Приложение № 1
к приказу от "21" июня 2017 г. №110-9

ПОЛОЖЕНИЕ

АКЦИОНЕРНОГО ОБЩЕСТВА «РУНА-БАНК»

О ЗАЩИТЕ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

г. Москва
2017 г.

Оглавление

1. Общие положения

1.1. Настоящее Положение о защите сведений конфиденцального характера при осуществлении переводов денежных средств («Положение») определяет требования по выполнению АО «РУНА-БАНК» («Оператор»), иными участниками, привлекаемыми Оператором на договорной основе к деятельности по оказанию услуг по переводу денежных средств («Участники расчетов»), требований к обеспечению защиты информации ограниченного доступа, включая персональные данные, при осуществлении переводов денежных средств.

Настоящее Положение обязательно к применению Оператором, сотрудниками Оператора, Участниками расчетов и сотрудниками Участников расчетов, привлеченными при обработке сведений конфиденциального характера, при осуществлении переводов денежных средств.

1.2. Положение разработано с учетом требований следующих нормативных правовых актов:

- Конституция РФ;
- Федеральный закон от 27.07.2011 №161-ФЗ «О национальной платежной системе» (со всеми изменениями) (далее – «Закон о национальной платежной системе»);
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (со всеми изменениями) (далее – «Закон о персональных данных»);
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Указ Президента РФ от 06.03.1997 «Об утверждении перечня сведений конфиденциального характера» №188;
- Постановление Правительства РФ от 13.06.2012 №584 «Об утверждении Положения о защите информации в платежной системе»;
- Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств (утв. Банком России 09.06.2012 №382-П) (далее - «Положение №382-П»);
- Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014;
- Указание Банка России «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» от 09.06.2012 №2831-У;
- иные нормативно - правовые акты органов государственной власти;

- Политика информационной безопасности АО «Руна-Банк» (далее – «Политика ИБ»);
- Политика обеспечения безопасности персональных данных, обрабатываемых в АО «РУНА-БАНК»;
- Политика АО «РУНА-БАНК» в отношении обработки персональных данных.

1.3. Настоящее Положение определяет основные требования и базовые подходы, а также общую стратегию системы защиты сведений конфиденцального характера при осуществлении переводов денежных средств.

2. Основные термины и определения.

Для целей настоящего Положения применяются следующие термины и определения:

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Банковский Платежный агент (БПА) – юридическое лицо, неявляющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются Оператором в целях осуществления отдельных банковских операций, на основании заключаемого договора;

Банковский платежный субагент (субагент) - юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются БПА в целях осуществления отдельных банковских операций, на основании заключаемого договора;

Оператор(Банк)– АО «РУНА-БАНК», созданное в соответствии с законодательством Российской Федерации и осуществляющее деятельность оператора по переводу денежных средств;

Оператор по переводу денежных средств - организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств;

Оператор платежной системы - организация, определяющая правила платежной системы, а также выполняющая обязанности, предусмотренные Федеральным законом «О национальной платежной системе»;

Оператор услуг платежной инфраструктуры - операционный центр, платежный клиринговый центр и расчетный центр;

Участник расчетов – оператор по переводу денежных средств, оператор электронных денежных средств, банковский платежный агент, банковский платежный субагент, оператор услуг платежной инфраструктуры, привлекаемые Оператором на

основе договорных отношений к деятельности по оказанию услуг по переводу денежных средств;

3.Требования к обеспечению защиты сведений конфиденцального характера, включая персональные данные при осуществлении переводов денежных средств

3.1. Требования к обеспечению защиты информации, включая персональные данные, при осуществлении переводов денежных средств применяются для обеспечения защиты следующей информации (далее – «Защищаемая информация» или «Информация ограниченного доступа»):

- информации об остатках денежных средств на банковских счетах;
- информации об остатках электронных денежных средств;
- информация о совершенных переводах денежных средств, в том числе информация, содержащаяся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Оператора, Участников расчетов, плательщиков и получателей денежных средств (клиентов), а также в извещениях (подтверждениях), касающихся исполнения распоряжений указанных лиц;
- информация, содержащаяся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов Оператора, Участников расчетов;
- информации о платежных клиринговых позициях;
- информация, необходимая для удостоверения клиентами права распоряжения денежными средствами, в том числе данных держателей платежных карт;
- ключевая информация средств криптографической защиты информации (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;
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащаяобязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств.

