ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«4» июня 2020 г. № 719-П

г. Москва

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» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) 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 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 в части требований к обеспечению защиты информации при осуществлении переводов денежных средств, 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 обеспечивать:

реализацию установленных настоящим Положением 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, определенных национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2017) (далее – ГОСТ Р 57580.1-2017);

ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры с учетом особенностей, предусмотренных пунктами 3.8 и 3.9 настоящего Положения;

проведение оценки соответствия уровням защиты информации, установленным настоящим Положением (далее – оценка соответствия защиты

информации), в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2018) (далее – ГОСТ Р 57580.2-2018), с учетом особенностей, предусмотренных 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 сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049) (далее соответственно – проверяющая организация, постановление Правительства Российской Федерации № 79).

Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры должны обеспечивать хранение отчета, подготовленного проверяющей организацией по результатам оценки соответствия защиты информации, 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 в части требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых

в отношении прикладного программного обеспечения автоматизированных систем и приложений, с учетом особенностей, предусмотренных пунктами 3.8–3.10, 4.6 и 6.10 настоящего Положения, должны обеспечивать использование прошедших сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю или оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «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 «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014) (далее – ГОСТ Р ИСО/МЭК 15408-3-2013), и обрабатывающих информацию, указанную в абзаце первом пункта 1.3 настоящего Положения:

прикладного программного обеспечения автоматизированных систем и приложений, распространяемых клиентам операторов по переводу денежных средств для совершения действий, непосредственно связанных с осуществлением переводов денежных средств;

программного обеспечения, эксплуатируемого 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»).

Для проведения оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений операторы по переводу денежных средств, банковские платежные агенты (субагенты) с учетом особенностей, предусмотренных пунктом 3.11 настоящего Положения,

операторы услуг информационного обмена, операторы услуг платежной инфраструктуры должны привлекать проверяющие организации.

1.3. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры в части требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых 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), должны обеспечивать:

целостность 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 должны обеспечивать регистрацию результатов совершения следующих действий, связанных с осуществлением доступа к защищаемой информации:

идентификация, аутентификация и авторизация клиентов операторов по переводу денежных средств при совершении действий в целях осуществления переводов денежных средств;

прием электронных сообщений от клиентов операторов по переводу денежных средств;

прием (передача) электронных сообщений при взаимодействии операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов услуг информационного обмена, операторов услуг платежной инфраструктуры 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;

реализация мер, направленных на проверку правильности формирования (подготовки) электронных сообщений (двойной контроль), применяемых в соответствии с подпунктом 1.9 пункта 1 приложения 1 к настоящему Положению;

осуществление доступа работников к защищаемой информации и осуществление действий клиентами операторов по переводу денежных средств с защищаемой информацией, выполняемых с использованием автоматизированных систем, программного обеспечения.

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.

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 части требований к обеспечению защиты информации при осуществлении переводов денежных средств, 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 с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения

и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, 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;

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 мероприятия.

Информирование осуществляется посредством предоставления в Банк России сведений, указанных в абзацах втором и третьем настоящего пункта. Информация о форме и сроке предоставления 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 части 6 статьи 5 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) (далее – Федеральный закон № 187-ФЗ) и размещается на официальном сайте Банка России в сети «Интернет».

1.6. В случае если защищаемая информация содержит персональные данные, должны применяться 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» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701).

Обеспечение защиты персональных данных 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», зарегистрированным Министерством юстиции Российской Федерации 14 мая 2013 года № 28375, 25 апреля 2017 года № 46487.

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 осуществляется в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794) (далее – Федеральный закон № 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 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года № 6382, 25 мая 2010 года № 17350 (далее – Положение ПКЗ-2005), и технической документацией на СКЗИ.

Обеспечение защиты персональных данных с использованием СКЗИ осуществляется в соответствии с 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», зарегистрированным Министерством юстиции Российской Федерации 18 августа 2014 года № 33620.

В случае если операторы по переводу денежных средств, банковский платежный агент (субагент), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа.

