ООО «Цифровой Платеж»
115093, г. Москва, Партийный пер., д.1, корп.57, стр.1, этаж 2, офис 319
ОГРН 1137746565934
ИНН/ КПП 7714909651/ 772501001
www.sendy.land , тел. 8 800 700 25 89

У Т В Е Р Ж Д Е Н О
Приказом Генерального директора
ООО «Цифровой Платеж»
от «23» января 2023 г. № 1/3

Введено в действие с 27.01.2023

ТРЕБОВАНИЯ
по обеспечению информационной безопасности к Участникам и Операторам услуг платежной инфраструктуры Платежной системы «Sendy»

Москва, 2023

Требования по обеспечению информационной безопасности к Участникам и Операторам услуг платежной инфраструктуры Платежной системы «Sendy»

СОДЕРЖАНИЕ

Используемые сокращения 3
Термины и определения 4
1. Общие положения 8
2. Требования к порядку обеспечения защиты информации при осуществлении переводов денежных средств 9
2.1. Назначение и распределение функциональных прав и обязанностей лиц, связанных с осуществлением переводов денежных средств 9
2.2. Обеспечение защиты информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры 10
2.3. Обеспечение защиты информации при осуществлении доступа к объектам информационной инфраструктуры (включая защиту от несанкционированного доступа) …… 11
2.4. Обеспечение защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники 13
2.5. Обеспечение защиты информации при осуществлении переводов денежных средств, при использовании информационно-телекоммуникационной сети Интернет ... 14
2.6. Реализация мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента 14
2.7. Обеспечение защиты информации при осуществлении переводов денежных средств с использованием СКЗИ 17
2.8. Обеспечение защиты информации с использованием организационных мер и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации 20
2.9. Определение и реализация порядка обеспечения защиты информации при осуществлении переводов денежных средств 20
2.10. Совершенствование защиты информации 21
3. Требования к порядку проведения проверки на соответствие требованиям по обеспечению защиты информации 22
4. Организация и обеспечение функционирования службы информационной безопасности 23
5. Применение средств защиты информации 24
6. Выявление инцидентов, связанных с нарушениями требований к обеспечению защиты информации, и реагирование на них 25
7. Обеспечение безопасности при обработке персональных данных 26

8. Информирование Оператора Участниками и Операторами услуг платежной инфраструктуры об обеспечении защиты информации.....27

Используемые сокращения

ИБ	Информационная безопасность
ПО	Программное обеспечение
ПС	Платежная система
СКЗИ	Средства криптографической защиты информации
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

Термины и определения

Банковский платежный агент	Юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются кредитной организацией (Участником ПС «Sendy») в целях осуществления отдельных банковских операций.
Банковский платежный субагент	Юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются банковским платежным агентом в целях осуществления отдельных банковских операций.
Информационная безопасность	Безопасность, связанная с угрозами в информационной сфере.
Инцидент информационной безопасности	Инцидент, связанный с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.
Обмен электронными сообщениями	Получение Операционным центром электронных сообщений, содержащих распоряжения Участников Платежной системы, передача указанных сообщений в Платежный клиринговый центр, Расчетный центр, а также передача извещений (подтверждений) о приеме и об исполнении распоряжений Участников Платежной системы.
Оператор по переводу денежных средств	Организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств.
Оператор электронных денежных средств	Оператор по переводу денежных средств, осуществляющий перевод электронных денежных средств без открытия банковского счета (перевод электронных денежных средств).
Оператор Платежной системы (Оператор)	Организация, определяющая Правила Платежной системы, а также выполняющая иные обязанности, предусмотренные Федеральным законом от 27.06.2011 №161-ФЗ «О национальной платежной

	системе» (далее – Закон №161-ФЗ).
Оператор услуг платежной инфраструктуры	Операционный центр, Платежный клиринговый центр и Расчетный центр.
Операционный центр	Организация, обеспечивающая в рамках Платежной системы для Участников Платежной системы и их клиентов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями.
Перевод денежных средств	Действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика.
Платежная система (ПС «Sendy»)	Совокупность организаций, взаимодействующих по Правилам Платежной системы в целях осуществления перевода денежных средств, включающая Оператора Платежной системы, Операторов услуг платежной инфраструктуры и Участников Платежной системы, из которых как минимум три организации являются Операторами по переводу денежных средств.
Платежный клиринговый центр	Организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках Платежной системы прием к исполнению распоряжений Участников Платежной системы об осуществлении перевода денежных средств и выполнение иных действий, предусмотренных Законом №161-ФЗ.
Пользователь	Лицо или организация, которое использует действующую систему для выполнения конкретной функции.
Правила Платежной системы	Документ (документы), содержащий (содержащие) условия участия в Платежной системе, осуществления перевода денежных средств, оказания услуг платежной инфраструктуры и иные условия, определяемые Оператором Платежной