3.2. Требования к обеспечению защиты персональных данных и иной защищаемой информации при осуществлении переводов денежных средств Оператором, Участниками расчетов включают в себя:

- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при назначении и распределении функциональных прав и обязанностей (далее - ролей) лиц, связанных с осуществлением переводов денежных средств;

- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;

- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при осуществлении доступа к объектам информационной инфраструктуры, включая требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от несанкционированного доступа;

- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код);

- требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет");

- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании СКЗИ;

- требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (далее - технологические меры защиты информации);

- требования к организации и функционированию подразделения (работников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации (далее - служба информационной безопасности);

- требования к повышению осведомленности работников оператора по переводу денежных средств, банковского платежного агента (субагента), являющегося юридическим лицом, оператора услуг платежной инфраструктуры и клиентов (далее - повышение осведомленности) в области обеспечения защиты информации;

- требования к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагированию на них;

- требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;

- требования к оценке выполнения оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств;

- требования к доведению оператором по переводу денежных средств, оператором услуг платежной инфраструктуры до оператора платежной системы информации об обеспечении в платежной системе защиты информации при осуществлении переводов денежных средств;

- требования к совершенствованию оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств.

4. Комплекс мер по обеспечению защиты сведений конфиденциального характера при осуществлении переводов денежных средств

4.1. Безопасность защищаемой информации, обрабатываемой Оператором, Участником расчетов при осуществлении переводов денежных средств,обеспечивается путем выполнения комплекса правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты информации.

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

- 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;

- 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;

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

4.2. Система защиты информации разрабатывается и реализуется с учетом следующих требований:

- управление доступом к защищаемой информации;
- регистрация и учет инцидентов информационной безопасности;
- обеспечение целостности, конфиденциальности и реализации ограниченного права на доступ к информации;
- иные требования.

Для защиты информации в информационных системах Оператора, Участников расчетов необходимо применять шифровальные (криптографические) средства, а также средства защиты информации от несанкционированного доступа, антивирусной защиты, межсетевого экранирования.

4.3. Выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств обеспечивается следующими способами:

4.3.1 Выбор организационных мер защиты:

- определение во внутренних документах Оператора, Участников расчетов порядка применения организационных мер защиты персональных данных и иной защищаемой информации;
- определение лиц, ответственных за применение организационных мер защиты информации;
- применение организационных мер защиты;
- реализация контроля применения организационных мер защиты информации;

- утверждение Оператором, Участниками расчетов перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- обеспечение использования при осуществлении перевода денежных средств средств защиты информации, прошедших оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- назначение должностных лиц ответственных за организацию обработки и обеспечение безопасности персональных данных;

- обеспечение доступа к содержанию электронного журнала сообщений информационной системы исключительно должностных лиц Оператора, Участника расчетов или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

- обеспечение учёта и хранения материальных носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение персональных данных и иные виды несанкционированного доступа;

4.3 Меры в части обеспечения защиты сведений конфиденцального характера при реализации банковских информационных технологических процессов:

- определение, выполнение, регистрация и контроль процедур использования коммуникационных портов, устройств ввода-вывода информации, съемных машинных носителей и внешних накопителей информации;

- защита электронных платежных сообщений от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации;

- доступ работников Оператора, Участников расчетов только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;

- взаимная (двусторонняя) аутентификация участников обмена электронными сообщениями;

- возможность ввода платежной информации в автоматизированную систему перевода денежных средств только для авторизованных пользователей;

- контроль, направленный на исключение возможности совершения злоумышленных действий ненадлежащими получателями денежных средств (установление ограничений в зависимости от суммы совершаемых операций, контроль отсутствия размещения на используемых платежных терминалах и банкоматах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств и т.д.);

- использование технических средств защиты информации от воздействия вредоносного кода (вируса) различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении переводов денежных средств, при наличии технической возможности;

- Резервное копирование и обеспечение возможности восстановления информации в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

- Фильтрация сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры Оператора,

Участника расчетов, и информационно-телекоммуникационной сетью Интернет;

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

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

- Применение иных организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения.