1.8. При взаимодействии операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов услуг информационного обмена, операторов услуг платежной инфраструктуры должно обеспечиваться подписание электронных сообщений усиленной электронной подписью.

1.9. Признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, должно осуществляться в соответствии со статьей 6 Федерального закона № 63-ФЗ (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794).

1.10. Настоящее Положение не распространяется на отношения, регулируемые Федеральным законом № 187-ФЗ.

При обеспечении безопасности автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается при осуществлении переводов денежных средств операторами по переводу денежных средств, операторами услуг платежной инфраструктуры, являющихся объектами критической информационной

инфраструктуры Российской Федерации, настоящее положение применяется наряду с требованиями Федерального закона № 187-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 обеспечивать выполнение требований 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», зарегистрированным Министерством юстиции Российской Федерации 16 мая 2019 года № 54637 (далее – Положение Банка России № 683-П).

2.2. Требования к обеспечению защиты информации при осуществлении переводов денежных средств выполняются операторами по переводу денежных средств для обеспечения защиты защищаемой информации, указанной в пункте 1 Положения Банка России № 683-П, а также защищаемой информации:

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, а также о конфигурации, определяющей параметры работы технических средств защиты информации.

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

2.4. Операторы по переводу денежных средств должны обеспечить уровень соответствия не ниже четвертого в соответствии с 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, должны обеспечить сертификацию прикладного программного обеспечения автоматизированных систем и приложений не ниже 4 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 30 июля 2018 года № 131 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», зарегистрированным Министерством юстиции Российской Федерации 14 ноября 2018 года № 52686 (далее – приказ ФСТЭК России № 131).

Операторы по переводу денежных средств, не указанные в абзаце первом настоящего пункта, должны обеспечить сертификацию прикладного программного обеспечения автоматизированных систем и приложений не ниже 5 уровня доверия в соответствии с приказом ФСТЭК России № 131.

2.6. Операторы по переводу денежных средств должны установить порядок их информирования привлекаемыми ими банковскими платежными агентами (субагентами), операторами услуг информационного обмена о выявленных 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 на основании заявлений клиентов, переданных способами, определенными договорами операторов по переводу денежных средств с клиентами, должны установить ограничения по параметрам операций, которые могут осуществляться клиентами операторов по переводу денежных средств с использованием сети «Интернет», 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 обеспечить реализацию технологических мер и (или) реализовать ограничения по параметрам операций по осуществлению переводов денежных средств, определяемые договорами операторов по переводу денежных средств с клиентами.

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

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

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

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 входных электронных сообщений;

взаимной (двухсторонней) аутентификации 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;

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

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

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

функций 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, связанных 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).

2.10. При реализации ограничений по параметрам операций по осуществлению переводов денежных средств могут применяться 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 могут применить иные ограничения по параметрам операций по осуществлению переводов денежных средств, определенные договорами операторов по переводу денежных средств с клиентами.

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 в соответствии с договорами между операторами

по переводу денежных средств и привлекаемыми ими банковскими платежными агентами.

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.

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 в соответствии с договорами между операторами по переводу денежных средств и операторами услуг информационного обмена.

2.12. Реализация операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств должна обеспечивать значение показателя, характеризующего уровень переводов денежных средств без согласия клиента, формируемого на ежеквартальной основе, не более 0,005 процента.

Значение показателя, характеризующего уровень переводов денежных средств без согласия клиента, должно рассчитываться как отношение суммы денежных средств, в отношении которых получены уведомления от клиентов операторов по переводу денежных средств о списании денежных средств с их банковских счетов без их согласия за оцениваемый квартал (за исключением случаев, предусмотренных законодательством Российской Федерации), к общей сумме денежных средств, списанных с банковских счетов клиентов операторов по переводу денежных средств.

2.13. 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.

2.14. При привлечении операторами по переводу денежных средств поставщики платежных приложений, предоставляющие приложения для их применения клиентами операторов по переводу денежных средств, должны обеспечить соответствие указанных приложений требованиям к защите информации, установленным в отношении проведения работ по разработке, сертификации и (или) оценке соответствия приложений требованиям к защите информации, 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 «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) (далее – Федеральный закон № 161-ФЗ).

