"Положение 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" (утв. Банком России 09.06.2012 № 382-П)

(в ред. Указаний Банка России от 05.06.2013 № 3007-У, от 14.08.2014 № 3361-У, от 07.05.2018 № 4793-У)

Зарегистрировано в Минюсте России 14.06.2012 № 24575

Глава 1. Общие положения

1.1. На основании Федерального закона от 27 июня 2011 года № 161-ФЗ "О национальной платежной системе" (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) (далее - Федеральный закон № 161-ФЗ) настоящее Положение устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств (далее - требования к обеспечению защиты информации при осуществлении переводов денежных средств), а также устанавливает 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.

1.2. Оператор по переводу денежных средств обеспечивает выполнение банковскими платежными агентами (субагентами), привлекаемыми к деятельности по оказанию услуг по переводу денежных средств, требований к обеспечению защиты информации при осуществлении переводов денежных средств, с учетом перечня операций, выполняемых банковскими платежными агентами (субагентами), и используемых автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается банковскими платежными агентами (субагентами).

Оператор по переводу денежных средств обеспечивает контроль соблюдения банковскими платежными агентами (субагентами), привлекаемыми к деятельности по оказанию услуг по переводу денежных средств, требований к защите информации при осуществлении переводов денежных средств.

1.3. Для проведения работ по обеспечению защиты информации при осуществлении переводов денежных средств операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры могут привлекать организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.

Глава 2. Требования к обеспечению защиты информации при осуществлении переводов денежных средств

2.1. Требования к обеспечению защиты информации при осуществлении переводов денежных средств применяются для обеспечения защиты следующей информации (далее - защищаемая информация): информации об остатках денежных средств на банковских счетах;
информации об остатках электронных денежных средств;
информации о совершенных переводах денежных средств, в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений участников платежной системы, а также в извещениях (подтверждениях), касающихся исполнения распоряжений участников платежной системы;
требование об отнесении информации о совершенных переводах денежных средств к защищаемой информации, хранящейся в операционных центрах платежных систем с использованием платежных карт или находящихся за пределами Российской Федерации, устанавливается оператором платежной системы;
информации, содержащейся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов операторов по переводу денежных средств (далее - клиентов), распоряжениях участников платежной системы, распоряжениях платежного клирингового центра;
информации о платежных клиринговых позициях;
информации, необходимой для удостоверения клиентами права распоряжения денежными средствами, в том числе данных держателей платежных карт;
ключевой информации средств криптографической защиты информации (далее - СКЗИ), используемых при осуществлении переводов денежных средств (далее - криптографические ключи);
информации о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается оператором по переводу денежных средств, оператором услуг платежной инфраструктуры, банковским платежным агентом (субагентом), и используемых для осуществления переводов денежных средств (далее - объекты информационной инфраструктуры), а также информации о

конфигурации, определяющей параметры работы технических средств защиты информации;
информации ограниченного доступа, в том числе персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемой при осуществлении переводов денежных средств.

2.2. Требования к обеспечению защиты информации при осуществлении переводов денежных средств включают в себя:
требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при назначении и распределении функциональных прав и обязанностей (далее - ролей) лиц, связанных с осуществлением переводов денежных средств;
требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;
требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при осуществлении доступа к объектам информационной инфраструктуры, включая требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от несанкционированного доступа;
требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код);
требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»);
требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании СКЗИ;
требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (далее - технологические меры защиты информации);
требования к организации и функционированию подразделения (работников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации (далее - служба информационной безопасности);
требования к повышению осведомленности работников оператора по переводу денежных средств, банковского платежного агента (субагента), являющегося юридическим лицом, оператора услуг платежной инфраструктуры и клиентов (далее - повышение осведомленности) в области обеспечения защиты информации;
требования к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагированию на них;
требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;
требования к оценке выполнения оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств;
требования к доведению оператором по переводу денежных средств, оператором услуг платежной инфраструктуры до оператора платежной системы информации об обеспечении в платежной системе защиты информации при осуществлении переводов денежных средств;
требования к совершенствованию оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств.

Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры к инцидентам, связанным с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, должен относить события, которые привели или могут привести к осуществлению переводов денежных средств без согласия клиента, неоказанию услуг по переводу денежных средств, в том числе включенные в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на официальном сайте Банка России в сети Интернет (далее - перечень типов инцидентов).

Абзацы семнадцатый - девятнадцатый утратили силу с 1 июля 2018 года. - Указание Банка России от 07.05.2018 № 4793-У.

Требования к обеспечению защиты информации при осуществлении переводов денежных средств помимо требований, указанных в абзацах втором - пятнадцатом настоящего пункта, включают в себя: требования к обеспечению защиты информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов;
требования к обеспечению защиты информации при осуществлении переводов денежных средств с применением платежных карт.

