Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Каким требованиям должен соответствовать аппаратный модуль безопасности для систем платёжных карт

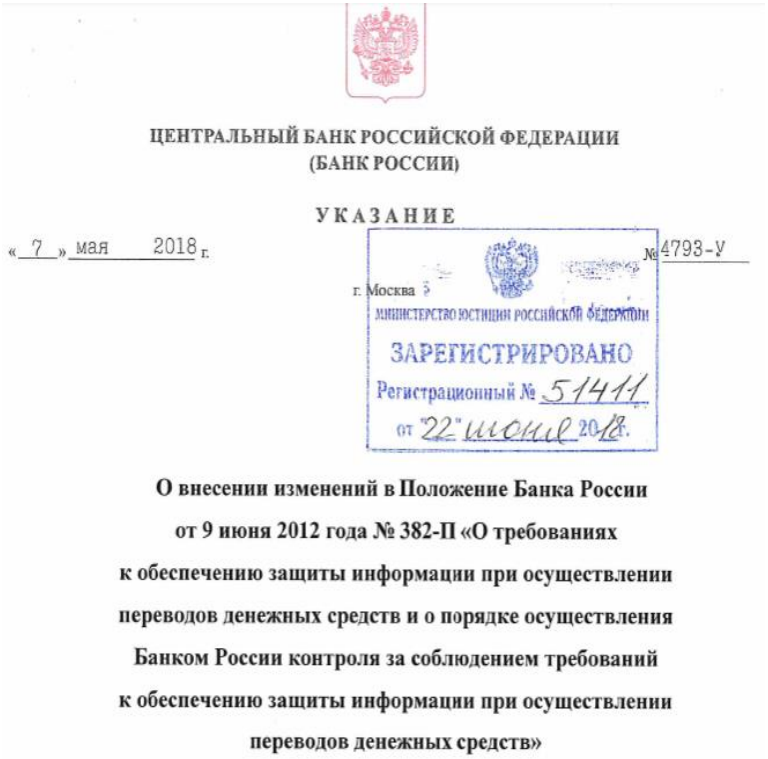
Елена Мареева, заместитель директора по НТР «Системы Практической Безопасности»
Елена Шкоркина, специалист по защите информации «Системы Практической Безопасности»

С чего всё началось – Изменения положения №382-П

Оператору значимой платежной системы в соответствии с правилами платежной системы необходимо обеспечить использование:

- в аппаратных модулях безопасности информационной инфраструктуры платежной системы **СКЗИ, реализующих криптографические алгоритмы, не определенные национальными стандартами РФ (далее - иностранные криптографические алгоритмы),** имеющих подтверждение соответствия требованиям, установленным ФОИВ в области обеспечения безопасности.
  Вступает в силу с 01.01.2024

- в аппаратных модулях безопасности информационной инфраструктуры платежной системы **СКЗИ, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы, определенные национальными стандартами РФ (далее - криптографические алгоритмы Российской Федерации),** имеющих подтверждение соответствия требованиям, установленным ФОИВ в области обеспечения безопасности
  Вступает в силу с 01.01.2024



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УКАЗАНИЕ

«7» мая 2018 г. № 4793-У

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 51411
от "22" июня 2018 г.

О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

Второй шаг – Разработка функционально технических требований

СОГЛАСОВАНО
Первый заместитель
руководителя Научно-
технической службы
ФСБ России

_____ А.М. Ивашко
«24» 01 2020 г.

УТВЕРЖДАЮ
Заместитель Председателя
Банка России

_____ Д.Г. Скобелкин
«28» 02 2020 г.

ФУНКЦИОНАЛЬНО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К АППАРАТНОМУ МОДУЛЮ БЕЗОПАСНОСТИ (HSM-МОДУЛЬ)

№ ФТ-56-3/35
28.02.2020

В состав ФТТ к HSM модулю включены требования к реализации иностранных криптографических алгоритмов и протоколов, используемых информационной инфраструктурой платёжных систем

https://cbr.ru/Content/Document/File/104755/FT_35.pdf

Третий шаг – Разработка требований к СКЗИ информационной инфраструктуры платёжной системы

СОГЛАСОВАНО

Заместитель Председателя Банка России

_____ Д.Г. Скобелкин

«15» 01 2020 г.

УТВЕРЖДАЮ

Первый заместитель руководителя Научно-технической службы ФСБ России

_____ А.М. Ивашко

«24» 01 2020 г.