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

3.1. Банковские платежные агенты (субагенты) 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 платежных терминалов и банкоматов;

выдача физическому лицу наличных денежных средств, в том числе с применением платежных терминалов и банкоматов.

3.2. Банковские платежные агенты, осуществляющие операции платежного агрегатора, должны обеспечивать защиту информации в процессе формирования (подготовки) электронных сообщений при обеспечении приема электронных средств платежа юридическими лицами, индивидуальными предпринимателями и иными лицами, указанными в части 13 статьи 14^1 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 27, ст. 3538), при участии в переводе денежных средств в пользу юридических лиц, индивидуальных предпринимателей и иных лиц, указанных в части 13 статьи 14^1 Федерального закона № 161-ФЗ, по операциям с использованием электронных средств платежа.

3.3. К защищаемой информации при совершении банковскими платежными агентами (субагентами) операций, указанных в пункте 3.1 настоящего Положения, относится информация в соответствии с графой «Защищаемая информация» строк 1 и 2 приложения 2 к настоящему Положению.

3.4. К защищаемой информации при совершении банковскими платежными агентами (субагентами), осуществляющими операции платежного агрегатора, указанные в пункте 3.2 настоящего Положения, относится информация в соответствии с графой «Защищаемая информация» строки 3 приложения 2 к настоящему Положению.

3.5. Банковские платежные агенты (субагенты) должны обеспечить реализацию минимального уровня защиты информации для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1-2017.

По решению банковских платежных агентов (субагентов) уровень защиты информации для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1-2017 может быть повышен на основе анализа рисков.

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

3.7. Банковские платежные агенты, осуществляющие операции платежного агрегатора, должны обеспечить уровень соответствия не ниже четвертого в соответствии с 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.

3.9. Банковские платежные агенты (субагенты), 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.

3.10. В случае принятия решения о необходимости проведения сертификации прикладного программного обеспечения автоматизированных систем и приложений банковские платежные агенты (субагенты) должны обеспечить сертификацию не ниже 6 уровня доверия в соответствии с приказом ФСТЭК России № 131.

3.11. По решению банковских платежных агентов (субагентов) оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений проводится самостоятельно или с привлечением проверяющей организации.

3.12. 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 на основании договоров 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. К защищаемой информации при осуществлении операторами услуг информационного обмена операций, указанных в пункте 4.1 настоящего Положения, относится информация в соответствии с графой «Защищаемая информация» 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 в соответствии с ГОСТ Р 57580.1-2017.

По решению операторов услуг информационного обмена уровень защиты информации для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1-2017 может быть повышен на основе анализа рисков.

4.4. Операторы услуг информационного обмена должны обеспечить проведение оценки соответствия защиты информации не реже одного раза в два года.

4.5. Операторы услуг информационного обмена должны обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018.

4.6. В случае принятия решения о проведении сертификации прикладного программного обеспечения автоматизированных систем и приложений операторы услуг информационного обмена должны обеспечить сертификацию не ниже 5 уровня доверия в соответствии с приказом ФСТЭК России № 131.

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. Оператор платежной системы в целях реализации пункта 11 части 3 статьи 28 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) в рамках системы управления рисками в платежной системе определяет в правилах платежной системы и иных документах порядок обеспечения защиты информации в платежной системе для операторов по переводу денежных средств, являющихся участниками платежной системы, операторов услуг платежной инфраструктуры с учетом требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее – требования к обеспечению защиты информации в платежной системе).