2.3. Выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств обеспечивается с учетом параметров и статистики выполняемых операций, связанных с осуществлением переводов денежных средств, количества и характера выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, путем:

2.3.1. выбора организационных мер защиты информации;
определения во внутренних документах оператора по переводу денежных средств, банковского платежного агента (субагента), оператора платежных систем, оператора услуг платежной инфраструктуры порядка применения организационных мер защиты информации;
определения лиц, ответственных за применение организационных мер защиты информации;
применения организационных мер защиты;
реализации контроля применения организационных мер защиты информации;
выполнения иных необходимых действий, связанных с применением организационных мер защиты информации;

2.3.2. выбора технических средств защиты информации;
определения во внутренних документах оператора по переводу денежных средств, банковского платежного агента (субагента), оператора платежных систем, оператора услуг платежной инфраструктуры порядка использования технических средств защиты информации, включающего информацию о конфигурации, определяющую параметры работы технических средств защиты информации;
назначения лиц, ответственных за использование технических средств защиты информации;
использования технических средств защиты информации;
реализации контроля за использованием технических средств защиты информации;
выполнения иных необходимых действий, связанных с использованием технических средств защиты информации;

2.3.3. применения объектов информационной инфраструктуры, обладающих функциональными и конструктивными особенностями, связанными с обеспечением защиты информации при осуществлении переводов денежных средств и реализации контроля за их функционированием.

2.4. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации при назначении и распределении ролей лиц, связанных с осуществлением переводов денежных средств, включаются следующие требования.

2.4.1. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами: по осуществлению доступа к защищаемой информации;
по управлению криптографическими ключами;
по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа.

Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию своих работников, обладающих правами по формированию электронных сообщений, содержащих распоряжения об осуществлении переводов денежных средств (далее - электронные сообщения).

2.4.2. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени следующих ролей: ролей, связанных с созданием (модернизацией) объекта информационной инфраструктуры и эксплуатацией объекта информационной инфраструктуры;
ролей, связанных с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и эксплуатацией объекта информационной инфраструктуры в части его технического обслуживания и ремонта.

2.4.3. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль и регистрацию действий лиц, которым назначены роли, определенные в подпункте 2.4.1 настоящего пункта.

2.5. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации на стадиях создания, эксплуатации, модернизации, снятия с эксплуатации объектов информационной инфраструктуры, включаются следующие требования.

2.5.1. Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств.

2.5.2. Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают участие службы информационной безопасности в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры.

2.5.3. Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий.

2.5.4. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают: наличие эксплуатационной документации на используемые технические средства защиты информации;
контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации;
восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе.

2.5.5. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры.

2.5.5.1. Оператору по переводу денежных средств, оператору услуг платежной инфраструктуры на стадиях создания и эксплуатации объектов информационной инфраструктуры необходимо обеспечить:
использование для осуществления переводов денежных средств прикладного программного обеспечения автоматизированных систем и приложений, сертифицированных в системе сертификации Федеральной службы по техническому и экспортному

контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом 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);
ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Для проведения анализа уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений оператору по переводу денежных средств, оператору услуг платежной инфраструктуры следует привлекать организацию, имеющую 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 - постановление Правительства Российской Федерации № 79).

При модернизации объектов информационной инфраструктуры по решению оператора по переводу денежных средств, оператора услуг платежной инфраструктуры проводится анализ уязвимостей только объектов информационной инфраструктуры, подвергнутых модернизации.

2.5.6. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают:
реализацию запрета несанкционированного копирования защищаемой информации;
защиту резервных копий защищаемой информации;
уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, правилами платежной системы и (или) договорами, заключенными оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором платежной системы, оператором услуг платежной инфраструктуры;
уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления.

2.5.7. При разработке программного обеспечения, предназначенного для использования клиентом при осуществлении переводов денежных средств, самостоятельно или с привлечением сторонних организаций, а также при разработке изменений указанного программного обеспечения оператор по переводу денежных средств обеспечивает реализацию в указанном программном обеспечении функций, связанных: с выполнением требований к защите информации при осуществлении переводов денежных средств;
с предотвращением несанкционированного доступа к защищаемой информации, передаваемой по информационно-телекоммуникационным сетям, в частности, по сети «Интернет».

Оператор по переводу денежных средств контролирует реализацию указанных функций при разработке программного обеспечения с привлечением сторонней организации, а также при закупке готового к использованию без дополнительной доработки программного обеспечения.

2.5.8. В случае если программное обеспечение, используемое клиентом при осуществлении переводов денежных средств, разрабатывалось оператором по переводу денежных средств самостоятельно или с привлечением сторонних организаций:
оператор по переводу денежных средств обеспечивает распространение изменений, вносимых в указанное программное обеспечение, направленных на устранение ставших известными оператору по переводу денежных средств уязвимостей указанного программного обеспечения;
оператор по переводу денежных средств определяет являющиеся актуальными версии указанного программного обеспечения и обеспечивает контроль использования клиентом актуальных версий указанного программного обеспечения.

2.5.9. В случае распространения программного обеспечения, используемого клиентом при осуществлении переводов денежных средств, оператор по переводу денежных средств доводит до клиента инструкцию по эксплуатации (эксплуатационную документацию) данного программного обеспечения и информацию об условиях его эксплуатации либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию) и информацию об условиях эксплуатации данного программного обеспечения.

В случае распространения изменений указанного программного обеспечения оператор по переводу денежных средств вносит соответствующие им изменения в инструкцию по эксплуатации (эксплуатационную документацию) данного программного обеспечения.

2.5.10. Оператор по переводу денежных средств регламентирует и контролирует внесение изменений в программное обеспечение, средства вычислительной техники в составе объектов информационной инфраструктуры, а также в программное обеспечение, используемое клиентом при осуществлении переводов денежных средств;
при этом в обязательном порядке должны вноситься изменения, направленные на устранение ставших известными оператору по переводу денежных средств уязвимостей программного обеспечения, средств вычислительной техники.