4.4. Оператор, Участник расчетов на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры, используемых при осуществлении перевода денежных средств, обеспечивают:

- реализацию предотвращения несанкционированного копирования защищаемой информации;

- защиту резервных копий защищаемой информации;

- уничтожение защищаемой информации после достижения целей ее обработки способом, обеспечивающим невозможность ее восстановления;

- сохранение защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, Правилами и (или) договорами, заключенными Оператором, Участником расчетов;

4.5. Оператор, Участник расчетов 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, путем использования ложных (фальсифицированных) ресурсов, включая ресурсы информационно-телекоммуникационной сети Интернет, и рекомендуемых мерах по по защите информации от несанкционированного доступа.

4.6. Оператор, Участник расчетов обеспечивают выполнение требований Стандарта безопасности данных индустрии платежных карт (PCI DSS) не ниже Версии 3.0 и Стандарта безопасности данных платежных приложений (PA-DSS) не ниже Версии 3.0 в

той степени, которая применима к ним в соответствии с распределенными ролями при осуществлении расчетов, при условии необходимости следования этим стандартам в рамках проводимых расчетов.

4.7. 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:

- включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств.

- участие службы информационной безопасности в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры.

- контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий.

- 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.

- реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры.

- 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 Банком;

- уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления.

При разработке программного обеспечения, предназначенного для использования клиентом при осуществлении переводов денежных средств, самостоятельно или с привлечением сторонних организаций, а также при разработке изменений указанного программного обеспечения обеспечивается реализацию в указанном программном обеспечении функций, связанных:

- с выполнением требований к защите информации при осуществлении переводов денежных средств;

- с предотвращением несанкционированного доступа к защищаемой информации, передаваемой по информационно-телекоммуникационным сетям, в частности, по сети "Интернет".

- контроль реализации указанных функций при разработке программного обеспечения с привлечением сторонней организации, а также при закупке готового к использованию без дополнительной доработки программного обеспечения.

- распространение изменений, вносимых в указанное программное обеспечение, направленных на устранение ставших известными Банку уязвимостей указанного программного обеспечения;

Банк определяет являющиеся актуальными версии программного обеспечения и обеспечивает контроль использования клиентом актуальных версий указанного программного обеспечения.

Банк доводит до клиента инструкцию по эксплуатации (эксплуатационную документацию) программного обеспечения и информацию об условиях его эксплуатации либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию) и информацию об условиях эксплуатации данного программного обеспечения, а также изменения такой документации

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

5. Назначении и распределении ролей лиц, связанных с осуществлением переводов денежных средств

5.1. Допуск работников к обработке информации ограниченного доступа и информации о средствах защиты в информационной системе Оператора, Участников расчетов должен осуществляться на основании Перечня должностей, допущенных к обработке информации.

5.2. Работники, осуществляющие обработку защищаемой информации и имеющие к ней доступ,должны быть проинформированы о факте обработки ими информации ограниченного доступа и информации о средствах защиты, а также об особенностях, ответственности и правилах осуществления такой обработки.

5.3. В трудовых договорах, должностных инструкциях или иных документах, определяющих должностные обязанности, работника, допущенного к обработке информации ограниченного доступа и информации о средствах защиты, должны быть предусмотрены:

- обязанность по ознакомлению с правилами по обработке информации в информационной системе;
- обязательство о неразглашении вверенной информации ограниченного доступа;
- ответственность за нарушение требований по защите информации.

5.4. Оператор, Участники расчетов 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;
- по формированию электронных сообщений, содержащих распоряжения об осуществлении переводов денежных средств (далее –«электронные сообщения»).

5.5. Не допускается выполнение 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.

5.6. Право доступа к сведениям конфиденцального характера имеют работники Оператора, Участника расчетов которым такая информация необходима в связи с исполнением ими трудовых обязанностей, в том числе, занимающие следующие должности:

- Единоличный исполнительный орган Оператора,Участника расчетов;
- Главный бухгалтер Оператора, Участника расчетов;
- Сотрудники службы информационной безопасности Оператора, Участника расчетов;
- Иные работники Оператора, Участника расчетов в порядке, предусмотренном п. 5.9.Положения.

