце третьем пункта 6.5 настоящего Положения, должны самостоятельно определять необходимость сертификации или проведения оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения по требованиям к ОУД не ниже чем ОУД 4, предусмотренного пунктом 7.6 раздела 7 ГОСТ Р ИСО/МЭК 15408-3-2013.

6.10. В случае принятия решения о необходимости проведении сертификации прикладного программного обеспечения автоматизированных

систем и приложений, а также отдельного программного обеспечения операторы услуг платежной инфраструктуры, указанные в абзаце втором пункта 6.5 настоящего Положения, 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.

В случае принятия решения о необходимости проведения сертификации прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения операторы услуг платежной инфраструктуры, указанные в абзаце третьем пункта 6.5 настоящего Положения, 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.

6.11. Операторы услуг платежной инфраструктуры при осуществлении операций, указанных в пунктах 6.1–6.3 настоящего Положения, должны реализовать технологические меры по обеспечению защиты информации в соответствии с приложениями 1 и 2 к настоящему Положению.

Глава 7. Требования к обеспечению операторами электронных платформ защиты информации при оказании услуг расчетов по сделкам, совершенным с использованием электронной платформы

7.1. Операторы электронных платформ, осуществляющие деятельность оператора финансовой платформы, должны обеспечивать выполнение требований к обеспечению защиты информации при оказании услуг, связанных с осуществлением переводов денежных средств, в соответствии с главой 2 Положения Банка России от 20 апреля 2021 года № 757-П.

7.2. Операторы электронных платформ, осуществляющие деятельность оператора информационной системы, в которой осуществляется выпуск

цифровых финансовых активов, оператора обмена цифровых финансовых активов, должны обеспечивать выполнение требований к обеспечению защиты информации при оказании услуг, связанных с осуществлением переводов денежных средств, в соответствии с главой 3 Положения Банка России от 20 апреля 2021 года № 757-П.

7.3. Операторы электронных платформ для объектов информационной инфраструктуры должны применять меры защиты информации, реализующие уровни защиты информации, установленные пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, в соответствии с подпунктами 1.4.3 и 1.4.4 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 757-П.

7.4. Операторы электронных платформ должны обеспечивать защиту информации при осуществлении операций по номинальному счету, указанных в частях 4 и 5 статьи 14^3 Федерального закона от 27 июня 2011 года № 161-ФЗ, в рамках расчетов по сделкам, совершенным с использованием электронной платформы.

7.5. Операторы электронных платформ при осуществлении операций по номинальному счету, указанных в частях 4 и 5 статьи 14^3 Федерального закона от 27 июня 2011 года № 161-ФЗ, в целях реализации требований к обеспечению защиты информации должны обеспечить защиту защищаемой информации, указанной в графе 3 строки 11 приложения 2 к настоящему Положению.

7.6. Операторы электронных платформ при осуществлении операций по номинальному счету, указанных в частях 4 и 5 статьи 14^3 Федерального закона от 27 июня 2011 года № 161-ФЗ, должны реализовать технологические меры по обеспечению защиты информации в соответствии с приложениями 1 и 2 к настоящему Положению.

Глава 8. Порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

8.1. При осуществлении контроля за соблюдением операторами по переводу денежных средств, являющимися кредитными организациями, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ требований к обеспечению защиты информации при осуществлении переводов денежных средств Банк России в рамках надзора в национальной платежной системе осуществляет следующие мероприятия:

8.1.1. Анализирует информацию (в том числе данные отчетности) о деятельности операторов платежных систем, операторов услуг платежной инфраструктуры, операторов электронных платформ, операторов по переводу денежных средств, являющихся кредитными организациями, в целях контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

8.1.2. Запрашивает и получает документы и информацию, в том числе содержащие персональные данные:

у операторов платежных систем, операторов услуг платежной инфраструктуры, операторов электронных платформ, операторов по переводу денежных средств, являющихся кредитными организациями, – в части выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;