	системы в соответствии с Законом №161-ФЗ.
Расчетный центр	Организация, созданная в соответствии с законодательством Российской Федерации, и обеспечивающая в рамках Платежной системы исполнение распоряжений Участников Платежной системы посредством списания и зачисления денежных средств по банковским счетам Участников Платежной системы, а также направление подтверждений, касающихся исполнения распоряжений Участников Платежной системы.
Риск нарушения информационной безопасности	Риск, связанный с угрозой ИБ.
Роль	Заранее определенная совокупность правил, устанавливающих допустимое множество действий, выполняемых кем-то или чем-то в рамках определенного процесса.
Угроза информационной безопасности	Угроза нарушения свойств ИБ – доступности, целостности или конфиденциальности информационных активов организации.
Участники Платежной системы (Участники)	Организации, присоединившиеся к Правилам Платежной системы в целях оказания услуг по переводу денежных средств.
Электронные денежные средства	Денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа.
Электронное средство платежа	Средство и(или) способ, позволяющие клиенту Оператора по переводу денежных средств

	составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Требования по обеспечению информационной безопасности к Участникам и Операторам услуг платежной инфраструктуры Платежной системы «Sendy»

1. Общие положения

Настоящие «Требования по обеспечению информационной безопасности к Участникам и Операторам услуг платежной инфраструктуры Платежной системы «Sendy» разработаны в целях реализации требований законодательства Российской Федерации в области защиты информации в Платежной системе «Sendy».

Настоящий документ определяет порядок обеспечения защиты информации в Платежной системе и содержит комплекс требований и рекомендаций по защите информации о переводе денежных средств для Участников и Операторов услуг платежной инфраструктуры Платежной системы «Sendy».

Участники обеспечивают защиту информации о переводе денежных средств, а также о средствах и методах обеспечения информационной безопасности, персональных данных Пользователей и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.

Защита информации в ПС «Sendy» организуется с учетом требований Постановления Правительства Российской Федерации от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе», Положения Банка России от 04.06.2020 № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (далее – Положение №719-П) и Правил ПС «Sendy».

Защита информации обеспечивается путем реализации Участниками организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении информации;
- соблюдение конфиденциальности информации;
- реализацию права на доступ к информации в соответствии с законодательством Российской Федерации.

Требования к обеспечению защиты информации при осуществлении переводов денежных средств применяются для обеспечения защиты следующей информации (далее – защищаемая информация):

- информация, используемая при осуществлении перевода денежных средств, в том числе:
  - информация об остатках денежных средств на банковских счетах Участников;
  - информация об остатках электронных денежных средств;
  - информация о совершенных переводах денежных средств;
  - информация, содержащаяся в распоряжениях клиентов, Участников и Платежного клирингового центра;
  - информация, содержащаяся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников и, в случае применимости, Платежного клирингового центра, а также в извещениях (подтверждениях), касающихся исполнения данных распоряжений;
  - информация, необходимая для удостоверения клиентами права распоряжения денежными средствами;
- информация о совершенных переводах и взаиморасчетах;

- персональные данные клиентов;
- информация, составляющая банковскую тайну;
- информация о средствах и методах обеспечения информационной безопасности в том числе:
  - ключевая информация средств криптографической защиты информации, используемая при осуществлении переводов денежных средств или при электронном документообороте;
  - информация о конфигурации автоматизированных систем, программного обеспечения, телекоммуникационного оборудования, используемого для осуществления переводов денежных средств;
  - иная информация, подлежащая защите, в соответствии с законодательством Российской Федерации.

Работы по обеспечению защиты информации осуществляются Участниками самостоятельно или с привлечением на договорной основе организаций, имеющих лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации и лицензию ФСБ России на деятельность, связанную с использованием СКЗИ.

Контроль и надзор за выполнением требований по защите информации при осуществлении переводов денежных средств осуществляется Банком России в рамках надзора в национальной платежной системе.

Контроль надлежащего обеспечения защиты информации Участниками и Операторами услуг платежной инфраструктуры в соответствии с требованиями Правил Платежной системы осуществляется Отделом информационной безопасности Оператора.

