*Анкета*

для проверки соответствия деятельности Банковского Платежного Агента

положению ЦБ РФ от 9 июня 2012 г. N 382-П

О ТРЕБОВАНИЯХ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ И О ПОРЯДКЕ

ОСУЩЕСТВЛЕНИЯ БАНКОМ РОССИИ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ

ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств** | **Есть/Нет** | **Комментарий** |
| П.1 | Банковский платежный агент (субагент) обеспечивает регистрацию лиц, обладающих правами по осуществлению доступа к защищаемой информации |  |  |
| П.2 | Банковский платежный агент (субагент) обеспечивает регистрацию лиц, обладающих правами по управлению криптографическими ключами |  |  |
| П.3 | Банковский платежный агент (субагент) обеспечивает регистрацию лиц, обладающих правами по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа |  |  |
| П.4 | Банковский платежный агент (субагент) обеспечивает регистрацию своих работников, обладающих правами по формированию электронных сообщений |  |  |
| П.5 | Банковский платежный агент (субагент) обеспечивает реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с созданием (модернизацией) объекта информационной инфраструктуры и эксплуатацией объекта информационной инфраструктуры |  |  |
| П.6 | Банковский платежный агент (субагент) обеспечивает реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и эксплуатацией объекта информационной инфраструктуры в части его технического обслуживания и ремонта |  |  |
| П.7 | Банковский платежный агент (субагент) обеспечивает контроль и регистрацию действий лиц, которым назначены роли с 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;  - по формированию электронных сообщений, содержащих распоряжения об осуществлении переводов денежных средств. |  |  |
| П.9 | Банковский платежный агент (субагент), являющийся юридическим лицом, обеспечивает участие службы информационной безопасности в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры |  |  |
| П.10 | Банковский платежный агент (субагент), являющийся юридическим лицом, обеспечивает контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий |  |  |
| П.11 | Банковский платежный агент (субагент) обеспечивает наличие эксплуатационной документации на используемые технические средства защиты информации |  |  |
| П.12 | Банковский платежный агент (субагент) обеспечивает контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации |  |  |
| П.13 | Банковский платежный агент (субагент) обеспечивает восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе |  |  |
| П.14 | Банковский платежный агент (субагент) обеспечивает реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры |  |  |
| П.15 | Банковский платежный агент (субагент) на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивает реализацию запрета несанкционированного копирования защищаемой информации |  |  |
| П.16 | Банковский платежный агент (субагент) на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивает защиту резервных копий защищаемой информации |  |  |
| П.17 | Банковский платежный агент (субагент) на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивает 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 банковским платежным агентом (субагентом). |  |  |
| П.18 | Банковский платежный агент (субагент) на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивает уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления |  |  |
| П.19 | Банковский платежный агент (субагент) обеспечивает учет объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматов и платежных терминалов |  |  |
| П.20 | Банковский платежный агент (субагент) обеспечивает применение некриптографических средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия |  |  |
| П.21 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает выполнение процедур идентификации, аутентификации, авторизации своих работников при осуществлении доступа к защищаемой информации |  |  |
| П.22 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает идентификацию, аутентификацию, авторизацию участников платежной системы при осуществлении переводов денежных средств |  |  |
| П.23 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает определение порядка использования информации, необходимой для выполнения аутентификации |  |  |
| П.24 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает регистрацию действий при осуществлении доступа своих работников к защищаемой информации |  |  |
| П.25 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает регистрацию действий, связанных с назначением и распределением прав доступа к защищаемой информации |  |  |
| П.26 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает выполнение процедур идентификации, аутентификации, авторизации лиц, осуществляющих доступ к программному обеспечению банкоматов и платежных терминалов |  |  |
| П.27 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает выполнение процедур идентификации и контроль деятельности лиц, осуществляющих техническое обслуживание банкоматов и платежных терминалов |  |  |
| П.28 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает регистрацию действий клиентов, выполняемую с использованием программного обеспечения и автоматизированных систем, при наличии технической возможности |  |  |
| П.29 | При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает регистрацию действий, связанных с назначением и распределением прав клиентов, предоставленных им в автоматизированных системах и программном обеспечении, при наличии технической возможности |  |  |