у операторов по переводу денежных средств, являющихся кредитными организациями, – в части обеспечения контроля за соблюдением:

банковскими платежными агентами (субагентами), привлекаемыми для участия в осуществлении переводов денежных средств, – требований к обеспечению защиты информации при осуществлении переводов денежных средств;

операторами услуг информационного обмена, предоставляющими услуги информационного обмена операторам по переводу денежных средств, являющимся кредитными организациями, – требований к обеспечению защиты информации при осуществлении переводов денежных средств;

поставщиками платежных приложений, предоставляющими операторам по переводу денежных средств, являющимся кредитными организациями,

платежные приложения для их использования клиентами указанных операторов по переводу денежных средств, – требований к обеспечению защиты информации при осуществлении переводов денежных средств.

8.1.3. Проводит проверки являющихся кредитными организациями операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств, операторов электронных платформ и инспекционные проверки не являющихся кредитными организациями операторов платежных систем, операторов услуг платежной инфраструктуры.

8.2. Банк России проводит проверки являющихся кредитными организациями операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств, операторов электронных платформ в порядке, установленном в соответствии с частью четвертой статьи 73 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – Федеральный закон от 10 июля 2002 года № 86-ФЗ).

Банк России проводит инспекционные проверки не являющихся кредитными организациями операторов платежных систем, операторов услуг платежной инфраструктуры в порядке, установленном в соответствии с частью 3 статьи 33 Федерального закона от 27 июня 2011 года № 161-ФЗ.

Банк России проводит проверки не являющихся кредитными организациями операторов электронных платформ в порядке, установленном в соответствии с частью второй статьи 76^5 Федерального закона от 10 июля 2002 года № 86-ФЗ.

8.3. Банк России применяет меры к являющимся кредитными организациями операторам платежных систем, операторам услуг платежной инфраструктуры, операторам по переводу денежных средств, операторам электронных платформ в порядке, установленном в соответствии с частью тринадцатой статьи 74 Федерального закона от 10 июля 2002 года № 86-ФЗ.

Банк России осуществляет действия и применяет меры принуждения в рамках надзорной деятельности в отношении не являющихся кредитными организациями операторов платежных систем, операторов услуг платежной

инфраструктуры в порядке, установленном в соответствии с частью 4 статьи 32 Федерального закона от 27 июня 2011 года № 161-ФЗ.

Банк России направляет операторам электронных платформ, не являющимся кредитными организациями, предписания об устранении нарушения с указанием срока его устранения и ограничивает оказание операторами электронных платформ, не являющимися кредитными организациями, услуг расчетов по сделкам, совершенным с использованием электронной платформы, на срок, не превышающий шести месяцев, в порядке, установленном в соответствии с частью 3^3 статьи 32 Федерального закона от 27 июня 2011 года № 161-ФЗ.

Глава 9. **Заключительные положения**

9.1. При обеспечении безопасности объектов информационной инфраструктуры, эксплуатация и использование которых осуществляются при осуществлении переводов денежных средств операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, операторами услуг платежной инфраструктуры, операторами электронных платформ и 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 информационной инфраструктуры Российской Федерации в соответствии со статьей 6 Федерального закона от 26 июля 2017 года № 187-ФЗ.

9.2. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 28 апреля 2023 года № ПСД-17) вступает в силу с 1 апреля 2024 года, за исключением абзацев третьего – пятого пункта 5.6 настоящего Положения.

Абзацы третий – пятый пункта 5.6 настоящего Положения вступают в силу с 1 января 2031 года.

9.3. Со дня вступления в силу настоящего Положения признать утратившим силу Положение Банка России от 4 июня 2020 года № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»[1].

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Согласовано:

Директор
Федеральной службы безопасности
Российской Федерации
_____ А.В. Бортников
_____ 2023 г.

Директор
Федеральной службы по техническому
и экспортному контролю
_____ В.В. Селин
_____ 2023 г.

[1] Зарегистрировано Минюстом России 23 сентября 2020 года, регистрационный № 59991.

