



конференция

РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто'2022»

Об обеспечении выполнения требований Положения ЦБ РФ от 04.06.2020 № 719-П об использовании в национально значимых платежных системах, начиная с 2024 года, аппаратных модулей, имеющих подтверждение соответствия требованиям ФСБ России.

Владимир Простов

Советник, ООО «КРИПТОПРО»

Оператор значимой платежной системы должен обеспечить использование:

- 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;
- в аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих иностранные 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;

Требования к СКЗИ

ФСБ + Банк России



№ФТ-56-3/32 от 28.02.2020

Опубликованы на официальных сайтах ФСБ России и Банка России

Требования международных платежных систем (VISA, MASTER CARD, UNION PAY)

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.

Взаимоотношения платежных систем



НСПК+ VISA (MASTER CARD)



НСПК +UNION PAY



В НСПК должны действовать только требования ФСБ России.

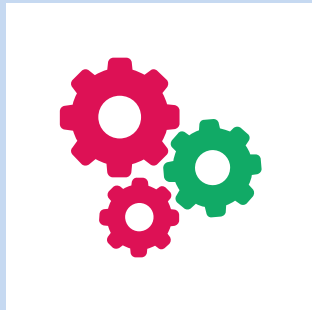
Взаимодействие с платежной системой UNION PAY



До завершения сертификации по требованиям PCI HSM. Для взаимодействия с платежной системой UNION PAY должны быть разделены потоки платежных транзакций.



На первом этапе 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

Наиболее важные требования в условиях кибератак

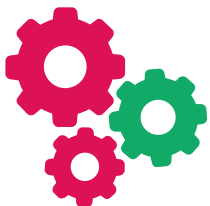


Контроль целостности программно-аппаратных средств должен применяться с использованием российских криптографических алгоритмов

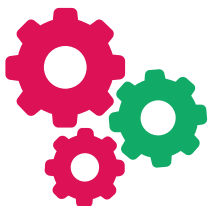


Удаленное обновление программного обеспечения должно осуществляться с использованием российских криптографических алгоритмов

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.

Вопросы



Контактная информация

Электронная почта:

prostov@cryptopro.ru

Телефон:

+7 495 995-48-20

Сайт:

cryptopro.ru