2.6. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации при осуществлении доступа к объектам информационной инфраструктуры, включаются следующие требования.

2.6.1. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают учет объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматов и платежных терминалов.

2.6.2. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение некриптографических средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия. Допускается применение некриптографических средств защиты информации от несанкционированного доступа иностранного производства.

2.6.3. При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 настоящего пункта, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают: выполнение процедур идентификации, аутентификации, авторизации своих работников при осуществлении доступа к защищаемой информации;
идентификацию, аутентификацию, авторизацию участников платежной системы при осуществлении переводов денежных средств;
определение порядка использования информации, необходимой для выполнения аутентификации;
регистрацию действий при осуществлении доступа своих работников к защищаемой информации;
регистрацию действий, связанных с назначением и распределением прав доступа к защищаемой информации.

При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 настоящего пункта, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают: выполнение процедур идентификации, аутентификации, авторизации лиц, осуществляющих доступ к программному обеспечению банкоматов и платежных терминалов;
выполнение процедур идентификации и контроль деятельности лиц, осуществляющих техническое обслуживание банкоматов и платежных терминалов;
регистрацию действий, связанных с назначением и распределением прав клиентов, предоставленных им в автоматизированных системах, входящих в состав объектов информационной инфраструктуры и используемых для осуществления переводов денежных средств (далее - автоматизированные системы), и программном обеспечении, входящем в состав объектов информационной инфраструктуры и используемом для осуществления переводов денежных средств (далее - программное обеспечение);
регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения.

Регистрации в соответствии с абзацем одиннадцатым настоящего подпункта подлежит следующая информация о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения: дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента;
набор символов, присвоенный клиенту и позволяющий идентифицировать его в автоматизированной системе, программном обеспечении (далее - идентификатор клиента);
код, соответствующий выполняемому действию;
идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления переводов денежных средств, которой в зависимости от технической возможности является IP-адрес, MAC-адрес, номер SIM-карты, номер телефона и (или) иной идентификатор устройства (далее - идентификатор устройства).

Банковский платежный агент (субагент) обеспечивает регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения, при наличии технической возможности с учетом выполняемого перечня операций и используемых автоматизированных систем, программного обеспечения, эксплуатация которых обеспечивается банковским платежным агентом (субагентом).

Оператор по переводу денежных средств обеспечивает хранение информации, указанной в абзацах тринадцатом - шестнадцатом настоящего подпункта, не менее пяти лет, начиная с даты осуществления клиентом действия, выполняемого с использованием автоматизированной системы, программного обеспечения.

Оператор по переводу денежных средств определяет во внутренних документах: порядок формирования уникального идентификатора клиента в автоматизированной системе, программном обеспечении;
перечень кодов действий клиентов, выполняемых при осуществлении переводов денежных средств с использованием автоматизированной системы, программного обеспечения;
подлежащий регистрации идентификатор устройства;
порядок регистрации и хранения информации, указанной в абзацах тринадцатом - шестнадцатом настоящего подпункта.

Оператор по переводу денежных средств определяет требования к порядку, форме и срокам передачи ему информации о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения, регистрируемой банковскими платежными агентами (субагентами).

При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 настоящего пункта, оператор по переводу денежных средств обеспечивает регистрацию действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов.

2.6.4. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают: реализацию запрета несанкционированного расширения прав доступа к защищаемой информации;

назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации.

2.6.5. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры принимают и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для: контроля физического доступа к объектам информационной инфраструктуры (за исключением банкоматов, платежных терминалов и электронных средств платежа), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, а также доступа в здания и помещения, в которых они размещаются;
предотвращения физического воздействия на средства вычислительной техники, эксплуатация которых обеспечивается оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором услуг платежной инфраструктуры и которые используются для осуществления переводов денежных средств (далее - средства вычислительной техники), и телекоммуникационное оборудование, эксплуатация которого обеспечивается оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором услуг платежной инфраструктуры и которое используется для осуществления переводов денежных средств (далее - телекоммуникационное оборудование), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа;
регистрации доступа к банкоматам, в том числе с использованием систем видеонаблюдения.

2.6.6. В случае принятия оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором услуг платежной инфраструктуры решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, указанных в подпункте 2.6.5 настоящего пункта, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение указанных организационных мер защиты информации и (или) использование указанных технических средств защиты информации.

2.6.7. Утратил силу. - Указание Банка России от 14.08.2014 № 3361-У.

2.6.8. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на предотвращение хищений носителей защищаемой информации.

2.6.9. Оператор по переводу денежных средств обеспечивает возможность приостановления (блокирования) клиентом приема к исполнению распоряжений об осуществлении переводов денежных средств от имени указанного клиента.

2.7. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации от воздействия вредоносного кода, включаются следующие требования.

2.7.1. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают: использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры (далее - технические средства защиты информации от воздействия вредоносного кода), на средствах вычислительной техники, включая банкоматы и платежные терминалы, при наличии технической возможности;
регулярное обновление версий технических средств защиты информации от воздействия вредоносного кода и баз данных, используемых в работе технических средств защиты информации от воздействия вредоносного кода и содержащих описание вредоносных кодов и способы их обезвреживания;
функционирование технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме, при наличии технической возможности.

2.7.2. Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода.

2.7.3. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении переводов денежных средств, при наличии технической возможности.