Приложение 1
к Положению Банка России
от 17 августа 2023 года № 821-П
«О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

Технологические меры по обеспечению защиты информации при осуществлении переводов денежных средств

1. В целях обеспечения защиты информации при совершении операций, связанных с осуществлением переводов денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, операторами услуг платежной инфраструктуры, операторами электронных платформ должны применяться следующие технологические меры:

1.1. Реализация механизма идентификации, аутентификации и авторизации клиентов операторов по переводу денежных средств при совершении ими действий в целях осуществления переводов денежных средств.

1.2. Реализация механизма двухфакторной аутентификации клиентов операторов по переводу денежных средств при совершении ими действий в целях осуществления переводов денежных средств.

1.3. Применение механизмов и (или) протоколов формирования и обмена электронными сообщениями, обеспечивающих защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации, в том числе аутентификацию входящих электронных сообщений.

1.4. Взаимная (двухсторонняя) аутентификация участников обмена

средствами вычислительной техники операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов услуг информационного обмена, операторов услуг платежной инфраструктуры, клиентов операторов по переводу денежных средств.

1.5. Использование электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ.

1.6. Использование усиленной электронной подписи в целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом.

1.7. Получение подтверждения от оператора по переводу денежных средств права клиента оператора по переводу денежных средств распоряжаться денежными средствами.

1.8. Проверка соответствия (сверка) результатов осуществления операций, связанных с переводом денежных средств, с информацией, содержащейся в электронных сообщениях.

1.9. Реализация мер, направленных на проверку правильности формирования (подготовки) электронных сообщений (двойной контроль).

1.10. Обеспечение хранения защищаемой информации, информации о событиях, подлежащих регистрации, информации об инцидентах защиты информации в течение пяти лет с даты формирования информации в неизменном виде.

1.11. Восстановление защищаемой информации в случае умышленного или случайного разрушения либо выхода из строя средств вычислительной техники.

2. Банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры, операторы электронных платформ при совершении операций, связанных с осуществлением переводов денежных средств, должны обеспечивать выполнение технологических мер по обеспечению защиты информации при осуществлении переводов денежных средств на соответствующих

технологических участках.

3. В рамках системы управления операционным риском при невозможности технической реализации отдельных технологических мер по обеспечению защиты информации при осуществлении переводов денежных средств, а также с учетом экономической целесообразности банковскими платежными агентами (субагентами), операторами услуг информационного обмена, операторами услуг платежной инфраструктуры, операторами электронных платформ могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию угроз безопасности защищаемой информации актуальных при осуществлении переводов денежных средств.

Приложение 2
к Положению Банка России
от 17 августа 2023 года № 821-П
«О требованиях к обеспечению защиты информации
при осуществлении переводов денежных средств и
о порядке осуществления Банком России контроля за
соблюдением требований к обеспечению защиты
информации при осуществлении переводов
денежных средств»

Таблица технологических мер
по обеспечению защиты информации при осуществлении переводов денежных средств на технологических участках

№ п/п	Операция	Защищаемая информация	Технологический участок	Действие	Технологические меры по обеспечению защиты информации при осуществлении переводов денежных средств, указанные в приложении 1 к Положению от 17 августа 2023 года № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»										
					1	2	3	4	5	6	7	8	9	10	11
1	2	3	4	5	6										
Банковские платежные агенты (субагенты)															