ТРЕБОВАНИЯ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНЫХ УСТРОЙСТВАХ С ТЕРМИНАЛЬНЫМ ЯДРОМ, СЕРВЕРНЫХ КОМПОНЕНТАХ ПЛАТЕЖНЫХ СИСТЕМ (HSM МОДУЛЯХ), ПЛАТЕЖНЫХ КАРТАХ 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

№ ФТ-56-3/32
28.02.2020

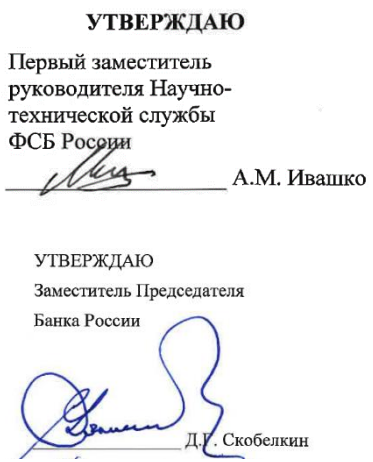
Определяет требования РФ по ИБ к ТС и ПО, реализующим криптографические механизмы в:

- платежных устройствах с терминальным ядром (терминалы и банкоматы),
- аппаратных модулях безопасности информационной инфраструктуры платёжных систем (HSM модулях),
- платежных картах,
- иных технических средствах информационной инфраструктуры платежной системы

https://cbr.ru/Content/Document/File/104752/FT_32.pdf

HSM должен соответствовать

1. ТРЕБОВАНИЯМ к СКЗИ в платежных устройствах с терминальным ядром, серверных компонентах платежных систем (HSM модулях), платежных картах и иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств – **это требования ФОИВ в области обеспечения безопасности в части HSM модулей**
2. Функционально-техническим требованиям к аппаратному модулю безопасности (HSM-модулю) – **это функциональные требования, консолидированные ЦБ к HSM модулям для применения в составе платёжных систем**
3. ТРЕБОВАНИЯМ к Hardware Security Module (HSM). Modular Security Requirements. Payment Card Industry (PCI). PIN Transaction Security (PTS). Version 3.0 June 2016 (PCI PTS HSM) – **это требование совета по стандартам безопасности данных индустрии платежных карт в области обеспечения безопасности HSM модулей для применения в составе платёжных систем**


УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко

УТВЕРЖДАЮ
Заместитель Председателя Банка России
Д.Г. Скобелкин

PCI Security Standards Council

Сравним документы

Требования PCI PTS HSM	Требования к СКЗИ в HSM
HSM предназначен для выполнения	
Различных приложений и процессов обработки платежей и аутентификации держателя карты: обработка PIN-кода, 3D-Secure, верификация, производство и персонализация карт, EFTPOS, взаимодействие с ATM, зачисление средств на карту, обеспечение целостности данных транзакций, обработка транзакций с использованием чиповых карт, генерация и ввод ключей	Криптографических преобразований при проведении платёжных операций, управления ключами шифрования и(или) шифрования данных платёжных карт, персонализации платёжных карт при эмиссии
На какие этапы ЖЦ распространяются	
Требования распространяются на все этапы жизненного цикла HSM	Действия нарушителя рассматриваются на всех этапах жизненного цикла СКЗИ (разработка, производство, хранение, транспортировка, ввод в эксплуатацию и эксплуатация)
Подход к формированию требований	
Требования, содержащиеся в PCI PTS HSM, построены по методике снижения рисков и являются минимально приемлемыми критериями для индустрии платежных карт (PCI)	Требования к СКЗИ построены по принципу обеспечения нейтрализации атак потенциального нарушителя. Совокупность предъявляемых требований к СКЗИ определяется классом СКЗИ и составом реализуемых данным СКЗИ криптографических функций

Сравним документы

Требования PCI PTS HSM	Требования к СКЗИ в HSM
Применение криптографических механизмов	
1) Устройство должно использовать принятые криптографические алгоритмы, режимы и размеры ключей 2) Методы управления ключами, реализованные в устройстве должны соответствовать стандартам ISO 11568 и/или ANSI X9.24. Методы управления ключами должны поддерживать методику ANSI TR-31 формирования ключа или эквивалентную методику для поддержки набора ключей для TDEA 3) Если устройство предназначено для управления PIN-кодом, оно должно соответствовать требованиям ISO-9564 по управлению PIN-кодом. Метод шифрования PIN-кода, реализованный в устройстве, является методом, включенным в ISO 9564	1) Должны использоваться криптографические механизмы, утвержденные в качестве национальных стандартов РФ или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований. 2) Кроме того, с целью обеспечения совместимости с действующими криптографическими решениями должны использоваться криптографические механизмы, отвечающие международным стандартам (ISO).
Криптографические механизмы, а также преобразования, реализующие обработку ключевой информации, ее выработку и удаление, должны быть реализованы непосредственно в СКЗИ.	

