

"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 N 382-П)

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, применяемые для защиты информации при использовании информационно-телекоммуникационной сети Интернет (далее - сеть Интернет) при осуществлении переводов денежных средств;
- 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, банковский платежный агент (субагент), оператор платежной системы, оператор услуг платежной инфраструктуры к инцидентам, связанным с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, относят события, которые возникли вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств и (или) условий осуществления (требований к осуществлению) перевода денежных средств, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, которые установлены оператором по переводу денежных средств и доведены им до клиента, и которые:

- привели к несвоевременности (к нарушению сроков, установленных законодательством Российской Федерации, правилами платежных систем и (или) договорами, заключаемыми клиентами, операторами по переводу денежных средств, операторами услуг платежной инфраструктуры, операторами платежных систем, банковскими платежными агентами (субагентами), участниками платежных систем) осуществления переводов денежных средств;
- привели или могут привести к осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;
- привели к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях клиентов, распоряжениях участников платежной системы, распоряжениях клирингового центра.

2.3. Выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств обеспечивается 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.

2.4. 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.

2.5.6. 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.

2.6. 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. Оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают контроль отсутствия размещения на платежных терминалах и банкоматах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств.

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 отдельную 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, применяемых для защиты информации при использовании сети Интернет при осуществлении переводов денежных средств, 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 доступа к содержанию 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;
- снижение тяжести последствий от воздействий на объекты информационной инфраструктуры с целью создания условий для невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств;
- фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет.

2.8.2. Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.

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

2.9.1. Работы по обеспечению защиты информации с помощью СКЗИ проводятся 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), 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 («Бюллетень нормативных актов федеральных органов исполнительной власти» от 14 марта 2005 года № 11, от 14 июня 2010 года № 24), и технической документацией на СКЗИ.

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.

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 инцидентах 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.

2.14. 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 осуществляется оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры самостоятельно или с привлечением сторонних организаций.

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.

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.

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 09 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

Порядок проведения оценки соответствия и документирования ее результатов

1. Для оценки соответствия используется следующая система оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств:

- требование к обеспечению защиты информации при осуществлении переводов денежных средств

полностью не выполняется - оценке присваивается числовое значение 0;

- требование к обеспечению защиты информации при осуществлении переводов денежных средств выполняется частично - оценке присваивается числовое значение 0.25, 0.5 или 0.75;
- требование к обеспечению защиты информации при осуществлении переводов денежных средств выполняется полностью - оценке присваивается числовое значение 1;
- выполнение требования к обеспечению защиты информации при осуществлении переводов денежных средств не является обязанностью субъекта платежной системы - оценке присваивается символическое значение «н/о» (нет оценки).

2. Оценка выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств определяется на основе следующих общих подходов.

2.1. Для оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств, реализуемых применением организационных мер защиты информации или использованием технических средств защиты информации, используется следующий подход (далее - требования категории проверки 1):

- оценка 0 выставляется, в случае если порядок применения организационных мер защиты информации или использования технических средств защиты информации не определен во внутренних документах оператора по переводу денежных средств, оператора платежных систем, оператора услуг платежной инфраструктуры;
- оценка 0.25 выставляется, в случае если порядок применения организационных мер защиты информации или использования технических средств защиты информации определен во внутренних документах оператора по переводу денежных средств, оператора платежных систем, оператора услуг платежной инфраструктуры, но соответствующие организационные меры защиты информации не применяются, или технические средства защиты информации не используются;
- оценка 0.5 выставляется, в случае если порядок применения организационных мер защиты информации или использования технических средств защиты информации определен во внутренних документах оператора по переводу денежных средств, оператора платежных систем, оператора услуг платежной инфраструктуры, но применение соответствующих организационных мер защиты информации или использование технических средств защиты информации осуществляется не в полном соответствии с указанным порядком;
- оценка 0.75 выставляется, в случае если порядок применения организационных мер защиты информации или использования технических средств защиты информации определен во внутренних документах оператора по переводу денежных средств, оператора платежных систем, оператора услуг платежной инфраструктуры, но применение соответствующих организационных мер защиты информации или использование технических средств защиты информации осуществляется почти в полном соответствии с указанным порядком;
- оценка 1 выставляется, в случае если порядок применения организационных мер защиты

информации или использования технических средств защиты информации определен во внутренних документах оператора по переводу денежных средств, оператора платежных систем, оператора услуг платежной инфраструктуры, и применение соответствующих организационных меры защиты информации и использование технических средств защиты информации осуществляется в полном соответствии с указанным порядком.