2.7.4. При наличии технической возможности оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выполнение: предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы;
проверки на отсутствие вредоносного кода средств вычислительной техники, включая банкоматы и платежные терминалы, выполняемой после установки или изменения программного обеспечения.

2.7.5. В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, банковский платежный агент (субагент), оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода.

Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор платежной системы, оператор услуг

платежной инфраструктуры приостанавливают при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом.

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают информирование оператора платежной системы;
оператор платежной системы обеспечивает информирование операторов услуг платежной инфраструктуры и участников платежной системы.

2.8. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств с использованием сети «Интернет» включаются следующие требования.

2.8.1. При использовании сети «Интернет» для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают: применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации, передаваемой по сети «Интернет»;
применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием сети «Интернет»;
применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения;
минимизацию негативных последствий, связанных с несвоевременностью осуществления переводов денежных средств, сбоями или отказами в работе объекта информационной инфраструктуры;
фильтрацию сетевых пакетов при обмене информацией между информационно-телекоммуникационными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью «Интернет» с целью защиты от негативного внешнего воздействия из сети «Интернет».

2.8.2. Оператор по переводу денежных средств обеспечивает идентификацию, аутентификацию и авторизацию клиента при составлении, удостоверении и передаче распоряжений в целях осуществления переводов денежных средств с использованием сети «Интернет», в частности, в следующих системах (далее при совместном упоминании - системы Интернет-банкинга): сайтах в сети «Интернет», используемых клиентом на основании договора с оператором по переводу денежных средств в целях формирования и передачи распоряжений о переводе денежных средств;
системах клиент-серверной архитектуры, передающих информацию через сеть «Интернет» и используемых клиентом в целях формирования и передачи распоряжений о переводе денежных средств (за исключением банкоматов, платежных терминалов и электронных устройств, предназначенных для совершения операций с использованием платежных карт и конструкция которых не предусматривает прием (выдачу) наличных денежных средств).

Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости использования пароля многоразового действия и одноразового кода подтверждения в целях аутентификации клиента при осуществлении переводов денежных средств с использованием системы Интернет-банкинга, а также при подтверждении клиентом права доступа к системе Интернет-банкинга.

В случае принятия соответствующего решения оператор по переводу денежных средств формирует и доводит до клиента информацию, необходимую для генерации одноразового кода подтверждения, или одноразовый код подтверждения, который:
действителен на протяжении ограниченного периода времени, установленного оператором по переводу денежных средств;
используется для подтверждения клиентом права доступа к системе Интернет-банкинга или для подтверждения распоряжения (нескольких распоряжений) о разовом переводе (разовых переводах) денежных средств или распоряжения (договора) о периодических переводах денежных средств в определенную дату и (или) период, при наступлении определенных распоряжением (договором) условий;
однозначно соответствует сеансу использования системы Интернет-банкинга или распоряжению (распоряжениям, договору), подтверждаемому (подтверждаемым) клиентом с использованием системы Интернет-банкинга;
доводится до клиента по альтернативному системе Интернет-банкинга каналу связи, или входит в набор возможных одноразовых кодов подтверждения, который доводится до клиента оператором по переводу денежных средств на материальном носителе, или создается клиентом с использованием технического средства, предназначенного для генерации одноразовых кодов подтверждения.

Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости направления клиенту по альтернативному системе Интернет-банкинга каналу связи сообщения, содержащего сведения о сформированном с использованием системы Интернет-банкинга распоряжении о переводе денежных средств, включая сумму и получателя денежных средств, до подтверждения клиентом указанного распоряжения с использованием одноразового кода подтверждения.

2.8.3. Оператор по переводу денежных средств на основании заявления клиента, переданного способом, определенным договором оператора по переводу денежных средств с клиентом, должен установить ограничения по параметрам операций, которые могут осуществляться клиентом с использованием системы Интернет-банкинга, в том числе указанные в подпункте 2.10.7 пункта 2.10 настоящего Положения.

2.8.4. Оператор по переводу денежных средств при передаче клиенту, являющемуся юридическим лицом, программного обеспечения, предназначенного для осуществления переводов денежных средств с использованием системы Интернет-банкинга, доводит до клиента программное средство контроля целостности указанного программного обеспечения и инструкцию по эксплуатации (эксплуатационную документацию) такого программного средства либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию).

2.8.5. При разработке программного обеспечения, используемого клиентом при осуществлении переводов денежных средств с использованием системы Интернет-банкинга и предназначенного для установки на мобильные устройства клиента (далее - система мобильного банкинга), самостоятельно или с привлечением сторонних организаций, а также при разработке изменений указанного программного обеспечения оператор по переводу денежных средств обеспечивает реализацию функций указанного программного обеспечения, связанных с предотвращением несанкционированного доступа к защищаемой информации, хранимой на мобильном устройстве и обрабатываемой в процессе использования системы мобильного банкинга, либо обеспечивает программную реализацию запрета на запись такой информации в мобильное устройство и ее хранение в мобильном устройстве по окончании сеанса использования системы мобильного банкинга.