1	2	3	4	5	6									
1	Принятие от физического лица, юридического лица, индивидуального предпринимателя и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года № 161-ФЗ, наличных денежных средств, в том числе с применением банкоматов	Информация, содержащаяся в электронных сообщениях физических лиц, юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года № 161-ФЗ. Информация, содержащаяся в электронных сообщениях, передаваемых при взаимодействии банковских платежных агентов (субагентов) и операторов по переводу денежных средств, в том числе в электронных сообщениях, составленных банковскими платежными агентами (субагентами) от имени операторов по переводу денежных средств. Информация, содержащаяся в реестрах, сформированных на основе электронных сообщений (далее – реестр электронных сообщений) физических лиц, юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года № 161-ФЗ. Ключевая информация средств криптографической защиты информации (далее – СКЗИ), используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств	ФПП[1]	Формирование (подготовка) физическими лицами, юридическими лицами, индивидуальными предпринимателями и иными лицами, указанными в части 12 статьи 14 Федерального закона от 27 июня 2011 года № 161-ФЗ, электронных сообщений			+		+					
				Прием банковским платежным агентом (субагентом) электронных сообщений			+	+	+					
				Формирование (передача) банковским платежным агентом (субагентом) электронных сообщений, передача электронных сообщений в адрес операторов по переводу денежных средств			+	+		+		+	+		
				Формирование банковским платежным агентом (субагентом) реестра электронных сообщений физических лиц, юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 12 статьи 14 Федерального закона от 27 июня 2011 года № 161-ФЗ			+			+		+	+		
			ХИ[2]	Хранение банковским платежным агентом (субагентом) электронных сообщений, обмен которыми осуществлялся при его взаимодействии с физическими лицами, юридическими лицами, индивидуальными предпринимателями, иными лицами, указанными в части 12 статьи 14 Федерального закона от 27 июня 2011 года № 161-ФЗ, и операторами по переводу денежных средств									+	+

[1] ФПП – формирование (подготовка), передача и прием электронных сообщений.
[2] ХИ – хранение электронных сообщений и информации об осуществленных переводах денежных средств.

1	2	3	4	5	6										
2	Выдача физическому лицу наличных денежных средств, в том числе с применением банкоматов	Информация, используемая для идентификации, аутентификации и авторизации физических лиц при осуществлении доступа к системам дистанционного банковского обслуживания. Информация, содержащаяся в электронных сообщениях физических лиц. Информация, содержащаяся в электронных сообщениях, передаваемых при взаимодействии банковских платежных агентов (субагентов) и операторов по переводу денежных средств, в том числе при подтверждении права физических лиц получать наличные денежные средства. Информация об осуществленных операциях по выдаче наличных денежных средств физических лиц. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств	ИАА[1]	Осуществление доступа физических лиц к системам дистанционного банковского обслуживания в целях осуществления выдачи наличных денежных средств на основании запросов физических лиц	+	+									
			ФПП	Формирование (подготовка) физическими лицами электронных сообщений			+		+						
				Формирование банковским платежным агентом (субагентом) реестра электронных сообщений физических лиц			+			+		+	+		
				Прием банковским платежным агентом (субагентом) электронных сообщений			+	+	+						
				Формирование (подготовка) банковским платежным агентом (субагентом) электронных сообщений и направление электронных сообщений в адрес операторов по переводу денежных средств			+	+		+		+	+		
			УП[2]	Получение банковским платежным агентом (субагентом) от оператора по переводу денежных средств подтверждения права физического лица получать наличные денежные средства			+	+		+	+				
			ОУ[3]	Выдача банковским платежным агентом (субагентом) физическим лицам наличных денежных средств			+					+			
			ХИ	Хранение банковским платежным агентом (субагентом) электронных сообщений, обмен которыми осуществлялся при его взаимодействии с физическими лицами и операторами по переводу денежных средств										+	+
Банковские платежные агенты, осуществляющие операции платежного агрегатора															

[1] ИАА – идентификация, аутентификация и авторизация клиентов операторов по переводу денежных средств при совершении действий в целях осуществления операций по переводу денежных средств.

[2] УП – удостоверение права клиентов операторов по переводу денежных средств распоряжаться денежными средствами.

[3] ОУ – осуществление операций по переводу денежных средств, учет результатов их осуществления.