2. Требования к порядку обеспечения защиты информации при осуществлении переводов денежных средств

Требования к порядку обеспечения защиты информации Участниками и Операторами услуг платежной инфраструктуры в Платежной системе входят в состав мероприятий управления рисками в Платежной системе, обеспечения надлежащего уровня бесперебойного функционирования Платежной системы и включают в себя:

2.1. Назначение и распределение функциональных прав и обязанностей лиц, связанных с осуществлением переводов денежных средств

Для обеспечения защиты информации и контроля за качеством обеспечения информационной безопасности в организации Участника должны быть определены роли, связанные с деятельностью по обеспечению защиты информации. Руководство организации Участника должно осуществлять координацию своевременности и качества выполнения ролей, связанных с обеспечением защиты информации.

Участник, 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.

Участник, Оператор услуг платежной инфраструктуры обеспечивают регистрацию своих работников, обладающих правами по формированию электронных сообщений, содержащих распоряжения об осуществлении переводов денежных средств.

Участник, Оператор услуг платежной инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени следующих ролей, связанных:

- с созданием (модернизацией) объекта информационной инфраструктуры и эксплуатацией объекта информационной инфраструктуры;
- с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и эксплуатацией объекта информационной инфраструктуры в части его технического обслуживания и ремонта.

Участник, Оператор услуг платежной инфраструктуры обеспечивают контроль и регистрацию действий лиц, которым назначены роли.

2.2. Обеспечение защиты информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры

Участник, Оператор услуг платежной инфраструктуры обеспечивают:

- включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований по защите информации;
- участие подразделения, ответственного за организацию и контроль обеспечения защиты информации (далее – служба 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, а также сбоев вследствие реализации инцидентов защиты информации;
- реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры.

Участник, Оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают:

- регулярное обновление версий программного обеспечения, используемого в ПС «Sendy»;
- 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 ПС «Sendy» и(или) заключенными договорами;

- уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления;
- протоколирование работы информационных систем, включая средства защиты информации;
- хранение протоколов в течение 3 (трех) месяцев с последующим архивированием;
- хранение архивов протоколов в течение 5 (пяти) лет;
- предоставление доступа к протоколам и архивам только уполномоченным сотрудникам, ответственным за обеспечение информационной безопасности.

2.3. Обеспечение защиты информации при осуществлении доступа к объектам информационной инфраструктуры (включая защиту от несанкционированного доступа)

Участник, 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;
- применение средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия. Допускается применение средств защиты информации от несанкционированного доступа иностранного производства (не криптографических средств);
- выполнение процедур идентификации, аутентификации, авторизации своих работников при осуществлении доступа к защищаемой информации;
- идентификацию, аутентификацию, авторизацию Участников 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;
- реализацию запрета несанкционированного расширения прав доступа к защищаемой информации;
- назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации.

При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и(или) передачи защищаемой информации, в том числе банкоматов и платежных терминалов, Участники обеспечивают:

- выполнение процедур идентификации, аутентификации, авторизации лиц, осуществляющих доступ к программному обеспечению платежных терминалов;
- выполнение процедур идентификации и контроль деятельности лиц, осуществляющих техническое обслуживание платежных терминалов;
- регистрацию действий, связанных с назначением и распределением прав Пользователей, 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 Пользователей, выполняемых с использованием автоматизированных систем программного обеспечения.

Участник, 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 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;
- регистрации доступа к банкоматам и платежным терминалам, в том числе с использованием систем видеонаблюдения.

Идентификация работника Участника при входе в информационную систему обеспечиваются по идентификатору (коду) и периодически обновляемому паролю.

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 службы информационной безопасности.

Порядок формирования и смены паролей, а также контроля исполнения этих процедур регламентируется разработчиком информационной системы в эксплуатационной документации в инструкциях (руководствах) уполномоченного работника службы информационной безопасности.

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

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

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

Участник, Оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на предотвращение хищений носителей защищаемой информации.

Участник 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.

Указанный порядок должен быть разработан структурным подразделением или должностным лицом (работником) Участника, ответственным за обеспечение режима физической безопасности Участника.

2.4. Обеспечение защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники

Участник, Оператор услуг платежной инфраструктуры обеспечивают:

- использование технических средств защиты информации, предназначенных для выявления вредоносного программного кода (далее – вредоносный код) 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;
- использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, а также на межсетевых экранах, при наличии технической возможности.

Участник, 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.

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Участник обеспечивает принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода.

Участник приостанавливает при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом.

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Участник обеспечивает информирование Оператора по адресу электронной почты security@sendy.land, а Оператор, в свою очередь, обеспечивает информирование иных Участников.

