Выписка из «Требований к техническим средствам и программному обеспечению, реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам» * для заказчиков указанных средств

---

* Разработчикам и специализированным организациям необходимо запрашивать полную редакцию документа «Требований к техническим средствам и программному обеспечению, реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам» в Центре защиты информации и специальной связи (8 Центр) ФСБ России и в АО «НСПК»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Введение

Требования к техническим средствам и программному обеспечению реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам (далее – Требования) определяет требования Российской Федерации по информационной безопасности к техническим средствам и программному обеспечению, реализующим криптографические механизмы в:

- аппаратных модулях безопасности информационной инфраструктуры платежных систем (HSM модулях),

- платежных устройствах с терминальным ядром,

- банкоматах,

- платежных картах,

- иных технических средствах информационной инфраструктуры платежной системы, которые разрабатываются и производятся российскими разработчиками с использованием средств криптографической защиты информации, прошедших оценку соответствия требованиям федерального органа исполнительной власти в области обеспечения безопасности (далее – СКЗИ).

Требования не распространяются на использование шифровальных (криптографических) средств и изделий иностранного производства, а также шифровальные (криптографические) средства, реализующие исключительно иностранные криптографические механизмы (то есть криптографические механизмы, не определяемые в документах национальной системы стандартизации в области криптографической защиты информации).

Криптографические механизмы в технических средствах и программном обеспечении информационной инфраструктуры платежных систем должны быть реализованы в СКЗИ.

Средства криптографической защиты информации, используемые в технических средствах и программном обеспечении, должны разрабатываться в соответствии с Положением ПКЗ-2005, утвержденным Приказом ФСБ России от 9 февраля 2005 года № 66 (зарегистрированном в Минюсте России 3 марта 2005 г., регистрационный № 6382).

Предельные числовые значения рассматриваемых в Требованиях механизмов безопасности определяются ФСБ России.

Методики подтверждения указанных в Требованиях свойств и обеспечения противодействия атакам согласуются с ФСБ России.

Требования не могут быть использованы при оценке стойкости иностранных криптографических механизмов, не распространяются на проверку функциональных требований, предъявляемых к техническим средствам и программному обеспечению

информационной инфраструктуры платежных систем, а также на проверку систем защиты от сетевых (компьютерных) атак.

Требования подготовлены взамен Требований к средствам криптографической защиты информации в платежных устройствах с терминальным ядром, серверных компонентах платежных систем (HSM Модулях), платежных карт и иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств, указанных в пункте 2.20 Положения Банка России от 9 июня 2012 г. № 382-П.

Настоящая выписка содержит обобщенные положения Требований и предназначена для заказчиков средств. Для разработчиков и специализированных организаций необходимо руководствоваться действующей редакцией Требований.

1.2. Термины и определения

В Требованиях применяются следующие термины с соответствующими определениями:

Термин	Определение
Аппаратный модуль безопасности информационной инфраструктуры платежных систем (HSM модуль)	Программно-аппаратный комплекс или его части, предназначенный для выполнения криптографических преобразований при проведении платежных операций, управления ключами шифрования и (или) шифрования данных платежных карт, персонализации платежных карт при эмиссии, инициализации платежных терминалов
Безопасный режим работы	Специальный режим работы устройства, при котором загружается минимальный набор драйверов и служб достаточный для администрирования. В таком режиме могут быть изменены настройки и ПО устройства
Двойной контроль	Процесс, в рамках которого двое или более лиц действуют совместно при выполнении критичных функций и/или получения доступа к защищаемой информации. Ни одному лицу не разрешается осуществлять единоличный доступ к защищаемым данным или к материалам (например, к криптографическому ключу), необходимым для выполнения критичных функций, или использовать их. При создании, передаче, вводе, распространении, хранении и восстановлении криптографического ключа вручную двойной контроль требует разделения знания о ключе между задействованными лицами
Доверенное уничтожение	Удаление ключевой информации штатными методами соответствующего СКЗИ без возможности ее восстановления. Удаление производится под двойным контролем администраторов (офицеров безопасности)
Закрытые/открытые ключи	Ключевая пара однозначно математически связанных криптографических ключей, используемых в асимметричной