1	2	3	4	5	6									
3	Формирование (подготовка) электронных сообщений при обеспечении приема электронных средств платежа юридическими лицами, индивидуальными предпринимателями и иными лицами, указанными в части 13 статьи 14[1] Федерального закона от 27 июня 2011 года № 161-ФЗ, при участии в переводе денежных средств в пользу юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 13 статьи 14[1] Федерального закона от 27 июня 2011 года № 161-ФЗ, по операциям с использованием электронных средств платежа	Информация, содержащаяся в электронных сообщениях при обеспечении приема электронных средств платежа банковскими платежными агентами, осуществляющими операции платежного агрегатора. Информация, содержащаяся в электронных сообщениях, направляемых банковскими платежными агентами, осуществляющими операции платежного агрегатора, операторам по переводу денежных средств, операторам услуг информационного обмена. Информация, содержащаяся в реестрах электронных сообщений при обеспечении приема электронных средств платежа банковскими платежными агентами, осуществляющими операции платежного агрегатора. Информация об осуществленных операциях по переводу денежных средств. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами, осуществляющими операции платежного агрегатора, операторами по переводу денежных средств, операторами услуг информационного обмена	ФПП	Формирование банковским платежным агентом, являющимся платежным агрегатором, электронных сообщений, передача и прием банковским платежным агентом, осуществляющим операции платежного агрегатора, сформированных электронных сообщений				+	+	+		+	+		
			ХИ	Хранение банковским платежным агентом, осуществляющим операции платежного агрегатора, информации об осуществленных операциях по переводу денежных средств										+	+
Операторы услуг информационного обмена														
4	Оказание услуг информационного обмена при	Информация, используемая для идентификации, аутентификации и авторизации клиентов операторов по	ИАА	Совершение действий, связанных с переводами денежных средств клиентами операторов по переводу денежных средств	+										

1	2	3	4	5	6									
	осуществлении переводов денежных средств с использованием электронных средств платежа на основании электронных сообщений клиентов операторов по переводу денежных средств	переводу денежных средств при осуществлении переводов денежных средств. Информация, содержащаяся в электронных сообщениях клиентов операторов по переводу денежных средств. Информация, содержащаяся в электронных сообщениях, обмен которыми осуществляется при взаимодействии операторов услуг информационного обмена с операторами по переводу денежных средств, клиентами операторов по переводу денежных средств. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между операторами услуг информационного обмена, операторами по переводу денежных средств, клиентами операторов по переводу денежных средств. Информация об осуществлении перевода денежных средств, содержащаяся в реестрах электронных сообщений клиентов операторов по переводу денежных средств. Информация, используемая для удостоверения права клиентов операторов по переводу денежных средств распоряжаться денежными средствами. Информация об осуществленных переводах денежных средств	ФПП	Формирование (подготовка) клиентом оператора по переводу денежных средств электронных сообщений, передача и прием оператором услуг информационного обмена электронных сообщений			+	+	+					
				Формирование оператором услуг информационного обмена реестра электронных сообщений клиентов операторов по переводу денежных средств			+				+	+		
			УП	Получение оператором услуг информационного обмена от оператора по переводу денежных средств подтверждения права клиента оператора по переводу денежных средств распоряжаться денежными средствами			+	+		+	+			
			ОУ	Осуществление оператором услуг информационного обмена операций, связанных с переводом денежных средств, путем обмена электронными сообщениями с операторами по переводу денежных средств, в том числе на основании реестра электронных сообщений клиентов операторов по переводу денежных средств			+	+		+		+	+	
				Получение оператором услуг информационного обмена результатов осуществления переводов денежных средств, в том числе путем обмена электронными сообщениями с операторами по переводу денежных средств			+	+		+		+		
			ХИ	Хранение оператором услуг информационного обмена электронных сообщений, обмен которыми осуществлялся при его взаимодействии с клиентами операторов по переводу денежных средств, операторами по переводу денежных средств									+	+
				Хранение оператором услуг информационного обмена результатов осуществления операций по переводам денежных средств									+	