2.5. Обеспечение защиты информации при осуществлении переводов денежных средств, при использовании информационно-телекоммуникационной сети Интернет

Участник, Оператор услуг платежной инфраструктуры обеспечивают:

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

Участник, Оператор по переводу денежных средств обеспечивает идентификацию, аутентификацию и авторизацию клиента при составлении, удостоверении и передаче распоряжений в целях осуществления переводов денежных средств с использованием сети «Интернет», в частности, в следующих системах (далее – системы Интернет-банкинга):

- сайтах в сети «Интернет», используемых клиентом на основании договора с Оператором по переводу денежных средств в целях формирования и передачи распоряжений о переводе денежных средств;
- системах клиент-серверной архитектуры, передающих информацию через сеть «Интернет» и используемых клиентом в целях формирования и передачи распоряжений о переводе денежных средств (за исключением банкоматов, платежных терминалов и электронных устройств, предназначенных для совершения операций с использованием платежных карт и конструкция которых не предусматривает прием (выдачу) наличных денежных средств).

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

В случае принятия соответствующего решения Оператор по переводу денежных средств формирует и доводит до клиента информацию, необходимую для генерации одноразового кода подтверждения, или одноразовый код подтверждения, который:

- действителен на протяжении ограниченного периода времени, установленного Оператором по переводу денежных средств;

- используется для подтверждения клиентом права доступа к системе Интернет-банкинга или для подтверждения распоряжения (нескольких распоряжений) о разовом переводе (разовых переводах) денежных средств или распоряжения (договора) о периодических переводах денежных средств в определенную дату и(или) период, при наступлении определенных распоряжением (договором) условий;
- однозначно соответствует сеансу использования системы Интернет-банкинга или распоряжению (распоряжениям, договору), подтверждаемому (подтверждаемым) клиентом с использованием системы Интернет-банкинга;
- доводится до клиента по каналу связи, альтернативному системе Интернет-банкинга, или входит в набор возможных одноразовых кодов подтверждения, который доводится до клиента Оператором по переводу денежных средств на материальном носителе, или создается клиентом с использованием технического средства, предназначенного для генерации одноразовых кодов подтверждения.

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

Участник, Оператор по переводу денежных средств на основании заявления клиента, переданного способом, определенным договором Оператора по переводу денежных средств с клиентом, определяет параметры операций, которые могут осуществляться клиентом с использованием системы Интернет-банкинга, в том числе устанавливает:

- максимальную сумму перевода денежных средств с использованием системы Интернет-банкинга за одну операцию и(или) за определенный период времени (например, один день, один месяц);
- перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга;
- перечень устройств, с использованием которых может осуществляться доступ к системе Интернет-банкинга с целью осуществления переводов денежных средств, на основе идентификаторов указанных устройств;
- перечень услуг, предоставляемых с использованием системы Интернет-банкинга;
- временной период, в который могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга.

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

При разработке программного обеспечения, используемого клиентом при осуществлении переводов денежных средств с использованием системы Интернет-банкинга и предназначенного для установки на мобильные устройства клиента (далее – система мобильного банкинга), самостоятельно или с привлечением сторонних

организаций, а также при разработке изменений указанного программного обеспечения Оператор по переводу денежных средств обеспечивает реализацию функций указанного программного обеспечения, связанных с предотвращением несанкционированного доступа к защищаемой информации, хранимой на мобильном устройстве и обрабатываемой в процессе использования системы мобильного банкинга, либо обеспечивает программную реализацию запрета на запись такой информации в мобильное устройство и ее хранение в мобильном устройстве по окончании сеанса использования системы мобильного банкинга.

Участник, Оператор по переводу денежных средств при распространении систем мобильного банкинга с использованием информационных систем (ресурсов), предназначенных, в том числе, для размещения, хранения и распространения с использованием сети «Интернет» программного обеспечения для мобильных устройств (далее – репозитории):

- осуществляет размещение установочных файлов системы мобильного банкинга в репозитории с указанием в качестве разработчика данной системы Оператора по переводу денежных средств либо уполномоченного им разработчика (при этом Оператор по переводу денежных средств обеспечивает информирование клиентов об уполномоченных им разработчиках по каналу, альтернативному репозиторию);
- обеспечивает выявление в репозитории систем мобильного банкинга, размещенных со ссылкой на Оператора по переводу денежных средств без получения согласия Оператора по переводу денежных средств, и оперативное уведомление клиентов и лиц, обладающих правами на управление репозиторием, о выявленных случаях размещения указанных систем, о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению, в том числе:
  - о рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом осуществлялся перевод денежных средств;
  - о рекомендуемых мерах по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода;
  - о появлении в сети «Интернет» ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых Оператором по переводу денежных средств систем Интернет-банкинга, и(или) использующих зарегистрированные товарные знаки и наименование Оператора по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения.