	криптографической системе и определяющих взаимосвязанные криптографические преобразования. *закрытый ключ:* Сохраняемый в тайне криптографический ключ из ключевой пары *открытый ключ*: Криптографический ключ из ключевой пары, который может быть сделан общедоступным без нарушения стойкости асимметричной криптографической системы, в которой используется данная ключевая пара
Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативно-правовых документов, нормативно-технических документов или требованиями, устанавливаемыми собственником информации
Защищенная клавиатура для ввода ПИН (пин-пад клавиатура, EPP, encrypting PIN pad)	Вид платежного терминала, предназначенный для ввода и обработки ПИН, использования в устройствах самообслуживания, в том числе банкоматах
Значимая платежная система	Платежная система, отвечающая критериям, установленным Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе»
Код верификации карты	Трехзначный (или более) код проверки подлинности платежной карты
Критичные данные аутентификации	Данные, связанные с безопасностью (включая, коды/значения проверки подлинности карты, полное содержимое магнитной полосы карты (с магнитной полосы или ее эквивалента из платежного приложения карты), ПИН-коды), используемые для аутентификации держателей карт и/или авторизации операций по платежным картам
Криптографическиопасная информация	Информация о состояниях СКЗИ, знание которой нарушителем позволяет ему строить алгоритмы определения ключевой информации (или её части) или алгоритмы бесключевого чтения.
Ключи шифрования ДПК	Ключи шифрования защищаемых данных платежной карты
Локальная аутентификация	Процесс аутентификации реализуемый при непосредственном доступе оператора/администратора к устройству без использования каналов связи проходящих вне визуального контроля аутентифицируемого оператора/администратора.
Оператор платежной системы	Организация, определяющая правила платежной системы, а также выполняющая иные обязанности, предусмотренные Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе»
ПИН-код, персональный идентификационный номер, (personal identification number)	Секретный цифровой пароль, известный только держателю платежной карты и владельцу платежной карты (эмитенту), используемый для аутентификации пользователя

Платежная карта	Программно-аппаратный комплекс или его части, предназначенный для обеспечения формирования платежных поручений, находящийся у клиента банка
Платежное устройство с терминальным ядром (платежный терминал)	Программно-аппаратный комплекс или его части, предназначенные для выполнения операций с использованием платежных карт
Сертификат открытого ключа	Электронный документ, содержащий открытый ключ, информацию о владельце ключа, области применения и т.п., подписанный закрытым ключом, чем подтверждается принадлежность открытого ключа владельцу
Тематические исследования	Исследования криптографических, инженерно-криптографических и специальных свойств средств криптографической защиты информации, целью которых является оценка достаточности мер противодействия возможным угрозам безопасности информации, определенным моделью нарушителя, изложенной (указанной) в техническом задании.

В дополнение к указанному списку следует руководствоваться терминами и определениями из документа Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации», Положения ПКЗ-2005, а также ПНСТ 799-2022. «Предварительный национальный стандарт Российской Федерации. Информационные технологии. Криптографическая защита информации. Термины и определения».

1.2. Список используемых сокращений

Сокращение	Определение
АС	Аппаратные средства
АС СКЗИ	Аппаратные средства СКЗИ
АС СФ СКЗИ	Аппаратные средства среды функционирования СКЗИ
ДПК	Данные платежной карты подлежащие защите
ДСЧ	Датчик случайных чисел
ИС	Информационная система
НСД	Несанкционированный доступ
ПДСЧ	Программный датчик случайных чисел
ПИН	ПИН-код
ПМИ	Программы и методики испытаний
ПО	Программное обеспечение

ПО АС СКЗИ	Программное обеспечение аппаратного средства СКЗИ
ПО СКЗИ	Программное обеспечение СКЗИ
ПО АС СФ СКЗИ	Программное обеспечение аппаратных средств среды функционирования СКЗИ
СКЗИ	Средство криптографической защиты информации
СФ	Среда функционирования СКЗИ
ТЗ	Техническое задание
ТКУИ	Технические каналы утечки информации
Усечение	Метод защиты PAN при его хранении путем удаления части цифр PAN
ФДСЧ	Физический датчик случайных чисел
ПО СФ СКЗИ	Программное обеспечение среды функционирования СКЗИ
API	Интерфейс программного приложения (application programming interface)
PAN	Номер платежной карты, отображенный на ее лицевой или обратной стороне (Primary Account Number)
HSM	Аппаратный модуль безопасности информационной инфраструктуры платежных систем (HSM модуль)