2.2. Для оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств, устанавливающих необходимость обеспечения наличия определенного настоящим Положением документа, используется следующий общий подход (далее - требования категории проверки 2):

- оценка 0 выставляется, в случае если документ отсутствует;
- оценка 1 выставляется, в случае если документ имеется в наличии.

2.3. Для оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств, устанавливающих необходимость выполнения определенной настоящим Положением деятельности, используется следующий общий подход (далее - требования категории проверки 3):

- оценка 0 выставляется, в случае если деятельность не выполняется;
- оценка 0.5 выставляется, в случае если деятельность выполняется частично;
- оценка 1 выставляется, в случае если деятельность выполняется полностью.

3. В приложении 2 к настоящему Положению определен перечень требований к обеспечению защиты информации при осуществлении переводов денежных средств с указанием соответствующей им категории проверки.

4. Для документирования результатов оценки соответствия используется следующая форма:

Форма 1. Документирование результатов оценки соответствия

№	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств	Оценка выполнения требования	Факторы, учитываемые при оценке, краткая формулировка обоснования выставленной оценки
1	2	3	4

В графе 2 Формы 1 отражаются формулировки проверяемых требований из перечня требований к обеспечению защиты информации при осуществлении переводов денежных средств, указанных в приложении 2 к настоящему Положению.

В графе 3 Формы 1 отражаются оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;

В графе 4 Формы 1 отражаются факторы, учитываемые при оценке, и краткая формулировка обоснования выставленной оценки.

5. Используя оценки выполнения требований, за исключением требований, по которым выставлены оценки «н/о», вычисляются три обобщающих показателя выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств:

- обобщающий показатель $EV1_{ПС}$ - характеризующий выполнение группы требований к обеспечению защиты информации при осуществлении переводов денежных средств, определенных в пунктах 2.4 - 2.10 настоящего Положения, и вычисляемый как среднее арифметическое оценок выполнения указанных требований, умноженное на корректирующий коэффициент k_1 ;
- обобщающий показатель $EV2_{ПС}$ - характеризующий выполнение группы требований к обеспечению защиты информации при осуществлении переводов денежных средств, определенных в пунктах 2.11 - 2.17 настоящего Положения, и вычисляемый как среднее арифметическое оценок выполнения указанных требований, умноженное на корректирующий коэффициент k_2 ;
- итоговый показатель $R_{ПС}$ - характеризующий выполнение всех требований к обеспечению защиты информации при осуществлении переводов денежных средств и принимаемый равным наименьшему из значений обобщающих показателей $EV1_{ПС}$ и $EV2_{ПС}$.

Точность измерения значений обобщающих показателей при расчете средней арифметической - два знака после запятой.

5.1. Корректирующий коэффициент k_1 определяется по следующим правилам:

- в случае отсутствия требований к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для вычисления обобщающего показателя $EV1_{ПС}$ и которые полностью не выполняются, корректирующий коэффициент k_1 принимается равным 1;
- для случая, когда количество требований к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для вычисления обобщающего показателя $EV1_{ПС}$ и которые полностью не выполняются, больше нуля, но меньше одиннадцати, корректирующий коэффициент k_1 принимается равным 0.85;
- для случая, когда количество требований к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для

вычисления обобщающего показателя $EV1_{ПС}$ и которые полностью не выполняются, больше или равно одиннадцати, корректирующий коэффициент k_1 принимается равным 0.7.

