КРИПТОПРО

Ключевое слово
в защите информации

Выполнение требований по безопасности при применении российских программно-аппаратных криптографических модулей (**HSM**) для обеспечения безопасности платежных систем

Практика реализации требований

ПРОСТОВ
Владимир Михайлович

Советник, ООО «КРИПТО-ПРО»
«Эксперт РОСЭУ»

АБИСС

Оператор значимой платежной системы с 01.01.2024 должен обеспечить использование:

- В аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих иностранные криптографические алгоритмы, криптографические алгоритмы, определенные национальными стандартами Российской Федерации (далее криптографические алгоритмы Российской Федерации), имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности

- В аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих криптографические алгоритмы, не определенные национальными стандартами Российской Федерации (далее - иностранные криптографические алгоритмы), имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности

ФСБ России + Банк России

Банк России

№ФТ-56-3/32 от 28.02.2020

Опубликованы на официальных сайтах ФСБ России и Банка России

Требования международных платежных систем

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) **Modular Security** Requirements Version 3.0 June 2016.

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) **Modular Derived Test** Requirements Version 3.0 June 2016.

Основные результаты работ по обеспечению выполнения требований PCI HSM

Проведено изучение открытой документации компании Thales.

Подготовлены технические решения по выполнению требований PCI HSM.

Технические решения направлены в сертификационную лабораторию PCI HSM.

Основные результаты работ по согласованию технических решений с сертификационной лабораторией

Согласованы следующие технические решения:

1. Общая конструкция HSM модуля.
2. Физическая защита HSM модуля от возможных проникновений.
3. Механизмы защиты от утечки информации по побочным каналам.
4. Микропрограммное и программное обеспечение HSM модуля.
5. Процедура загрузки программного обеспечения.
6. Механизмы защиты от изменений условий окружающей среды и целенаправленных изменений условий эксплуатации.
7. Датчик случайных чисел.

Наиболее важные требования в условиях кибератак

Контроль целостности программно-аппаратных средств должен применяться с использованием российских криптографических алгоритмов

Удаленное обновление программного обеспечения должно осуществляться с использованием российских криптографических алгоритмов

НСПК + VISA (MASTER CARD)

НСПК +UNION PAY ?

THALES

Компания Thales **прекратила поставки и техническую поддержку** HSM модулей для кредитных и иных организаций на территории Российской Федерации.

Взаимодействие с платежной системой UNION PAY

До решения вопроса о необходимости сертификации по требованиям PCI HSM для взаимодействия с платежной системой UNION PAY **должны быть разделены потоки платежных транзакций**.

Следует договориться о **возможности корректировки требований** для эксплуатации СКЗИ на территории РФ. Выполнить только **требования ФСБ России**.

Привлечь лаборатории КНР для сертификации российских СКЗИ по требованиям PCI HSM. Не очевидна возможность получения сертификата PCI SSC.

Изменение нормативной базы АО НСПК

НСПК является **национально значимой платежной системой** и при ее функционировании должны выполняться положения Федерального закона "О национальной платежной системе" от 27.06.2011 N 161-ФЗ.

Выполнение требований разработанных совместно Центральным банком и ФСБ России должны являться достаточным условием для возможности эксплуатации HSM модулей в национально значимых платежных системах, в том числе НСПК.

В текущих условиях **обязательное требование** по применению нормативных документов **PCI SSC должно быть исключено**.

КРИПТОПРО

Ключевое слово
в защите информации

Ваши вопросы?

КРИПТОПРО

Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Сущевский Вал, д.18
Тел./факс: +7 (495) 995-48-20

https://cryptopro.ru

Простов Владимир Михайлович
prostov@cryptopro.ru