| П.29.1 | Требования данного пункта: При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматах и платежных терминалах, банковский платежный агент (субагент) обеспечивает регистрацию следующей информации о действиях клиентов, выполняемых с использованием автоматизированной системы, программного обеспечения:  -дата (день, месяц, год) и время (часы, минуты, секунды) осуществления -действия клиента; -идентификатор клиента; -код, соответствующий выполняемому действию; -идентификатор устройства |  |  |
| П.31 | Банковский платежный агент (субагент) обеспечивает реализацию запрета несанкционированного расширения прав доступа к защищаемой информации |  |  |
| П.32 | Банковский платежный агент (субагент) обеспечивает назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации |  |  |
| П.33 | Банковский платежный агент (субагент) принимает и фиксирует 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 |  |  |
| П.34 | Банковский платежный агент (субагент) принимает и фиксирует во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для предотвращения физического воздействия на средства вычислительной техники и телекоммуникационное оборудование, сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа |  |  |
| П.35 | Банковский платежный агент (субагент) принимает и фиксирует во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для регистрации доступа к банкоматам, в том числе с использованием систем видеонаблюдения |  |  |
| П.36 | В случае принятия банковским платежным агентом (субагентом) решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для:  - контроля физического доступа к объектам информационной инфраструктуры (за исключением банкоматов, платежных терминалов и электронных средств платежа), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, а также доступа в здания и помещения, в которых они размещаются;  - предотвращения физического воздействия на средства вычислительной техники, эксплуатация которых обеспечивается банковским платежным агентом (субагентом) и которые используются для осуществления переводов денежных средств (далее - средства вычислительной техники), и телекоммуникационное оборудование, эксплуатация которого обеспечивается банковским платежным агентом (субагентом) и которое используется для осуществления переводов денежных средств (далее - телекоммуникационное оборудование), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа;  - регистрации доступа к банкоматам, в том числе с использованием систем видеонаблюдения;  банковский платежный агент (субагент) обеспечивает применение указанных организационных мер защиты информации и (или) использование указанных технических средств защиты информации |  |  |
| П.37 | Банковский платежный агент (субагент) обеспечивает контроль отсутствия размещения на платежных терминалах и банкоматах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств |  |  |
| П.38 | Банковский платежный агент (субагент) обеспечивает принятие мер, направленных на предотвращение хищений носителей защищаемой информации |  |  |
| П.40 | Банковский платежный агент (субагент) обеспечивает использование технических средств защиты информации от воздействия вредоносного кода на средствах вычислительной техники, включая банкоматы и платежные терминалы, при наличии технической возможности |  |  |
| П.41 | Банковский платежный агент (субагент) обеспечивает 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 |  |  |
| П.42 | Банковский платежный агент (субагент) обеспечивает функционирование технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме, при наличии технической возможности |  |  |
| П.44 | Банковский платежный агент (субагент) обеспечивает использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении переводов денежных средств, при наличии технической возможности |  |  |
| П.45 | Банковский платежный агент (субагент) обеспечивает выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы |  |  |
| П.46 | При наличии технической возможности банковский платежный агент (субагент) обеспечивает выполнение проверки на отсутствие вредоносного кода средств вычислительной техники, включая банкоматы и платежные терминалы, выполняемой после установки или изменения программного обеспечения |  |  |
| П.47 | В случае обнаружения вредоносного кода или факта воздействия вредоносного кода банковский платежный агент (субагент) обеспечивает принятие мер, направленных на предотвращение распространения вредоносного кода |  |  |
| П.48 | В случае обнаружения вредоносного кода или факта воздействия вредоносного кода банковский платежный агент (субагент) обеспечивает принятие мер, направленных на устранение последствий воздействия вредоносного кода |  |  |
| П.49 | Банковский платежный агент (субагент) приостанавливает при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом |  |  |
| П.52 | При использовании сети Интернет для осуществления переводов денежных средств банковский платежный агент (субагент) обеспечивает применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения доступа к содержанию защищаемой информации, передаваемой по сети Интернет |  |  |
| П.53 | При использовании сети Интернет для осуществления переводов денежных средств банковский платежный агент (субагент) обеспечивает 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 |  |  |
| П.54 | При использовании сети Интернет для осуществления переводов денежных средств банковский платежный агент (субагент) обеспечивает 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 |  |  |