Оператор по переводу денежных средств обеспечивает возможность оперативной блокировки доступа (прекращения использования с целью осуществления переводов денежных средств) клиента к системам Интернет-банкинга на основании уведомления, переданного способом, определенным договором Оператора по переводу денежных средств с клиентом, например, на основании:

- письменного уведомления клиента;

- устного уведомления клиента, переданного в соответствии с порядком, установленным Оператором по переводу денежных средств;
- сообщения (команды), переданного с использованием системы Интернет-банкинга.

Оператор по переводу денежных средств обеспечивает приостановление пересылки клиенту извещений (подтверждений) о принятии к исполнению распоряжений и иной защищаемой информации, и осуществления перевода денежных средств на основании сообщений (кодов), отправленных с номера телефона, указанного в договоре с клиентом, в случае если Оператору по переводу денежных средств стало известно о признаках, указывающих на изменение:

- получателя информации, направленной Оператором по переводу денежных средств и используемой при аутентификации клиента;
- отправителя сообщений (кодов) с номера телефона, указанного в договоре с клиентом, на основании которых осуществляется перевод денежных средств.

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

2.6. Реализация мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента

Участник обязан выполнять следующие требования в рамках реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента:

- выявлять операции по переводу денежных средств, соответствующие признакам осуществления перевода денежных средств без согласия клиента;
- выявлять операции по переводу денежных средств, совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры оператора по переводу денежных средств;
- выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и(или) их клиентов, которые могут привести к случаям и(или) попыткам осуществления переводов денежных средств без согласия клиента;
- осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и(или) их клиентов, при их наличии;
- осуществлять сбор сведений об обращении плательщика в правоохранительные органы при их наличии;
- рассматривать случаи и(или) попытки осуществления переводов денежных средств без согласия клиента, вызванные компьютерными атаками, направленные на объекты информационной инфраструктуры участников информационного обмена;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и(или) их клиентов, и дальнейшему предотвращению случаев и(или) попыток осуществления переводов денежных средств без согласия клиента;
- определять в документах, регламентирующих процедуры управления рисками,

процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объема совершаемых клиентами оператора по переводу денежных средств операций (осуществляемой клиентами деятельности) в соответствии с ч.5.1 ст.8 Закона №161-ФЗ;

- реализовывать в отношении клиента - получателя средств, в адрес которого ранее совершались операции по переводу денежных средств без согласия клиента, в случаях, предусмотренных договором банковского счета, ограничения по параметрам операций по осуществлению переводов денежных средств (переводов электронных денежных средств) с использованием платежных карт, а также ограничения на получение наличных денежных средств в банкоматах за одну операцию и(или) за определенный период времени;
- использовать выявленную оператором по переводу денежных средств информацию о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры оператора по переводу денежных средств и(или) его клиентов, применительно к своей инфраструктуре в целях противодействия осуществлению переводов денежных средств без согласия клиента.

Оператор услуг платежной инфраструктуры обязан выполнять следующие требования в рамках реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента:

- реализовывать меры по противодействию осуществлению переводов денежных средств без согласия клиента (Участника) в соответствии с порядком, установленным Оператором;
- выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и(или) их клиентов, которые могут привести к случаям и(или) попыткам осуществления переводов денежных средств без согласия клиента;
- рассматривать случаи и(или) попытки осуществления переводов денежных средств без согласия клиента, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры участников информационного обмена;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и(или) их клиентов, и дальнейшему предотвращению случаев и(или) попыток осуществления переводов денежных средств без согласия клиента;
- использовать информацию о переводах без согласия клиента (Участника) для выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента (Участника);
- осуществлять анализ операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента (Участника), в рамках Платежной системы.

2.7. Обеспечение защиты информации при осуществлении переводов денежных средств с использованием СКЗИ

Работы по обеспечению защиты информации при осуществлении переводов денежных средств с использованием СКЗИ проводятся в соответствии с:

- Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- технической документацией на СКЗИ.

В случае использования Участником СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты ФСБ России.

Участник, 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.

В случае применения СКЗИ Участник, Оператор услуг платежной инфраструктуры определяют во внутренних документах:

- 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, а также сбоев вследствие реализации инцидентов защиты информации;
- 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.

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.