5.7. Процедура оформления доступа к защищаемой информации включает в себя:

- ознакомление работника Оператора, Участника расчетов под роспись с настоящим Положением или соответствующим локальным актом о защите персональных данных и иной информации ограниченного доступа Участника оператора;
- истребование от работника Оператора, Участника расчетов письменного обязательства о соблюдении конфиденциальности информации и правил ее обработки.

5.8 Допуск к защищаемой информации работников, не имеющих надлежащим образом оформленного доступа, не допускается.

5.9 В целях выполнения трудовых обязанностей доступ к информации ограниченного доступа может быть предоставлен иному работнику, должность которого не включена в вышеуказанный перечень должностей, на основании приказа единоличного исполнительного органа Оператора, Участника расчетов.

5.10 Работники Оператора, Участника расчетов, виновные в нарушении норм, регулирующих получение, обработку и защиту информации ограниченного доступа и информации о средствах защиты, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

6.Определение порядка доступа к объектам инфраструктуры, обрабатывающим информацию

6.1. Оператор, Участник расчетов осуществляет контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемными носителями данных (USB-накопители, съемные жесткие диски, компакт-диски т.п.) и внешним накопителям информации.

6.2. Оператор, Участник расчетов определяет и документально фиксирует порядок доступа в помещения, в которых размещаются технические средства информационных систем и хранятся носители данных, предусматривающий контроль

доступа в помещения посторонних лиц и наличие препятствий для несанкционированного проникновения в помещения.

Идентификация и аутентификация (проверка подлинности) работника Оператора, Участника расчетов при входе в информационную систему обеспечиваются по идентификатору (коду) и периодически обновляемому паролю.

6.3. При наличии технической возможности количество последовательных неудачных попыток ввода пароля должно быть ограничено от 3 до 5 попыток. При превышении указанного количества средства защиты и механизмы защиты должны блокировать возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства уполномоченного работника структурного подразделения по защите информации.

6.4. Порядок формирования и смены паролей, а также контроля исполнения этих процедур регламентируется разработчиком информационной системы в эксплуатационной документации в инструкциях (руководствах) уполномоченного работника Структурного подразделения по защите информации Оператора, Участника расчетов.

6.5. Регистрация входа/выхода в информационную систему работника является обязательной. В журнале регистрации событий, который ведется в электронном виде, указываются следующие параметры:

- дата и время входа в систему (выхода из системы) работника;
- идентификатор работника, предъявленный при запросе доступа; □
- результат попытки входа: успешная или неуспешная (несанкционированная); □
- идентификатор (адрес) устройства (компьютера), используемого для входа в систему.

6.6. Контроль доступа работников к защищаемым информационным ресурсам в соответствии с правами доступа указанных работников является обязательным.

7. Использование средств криптографической защиты информации (СКЗИ)

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

7.1.1. Работы по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», 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 N 66 и технической документацией на СКЗИ.

7.1.2. В случае если Оператор, Участник расчетов применяют СКЗИ российского

производителя, указанные СКЗИ должны иметь сертификаты соответствия уполномоченного государственного органа.

7.1.3. Оператор, Участник расчетов 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.

7.2. В случае применения СКЗИ Оператор, Участник расчетов 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.

7.3. Криптографические ключи изготавливаются клиентом (самостоятельно), Оператором и (или) Участником расчетов.

7.4. 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.

8.Выявление инцидентов, связанных с нарушением требований к защите информации

8.1. Инциденты информационной безопасности могут подразделяться на внутренние и внешние в зависимости от источника угрозы. Примером источника внутренних инцидентов информационной безопасности являются собственные работники, партнеры или иные организации. Источником внешних инцидентов информационной безопасности могут выступать бывшие работники и третьи лица.

8.2. В организационной структуре Оператора, Участника расчетов создается и поддерживается в актуальном состоянии единый информационный ресурс (базу данных), содержащий информацию об инцидентах информационной безопасности.

8.3. Оператором, Участником расчетов разрабатываются внутренние документы, регламентирующие процедуры обработки инцидентов информационной безопасности, включающие:

- обнаружение инцидентов информационной безопасности;
- информирование об инцидентах информационной безопасности;
- классификацию инцидентов информационной безопасности и оценку ущерба, нанесенного ими;
- реагирование на инцидент информационной безопасности;
- анализ причин инцидентов информационной безопасности и оценку
- результатов реагирования на них (при необходимости с участием внешних экспертов в области информационной безопасности).