| П.55 | При использовании сети Интернет для осуществления переводов денежных средств банковский платежный агент (субагент) обеспечивает снижение тяжести последствий от воздействий на объекты информационной инфраструктуры с целью создания условий для невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств |  |  |
| П.56 | При использовании сети Интернет для осуществления переводов денежных средств банковский платежный агент (субагент) обеспечивает фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет |  |  |
| П.58 | Работы по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 и технической документацией на СКЗИ |  |  |
| П.59 | В случае если банковский платежный агент (субагент) применяет СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа. |  |  |
| П.60 | Банковский платежный агент (субагент) применяет 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 |  |  |
| П.61 | Банковский платежный агент (субагент) применяет СКЗИ, которые поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения |  |  |
| П.62 | Банковский платежный агент (субагент) применяет СКЗИ, которые поддерживают непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований |  |  |
| П.63 | В случае применения СКЗИ банковский платежный агент (субагент) определяет 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 |  |  |
| П.64 | В случае применения СКЗИ банковский платежный агент (субагент) определяет во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок эксплуатации СКЗИ |  |  |
| П.65 | В случае применения СКЗИ банковский платежный агент (субагент) определяет во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе |  |  |
| П.66 | В случае применения СКЗИ банковский платежный агент (субагент) определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ |  |  |
| П.67 | В случае применения СКЗИ банковский платежный агент (субагент) определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок снятия с эксплуатации СКЗИ |  |  |
| П.68 | В случае применения СКЗИ банковский платежный агент (субагент) определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок управления ключевой системой |  |  |
| П.69 | В случае применения СКЗИ банковский платежный агент (субагент) определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей |  |  |
| П.71 | Банковский платежный агент (субагент) обеспечивает учет и контроль состава установленного и (или) используемого на средствах вычислительной техники программного обеспечения |  |  |
| П.74 | Распоряжение клиента, распоряжение участника платежной системы и распоряжение платежного клирингового центра в электронном виде может быть удостоверено электронной подписью, а также в соответствии с пунктом 3 статьи 847 Гражданского кодекса Российской Федерации аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом |  |  |
| П.75 | При эксплуатации объектов информационной инфраструктуры банковский платежный агент (субагент) обеспечивает защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации |  |  |
| П.76 | При эксплуатации объектов информационной инфраструктуры банковский платежный агент (субагент) обеспечивает контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры |  |  |
| П.77 | При эксплуатации объектов информационной инфраструктуры банковский платежный агент (субагент) обеспечивает аутентификацию входных электронных сообщений |  |  |
| П.78 | При эксплуатации объектов информационной инфраструктуры банковский платежный агент (субагент) обеспечивает взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями |  |  |
| П.79 | При эксплуатации объектов информационной инфраструктуры банковский платежный агент (субагент) обеспечивает восстановление информации об остатках денежных средств на банковских счетах, информации об остатках электронных денежных средств и данных держателей платежных карт в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники |  |  |
| П.80 | При эксплуатации объектов информационной инфраструктуры банковский платежный агент (субагент) обеспечивает сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчетов в платежной системе |  |  |
| П.81 | При эксплуатации объектов информационной инфраструктуры банковский платежный агент (субагент) обеспечивает выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации |  |  |
| П.82 | Банковский платежный агент (субагент), являющийся юридическим лицом, обеспечивает формирование службы информационной безопасности, а также определяет во внутренних документах цели и задачи деятельности этой службы |  |  |
| П.83 | Банковский платежный агент (субагент), являющийся юридическим лицом, предоставляет полномочия и выделяет ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач |  |  |
| П.88 | Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств |  |  |
| П.89 | Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями определять требования к техническим средствам защиты информации и организационным мерам защиты информации |  |  |
| П.90 | Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями контролировать выполнение работниками требований к обеспечению защиты информации при осуществлении переводов денежных средств |  |  |
| П.91 | Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации |  |  |
| П.92 | Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых при восстановлении предоставления услуг платежной системы после сбоев и отказов в работе объектов информационной инфраструктуры |  |  |
| П.93 | Банковский платежный агент (субагент), являющийся юридическим лицом, обеспечивает повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации |  |  |
| П.94 | Банковский платежный агент (субагент), являющийся юридическим лицом, обеспечивает повышение осведомленности работников в области обеспечения защиты информации по порядку использования технических средств защиты информации |  |  |