Оператор платежной системы должен определить требования к обеспечению защиты информации в платежной системе в отношении следующих мероприятий:

управление риском информационной безопасности в платежной системе как одним из видов операционного риска в платежной системе, источниками реализации которого являются: недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации, недостатки прикладного программного обеспечения автоматизированных систем и приложений, а также несоблюдение требований к указанным процессам деятельности операторами по переводу денежных средств, являющимися участниками платежной системы, операторами услуг платежной инфраструктуры (далее – риск информационной безопасности в платежной системе);

установление состава показателей уровня риска информационной безопасности в платежной системе;

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 в платежной системе в отношении объектов информационной инфраструктуры участников платежной системы, операторов услуг платежной инфраструктуры;

выявление и анализ операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры риска информационной безопасности в платежной системе;

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 2.2 и 2.4 Указания Банка России от 8 октября 2018 года № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и 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 мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента», зарегистрированного Министерством юстиции Российской Федерации 12 декабря 2018 года № 52988;

реализация операторами платежных систем 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 значений

показателей уровня риска информационной безопасности в платежной системе, в том числе условий снятия таких ограничений.

5.2. Оператор платежной системы в целях снижения риска информационной безопасности в платежной системе должен реализовывать механизмы совершенствования требований, указанных в пункте 5.4 настоящего Положения, предусматривающие в том числе накопление и учет опыта реагирования на инциденты защиты информации и восстановления функционирования платежной системы после их реализации.

5.3. Оператор платежной системы должен 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.

Оператор национально значимой платежной системы должен уведомлять федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, об установленных им требованиях к содержанию, форме и периодичности направления указанной в абзаце первом настоящего пункта информации в части применения СКЗИ.

5.4. Оператор платежной системы должен 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 методиках анализа и реагирования на инциденты защиты информации.

5.5. Оператор значимой платежной системы в соответствии с правилами платежной системы должен 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 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 в области обеспечения безопасности;

СКЗИ, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы Российской Федерации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств, типы которых определяются Банком России по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности.

В целях обеспечения бесперебойности функционирования информационной инфраструктуры платежной системы и ее устойчивости от внешних воздействий оператору национально значимой платежной системы в правилах платежной системы следует 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», зарегистрированным Министерством юстиции Российской Федерации 9 октября 2014 года № 34269.

Операторы по переводу денежных средств, операторы услуг информационного обмена, операторы услуг платежной инфраструктуры вправе применять для обеспечения защиты информации при осуществлении переводов денежных средств СКЗИ иностранного производства в части, не противоречащей требованиям настоящего пункта.

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

5.6. Оператор платежной системы в составе требований к обеспечению защиты информации в платежной системе определяет порядок проведения работ по разработке, сертификации и (или) оценке соответствия в отношении прикладного программного обеспечения автоматизированных систем и приложений, 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 осуществлении обмена электронными сообщениями между операторами по переводу денежных средств, между операторами по переводу денежных средств и их клиентами, 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 установленным требованиям, 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. К защищаемой информации при осуществлении операторами услуг платежной инфраструктуры операций, указанных в пунктах 6.1–6.3 настоящего Положения, относится информация в соответствии с графой «Защищаемая информация» строк 6–10 приложения 2 к настоящему Положению.

6.5. Операторы услуг платежной инфраструктуры должны обеспечить реализацию следующих уровней защиты информации для

объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1-2017:

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

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

6.6. Операторы услуг платежной инфраструктуры, которые должны реализовывать стандартный уровень защиты информации, ставшие операторами услуг платежной инфраструктуры, которые должны реализовывать усиленный уровень защиты информации, должны обеспечить реализацию усиленного уровня защиты информации не позднее восемнадцати месяцев после того, как стали операторами услуг платежной инфраструктуры, указанными в абзаце втором пункта 6.5 настоящего Положения.

6.7. Операторы услуг платежной инфраструктуры должны обеспечить проведение оценки соответствия защиты информации не реже одного раза в два года.

6.8. Операторы услуг платежной инфраструктуры должны обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018.

6.9. Операторы услуг платежной инфраструктуры, которые должны реализовывать стандартный уровень защиты информации, вправе самостоятельно определять необходимость сертификации или проведения оценки соответствия по требованиям к ОУД не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013 в отношении прикладного программного обеспечения автоматизированных систем и приложений.