1	2	3	4	5	6										
5	Оказание услуг информационного обмена при осуществлении переводов денежных средств с использованием электронных средств платежа на основании электронных сообщений иностранных поставщиков платежных услуг	Информация, содержащаяся в электронных сообщениях иностранных поставщиков платежных услуг. Информация, содержащаяся в электронных сообщениях, обмен которыми осуществляется при взаимодействии операторов услуг информационного обмена с иностранными поставщиками платежных услуг. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между операторами услуг информационного обмена и иностранными поставщиками платежных услуг. Информация, содержащаяся в реестрах электронных сообщений иностранных поставщиков платежных услуг. Информация, используемая для удостоверения права клиентов операторов по переводу денежных средств распоряжаться денежными средствами. Информация об осуществленных переводах денежных средств	ФПП	Формирование (подготовка) иностранным поставщиком платежных услуг электронных сообщений, передача и прием оператором услуг информационного обмена электронных сообщений			+	+	+						
				Формирование оператором услуг информационного обмена реестра электронных сообщений иностранных поставщиков платежных услуг			+					+	+		
			УП	Получение оператором услуг информационного обмена от оператора по переводу денежных средств подтверждения права клиента оператора по переводу денежных средств распоряжаться денежными средствами			+	+		+	+				
			ОУ	Осуществление оператором услуг информационного обмена операций, связанных с переводом денежных средств, путем обмена электронными сообщениями с операторами по переводу денежных средств			+	+		+		+	+		
				Получение оператором услуг информационного обмена результатов осуществления переводов денежных средств, в том числе путем обмена электронными сообщениями с операторами по переводу денежных средств			+	+		+		+			
			ХИ	Хранение оператором услуг информационного обмена электронных сообщений, обмен которыми осуществлялся при его взаимодействии с иностранными поставщиками платежных услуг, операторами по переводу денежных средств										+	+
				Хранение оператором услуг информационного обмена результатов осуществления операций по переводам денежных средств										+	

1	2	3	4	5	6										
Операторы услуг платежной инфраструктуры, осуществляющие деятельность операционных центров (ОЦ)															
6	Обеспечение обмена электронными сообщениями между операторами по переводу денежных средств, между операторами по переводу денежных средств и их клиентами, ПКЦ, РЦ, между ПКЦ и РЦ	Информация, содержащаяся в электронных сообщениях операторов по переводу денежных средств, направленных ОЦ или полученных от ПКЦ, РЦ. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между операторами по переводу денежных средств, ОЦ, ПКЦ, РЦ	ФПП	Прием и передача электронных сообщений между операторами по переводу денежных средств и их клиентами, операторами услуг платежной инфраструктуры			+	+		+			+		
			ХИ	Хранение ОЦ электронных сообщений, обмен которыми осуществлялся при его взаимодействии с операторами по переводу денежных средств, их клиентами, операторами услуг платежной инфраструктуры										+	+
Операторы услуг платежной инфраструктуры, осуществляющие деятельность платежных клиринговых центров (ПКЦ)															
7	Выполнение процедур приема к исполнению электронных сообщений операторов по переводу денежных средств, включая проверку соответствия электронных сообщений операторов по переводу денежных средств установленным требованиям, определение достаточности денежных средств для исполнения	Информация, содержащаяся в электронных сообщениях операторов по переводу денежных средств, направленных ПКЦ или полученных от ОЦ. Информация о платежных клиринговых позициях. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между операторами по переводу денежных средств, ОЦ, ПКЦ	ФПП	Прием ПКЦ электронных сообщений операторов по переводу денежных средств			+	+		+					
				Направление ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения, касающиеся приема к исполнению электронных сообщений операторов по переводу денежных средств			+	+		+		+	+		
			ОУ	Проверка ПКЦ соответствия электронных сообщений операторов по переводу денежных средств установленным требованиям			+								
				Определение ПКЦ достаточности денежных средств для исполнения электронных сообщений операторов по переводу денежных средств, в том числе путем обмена электронными сообщениями с операторами услуг платежной инфраструктуры			+	+		+		+	+		
				Определение ПКЦ платежных клиринговых позиций для исполнения принятых электронных сообщений операторов по переводу денежных средств			+					+			