| П.95 | Банковский платежный агент (субагент), являющийся юридическим лицом, обеспечивает повышение осведомленности работников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации |  |  |
| П.101 | Банковский платежный агент (субагент) 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 |  |  |
| П.102 | Банковский платежный агент (субагент) обеспечивает информирование службы информационной безопасности, в случае ее наличия, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств |  |  |
| П.103 | Банковский платежный агент (субагент) обеспечивает реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств |  |  |
| П.104 | Банковский платежный агент (субагент) обеспечивает анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты |  |  |
| П.105 | Банковский платежный агент (субагент) обеспечивает проведение классификации терминальных устройств дистанционного банковского обслуживания, к которым относятся банкоматы и платежные терминалы, используемые при осуществлении переводов денежных средств (далее при совместном упоминании - ТУ ДБО), с учетом следующего:  возможностей несанкционированного получения информации, необходимой для осуществления переводов денежных средств;  возможностей осуществления воздействия, приводящего к сбоям, отказам, повреждению ТУ ДБО;  особенностей конструкции ТУ ДБО;  места установки ТУ ДБО. |  |  |
| П.106 | Банковский платежный агент (субагент) фиксирует во внутренних документах отнесение каждого ТУ ДБО к одному из определенных в ходе классификации типов (далее - результаты классификации ТУ ДБО) и проводит пересмотр результатов классификации ТУ ДБО при изменении факторов, влияющих на классификацию ТУ ДБО. |  |  |
| П.107 | Банковский платежный агент (субагент) учитывает результаты классификации ТУ ДБО при выборе организационных мер защиты информации, технических средств защиты информации, а также функциональных и конструктивных особенностей ТУ ДБО, связанных с обеспечением защиты информации при осуществлении переводов денежных средств |  |  |
| П.108 | Банковский платежный агент (субагент) средств принимает и фиксирует во внутренних документах решения о необходимости установки на (в) ТУ ДБО технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного оборудования. |  |  |
| П.109 | Банковский платежный агент (субагент) обеспечивает контроль состава объектов информационной инфраструктуры в сегментах информационно-телекоммуникационных сетей, в составе которых присутствуют ТУ ДБО, за исключением случая использования услуг радиотелефонной подвижной связи. |  |  |
| П.110 | Банковский платежный агент (субагент) обеспечивает размещение на лицевой панели ТУ ДБО или в непосредственной близости от ТУ ДБО сведений, включающих:  наименование банковского платежного агента (субагента), которому принадлежит ТУ ДБО на правах собственности, аренды, лизинга;  идентификатор ТУ ДБО;  телефонный номер (телефонные номера), адреса электронной почты, предназначенные для связи клиентов, использующих данное ТУ ДБО, с банковским платежным агентом (субагентом) по вопросам, связанным с использованием данного ТУ ДБО;  порядок действий клиента в случае возникновения подозрения о нарушении порядка штатного функционирования ТУ ДБО, а также в случае выявления признаков событий, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО. |  |  |
| П.111 | Банковский платежный агент (субагент) определяет во внутренних документах порядок работы с заявлениями клиентов о выявленных событиях, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО, и обеспечивает выполнение указанного порядка. |  |  |
| П.112 | Банковский платежный агент (субагент) определяет порядок настройки программного обеспечения, средств вычислительной техники в составе ТУ ДБО, включая информацию о конфигурации, определяющей параметры работы технических средств защиты информации, и обеспечивает выполнение указанного порядка. |  |  |
| П.113 | Банковский платежный агент (субагент) обеспечивает периодический контроль состояния ТУ ДБО с целью выявления событий, влияющих на обеспечение защиты информации при осуществлении переводов денежных средств. К таким событиям, в том числе, относятся:  несанкционированное внесение изменений в программное обеспечение ТУ ДБО, включая внедрение вредоносного кода;  несанкционированное внесение изменений в аппаратное обеспечение ТУ ДБО (установка несанкционированного оборудования на (в) ТУ ДБО), включая несанкционированное использование коммуникационных портов;  сбои и отказы в работе технических средств защиты информации, устройств приема платежных карт (при наличии данных устройств), устройств приема наличных денежных средств (при наличии данных устройств), устройств выдачи наличных денежных средств (при наличии данных устройств).  В случае выявления событий, указанных в настоящем подпункте, банковский платежный агент (субагент) обеспечивает приведение ТУ ДБО в такое состояние, при котором обслуживание клиентов невозможно, до минимизации возможности наступления негативных последствий выявленных событий или устранения несанкционированных изменений в программном и аппаратном обеспечении ТУ ДБО. |  |  |
| П.114 | Банковский платежный агент (субагент) определяет во внутренних документах и обеспечивает выполнение порядка проведения контроля, предусмотренного п. 113 настоящей анкеты |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ответственное лицо со стороны ФИО / Подпись

Банковского Платежного Агента

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование юридического лица Дата

М.П.