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

приложений операторы услуг платежной инфраструктуры, которые должны реализовывать усиленный уровень защиты информации, должны обеспечить сертификацию не ниже 4 уровня доверия в соответствии с приказом ФСТЭК России № 131.

В случае принятия решения о необходимости проведения сертификации прикладного программного обеспечения автоматизированных систем и приложений операторы услуг платежной инфраструктуры, которые должны реализовывать стандартный уровень защиты информации, должны обеспечить сертификацию не ниже 5 уровня доверия в соответствии с приказом ФСТЭК России № 131.

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

Глава 7. Порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

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

7.1.1. Анализирует информацию (в том числе данные отчетности) о деятельности операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств, являющихся

кредитными организациями, в целях контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

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

у операторов платежных систем, операторов услуг платежной инфраструктуры и 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 к деятельности по оказанию услуг по переводу 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.

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

7.2. Банк России проводит проверки являющихся кредитными организациями операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств 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)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2019, № 29, ст. 3857) (далее – Федеральный закон № 86-ФЗ).

Банк России проводит инспекционные проверки не являющихся кредитными организациями операторов платежных систем и операторов услуг платежной инфраструктуры в порядке, установленном в соответствии с частью 3 статьи 33 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423).

7.3. Банк России применяет меры к являющимся кредитными организациями операторам платежных систем, операторам услуг платежной инфраструктуры и операторам по переводу денежных средств в порядке, установленном в соответствии с частью двенадцатой статьи 74 Федерального закона № 86-ФЗ (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2019, № 18, ст. 2198).

Банк России осуществляет действия и применяет меры принуждения в отношении не являющихся кредитными организациями операторов платежных систем и операторов услуг платежной инфраструктуры в порядке, установленном в соответствии с частью 4 статьи 32 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423).

Глава 8. **Заключительные положения**

8.1. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол

заседания Совета директоров Банка России от 24 января 2020 года № 1) вступает в силу с 1 января 2022 года, за исключением положений, для которых настоящим пунктом установлены иные сроки вступления их в силу.

Абзацы первый, второй и шестой пункта 5.5 настоящего Положения вступают в силу с 1 января 2024 года.

Абзацы третий – пятый пункта 5.5 настоящего Положения вступают в силу с 1 января 2031 года.

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

Положение Банка России от 9 июня 2012 года № 382-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», зарегистрированное Министерством юстиции Российской Федерации 14 июня 2012 года № 24575;

Указание Банка России от 5 июня 2013 года № 3007-У «О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-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», зарегистрированное Министерством юстиции Российской Федерации 1 июля 2013 года № 28930;

Указание Банка России от 14 августа 2014 года № 3361-У «О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-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», зарегистрированное Министерством юстиции Российской Федерации 10 сентября 2014 года № 34017;

Указание Банка России от 7 мая 2018 года № 4793-У «О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-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», зарегистрированное Министерством юстиции Российской Федерации 22 июня 2018 года № 51411.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Согласовано:

Директор
Федеральной службы безопасности
Российской Федерации
_____ А В. Бортников

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

Приложение 1
к Положению 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»

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 могут 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 входных 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 простой или усиленной электронной подписи в соответствии с Федеральным законом № 63-ФЗ.

1.6. Использование усиленной электронной подписи для контроля целостности и подтверждения подлинности электронных сообщений в соответствии с Федеральным законом № 63-ФЗ.

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 (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники.

2. Банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры 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 могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности защищаемой информации.

Приложение 2
к Положению 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»

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										
					1	2	3	4	5	6	7	8	9	10	11
Банковские платежные агенты (субагенты)															
1	Принятие от физического лица наличных денежных средств, в том числе с применением платежных	Информация, содержащаяся в электронных сообщениях физических лиц. Информация, содержащаяся в электронных сообщениях, передаваемых при взаимодействии банковских платежных агентов (субагентов) и	ФПП[1]	Формирование (подготовка) физическими лицами электронных сообщений			+		+						
				Прием банковским платежным агентом (субагентом) электронных сообщений			+	+	+						

[1] ФПП – формирование (подготовка), передача и прием электронных сообщений.