8.4. Оператором, Участником расчетов должны быть документально определены обязанности работников по обнаружению, классификации, реагированию, анализу и расследованию инцидентов информационной безопасности.

8.5. Оператор, Участники расчетов принимают меры к обеспечению безопасности, исключающие злоупотребления с использованием карт клиентов, информацией о клиентах или их счетах, при выполнении действий технологического цикла, а именно:

- обеспечить секретность ПИН-кодов на этапах персонализации и выдачи карт;
- выполнять процедуры безопасного распределения ключей, применяемые при персонализации, авторизации, защите данных при переводе денежных средств в соответствии с регламентами работы с ключами и обмена криптографическими ключами;
- применять электронную подпись для входящих и исходящих электронных документов в рамках документооборота.

8.6. Все операции, связанные с обработкой информации по картам и иным платежным документам клиентов, а также с их хранением, персонализацией и уничтожением, должны производиться в помещениях, доступ к которым имеют только

уполномоченные лица Оператора, Участника расчетов.

9.Организация структурного подразделения по защите информации ограниченного доступа

9.1. Для проведения мероприятий по защите персональных данных и иной защищаемой информациии надлежащего контроля за нормальным функционированием системы защиты информации ограниченного доступа Оператор, Участники расчетов обязаны иметь структурное подразделение по защите информации или назначить ответственное лицо - (далее – «структурное подразделение»).

9.2. Структурное подразделение выполняет следующие обязанности:

- организация и проведение мероприятий по обеспечению защиты сведений конфиденцального характера;

- участие в разработке внутренних методик анализа рисков, актуальных угроз;

- выявление и расследование инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;

- периодическое проведение аудита системы защиты информации и ее соответствия требованиям нормативных актов Российской Федерации и внутренних документов Оператора, Участника расчетов;

- оценка обоснованности и эффективности принятых мер по защите персональных

- контроль за предотвращением и (или) прекращением несанкционированного доступа работников, третьих лиц к защищаемой информации.

10. Контроль соблюдения законодательства о защите персональных данных при осуществлении переводов денежных средств

10.1. Участники расчетов в целях обеспечения защиты информации при переводе денежных средств обязаны:

- соблюдать требования Оператора к обеспечению защиты информации;
- выявлять инциденты, связанные с нарушением требований к обеспечению защиты информации, и оперативно реагировать на них;
- сообщать Оператору о случаях нарушения безопасности информации и мерах, принятых по их устранению;
- при получении от Оператора требования об устранении нарушений в срок не более 30 (тридцати) дней устранить все нарушения и уведомить Оператора об исполнении требований;

- осуществлять мероприятия, направленные на выявление угроз безопасности информации, и принимать меры по предотвращению выявленных угроз;

- анализировать уязвимости информационных систем, осуществлять мониторинг законодательства Российской Федерации в области защиты информации и принимать меры к совершенствованию способов и средств защиты информации;

- принимать иные меры, направленные на обеспечение защиты информации, с учетом требований законодательства о защите персональных данных, Постановления Правительства РФ от 13.06.2012 №584 «Об утверждении Положения о защите информации в платежной системе» и Положения №382-П, и данного Положения.

10.2. Участники расчетов обязуются взаимодействовать с Оператором, в частности, своевременнопередавать ему информацию:

- о степени выполнения требований к обеспечению защиты информации;
- о реализации порядка обеспечения защиты информации;
- о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации;
- о выявленных угрозах и уязвимостях в обеспечении защиты информации;
- результаты проведенных оценок соответствия.

10.3. Оператор устанавливает требования к содержанию, форме и периодичности представления информации, направляемой Участниками расчетов для целей анализа обеспечения защиты информации при осуществлении переводов денежных средств.

На основе полученной информации Оператор разрабатывает рекомендации по обеспечению безопасности, которые по необходимости рассылает Участникам расчетов, а также создает и корректирует стратегию обеспечения безопасности при осуществлении переводов денежных средств.

Оператор в праве осуществлять проверки и требовать отчета о соблюдении Участниками расчетов требований к обеспечению защиты при осуществлении переводов денежных средств, не вмешиваясь в их хозяйственную деятельность.