5.2. Корректирующий коэффициент k_2 определяется по следующим правилам:

- в случае отсутствия требований к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для вычисления обобщающего показателя $EV2_{ПС}$ и которые полностью не выполняются, корректирующий коэффициент k_2 принимается равным 1;
- для случая, когда количество требований к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для вычисления обобщающего показателя $EV2_{ПС}$ и которые полностью не выполняются, больше нуля, но меньше шести, корректирующий коэффициент k_2 принимается равным 0.85;
- для случая, когда количество требований к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для вычисления обобщающего показателя $EV2_{ПС}$ и которые полностью не выполняются, больше или равно шести, корректирующий коэффициент k_2 принимается равным 0.7.

6. Для документирования результатов вычисления обобщающих показателей выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств используется следующая форма:

Форма 2. Документирование результатов вычислений обобщающих показателей выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств

Обобщающий показатель	Значение обобщающего показателя
1	2
$EV1_{ПС}$	
$EV2_{ПС}$	
$R_{ПС}$	

В графе 2 Формы 2 отражаются значения обобщающих показателей.

7. На основе вычисленного значения итогового показателя $R_{ПС}$ формируется обобщенное суждение о выполнении субъектом платежной системы требований к обеспечению защиты информации при осуществлении переводов денежных средств в соответствии со следующим общим подходом:

- в случае если значение итогового показателя $R_{ПС}$ больше или равно 0.85, работа по обеспечению защиты информации при осуществлении переводов денежных средств на необходимом уровне

- обеспечивает выполнение установленных требований (значение качественной оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств «хорошая»);
- в случае если значение итогового показателя $R_{ПС}$ больше или равно 0.70 и меньше 0.85, работа по обеспечению защиты информации при осуществлении переводов денежных средств в целом обеспечивает выполнение установленных требований (значение качественной оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств «удовлетворительная»);
 - в случае если значение итогового показателя $R_{ПС}$ больше или равно 0.5 и меньше 0.7, работа по обеспечению защиты информации при осуществлении переводов денежных средств не в полной мере обеспечивает выполнение установленных требований (значение качественной оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств «сомнительная»);
 - в случае если значение итогового показателя $R_{ПС}$ меньше 0.5, работа по обеспечению защиты информации при осуществлении переводов денежных средств не обеспечивает выполнение установленных требований (значение качественной оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств «неудовлетворительная»).

Приложение 2 к Положению Банка России от 09 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 защит

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

№	Номер подпункта настоящего Положения	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств	Категории проверки требования
1	2	3	4
<p>Требования к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для вычисления обобщающего показателя EV 1 ПС</p>			

П.1	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	Требование категории проверки 1
П.2	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по управлению криптографическими ключами	Требование категории проверки 1
П.3	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами 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	Требование категории проверки 1
П.4	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию своих работников, обладающих правами по формированию электронных сообщений	Требование категории проверки 1

П.5	2.4.2	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с созданием (модернизацией) объекта информационной инфраструктуры и эксплуатацией объекта информационной инфраструктуры</p>	Требование категории проверки 1
П.6	2.4.2	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени 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</p>	Требование категории проверки 1
П.7	2.4.3	<p>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 пункта 2.4 настоящего Положения</p>	Требование категории проверки 1

П.8	2.5.1	<p>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</p>	Требование категории проверки 3
П.9	2.5.2	<p>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</p>	Требование категории проверки 3
П.10	2.5.3	<p>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</p>	Требование категории проверки 1

П.11	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	Требование категории проверки 2
П.12	2.5.4	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации	Требование категории проверки 1
П.13	2.5.4	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе	Требование категории проверки 1

П.14	2.5.5	<p>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</p>	Требование категории проверки 1
П.15	2.5.6	<p>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</p>	Требование категории проверки 1
П.16	2.5.6	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают защиту резервных копий защищаемой информации</p>	Требование категории проверки 1

П.17	2.5.6	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают 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</p>	Требование категории проверки 1
П.18	2.5.6	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления</p>	Требование категории проверки 1