2.8.6. Оператор по переводу денежных средств при распространении систем мобильного банкинга с использованием информационных систем (ресурсов), предназначенных, в том числе, для размещения, хранения и распространения с использованием сети «Интернет» программного обеспечения для мобильных устройств (далее - репозитории): осуществляет размещение установочных файлов системы мобильного банкинга в репозитории с указанием в качестве разработчика данной системы оператора по переводу денежных средств либо уполномоченного им разработчика (при этом оператор по переводу денежных средств обеспечивает информирование клиентов об уполномоченных им разработчиках по каналу, альтернативному репозиторию);
обеспечивает выявление в репозитории систем мобильного банкинга, размещенных со ссылкой на оператора по переводу денежных средств без получения согласия оператора по переводу денежных средств, и оперативное уведомление клиентов и лиц, обладающих правами на управление репозиторием, о выявленных случаях размещения указанных систем в соответствии с подпунктом 2.12.3 пункта 2.12 настоящего Положения.

2.8.7. Оператор по переводу денежных средств обеспечивает возможность оперативной блокировки доступа (прекращения использования с целью осуществления переводов денежных средств) клиента к системам Интернет-банкинга на основании уведомления, переданного способом, определенным договором оператора по переводу денежных средств с клиентом, например, на основании: письменного уведомления клиента;
устного уведомления клиента, переданного в соответствии с порядком, установленным оператором по переводу денежных средств;
сообщения (команды), переданного с использованием системы Интернет-банкинга.

2.8.8. Оператор по переводу денежных средств обеспечивает приостановление пересылки клиенту извещений (подтверждений) о принятии к исполнению распоряжений и иной защищаемой информации и осуществления перевода денежных средств на основании сообщений (кодов), отправленных с номера телефона, указанного в договоре с клиентом, в случае если оператору по переводу денежных средств стало известно о признаках, указывающих на изменение: получателя информации, направленной оператором по переводу денежных средств и используемой при аутентификации клиента;
отправителя сообщений (кодов) с номера телефона, указанного в договоре с клиентом, на основании которых осуществляется перевод денежных средств.

К указанным признакам может быть отнесена информация о замене SIM-карты клиента, прекращении обслуживания или смене номера телефона, указанного в договоре с клиентом.

2.9. Защита информации при осуществлении переводов денежных средств с использованием СКЗИ осуществляется в следующем порядке.

2.9.1. Обеспечение защиты информации с помощью СКЗИ осуществляется в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880; 2012, № 29, ст. 3988; 2013, № 14, ст. 1668; № 27, ст. 3463, ст. 3477; 2014, № 11, ст. 1098; № 26, ст. 3390; 2016, № 1, ст. 65; № 26, ст. 3889), Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66, зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года № 6382, 25 мая 2010 года № 17350 (далее - Положение ПКЗ-2005), и технической документацией на СКЗИ.

Обеспечение защиты персональных данных с помощью 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 оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа.

2.9.2. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые: допускают встраивание СКЗИ в технологические процессы осуществления переводов денежных средств, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;
поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
поддерживают непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

2.9.3. В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий:
порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления переводов денежных средств;
порядок эксплуатации СКЗИ;
порядок восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе;
порядок внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ;
порядок снятия с эксплуатации СКЗИ;
порядок управления ключевой системой;
порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей.

2.9.4. Криптографические ключи изготавливаются клиентом (самостоятельно), оператором услуг платежной инфраструктуры и (или) оператором по переводу денежных средств.

Безопасность процессов изготовления криптографических ключей СКЗИ обеспечивается комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.

2.9.5. Оператор платежной системы определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации.

2.10. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации с использованием технологических мер защиты информации, включаются следующие требования.

2.10.1. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают учет и контроль состава установленного и (или) используемого на средствах вычислительной техники программного обеспечения.

2.10.2. Оператор платежной системы определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств. Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанного порядка.

2.10.3. Распоряжение клиента, распоряжение участника платежной системы и распоряжение платежного клирингового центра в электронном виде может быть удостоверено электронной подписью, а также в соответствии с пунктом 3 статьи 847 Гражданского кодекса Российской Федерации (Собрание законодательства Российской Федерации, 1996, № 5, ст. 410) аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом.

2.10.4. При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают: защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации;
контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры;
аутентификацию входных электронных сообщений;
взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями;
восстановление информации об остатках денежных средств на банковских счетах, информации об остатках электронных денежных средств и данных держателей платежных карт в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчетов в платежной системе;
выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации.

2.11. В состав требований к организации и функционированию службы информационной безопасности включаются следующие требования.

2.11.1. Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры: обеспечивают формирование службы информационной безопасности, а также определяют во внутренних документах цели и задачи деятельности этой службы;
предоставляют полномочия и выделяют ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач.

Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры назначают куратора службы информационной безопасности из состава своего органа управления и определяют его полномочия. При этом служба информационной безопасности и служба информатизации (автоматизации) не должны иметь общего куратора.

2.11.2. Оператор по переводу денежных средств, имеющий филиалы: обеспечивает формирование служб информационной

безопасности в указанных филиалах, определяет для них необходимые полномочия и выделяет необходимые ресурсы;
обеспечивает взаимодействие и координацию работ служб информационной безопасности.

2.11.3. Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется следующими полномочиями: осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств;
определять требования к техническим средствам защиты информации и организационным мерам защиты информации;
контролировать выполнение работниками требований к обеспечению защиты информации при осуществлении переводов денежных средств;
участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации;
участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых при восстановлении предоставления услуг платежной системы после сбоев и отказов в работе объектов информационной инфраструктуры.

2.12. В состав требований к повышению осведомленности в области обеспечения защиты информации включаются следующие требования.

2.12.1. Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников в области обеспечения защиты информации: по порядку применения организационных мер защиты информации;
по порядку использования технических средств защиты информации.