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

2.8. Обеспечение защиты информации с использованием организационных мер и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации

Каждый Участник должен самостоятельно обеспечить техническую и технологическую возможность осуществлять свою деятельность в ПС «Sendy» в соответствии с требованиями Правил ПС «Sendy».

Перед началом работы Участник в обязательном порядке проводит процедуры тестирования подключения к ПО ПС «Sendy».

При эксплуатации объектов информационной инфраструктуры Участник, Оператор услуг платежной инфраструктуры обеспечивают:

- учет и контроль состава, установленного и(или) используемого на средствах вычислительной техники, программного обеспечения;
- 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 Пользователей 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 ПС «Sendy»;
- выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий Пользователей при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного Пользователя (подмена авторизованного Пользователя) после выполнения процедуры авторизации.

2.9. Определение и реализация порядка обеспечения защиты информации при осуществлении переводов денежных средств

Оператор самостоятельно определяет порядок обеспечения защиты информации при осуществлении переводов денежных средств, для чего использует:

- 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 Участниками.

Участник, Оператор услуг платежной инфраструктуры обеспечивают:

- выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- назначение лиц, ответственных за выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств.

Служба информационной безопасности Участника, 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.

2.10. Совершенствование защиты информации

Оператор регламентирует пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в связи:

- с изменениями требований к защите информации, определенных Правилами ПС «Sendy»;
- с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе.

Участник, 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 ПС «Sendy»;
- 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.

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

3. Требования к порядку проведения проверки на соответствие требованиям по обеспечению защиты информации

Участники и Операторы услуг платежной инфраструктуры обязаны обеспечить проведение проверки на соответствие требованиям по обеспечению защиты информации.

Оператор в целях обеспечения защиты информации в ПС «Sendy» осуществляет проверку Участников и Операторов услуг платежной инфраструктуры:

- при присоединении к Правилам ПС «Sendy», а также при изменении технологических или организационных условий работы Участника в ПС «Sendy»;
- на плановой основе;
- по решению Оператора при наличии предпосылок к нарушениям требований по защите информации.

Оператор осуществляет контроль за соблюдением Правил ПС «Sendy» Участниками, Операторами услуг платежной инфраструктуры следующими способами:

- рассмотрение обращений, поступивших от клиентов, Участников, Операторов услуг платежной инфраструктуры в отношении действий (бездействий) Участников при оказании услуг;
- рассмотрение обращений, поступивших от Участников в отношении действий (бездействий) Операторов услуг платежной инфраструктуры при оказании услуг;
- получение по запросу Оператора по Согласованным каналам связи информации о деятельности Участника в рамках Платежной системы от самого Участника, иных Участников включая, но не ограничиваясь: финансовую документацию (в том числе публично размещаемую), формы отчетности Банка России кредитной организации, внутреннюю нормативную документацию, в том числе документацию по обеспечению непрерывности и восстановлению деятельности и пр.;
- получение по запросу Оператора по Согласованным каналам связи информации о деятельности Операторов услуг платежной инфраструктуры от самих Операторов услуг платежной инфраструктуры, Участников включая, но не ограничиваясь: финансовую документацию (в том числе публично размещаемую), формы отчетности Банка России кредитной организации, внутреннюю нормативную документацию, в том числе документацию по обеспечению непрерывности и восстановлению деятельности и пр.;
- организация Оператором письменных опросов Участников, Операторов услуг платежной инфраструктуры;
- организация Оператором рабочих встреч, семинаров, теле- и видеоконференций с представителями Участников, Операторов услуг платежной инфраструктуры.

При выявлении нарушений Оператор имеет право направить требование об устранении нарушений, а при повторном нарушении требований по защите информации в течение последних 12 (двенадцати) месяцев или бездействии принять меры вплоть до приостановления/ прекращения участия в ПС «Sendy» или расторжения соответствующего договора с Оператором услуг платежной инфраструктуры. Если такое нарушение требований безопасности ставит под угрозу безопасность других Участников,

то Оператор имеет право без предварительного уведомления приостановить деятельность Участника в ПС «Sendy» до устранения таких нарушений либо прекратить его участие в рамках ПС «Sendy».

Проверке подлежат организационные и технологические процессы, информационные системы и их компоненты, задействованные в осуществлении переводов денежных средств в рамках ПС «Sendy».

При осуществлении проверки, привлекаемой Оператором сторонней организацией, передача защищаемой информации осуществляется на основании соглашения между такой организацией и Оператором, при этом, соглашением должны быть определены обязательства по обеспечению конфиденциальности передаваемой информации и ответственность за их невыполнение.