П.19	2.6.1	<p>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</p>	Требование категории проверки 1
П.20	2.6.2	<p>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</p>	Требование категории проверки 3
П.21	2.6.3	<p>При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, 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</p>	Требование категории проверки 1

П.22	2.6.3	<p>При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают идентификацию, аутентификацию, авторизацию участников платежной системы при осуществлении переводов денежных средств</p>	Требование категории проверки 1
П.23	2.6.3	<p>При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают определение порядка использования информации, необходимой для выполнения аутентификации</p>	Требование категории проверки 2

П.24	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию действий при осуществлении доступа своих работников к защищаемой информации	Требование категории проверки 1
П.25	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию действий, связанных с назначением и распределением прав доступа к защищаемой информации	Требование категории проверки 1

П.26	2.6.3	<p>При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, 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</p>	Требование категории проверки 1
П.27	2.6.3	<p>При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают выполнение процедур идентификации и контроль деятельности лиц, осуществляющих техническое обслуживание банкоматов и платежных терминалов</p>	Требование категории проверки 1

П.28	2.6.3	<p>При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию действий, связанных с назначением и распределением прав клиентов, предоставленных им в автоматизированных системах и программном обеспечении</p>	Требование категории проверки 1
------	-------	--	---------------------------------

П.29	2.6.3	<p>При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения. Банковским платежным агентом (субагентом) обеспечивается регистрация 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)</p>	Требование категории проверки 1
------	-------	---	---------------------------------

П.29.1	2.6.3	<p>При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию следующей информации о действиях клиента, выполняемых с использованием автоматизированной системы, программного обеспечения:</p> <ul style="list-style-type: none"> • дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента; • идентификатор клиента; • код, соответствующий выполняемому действию; • идентификатор устройства 	Требование категории проверки 1
П.29.2	2.6.3	<p>Оператор по переводу денежных средств обеспечивает хранение информации, указанной в абзацах тринадцатом - шестнадцатом подпункта 2.6.3 пункта 2.6 настоящего Положения, не менее пяти лет, начиная с даты осуществления клиентом действия, выполняемого с использованием автоматизированной системы, программного обеспечения</p>	Требование категории проверки 3

П.29.3	2.6.3	<p>Оператор по переводу денежных средств определяет во внутренних документах:</p> <ul style="list-style-type: none"> • 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 подпункта 2.6.3 пункта 2.6 настоящего Положения 	Требование категории проверки 2
П.29.4	2.6.3	<p>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)</p>	Требование категории проверки 2

П.30	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств обеспечивает регистрацию действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов	Требование категории проверки 1
П.31	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	Требование категории проверки 1
П.32	2.6.4	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации	Требование категории проверки 1

П.33	2.6.5	<p>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), сбоев 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</p>	Требование категории проверки 3
------	-------	---	---------------------------------

П.34	2.6.5	<p>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 предотвращения физического воздействия на средства вычислительной техники и 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</p>	Требование категории проверки 3
П.35	2.6.5	<p>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 регистрации доступа к банкоматам, в том числе с использованием систем видеонаблюдения</p>	Требование категории проверки 3

П.36	2.6.6	<p>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 пункта 2.6 настоящего Положения, 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</p>	Требование категории проверки 1
П.37	2.6.7	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают контроль отсутствия размещения на платежных терминалах и банкоматах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств</p>	Требование категории проверки 1

П.38	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	Требование категории проверки 1
П.39	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	Требование категории проверки 1
П.40	2.7.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают использование технических средств защиты информации от воздействия вредоносного кода на средствах вычислительной техники, включая банкоматы и платежные терминалы, при наличии технической возможности	Требование категории проверки 1

П.41	2.7.1	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают 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</p>	Требование категории проверки 3
П.42	2.7.1	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают функционирование технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме, при наличии технической возможности</p>	Требование категории проверки 3
П.43	2.7.2	<p>Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода</p>	Требование категории проверки 2

П.44	2.7.3	<p>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 отдельную 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</p>	Требование категории проверки 3
П.45	2.7.4	<p>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</p>	Требование категории проверки 3