2.12.2. Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации.

2.12.3. Оператор по переводу денежных средств обеспечивает доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению, в том числе информации о: рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом осуществлялся перевод денежных средств;
рекомендуемых мерах по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода;
появлении в сети «Интернет» ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых оператором по переводу денежных средств систем Интернет-банкинга, и (или) использующих зарегистрированные товарные знаки и наименование оператора по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения.

2.13. В состав требований к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагирования на них включаются следующие требования.

2.13.1. Оператор платежной системы определяет: требования к порядку, форме и срокам информирования оператора платежной системы, операторов по переводу денежных средств и операторов услуг платежной инфраструктуры о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
информирование оператора платежной системы о выявленных операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры, привлекаемыми для оказания услуг платежной инфраструктуры в платежной системе, инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, осуществляется ежемесячно;
требования к взаимодействию оператора платежной системы, операторов по переводу денежных средств и операторов услуг платежной инфраструктуры в случае выявления в платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанных в настоящем подпункте требований.

2.13.2. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают: применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
информирование службы информационной безопасности, в случае ее наличия, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты.

2.13.3. Оператор платежной системы обеспечивает учет и доступность для операторов по переводу денежных средств,

являющихся участниками платежной системы, и операторов услуг платежной инфраструктуры, привлекаемых для оказания услуг платежной инфраструктуры в платежной системе, информации: о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
о методиках анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

2.13.4. Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают регистрацию самостоятельно выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Оператор по переводу денежных средств обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных клиентами данного оператора по переводу денежных средств.

Оператор по переводу денежных средств обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных банковскими платежными агентами (субагентами).

Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры определяют во внутренних документах порядок регистрации и хранения сведений об инцидентах, указанных в абзацах первом - третьем настоящего подпункта.

2.13.(1) Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры должны осуществлять информирование Банка России:
о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе включенных в перечень типов инцидентов;
о планируемых мероприятиях по раскрытию информации об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, включая размещение информации на официальных сайтах в сети Интернет, выпуск пресс-релизов и проведение пресс-конференций не позднее одного рабочего дня до проведения мероприятия.

Информирование осуществляется в форме предоставления оператором по переводу денежных средств, оператором услуг платежной инфраструктуры 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), и размещается на официальном сайте Банка России в сети «Интернет».

2.14. В состав требований к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств включаются следующие требования.

2.14.1. Документы, составляющие порядок обеспечения защиты информации при осуществлении переводов денежных средств, определяют: состав и порядок применения организационных мер защиты информации;
состав и порядок использования технических средств защиты информации, включая информацию о конфигурации технических средств защиты информации, определяющую параметры их работы;
порядок регистрации и хранения информации на бумажных носителях и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации.

2.14.2. Оператор платежной системы устанавливает распределение обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств путем: самостоятельного определения оператором платежной системы порядка обеспечения защиты информации при осуществлении переводов денежных средств;
распределения обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы;
передачи функций по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств оператором платежной системы, не являющимся кредитной организацией, расчетному центру.

Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают определение порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках распределения обязанностей, установленных оператором платежной системы.

Для определения порядка обеспечения защиты информации при осуществлении переводов денежных средств оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры в рамках обязанностей, установленных оператором платежной системы, могут использовать: положения национальных стандартов по защите информации, стандартов организаций, в том числе стандартов Банка России, рекомендаций в области стандартизации, в том числе рекомендаций Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании;
положения документов, определяемых международными платежными системами;
результаты анализа рисков при обеспечении защиты информации при осуществлении переводов денежных средств на основе моделей угроз и нарушителей безопасности информации, определенных в национальных стандартах по защите информации,

стандартах организаций, в том числе стандартах Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании, или на основе моделей угроз и нарушителей безопасности информации, определенных оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры.

2.14.3. Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств.

2.14.4. Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают назначение лиц, ответственных за выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств.

2.14.5. Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств, включая: контроль (мониторинг) применения организационных мер защиты информации;
контроль (мониторинг) использования технических средств защиты информации.

2.15. В состав требований к оценке выполнения оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств включаются следующие требования.

2.15.1. Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее - оценка соответствия).

Оценка соответствия осуществляется на основе: информации на бумажном носителе и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации;
анализа соответствия порядка применения организационных мер защиты информации и использования технических средств защиты информации требованиям настоящего Положения;
результатов контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств.

Оценка соответствия должна осуществляться оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры с привлечением 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 № 79.

2.15.2. Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России.

Организация, ставшая оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, должна провести первую оценку соответствия в течение шести месяцев после получения соответствующего статуса.

2.15.3. Порядок проведения оценки соответствия и документирования ее результатов определен в приложении 1 к настоящему Положению.

Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры по результатам оценки соответствия в целях ее документального подтверждения формируют отчет, который утверждается исполнительными органами управления и хранится в порядке, установленном соответствующим оператором. Отчет включает сведения о проведении оценки соответствия, в том числе: заполненную форму 1, установленную приложением 1 к настоящему Положению и содержащую оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;
заполненную форму 2, установленную приложением 1 к настоящему Положению и содержащую оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;
сроки проведения оценки соответствия;
сведения о сторонней организации (наименование и местонахождение) в случае ее привлечения оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры для проведения оценки соответствия.

2.15.4. Перечень требований к обеспечению защиты информации при осуществлении переводов денежных средств, выполнение которых проверяется при проведении оценки соответствия, определен в приложении 2 к настоящему Положению.