Сравним документы

Требования PCI PTS HSM	Требования к СКЗИ в HSM
Структура требований	
Делятся на 4 модуля: Модуль 1 – Базовые требования с делением на: A) требования к физической безопасности, B) логические требования и C) политики и процедуры Модуль 2 – Устройства загрузки ключей D) Загрузка ключей Модуль 3 – Удалённое администрирование E)Логическая безопасность F)Устройства с функциями аутентификации сообщений G)Устройства с функциями генерации ключей H) Устройства с функциями цифровой подписи Модуль 4 – Требования к безопасности управления устройством I) Требования к безопасности устройства при изготовлении J) Требования по безопасности устройства между производителем и местом первоначальной установки	1. Описание модели нарушителя СКЗИ 2. Общие принципы построения СКЗИ 3. Принципы применения криптографических механизмов защиты - общие положения - реализация в ДСЧ - выработка КИ, использование КИ - аутентификация субъектов доступа - имитозащита 4. Принципы применения ИК механизмов защиты - общие положения - базовые положения ПО СКЗИ - положения по соответствию ПО СФ СКЗИ - положения по АС СКЗИ - положения по физической защите СКЗИ и СФ СКЗИ - доп. требования по безопасности конфиденциальных данных в HSM - положения по защите от ПЭМИН
HSM могут быть сертифицированы в качестве предназначенных к использованию в контролируемой среде или для использования в любой среде	

Обязательные требования по использованию российских криптографических механизмов

Криптографические механизмы, утвержденные в качестве национальных стандартов РФ или рекомендаций по стандартизации Росстандарта, либо имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований **должны** применяться:

- ✓ При передаче по каналам связи, хранении и дистанционном управлении ключевой информацией
- ✓ В СКЗИ всех классов для обеспечения аутентификации субъектов и/или процессов доступа, осуществляющих доступ или взаимодействующих с СКЗИ, а также удаленной аутентификации при организации защищенной передачи данных и аутентификации при взаимодействии с СКЗИ по каналам управления
- ✓ Для имитозащиты информации каналов управления и передачи данных

Следует обратить внимание в требованиях к СКЗИ в HSM

- ✓ Для аппаратных модулей безопасности информационной инфраструктуры платежных систем необходимо обеспечить защиту ключевой информации пользователей от администратора (привилегированного пользователя) модуля
- ✓ В HSM для выработки первичной ключевой информации должен использоваться ФДСЧ
- ✓ Используемая СКЗИ незашифрованная ключевая информация должна храниться непосредственно в СКЗИ на протяжении установленного срока действия и должен быть реализован механизм контроля срока действия криптографических ключей
- ✓ Для обеспечения локальной аутентификации физических лиц, осуществляющих доступ к СКЗИ в HSM, должна быть реализована ролевая аутентификация:
  - роль пользователя (выполнение криптографических функций);
  - роль привилегированного пользователя (функции управления СКЗИ).
- ✓ В HSM критические функции управления ключами (формирование (загрузка) и резервирования локальных мастер-ключей HSM, предназначенных для защищенного хранения в сервере ключей держателей карт) должны выполняться под двойным контролем (т. е. при обязательной аутентификации не менее двух привилегированных пользователей).

Следует обратить внимание в требованиях к СКЗИ в HSM

- ✓ Для СКЗИ в HSM контроль целостности должен осуществляться только с использованием криптографических механизмов. Механизм контроля целостности должен включать средства контроля собственной корректной работы
- ✓ Должен быть реализован криптографический контроль целостности журналов регистрации событий
- ✓ Для СКЗИ в HSM модулях на тематические исследования (ТИ) предоставляются исходные коды ПО СФ СКЗИ
- ✓ Для HSM должны быть реализованы следующие меры защиты, входящие в АС СКЗИ:
  - распределенный датчик объема регистрирующий любое проникновение в корпус изделия;
  - датчик вскрытия корпуса;
  - модуль уничтожения ключевой информации в случае регистрации НСД.
- ✓ Принятые в технических средствах информационной инфраструктуры платежной системы меры защиты должны исключать возможность определения PIN кода и ключей шифрования, а также другой конфиденциальной информации путем анализа каналов ПЭМИН

Следует обратить внимание в требованиях к СКЗИ в HSM

- ✓ СКЗИ в HSM должны гарантировать использование разных ключей для разных криптографических функций. Например, недопустимо использование ключа шифрования ключа для шифрования ПИН-кода
- ✓ СКЗИ в HSM не должны содержать механизма, позволяющего выводить закрытые или симметричные ключи в открытом виде, а также шифрование ключа или ПИН-кода с использованием ключа, помеченного как скомпрометированный
- ✓ В СКЗИ HSM должна быть отключена возможность вывода ПИН-кода в открытом виде. Управление ПИН-кодами СКЗИ HSM должно производиться в соответствии с требованиями рекомендаций по стандартизации Росстандарта или международного стандарта ISO 9564
- ✓ Технические средства информационной инфраструктуры платежной системы могут предусматривать возможность обновления программного обеспечения СФ СКЗИ по каналам управления с аутентификацией субъекта проводящего обновление и технического средства информационной инфраструктуры платежной системы. Если аутентификация не подтверждается, обновление отменяется и удаляется с устройства

Выводы

Требования к СКЗИ в HSM гармонизированы с требованиями PCI PTS HSM, и их реализация позволяет пройти сертификацию в обеих системах сертификации

Вопросы

Контактная информация

Электронная почта:

mareeva@systempb.ru

Телефон:

+7 812 468-15-61 доб.210

+7 921 301-92-70

Сайт:

systempb.ru

www.skzi.ru