П.46	2.7.4	<p>При наличии технической возможности оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выполнение проверки на отсутствие вредоносного кода средств вычислительной техники, включая банкоматы и платежные терминалы, выполняемой после установки или изменения программного обеспечения</p>	Требование категории проверки 3
П.47	2.7.5.	<p>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</p>	Требование категории проверки 1
П.48	2.7.5	<p>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 устранение последствий воздействия вредоносного кода</p>	Требование категории проверки 1

П.49	2.7.5	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	Требование категории проверки 1
П.50	2.7.5	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают информирование оператора платежной системы	Требование категории проверки 3
П.51	2.7.5	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор платежной системы обеспечивает информирование операторов услуг платежной инфраструктуры и участников платежной системы	Требование категории проверки 3

П.52	2.8.1	<p>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 доступа к содержанию защищаемой информации, передаваемой по сети Интернет</p>	Требование категории проверки 1
П.53	2.8.1	<p>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 на объектах информационной инфраструктуры с использованием сети Интернет</p>	Требование категории проверки 1

П.54	2.8.1	<p>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 путем использования уязвимостей программного обеспечения</p>	Требование категории проверки 1
П.55	2.8.1	<p>При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают снижение тяжести последствий от воздействий на объекты информационной инфраструктуры с целью создания условий для невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств</p>	Требование категории проверки 1

П.56	2.8.1	<p>При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет</p>	Требование категории проверки 1
П.57	2.8.2	<p>Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет</p>	Требование категории проверки 3
П.58	2.9.1	<p>Работы по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», 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 и технической документацией на СКЗИ</p>	Требование категории проверки 3

П.59	2.9.1	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	Требование категории проверки 3
П.60	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	Требование категории проверки 3
П.61	2.9.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения	Требование категории проверки 3

П.62	2.9.2	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые 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</p>	Требование категории проверки 3
П.63	2.9.3	<p>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</p>	Требование категории проверки 1

П.64	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 эксплуатации СКЗИ	Требование категории проверки 1
П.65	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 восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе	Требование категории проверки 1
П.66	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 внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ	Требование категории проверки 1

П.67	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 снятия с эксплуатации СКЗИ	Требование категории проверки 1
П.68	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 управления ключевой системой	Требование категории проверки 1
П.69	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 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	Требование категории проверки 2

П.70	2.9.5	Оператор платежной системы определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации	Требование категории проверки 2
П.71	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	Требование категории проверки 1
П.72	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	Требование категории проверки 1
П.73	2.10.2	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанного в подпункте 2.10.2 пункта 2.10 настоящего Положения порядка	Требование категории проверки 3

П.74	2.10.3	<p>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 аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом</p>	Требование категории проверки 3
П.75	2.10.4	<p>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</p>	Требование категории проверки 1
П.76	2.10.4	<p>При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры</p>	Требование категории проверки 1

П.77	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают аутентификацию входных электронных сообщений	Требование категории проверки 1
П.78	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями	Требование категории проверки 1
П.79	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают 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	Требование категории проверки 1

П.80	2.10.4	<p>При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчетов в платежной системе</p>	Требование категории проверки 1
П.81	2.10.4	<p>При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают 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</p>	Требование категории проверки 1
<p>Требования к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для вычисления обобщающего показателя EV 2 ПС</p>			

П.82	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	Требование категории проверки 3
П.83	2.11.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющейся юридическим лицом, оператор услуг платежной инфраструктуры предоставляют полномочия и выделяют ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач	Требование категории проверки 3
П.84	2.11.1	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры назначают куратора службы информационной безопасности из состава своего органа управления и определяют его полномочия	Требование категории проверки 3
П.85	2.11.1	Служба информационной безопасности и служба информатизации (автоматизации) не должны иметь общего куратора	Требование категории проверки 3

П.86	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	Требование категории проверки 3
П.87	2.11.2	Оператор по переводу денежных средств, имеющий филиалы, обеспечивает взаимодействие и координацию работ служб информационной безопасности	Требование категории проверки 1
П.88	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств	Требование категории проверки 3
П.89	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями определять требования к техническим средствам защиты информации и организационным мерам защиты информации	Требование категории проверки 3