2.16. В состав требований к доведению оператором по переводу денежных средств, оператором услуг платежной инфраструктуры до оператора платежной системы информации об обеспечении в платежной системе защиты информации при осуществлении переводов денежных средств включаются следующие требования.

2.16.1. Оператор платежной системы устанавливает требования к содержанию, форме и периодичности представления информации, направляемой операторами по переводу денежных средств и операторами услуг платежной инфраструктуры оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств.

Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанных требований.

Оператору национально значимой платежной системы следует уведомлять федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, об установленных требованиях к содержанию, форме и периодичности представления указанной в абзаце первом настоящего подпункта информации в части применения СКЗИ.

2.16.2. Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает следующую информацию: о степени выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;
о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;
о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
о результатах проведенных оценок соответствия;
о выявленных угрозах и уязвимостях в обеспечении защиты информации.

Состав информации, направляемой операционным центром, находящимся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, определяется оператором платежной системы.

2.17. В состав требований к совершенствованию оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств включаются следующие требования.

2.17.1. Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи: с изменениями требований к защите информации, определенных правилами платежной системы;
с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе.

2.17.2. Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях: изменения требований к защите информации, определенных правилами платежной системы;
изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе;
изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств;
выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств;
выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств;
выявления недостатков при проведении оценки соответствия.

2.17.3. Принятие решений оператора по переводу денежных средств, оператора услуг платежной инфраструктуры по совершенствованию защиты информации при осуществлении переводов денежных средств согласуется со службой информационной безопасности.

2.18. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов включаются следующие требования.

2.18.1. Оператор по переводу денежных средств обеспечивает проведение классификации терминальных устройств дистанционного банковского обслуживания, к которым относятся банкоматы и платежные терминалы, используемые при осуществлении переводов денежных средств (далее при совместном упоминании - ТУ ДБО), с учетом следующего: возможностей несанкционированного получения информации, необходимой для осуществления переводов денежных средств;
возможностей осуществления воздействия, приводящего к сбоям, отказам, повреждению ТУ ДБО;
особенностей конструкции ТУ ДБО;
места установки ТУ ДБО.

Оператор по переводу денежных средств фиксирует во внутренних документах отнесение каждого ТУ ДБО к одному из определенных в ходе классификации типов (далее - результаты классификации ТУ ДБО) и проводит пересмотр результатов классификации ТУ ДБО при изменении факторов, влияющих на классификацию ТУ ДБО.

Оператор по переводу денежных средств, наряду с факторами, указанными в абзаце первом пункта 2.3 настоящего Положения, учитывает результаты классификации ТУ ДБО при выборе организационных мер защиты информации, технических средств защиты информации, а также функциональных и конструктивных особенностей ТУ ДБО, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, с целью выполнения требований подпунктов 2.18.3 - 2.18.8 настоящего пункта.

2.18.2. Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости установки на (в) ТУ ДБО технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного оборудования.

2.18.3. Оператор по переводу денежных средств обеспечивает контроль состава объектов информационной инфраструктуры в сегментах информационно-телекоммуникационных сетей, в составе которых присутствуют ТУ ДБО, за исключением случая использования услуг радиотелефонной подвижной связи.

2.18.4. Оператор по переводу денежных средств обеспечивает размещение на лицевой панели ТУ ДБО или в непосредственной близости от ТУ ДБО сведений, включающих: наименование оператора по переводу денежных средств, которому принадлежит ТУ ДБО на правах собственности, аренды, лизинга;
идентификатор ТУ ДБО;
телефонный номер (телефонные номера), адреса электронной почты, предназначенные для связи клиентов, использующих данное ТУ ДБО, с оператором по переводу денежных средств, банковским платежным агентом (субагентом) по вопросам, связанным с использованием данного ТУ ДБО;
порядок действий клиента в случае возникновения подозрения о нарушении порядка штатного функционирования ТУ ДБО, а также в случае выявления признаков событий, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО.

Оператор по переводу денежных средств определяет во внутренних документах порядок работы с заявлениями клиентов о выявленных событиях, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО, и обеспечивает выполнение указанного порядка.

2.18.5. Оператор по переводу денежных средств определяет порядок настройки программного обеспечения, средств вычислительной техники в составе ТУ ДБО, включая информацию о конфигурации, определяющей параметры работы технических средств защиты информации, и обеспечивает выполнение указанного порядка.

2.18.6. Оператор по переводу денежных средств обеспечивает периодический контроль состояния ТУ ДБО с целью выявления событий, влияющих на обеспечение защиты информации при осуществлении переводов денежных средств. К таким событиям, в том числе, относятся: несанкционированное внесение изменений в программное обеспечение ТУ ДБО, включая внедрение вредоносного кода;
несанкционированное внесение изменений в аппаратное обеспечение ТУ ДБО (установка несанкционированного оборудования на (в) ТУ ДБО), включая несанкционированное использование коммуникационных портов;
сбои и отказы в работе технических средств защиты информации, устройств приема платежных карт (при наличии данных устройств), устройств приема наличных денежных средств (при наличии данных устройств), устройств выдачи наличных денежных средств (при наличии данных устройств).

В случае выявления событий, указанных в настоящем подпункте, оператор по переводу денежных средств обеспечивает приведение ТУ ДБО в такое состояние, при котором обслуживание клиентов невозможно, до минимизации возможности наступления негативных последствий выявленных событий или устранения несанкционированных изменений в программном и аппаратном обеспечении ТУ ДБО.