2. Структура Требований к техническим средствам и программному обеспечению реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам

Требования содержат описание модели нарушителя, общие принципы построения СКЗИ, требования к мерам безопасности на этапах жизненного цикла, требования к эксплуатационной документации, а также обязательные приложения[1], описывающие специальные требования

- по защите устройств типа HSM и их среды функционирования;
- по защите устройств типа Терминал и их среды функционирования;
- по защите изделий типа банкомат и их среды функционирования;
- по защите устройств типа карта и их среды функционирования.

[1] Приложение №1 Требования к безопасности устройств типа HSM, Приложение №2 Требования к безопасности устройств типа терминал, Приложение №3 Требования к безопасности устройств типа банкомат, Приложение №4 Требования к безопасности устройств типа платежная карта

3. ОБЩЕЕ ОПИСАНИЕ МОДЕЛИ НАРУШИТЕЛЯ ДЛЯ СКЗИ, ИСПОЛЬЗУЕМЫХ В ТЕХНИЧЕСКИХ СРЕДСТВАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПЛАТЕЖНЫХ СИСТЕМ

3.1. Сведения, используемые при создании способов, подготовке и проведении атак

СКЗИ должны противостоять атакам, при создании которых используются следующие сведения:

а) Сведения о СКЗИ:

- общие сведения об информации, используемой в процессе эксплуатации СКЗИ;

- защищенная СКЗИ информация;

- все данные, передаваемые по каналам связи, не защищенным от несанкционированного доступа к информации организационно-техническими мерами;

- сведения, получаемые в результате анализа информативных сигналов;

- документированные и опубликованные возможности ПО СКЗИ, ПО АС СКЗИ и АС СКЗИ;

- сведения конструкторской документации на СКЗИ, в том числе сведения о мерах защиты от внешних воздействий;

- сведения обо всех нарушениях правил пользования СКЗИ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами;

- сведения обо всех неисправностях и сбоях АС СКЗИ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами;

- содержание (эксплуатационной) документации на СКЗИ;

- исходные коды ПО СКЗИ и ПО АС СКЗИ.

б) Сведения о СФ (АС СФ СКЗИ)

- содержание документации на СФ;

- опубликованные возможности и уязвимости ПО СФ СКЗИ, ПО АС СФ СКЗИ и АС СФ СКЗИ;

- сведения обо всех нарушениях правил эксплуатации СФ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами;

- сведения обо всех неисправностях и сбоях АС СФ СКЗИ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами.

в) Сведения о платежной информационной системе:

- общие сведения об ИС, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы ИС;

- документированные и опубликованные сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИС совместно с СКЗИ;

- сведения обо всех сетях связи в составе ИС, работающих на едином криптографическом ключе.

3.2. Технические средства, используемые при создании способов, подготовке и проведении атак

СКЗИ должны противостоять атакам, реализуемым посредством использования следующих средств:

а) штатные средства СКЗИ (ПО СКЗИ, АС СКЗИ, СФ СКЗИ);

б) специально разработанные АС и ПО;

в) средства перехвата и проведения исследований информативных сигналов.

3.3. Формы доступа, используемые при создании способов, подготовке и проведении атак

СКЗИ должны противостоять атакам, реализуемым из-за пределов контролируемой зоны, посредством целенаправленного пассивного и/или активного воздействия на каналы связи технических средств информационной инфраструктуры платежной системы, устройства питания.

СКЗИ должны противостоять атакам, реализуемым нарушителем, имеющим непосредственный доступ к техническим средствам информационной инфраструктуры платежной системы, посредством попыток несанкционированного доступа, с целью компрометации ключа или искажения ПО СФ СКЗИ, ПО СКЗИ, АС СКЗИ и протоколов взаимодействия[2].

4. ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СКЗИ В ТЕХНИЧЕСКИХ СРЕДСТВАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПЛАТЕЖНОЙ СИСТЕМЫ

СКЗИ должно обеспечивать безопасность защищаемой информации при реализации атак в процессе обработки защищаемой информации в технических средствах информационной инфраструктуры платежной системы и/или при условии несанкционированного доступа к защищенной СКЗИ информации в процессе ее хранения или передачи по каналам связи.

При проектировании комплекса средств защиты технических средств информационной инфраструктуры платежной системы необходимо применять подход, при котором выход из строя (отказа или обхода нарушителем) или нарушение работы одного механизма обеспечения безопасности технического средства информационной инфраструктуры платежной системы не должен приводить выходу из строя других механизмов защиты.

К защищаемым данным относятся: ПИН-код, код верификации карты, ключи шифрования, ключи аутентификации, иные криптографические ключи, критичные данные аутентификации, пароли/коды аутентификации, а также в некоторых случаях PAN.

---

[2] Для отдельных видов устройств могут быть определены дополнительные виды атак.

Если используется дистанционное распределение ключей, то устройство должно поддерживать взаимную аутентификацию между отправляющим хостом распространения ключей и принимающим устройством.

Кроме дистанционного распределения ключей, к удаленным административным функциям также относятся:

- Изменение параметров устройства, включая активацию или деактивацию функций устройства, влияющих на его безопасность.
- Удаление журналов транзакций или журналов регистрации событий информационной безопасности (например, ошибок /срабатываний средств защиты от НСД).
- Изменение паролей/кодов аутентификации или данных, позволяющих устройству переходить в безопасный режим работы СКЗИ.

В ТЗ на разработку (модернизацию) СКЗИ могут предъявляться дополнительные требования к СКЗИ, не противоречащие принципам Требований.

СКЗИ считается прошедшим оценку соответствия требованиям, если для ввода СКЗИ в эксплуатацию не требуется проведение дополнительных тематических исследований СКЗИ после получения положительного заключения ФСБ России о соответствии СКЗИ Требованиям и требованиям ФСБ России к СКЗИ соответствующего класса защиты.

В отдельных случаях, при наличии соответствующего обоснования по решению Банка России и ФСБ России может быть разрешена эксплуатация СКЗИ, когда отдельные положения требований по безопасности информации к ним не выполнены.

4.1. Требования к используемым криптографическим механизмам

4.1.1. Общие положения

При разработке (модернизации) СКЗИ должны использоваться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.

Кроме того, с целью обеспечения совместимости с действующими криптографическими средствами могут использоваться криптографические механизмы (включая симметричные и асимметричные алгоритмы, функции хэширования, выработки кода целостности (MAC)), отвечающие международным стандартам (ISO). Корректная реализация и перечень механизмов подтверждается протоколом проведения испытаний в соответствии с ПМИ, согласованной с оператором платежной системы. Перечень необходимых стандартов устанавливает Банк России.

При этом в ходе тематических исследований СКЗИ должно быть обосновано невлияние процессов функционирования криптографических механизмов, отвечающих международным стандартам (ISO), на реализацию криптографических механизмов, утвержденных в качестве

национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографических механизмов, имеющих положительное заключение ФСБ России по результатам их экспертных криптографических исследований.

Криптографические механизмы, а также преобразования, реализующие обработку ключевой информации, ее создание, ввод, выработку и удаление, должны быть реализованы непосредственно в СКЗИ.

4.1.2. Требования к датчикам случайных чисел, выработке и использованию ключевой информации

Датчик (псевдо)случайных чисел является составной частью СКЗИ и должен проходить тематические исследования совместно с СКЗИ, в котором он применяется.

Датчик случайных чисел должен использоваться для генерации случайных (псевдослучайных) последовательностей с целью выработки ключевой информации и/или другой случайной (псевдослучайной) информации, используемой в СКЗИ.

Процесс генерации ключей должно быть невозможно скомпрометировать без сговора как минимум двух доверенных лиц. Достаточность мер защиты информации, направленных на противодействие сговору доверенных лиц при генерации ключей, должна обосновываться в рамках тематических исследований СКЗИ.