№ п/п	Операция	Защищаемая информация	Техно-логи-ческий участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
	терминалов и банкоматов	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. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств		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			+			+		+	+		
			ХИ[1]	Хранение банковским платежным агентом (субагентом) электронных сообщений, обмен которыми осуществлялся при его взаимодействии с физическими лицами и операторами по переводу денежных средств										+	+
2	Выдача физическому лицу наличных денежных средств, в том числе с применением платежных терминалов и 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	ИАА[2]	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			+	+	+						

[1] ХИ – хранение электронных сообщений и информации об осуществленных переводах денежных средств.

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

№ п/п	Операция	Защищаемая информация	Техно-логи-ческий участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
		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		Формирование (подготовка) банковским платежным агентом (субагентом) электронных сообщений и направление электронных сообщений в адрес операторов по переводу денежных средств			+	+		+		+	+		
			УП[1]	Получение банковским платежным агентом (субагентом) от оператора по переводу денежных средств подтверждения права физического лица получать наличные денежные средства			+	+		+	+				
			ОУ[2]	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															
3	Формирование (подготовка) электронных сообщений при обеспечении приема электронных средств платежа юридическими лицами, индивидуальными предпринимателями	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	ФПП	Формирование банковским платежным агентом, являющимся платежным агрегатором, электронных сообщений, передача и прием банковским платежным агентом, осуществляющим операции платежного агрегатора, сформированных электронных сообщений			+	+	+			+	+		

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

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

№ п/п	Операция	Защищаемая информация	Техно-логи-ческий участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
	и иными лицами, указанными в части 13 статьи 14[1] Федерального закона № 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 № 161-ФЗ, по операциям с использованием электронных средств платежа	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	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 осуществлении переводов денежных средств с использованием электронных средств платежа на основании электронных сообщений клиентов	Информация, используемая для идентификации, аутентификации и авторизации клиентов операторов по 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	ИАА	Совершение действий, связанных с переводами денежных средств клиентами операторов по переводу 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			+					+	+		

№ п/п	Операция	Защищаемая информация	Технологический участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
	операторов по переводу денежных средств	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	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										+	
5	Оказание услуг информационного обмена при осуществлении переводов денежных	Информация, содержащаяся в электронных сообщениях иностранных поставщиков платежных услуг. Информация, содержащаяся в электронных сообщениях, обмен	ФПП	Формирование (подготовка) иностранным поставщиком платежных услуг электронных сообщений, передача и прием оператором услуг информационного обмена электронных сообщений			+	+	+						

№ п/п	Операция	Защищаемая информация	Технологический участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
	средств с использованием электронных средств платежа на основании электронных сообщений иностранных поставщиков платежных услуг	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		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										+	
Операторы услуг платежной инфраструктуры, осуществляющие деятельность операционных центров (ОЦ)															
6	Обеспечение обмена электронными сообщениями между операторами по	Информация, содержащаяся в электронных сообщениях операторов по переводу денежных средств, направленных ОЦ или полученных от	ФПП	Прием и передача электронных сообщений между операторами по переводу денежных средств и их клиентами, операторами услуг платежной инфраструктуры			+	+		+			+		

№ п/п	Операция	Защищаемая информация	Техно-логи-ческий участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
	переводу денежных средств, между операторами по переводу денежных средств и их клиентами, ПКЦ, РЦ, между ПКЦ и РЦ	ПКЦ, РЦ. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между операторами по переводу денежных средств, ОЦ, ПКЦ, РЦ	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			+					+			

№ п/п	Операция	Защищаемая информация	Техно-логи-ческий участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
	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			+	+		+		+			

№ п/п	Операция	Защищаемая информация	Технологический участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
	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	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	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			+	+		+		+	+		

№ п/п	Операция	Защищаемая информация	Техно-логи-ческий участок	Действие	Технологические меры										
					1	2	3	4	5	6	7	8	9	10	11
	по переводу денежных средств	операциях 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			+					+			
			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										+	