Участник вправе отказать в предоставлении защищаемой информации в случае, 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 были причинены убытки, такие убытки подлежат возмещению в соответствии с законодательством Российской Федерации.

Проверка проводится на соответствие требованиям, установленным Положением № 719-П и разделом 10 Правил ПС «Sendy».

По результатам проверки соблюдения Участником требований к защите информации Оператор составляет отчет о выявленных несоответствиях. По итогам указанной проверки Оператор имеет право приостановить или прекратить участие соответствующего Участника в ПС «Sendy» либо инициировать процедуру расторжения договора с соответствующим Оператором услуг платежной инфраструктуры.

4. Организация и обеспечение функционирования службы информационной безопасности

Участник и Оператор услуг платежной инфраструктуры:

- обеспечивает формирование службы информационной безопасности, а также определяет во внутренних документах цели и задачи деятельности этой службы;
- предоставляет полномочия и выделяет ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач;
- назначает куратора службы информационной безопасности из состава своего органа управления и определяет его полномочия. Служба информационной безопасности и служба информатизации (автоматизации) не должны иметь общего куратора.

Также, Участник, имеющий филиалы, обеспечивает взаимодействие и координацию работ служб информационной безопасности.

Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации, для чего наделяется следующими полномочиями:

- осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты;
- определять требования к техническим средствам защиты информации и организационным мерам защиты информации;
- контролировать выполнение работниками требований к обеспечению защиты информации;
- реализовывать процессы выявления, идентификации и анализа риска информационной безопасности;

- участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации;
- участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации, применяемых при восстановлении предоставления услуг ПС «Sendy» после сбоев и отказов в работе объектов информационной инфраструктуры, а также сбоев вследствие реализации инцидентов защиты информации.

Участник, 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.

Работникам службы информационной безопасности необходимо произвести проверку должностных обязанностей работников, участвующих в обработке защищаемой информации, на соответствие требованиям раздела 10 Правил ПС «Sendy» и законодательства Российской Федерации по защите информации. В случае выявления несоответствия должностных обязанностей инициировать переработку или корректировку трудовых договоров, должностных инструкций или иных документов, определяющих должностные обязанности.

Допуск работников к обработке защищаемой информации в информационной системе Участника должен осуществляться на основании перечня должностей, допущенных к обработке защищаемой информации. В трудовых договорах, должностных инструкциях или иных документах, определяющих должностные обязанности, работника, допущенного к обработке защищаемой информации, должны быть предусмотрены:

- обязанность по ознакомлению с Правилами ПС «Sendy»;
- обязательство о неразглашении вверенной защищаемой информации;
- ответственность за нарушение требований по защите информации.

Работники, осуществляющие обработку информации без использования средств автоматизации, защищаемой информации, должны быть проинформированы об особенностях, ответственности и правилах осуществления такой обработки.

Работники Участника, виновные в нарушении норм, регулирующих получение, обработку и обеспечение безопасности защищаемой информации, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

5. Применение средств защиты информации

Для защиты информации Участниками применяются технические средства защиты информации от несанкционированного доступа (далее – средства от НСД), средства антивирусной защиты и межсетевого экранирования, а также СКЗИ.

Средства от НСД должны включать функционал:

- регистрации действий, связанных с назначением и распределением прав Пользователей;
- регистрации действий Пользователей, выполняемых с использованием автоматизированных систем/ программного обеспечения;
- регистрации действий с информацией, используемой при переводах денежных средств.

Применяемые средства антивирусной защиты должны иметь возможность регулярного обновления, обеспечивать защиту от всех известных видов вредоносного программного обеспечения, а также функционировать в автоматическом режиме. Для защиты от вредоносного программного обеспечения необходимо использовать средства антивирусной защиты различных производителей. Конфигурация средств антивирусной защиты должна предусматривать невозможность отключения/ изменения ее Пользователем.

Для криптографической защиты информации в ПС «Sendy» применяются:

- криптографический алгоритм ECDSA с длиной ключа не менее 320 бит;
- криптографический алгоритм ГОСТ 28147-89, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012;
- криптографические протоколы SSL, SSH, HTTPS.

При информационном обмене между Оператором и Участником, все электронные документы сопровождаются электронной подписью стороны, сформировавшей документ, и передаются в зашифрованном виде в порядке, установленном «Правилами электронного документооборота в Платежной системе «Sendy».

Участники самостоятельно обеспечивают защиту информации внутри своей корпоративной информационной системы.