1	2	3	4	5	6										
	электронных сообщений операторов по переводу денежных средств и определение платежных клиринговых позиций		ХИ	Хранение ПКЦ электронных сообщений, обмен которыми осуществлялся при его взаимодействии с операторами услуг платежной инфраструктуры										+	+
8	Передача РЦ для исполнения электронных сообщений ПКЦ, принятых электронных сообщений операторов по переводу денежных средств	Информация, содержащаяся в электронных сообщениях ОЦ, ПКЦ по осуществлению операций по банковским (корреспондентским) счетам участников платежной системы. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между ОЦ, ПКЦ	ФПП	Формирование ПКЦ электронных сообщений по осуществлению операций по банковским (корреспондентским) счетам операторов по переводу денежных средств, передача электронных сообщений в адрес операторов услуг платежной инфраструктуры				+	+		+		+	+		
			ХИ	Хранение ПКЦ электронных сообщений, обмен которыми осуществлялся при его взаимодействии с операторами услуг платежной инфраструктуры										+	+
9	Направление операторам по переводу денежных средств извещений (подтверждений), касающихся приема	Информация об осуществленных операциях по переводу денежных средств. Информация, содержащаяся в электронных сообщениях ОЦ, ПКЦ по осуществлению операций по банковским (корреспондентским) счетам участников	ФПП	Направление ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения о приеме, об исполнении принятых электронных сообщений операторов по переводу денежных средств				+	+		+		+			

1	2	3	4	5	6										
	к исполнению электронных сообщений операторов по переводу денежных средств, а также передача извещений (подтверждений), касающихся исполнения электронных сообщений операторов по переводу денежных средств	платежной системы. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между операторами по переводу денежных средств, ОЦ	ХИ	Хранение ПКЦ электронных сообщений, обмен которыми осуществлялся при его взаимодействии с операторами услуг платежной инфраструктуры										+	+
Операторы услуг платежной инфраструктуры, осуществляющие деятельность расчетных центров (РЦ)															
10	Исполнение поступивших от ПКЦ электронных сообщений ПКЦ, операторов по переводу денежных средств посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств	Информация, содержащаяся в электронных сообщениях ОЦ, ПКЦ по осуществлению операций по банковским (корреспондентским) счетам операторов по переводу денежных средств. Информация, содержащаяся в электронных сообщениях при взаимодействии РЦ с ОЦ и ПКЦ. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между ОЦ, РЦ. Информация об осуществленных операциях по переводу денежных средств	ФПП	Прием РЦ поступивших от ПКЦ, ОЦ электронных сообщений ПКЦ, операторов по переводу денежных средств в целях списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств			+	+		+					
				Направление РЦ в адрес ПКЦ электронных сообщений, содержащих извещения об исполнении поступивших от ПКЦ электронных сообщений посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств			+	+		+		+	+		
			ОУ	Исполнение РЦ поступивших от ПКЦ электронных сообщений ПКЦ, операторов по переводу денежных средств посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств			+					+			

1	2	3	4	5	6										
			ХИ	Хранение РЦ информации об осуществленных списаниях и зачислениях денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств									+	+
				Хранение РЦ электронных сообщений, обмен которыми осуществлялся при его взаимодействии с операторами услуг платежной инфраструктуры									+	
Операторы электронных платформ															
11	Перевод денежных средств по номинальным счетам оператора электронной платформы, открытым для осуществления расчетов по сделкам, совершаемым с использованием электронной платформы	Информация, содержащаяся в электронных сообщениях, направляемых операторами электронных платформ в рамках перевода денежных средств по номинальному счету. Информация об осуществленных операциях по переводу денежных средств по номинальному счету. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между операторами электронных платформ и операторами по переводу денежных средств	ФПП	Формирование оператором электронных платформ электронных сообщений, и направление электронных сообщений в адрес оператора по переводу денежных средств			+	+		+		+	+		
			ХИ	Хранение оператором электронных платформ информации об осуществленных операциях по переводу денежных средств									+	+