2.18.7. Оператор по переводу денежных средств определяет во внутренних документах и обеспечивает выполнение порядка проведения контроля, предусмотренного подпунктом 2.18.6 настоящего пункта, включая его периодичность, в зависимости от факторов, указанных в абзаце первом пункта 2.3 настоящего Положения, а также в зависимости от: использования систем удаленного мониторинга состояния ТУ ДБО, применения в соответствии с подпунктом 2.18.2 настоящего пункта технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного на (в) ТУ ДБО оборудования;
результатов классификации ТУ ДБО в соответствии с подпунктом 2.18.1 настоящего пункта.

2.18.8. Оператор по переводу денежных средств определяет требования к обеспечению привлеченными к деятельности по оказанию услуг по переводу денежных средств банковскими платежными агентами (субагентами) защиты информации при использовании ТУ ДБО. Банковский платежный агент (субагент) обеспечивает выполнение указанных требований.

2.19. Оператор по переводу денежных средств осуществляет переводы денежных средств с применением расчетных (дебетовых), кредитных карт: оснащенных микропроцессором, оснащенных микропроцессором и магнитной полосой, выданных (эмитированных) кредитными организациями на территории Российской Федерации, срок действия которых начинается после 1 июля 2015 года;
оснащенных магнитной полосой и (или) микропроцессором, выданных (эмитированных) кредитными организациями на территории Российской Федерации, срок действия которых начинается до 1 июля 2015 года.

Глава 3. Порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

3.1. Контроль за соблюдением операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств осуществляется Банком России в следующем порядке:

Банк России проводит проверки операторов платежных систем, являющихся кредитными организациями, операторов услуг платежной инфраструктуры, являющихся кредитными организациями, операторов по переводу денежных средств, являющихся кредитными организациями, и инспекционные проверки операторов платежных систем, не являющихся кредитными организациями, операторов услуг платежной инфраструктуры, не являющихся кредитными организациями;

Банк России запрашивает и получает у операторов платежных систем, операторов услуг платежной инфраструктуры, операторов

по переводу денежных средств документы и информацию, в том числе содержащую персональные данные, о деятельности операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств, связанной с выполнением требований к обеспечению защиты информации при осуществлении переводов денежных средств;
требует разъяснения по полученной информации;

Банк России запрашивает и получает у операторов по переводу денежных средств документы и информацию, в том числе содержащую персональные данные, о деятельности операторов по переводу денежных средств по обеспечению контроля соблюдения банковскими платежными агентами (субагентами), привлекаемыми к деятельности по оказанию услуг по переводу денежных средств, требований к защите информации при осуществлении переводов денежных средств.

3.2. Проверки операторов платежных систем, являющихся кредитными организациями, операторов услуг платежной инфраструктуры, являющихся кредитными организациями, операторов по переводу денежных средств, являющихся кредитными организациями, проводятся на основании 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; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973) в соответствии с порядком, установленным Инструкцией Банка России от 25 августа 2003 года № 105-И «О порядке проведения проверок кредитных организаций (их филиалов) уполномоченными представителями Центрального банка Российской Федерации», зарегистрированной Министерством юстиции Российской Федерации 26 сентября 2003 года № 5118, 28 января 2005 года № 6284, 15 ноября 2006 года № 8479, 23 апреля 2007 года № 9310, 8 октября 2008 года № 12417, 6 апреля 2009 года № 13684, 13 октября 2010 года № 18715, 31 декабря 2010 года № 19515 («Вестник Банка России» от 9 декабря 2003 года № 67, от 9 февраля 2005 года № 7, от 20 декабря 2006 года № 70, от 25 апреля 2007 года № 23, от 15 октября 2008 года № 57, от 15 апреля 2009 года № 23, от 20 октября 2010 года № 57, от 19 января 2011 года № 2).

Указанные проверки могут осуществляться с участием территориального учреждения Банка России (его структурного подразделения, к компетенции которого относятся вопросы защиты информации) по местонахождению кредитной организации (ее филиала).

3.3. Инспекционные проверки операторов платежных систем, не являющихся кредитными организациями, операторов услуг платежной инфраструктуры, не являющихся кредитными организациями, проводятся в соответствии с порядком, установленным Банком России на основании Федерального закона № 161-ФЗ.

Указанные инспекционные проверки могут осуществляться с участием территориального учреждения Банка России (его структурного подразделения, к компетенции которого относятся вопросы защиты информации) по местонахождению оператора платежной системы, не являющегося кредитной организацией, оператора услуг платежной инфраструктуры, не являющегося кредитной организацией.

Глава 4. Заключительные положения

Настоящее Положение подлежит официальному опубликованию в «Вестнике Банка России» и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 31 мая 2012 года № 10) вступает в силу с 1 июля 2012 года.

Председатель Центрального банка
Российской Федерации
С.М.Игнатьев

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 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"

Порядок проведения оценки соответствия и документирования ее результатов

Приложение 2 к Положению 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"

Перечень требований к обеспечению защиты информации при осуществлении переводов денежных средств, выполнение которых проверяется при проведении оценки соответствияи

защита информации в национальной платежной системе, техническая защита информации, сертификация, лицензирование

From:
http://sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://sps-ib.ru/npa:cb382-p_09.06.2012

Last update: **2018/10/29 14:03**