Для повышения защищенности информационных систем, обеспечивающих работу ПС «Sendy», Участники внедряют, по возможности, системы обнаружения и предотвращения вторжений и средства анализа защищенности объектов информатизации, а также проводят периодический анализ уязвимостей информационных систем. Кроме того, Участники обеспечивают, по возможности, внедрение на объектах информатизации систем видеонаблюдения, видеорегистрации и контроля физического доступа.

Оператор организует проведение мероприятий, связанных с минимизацией возможного ущерба от компрометации информации в ПС «Sendy».

6. Выявление инцидентов, связанных с нарушениями требований к обеспечению защиты информации, и реагирование на них

Оператор определяет:

- требования к порядку, форме и срокам информирования Оператора Участниками о выявленных в ПС «Sendy» инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- требования к взаимодействию Оператора и Участников в случае выявления в ПС «Sendy» инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Оператор обеспечивает учет и доступность для Участников информации:

- о выявленных в ПС «Sendy» 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.

Участник обеспечивает:

- 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;

- регистрацию самостоятельно выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- информирование службы информационной безопасности 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.

В организации Участника рекомендуется создать и поддерживать в актуальном состоянии единый информационный ресурс (базу данных), содержащий информацию об инцидентах, связанных с нарушениями требований к обеспечению защиты информации.

В организации Участника должны быть документы, регламентирующие процедуры обработки информации об инцидентах, связанных с нарушениями требований к обеспечению защиты информации, включающие:

- обнаружение инцидентов, связанных с нарушениями требований к обеспечению защиты информации;
- информирование об инцидентах, связанных с нарушениями требований к обеспечению защиты информации;
- классификацию инцидентов, связанных с нарушениями требований к обеспечению защиты информации;
- реагирование на инциденты, связанные с нарушениями требований к обеспечению защиты информации;
- анализ причин инцидентов, связанных с нарушениями требований к обеспечению защиты информации и оценку результатов реагирования на них (при необходимости с участием внешних экспертов в области информационной безопасности).

В организации Участника должны быть документально определены обязанности работников по обнаружению, классификации, реагированию, анализу и расследованию инцидентов, связанных с нарушениями требований к обеспечению защиты информации.

7. Обеспечение безопасности при обработке персональных данных

Система защиты персональных данных включает в себя организационные и(или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также нормативными правовыми актами, принятыми ФСБ

России[1] и ФСТЭК России[2] во исполнение части 4 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

8. Информирование Оператора Участниками и Операторами услуг платежной инфраструктуры об обеспечении защиты информации

Оператор устанавливает требования к содержанию, форме и периодичности представления информации, направляемой Участниками и Операторами услуг платежной инфраструктуры Оператору для целей анализа обеспечения в ПС «Sendy» защиты информации при осуществлении переводов денежных средств.

Участники и Операторы услуг платежной инфраструктуры обеспечивают выполнение указанных требований.

Предоставляемая информация содержит сведения:

- 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, а также о сроках их устранения;
- о наличии лицензий на осуществление лицензируемых видов деятельности в области защиты информации.

На основе полученной информации Оператор разрабатывает рекомендации по обеспечению безопасности, которые, по необходимости, рассылает Участникам и Операторам услуг платежной инфраструктуры.

Оператор устанавливает форму отчетности по обеспечению защиты информации при осуществлении переводов денежных средств (далее – отчетность), срок предоставления отчетности и методику составления отчетности, руководствуясь Указанием Банка России от 12.01.2022 № 6060-У «О формах и методиках составления, порядке и сроках представления операторами услуг платежной инфраструктуры, операторами по переводу денежных средств отчетности по обеспечению защиты информации при осуществлении переводов денежных средств».

Отчетность по форме 0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств» предоставляется Операторами услуг платежной инфраструктуры, осуществляющими деятельность расчетных центров, Оператору:

---

[1] «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», Приказ ФСБ России от 10.07.2014 № 378.

[2] «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18.02.2013 № 21.

- ежеквартально не позднее 15 (пятнадцатого) рабочего дня месяца, следующего за отчетным кварталом;
- по требованию Оператора – не позднее 15 (пятнадцатого) рабочего дня со дня получения письменного требования Оператора.

Данная отчетность предоставляется по Согласованным каналам связи в текстовом формате.

Оператор может изменить требования к содержанию, форме и периодичности представляемой информации, в порядке, установленном Правилами ПС «Sendy».

Форма и методика составления Операторами услуг платежной инфраструктуры, осуществляющими деятельность расчетных центров, отчетности по форме 0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств» приведены в Правилах ПС «Sendy».