Максимальные сроки действия криптографических ключей СКЗИ должны определяться в ТЗ на разработку СКЗИ и могут уточняться в ходе проведения тематических исследований.

При хранении ключевой информации в СКЗИ или доведении ключевой информации до СКЗИ в зашифрованном виде с использованием симметричного шифрования, а также при дистанционном распределении ключей в зашифрованном виде с использованием асимметричного шифрования, СКЗИ должно поддерживать представление ключевой информации в формате ключевых блоков (ключевых контейнеров).

Должен быть реализован метод доверенного уничтожения (стирания) не защищенного от НСД ключа для всех состояний устройства (включено, выключено, в спящем режиме).

В СКЗИ должен быть реализован механизм контроля срока действия криптографических ключей.

4.1.3. Требования к аутентификации субъектов доступа и имитозащите

В СКЗИ технических средств информационной инфраструктуры платежной системы должны быть реализованы криптографические механизмы, удовлетворяющие п. 4.1.1 и обеспечивающие аутентификацию субъектов и/или процессов доступа, осуществляющих доступ или взаимодействующих с СКЗИ.

При этом для обеспечения удаленной аутентификации при организации защищенной передачи данных и для обеспечения аутентификации при взаимодействии с СКЗИ по каналам удаленного управления должны применяться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций

по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.

Использование паролей для аутентификации субъектов доступа (пользователей), являющихся физическими лицами и осуществляющих доступ к техническим средствам информационной инфраструктуры платежной системы, допускается только для локальной аутентификации СКЗИ.

Для проведения локальной аутентификации с целью изменения настроек безопасности, а также загрузки/смены/уничтожения ключей (администрирования) требуется использовать как минимум два аутентифицирующих фактора (знание, владение)[3].

Для обеспечения локальной аутентификации субъектов доступа, являющихся физическими лицами и осуществляющих доступ к СКЗИ во всех объектах информационной инфраструктуры платежных систем (за исключением платежных карт), должна быть реализована ролевая аутентификация субъектов доступа. При этом требуется поддержка следующих ролей:

- роль пользователя, в рамках которой выполняются реализованные в СКЗИ криптографические функции;

- роль привилегированного пользователя, в рамках которой могут выполняться функции управления СКЗИ (настройка, конфигурирование и т.п.).

При аутентификации субъектов доступа, являющихся процессами и осуществляющих взаимодействие с СКЗИ, должен быть реализован криптографический механизм взаимной аутентификации.

Допускается использование механизмов формирования и проверки электронной подписи для обеспечения имитозащиты передаваемых сообщений, достаточность которых должна быть обоснована в рамках тематических исследований СКЗИ. Механизм формирования имитовставки не должны приводить к возможности реализации эффективных атак на конфиденциальность защищаемых данных, что должно быть обосновано в рамках тематических исследований СКЗИ.

4.2. Требования по реализации инженерно-криптографической защиты

Использование инженерно-криптографических механизмов в СКЗИ основывается на следующих принципах:

- Инженерно-криптографическая защита СКЗИ должна исключить опасные события, возникающие вследствие неисправностей или сбоев АС СКЗИ и АС СФ и приводящие к возможности осуществления успешных атак на СКЗИ и технические средства информационной инфраструктуры платежной системы.

- Инженерно-криптографическая защита СКЗИ должна предусматривать защиту от возможных непреднамеренных действий оператора/пользователя/администратора,

[3] В качестве фактора владения должно использоваться сертифицированное ФСБ России устройство типа «токен» или смарт-карта. В случае использования пароля в качестве фактора знания, длина пароля должна обосновываться на этапе тематических исследований.

не предусмотренных правилами пользования СКЗИ и приводящих к возможности осуществления успешных атак на СКЗИ, включая, но не ограничиваясь вводом непредусмотренных последовательностей команд, ввод непредусмотренных команд, вводом команд в неправильном режиме работы устройства, ввод непредусмотренных параметров или данных, которые могут привести к выводу СКЗИ конфиденциальной информации. Защита от непреднамеренных действий должна быть реализована для всех физических и логических интерфейсов, предоставляемых СКЗИ.