П.90	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями контролировать выполнение работниками требований к обеспечению защиты информации при осуществлении переводов денежных средств	Требование категории проверки 3
П.91	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями 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	Требование категории проверки 3

П.92	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями 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	Требование категории проверки 3
П.93	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	Требование категории проверки 1
П.94	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 использования технических средств защиты информации	Требование категории проверки 1

П.95	2.12.2	<p>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</p>	Требование категории проверки 1
П.96	2.12.3	<p>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</p>	Требование категории проверки 3
П.97	2.13.1	<p>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</p>	Требование категории проверки 2

П.98	2.13.1	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	Требование категории проверки 3
П.99	2.13.1	Оператор платежной системы определяет 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	Требование категории проверки 2
П.100	2.13.1	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанных в подпункте 2.13.1 пункта 2.13 настоящего Положения требований	Требование категории проверки 3

П.101	2.13.2	<p>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</p>	Требование категории проверки 1
П.102	2.13.2	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают информирование службы информационной безопасности, в случае ее наличия, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств</p>	Требование категории проверки 3
П.103	2.13.2	<p>Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств</p>	Требование категории проверки 1

П.104	2.1 3 .2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты	Требование категории проверки 3
П.105	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	Требование категории проверки 3

П.106	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 методиках анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Требование категории проверки 3
-------	---------	--	---------------------------------

П.106.1	2.13.4	<p>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)</p>	Требование категории проверки 3
П.106.2	2.13.4	<p>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 подпункта 2.13.4 пункта 2.13 настоящего Положения</p>	Требование категории проверки 2

П.107	2.14.2	<p>Оператор платежной системы устанавливает распределение обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств путем:</p> <ul style="list-style-type: none">• 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	Требование категории проверки 3
-------	--------	---	---------------------------------

П.108	2.14.2	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	Требование категории проверки 3
П.109	2.14.3	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств	Требование категории проверки 3
П.110	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	Требование категории проверки 3
П.111	2.14.5	Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) применения организационных мер защиты информации	Требование категории проверки 1

П.112	2.14.5	Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) использования технических средств защиты информации	Требование категории проверки 1
П.113	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	Требование категории проверки 3
П.113.1	2.15.2	Организация, ставшая оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры должны провести первую оценку соответствия в течение шести месяцев после получения соответствующего статуса	Требование категории проверки 3

П.113.2

2.15.2

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

Требование категории проверки 2

П.114	2.16.1	<p>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</p>	Требование категории проверки 2
П.115	2.16.1	<p>Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанных в подпункте 2.16.1 пункта 2.16 настоящего Положения требований</p>	Требование категории проверки 3
П.116	2.16.2	<p>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 информацию о степени выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств</p>	Требование категории проверки 3

П.117	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 информацию о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств	Требование категории проверки 3
П.118	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 информацию о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Требование категории проверки 3

П.119	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 информацию о результатах проведенных оценок соответствия	Требование категории проверки 3
П.120	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 информацию о выявленных угрозах и уязвимостях в обеспечении защиты информации	Требование категории проверки 3

П.121	2.17.1	<p>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</p>	Требование категории проверки 3
П.122	2.17.1	<p>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, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе</p>	Требование категории проверки 3

П.123	2.17.2	<p>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</p>	Требование категории проверки 3
П.124	2.17.2	<p>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 изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующих отношения в национальной платежной системе</p>	Требование категории проверки 3
П.125	2.17.2	<p>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 порядка обеспечения защиты информации при осуществлении переводов денежных средств</p>	Требование категории проверки 3

П.126	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 выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств	Требование категории проверки 3
П.127	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 выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств	Требование категории проверки 3
П.128	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 выявления недостатков при проведении оценки соответствия	Требование категории проверки 3

П.129	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	Требование категории проверки 3
-------	--------	--	---------------------------------