10.4. Участник расчетов вправе отказать Оператору в предоставлении информации, если ее предоставление нарушает права и законные интересы третьих лиц. В случае если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации Оператору были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

10.5. Оператор вправе также требовать предоставления ему доказательств соблюдения Участником расчетов и привлекаемыми им при осуществлении переводов денежных средств третьих лиц требований, установленных Положением №382-П, Закона о персональных данных и настоящего Положения;

10.6 Участник расчетов может быть освобожден от очередной проверки (по усмотрению Оператора), если в текущем году Участником расчетов было получено подтверждение о соответствии стандарту PCI DSS и/или PA-DSS, или если в текущем году Участник расчетов проходил проверку Банка России на соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств согласно Положению №382-П и получил итоговый показатель оценки обеспечения защиты информации не ниже 0,75.

10.7. Информация о выявленных нарушениях и рекомендации по их устранению доводится Оператором до Участника расчетов в письменном виде не позднее 5 (Пяти) рабочих дней с момента проведения проверки с указанием сроков устранения выявленных Оператором нарушений.

10.8. Условия настоящего Положения являются существенными условиями договора, заключаемого между Оператором и Участником расчетов в рамках оказания услуг по переводу денежных средств или информационно – технологического взаимодействия. В случае неисполнения, частичного неисполнения, нарушения Участником расчетов условий настоящего Положения:

10.8.1 Оператор вправе досрочно расторгнуть договор путем уведомления Участника расчетов;

10.8.2 Участник расчетов обязан возместить Оператору причиненные таким нарушением убытки в полном объеме. Для целей настоящего пункта под убытками Оператора подразумеваются, в том числе суммы любых штрафов и взысканий, возложенных уполномоченными органами за нарушение Оператором законодательства о защите персональных данных и иной информации ограниченного доступа, если такое нарушение вызвано действиями Участника расчетов, а также ущерб, вызванный приостановлением (ограничением) деятельности Оператора и ее руководителей вследствие таких действий.

11. Оценка выполнения Оператором, Участником расчетов, требований к обеспечению защиты ПДн и иной защищаемой информации при осуществлении переводов денежных средств

11.1. Оператор, Участник расчетов обеспечивают проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее –«оценка соответствия»).

11.2. Оценка соответствия осуществляется на основе:

- 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 законодательству Российской Федерации;

- результатов контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств.

11.3. Оценка соответствия осуществляется Оператором, Участником расчетов самостоятельно или с привлечением сторонних организаций.

11.4. Оператор, Участник расчетов обеспечивают проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России.

12. Заключительные положения

12.1. Настоящее Положение вступает в силу с даты его утверждения Решением Совета Директоров Оператора и действует бессрочно до замены Положения новой редакцией.

12.2. Новая редакция Положения становится обязательной для Оператора, Участников расчетов с момента опубликования. Участники расчетов самостоятельно отслеживают изменения и/или дополнения к настоящему Положению.

12.3. Вопросы, не урегулированныенастоящим Положением,определяются действующим законодательством РФ в области защиты персональных данных и иной информации при осуществлении переводов денежных средств и могут регулироваться отдельными локальными актами Оператора.

12.4. В случае вступления отдельных пунктов Положения в противоречие с новыми законодательными актами, эти пункты утрачивают юридическую силу до момента внесения изменений в настоящее Положение. Положение продолжает действовать в части, не противоречащей указанным актам.

12.5. Работники Оператора, Участника расчетов, виновные в нарушении норм, регулирующих обработку и защиту персональных данных и иной защищаемой информации, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

12.6 Убытки, причиненные Оператору действиями Участника расчетов или его работников вследствие нарушения законодательства об обработке персональных данных и их защиты, подлежат возмещению Оператору в полном объеме. Убытки включают в себя реальный ущерб и упущенную выгоду, а также размер любых штрафов и иных денежных взысканий, которые могут быть возложены на Оператора органами, уполномоченными в области надзора за соблюдением законодательства о защите информации в платежной системе, обработке и защите персональных данных.

12.7. Убытки, а такжеморальный вред, причиненные субъекту персональных данных вследствие нарушения его прав, предусмотренных Законом о персональных данных,настоящим Положением и иными нормативно –правовыми актами, подлежат возмещению в соответствии с законодательством РФ.