- В СКЗИ должна быть реализована система защиты от несанкционированного доступа к используемой СКЗИ ключевой и криптографически опасной информации. Также в СКЗИ должна быть реализована система защиты от несанкционированного доступа к СКЗИ, в том числе защита от компрометации пароля, включая несанкционированную запись/копирования ввода с клавиатуры.

- В ходе тематических исследований СКЗИ должны быть определены технические характеристики СКЗИ и их предельные значения, позволяющие обеспечить выполнение предъявляемых к СКЗИ требований.

- В СКЗИ должен быть реализован контролирующий механизм, сигнализирующий или блокирующий работу СКЗИ при достижении предельных значений технических характеристик СКЗИ.

Для СКЗИ, реализованного в технических средствах информационной инфраструктуры платежной системы, должен быть обеспечен контроль целостности СКЗИ на этапах хранения, транспортирования, ввода в эксплуатацию и эксплуатации жизненного цикла СКЗИ, а также контроль целостности СФ на этапе эксплуатации жизненного цикла СКЗИ с использованием криптографических механизмов контроля целостности. Перечень объектов среды функционирования СКЗИ, контроль целостности которых осуществляется СКЗИ, определяется и обосновывается в ходе проведения тематических исследований. Контроль целостности следует проводить до начала обработки информации, безопасность которой должна обеспечиваться СКЗИ.

В начале работы СКЗИ (при включении питания) необходимо обеспечить выполнение диагностического контроля (самотестирование). В рамках диагностического контроля должны выполняться следующие проверки: контроль работоспособности мер криптографической и инженерно-криптографической защиты; контроль работоспособности реализации криптографических алгоритмов; контроль статистического качества выходной последовательности ДСЧ; контроль целостности (подлинности) ПО СКЗИ, ПО АС СКЗИ, ПО СФ СКЗИ.

СКЗИ может поддерживать обновление ПО СКЗИ (а также ПО СФ СКЗИ). СКЗИ должно проводить криптографическую проверку подлинности устанавливаемых обновлений. Если подлинность не подтверждается, обновление микропрограммы должно отклоняться и удаляться.

СКЗИ должно предоставлять функционал по выводу уникального идентификатора устройства с применением мер криптографической защиты. Каждое устройство также должно иметь уникальный видимый идентификатор (легко читаемый номер устройства), прикрепленный к нему. В дополнение к выводу уникального идентификатора, устройство должно предоставлять функционал по выводу уникальных версий ПО СКЗИ, ПО АС СКЗИ, ПО СФ СКЗИ, в том числе на экран в читаемом виде, в ответе на запрос к API. Если может производиться изменение (обновление) отдельных компонентов ПО СКЗИ, ПО АС СКЗИ, ПО СФ СКЗИ, то версии таких компонентов должны выводиться отдельно, или общая версия ПО должна изменяться при изменении (обновлении) отдельных компонент.

СКЗИ должно автоматически очищать или повторно инициализировать свои внутренние буферы, содержащие защищаемую и иную конфиденциальную информацию, как только достигается цель их использования, в том числе, когда:

- Транзакция завершена.
- Время ожидания действий от держателя карты или оператора истекло.
- Работа СКЗИ была восстановлена после ошибки.

В СКЗИ необходимо реализовать механизм регистрации событий. В состав СКЗИ должен входить модуль, производящий регистрацию в электронном журнале регистрации событий в СКЗИ и СФ, связанных с выполнением СКЗИ определенных в ТЗ криптографических функций.

Перечень событий, регистрируемых в журнале регистрации событий, определяется в ТЗ на разработку (модернизацию) СКЗИ.

В Требованиях к техническим средствам и программному обеспечению реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам также описываются условия и порядок проведения исследований ПО СКЗИ, СФ СКЗИ, АС СКЗИ, требования по защите от ТКУИ и порядок реализации обновления ПО СФ СКЗИ.

5. ТРЕБОВАНИЯ К МЕРАМ БЕЗОПАСНОСТИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА

На всех этапах жизненного цикла устройства производитель СКЗИ должен принимать меры по обеспечению безопасности компонентов СКЗИ.

Производитель СКЗИ должен определить и выполнять требования по обеспечению физической, логической безопасности, а также безопасности при управлении персоналом, необходимые для обеспечения защищенности разработанного (разрабатываемого) изделия и реализации компонентов СКЗИ. Производитель СКЗИ должен вести свидетельства реализации установленных требований и процедур, которые должны быть достаточными для подтверждения того, что меры обеспечения безопасности соблюдаются во время разработки и обслуживания компонентов СКЗИ.

Производитель СКЗИ должен разработать и внедрить процедуру контроля изменений

(контроля целостности) физических или функциональных характеристик СКЗИ, фиксирующую любое изменение физических или функциональных характеристик. Перечень допустимых изменений определяется в рамках тематических исследований.

Производитель СКЗИ должен разработать и внедрить процедуру контроля аппаратных компонентов, используемых для производства СКЗИ, чтобы исключить их несанкционированную замену.

Производитель СКЗИ должен определить и выполнять требования по защите ПО СКЗИ, ПО АС СКЗИ, ПО СФ СКЗИ от несанкционированного доступа и модификации в течение всего жизненного цикла. ПО СКЗИ, ПО АС СКЗИ, ПО СФ СКЗИ, которое загружается в устройство во время изготовления, должно транспортироваться, храниться и использоваться с соблюдением принципа двойного контроля и/или процедур криптографической аутентификации, для предотвращения несанкционированного доступа и модификации.

При проведении тематических исследований должна проводиться проверка ПО СКЗИ, ПО АС СКЗИ, ПО СФ СКЗИ, а также их последующих изменений и обновлений, на наличие скрытых, несанкционированных или недокументированных функций.

После производства устройства, но до отгрузки с площадки производителя или третьих лиц, привлекаемых производителем, устройство и любые его компоненты должны храниться в месте хранения, защищенном от несанкционированного доступа, или в упаковке, гарантирующей обнаружение вскрытия (например, в сейф-пакете), с целью предотвращения несанкционированного изменения физических или функциональных характеристик устройства.

Если процедура ввода в эксплуатацию СКЗИ подразумевает выполнение аутентификации СКЗИ с помощью конфиденциальной информации, помещенной в СКЗИ на этапе производства, то эта конфиденциальная информация должна быть уникальна для каждого устройства, неизвестна и непредсказуема для любого человека и установлена внутри устройства. Возможность реализации указанных свойств должна быть реализована в рамках тематических исследований СКЗИ. Конфиденциальная информация должна быть загружена в устройство при соблюдении принципа двойного контроля, чтобы гарантировать, что она не будет раскрыта во время установки, или устройство может использовать метод аутентификации с открытым ключом.

Производитель СКЗИ должен определить и выполнять требования по защите СКЗИ при выполнении ремонтных работ и тестировании СКЗИ после выполнения ремонтных работ.

При передаче от производителя устройства в место эксплуатации, устройство должно быть защищено от несанкционированного доступа с помощью средств обнаружения вскрытия. Клиентам должна быть предоставлена документация (поставляемая вместе с продуктом и/или поставляемая доверенным образом), содержащая инструкции по проверке подлинности и целостности устройства. Если это невозможно, устройство должно доставляться с площадки производителя в место эксплуатации и храниться по пути следования под проверяемым

контролем, позволяющим определить местонахождение каждого устройства в каждый момент времени. Если в организации транспортировки участвуют несколько сторон, каждая из них несет ответственность за то, чтобы транспортировка и хранение, которыми они управляют, соответствовали данному требованию.

Если СКЗИ поставляется конечным клиентам с привлечением третьих лиц, ответственность за обеспечение безопасности устройств должна быть возложена на третьи лица с момента получения ими устройства до момента его получения другим третьи лицом и/или конечным клиентом.

Во время транспортировки от производителя устройства в место эксплуатации устройство должно быть защищено с помощью одного или нескольких из следующих способов:

- Устройство должно поставляться и храниться в упаковке, гарантирующей обнаружение вскрытия (например, в сейф-пакете).
- Устройство должно поставляться и храниться с секретом, который немедленно и автоматически стирается при попытке любого физического или функционального изменения устройства, и может быть проверен в месте ввода в эксплуатацию, но не может быть определен неавторизованным персоналом.

Если производитель СКЗИ выполняет первоначальную загрузку ключей, он должен выполнять проверку подлинности СКЗИ. Если производитель СКЗИ не выполняет первоначальную загрузку ключей, он должен предоставить клиенту способ обеспечения проверки подлинности и целостности СКЗИ.

6. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ К ТЕХНИЧЕСКИМ СРЕДСТВАМ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ, РЕАЛИЗУЮЩИМ КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ЗНАЧИМОЙ ПЛАТЕЖНОЙ СИСТЕМЫ

Комплект эксплуатационной документации СКЗИ должен содержать как минимум: формуляр, правила пользования, технические условия.

Производитель СКЗИ должен разработать, поддерживать в актуальном состоянии и обеспечить доступность для клиентов правил пользования на СКЗИ, регламентирующей использование, обслуживание и администрирование СКЗИ.

В Правилах пользования, помимо сведений, указанных в ТС 26.2.001-2020 «Состав и содержание правил пользования средств криптографической защиты информации» должно быть отражено следующее:

- Описание функционала, предоставляемого устройством.
- Описание процедур управления ключами, необходимых для безопасного функционирования устройства.
- Описание административных процедур, необходимых для безопасного функционирования устройства.

- Описание процедур изъятия устройства из эксплуатации, в том числе процедур удаления обрабатываемых и хранимых в устройстве конфиденциальных данных (включая криптографические ключи, ПИН-коды, PAN).
- Установленные рабочие диапазоны температуры, напряжения или влажности, выход за пределы которых вызывает срабатывание датчиков контроля условий эксплуатации устройства.
- Описание порядка действий в случае срабатывания механизмов логической и физической защиты устройства.
- Перечень всех интерфейсов и протоколов внешнего взаимодействия устройства, а также порядок безопасного конфигурирования для каждого интерфейса и протокола, включая следующее:
  - перечень всех ключей и сертификатов, которые необходимо использовать для защиты интерфейсов внешнего взаимодействия устройства, включающий алгоритмы и длины ключей;
  - порядок безопасного использования ключей и сертификатов, включая описание всех статусов сертификата (например, отозван), процедур безопасной загрузки и смены ключей;
  - описание обязанностей производителя изделия с СКЗИ, разработчиков платежного ПО, предназначенного для взаимодействия с СКЗИ, и конечных пользователей устройства, по безопасному управлению ключами и сертификатами защиты интерфейсов внешнего взаимодействия устройства.
- Политика безопасности, которая определяет роли, поддерживаемые устройством, и указывать функции, доступные для каждой роли.
- Устройство должно выполнять только предназначенные для него функции, т.е. скрытая функциональность должна отсутствовать. Единственными разрешенными функциями, выполняемыми устройством, должны являться функции, указанные в Правилах пользования.
- Информация о регистрации всего жизненного цикла компонентов СКЗИ, включая:
  - Данные о производстве и персонализации.
  - Физическое/хронологическое местонахождение.
  - Ремонт и обслуживание.
  - Изъятие из эксплуатации.
  - Потеря или кража.
- Описание порядка проверки подлинности аппаратных и программных компонентов СКЗИ. Перечень программных компонентов СКЗИ должен включать версии ПО СКЗИ, ПО АС СКЗИ, ПО СФ СКЗИ.

В дополнение к этому, производитель СКЗИ должен разработать, поддерживать в актуальном состоянии и обеспечить доступность для клиентов инструкции разработчиков

платежного ПО, предназначенного для взаимодействия с СКЗИ, в которых должно быть отражено следующее:

- порядок использования приложениями предоставляемых СКЗИ криптографических функций, функций управления ключами и API, включающий образцы вызова функций.

- порядок использования приложениями предоставляемых СКЗИ интерфейсов и протоколов внешнего взаимодействия, включающий полный перечень всех интерфейсов и протоколов и порядок безопасной настройки для каждого интерфейса и протокола, а также включающий образцы вызова функций.