О технических требованиях по безопасности к компонентам платежной инфраструктуры

Бондаренко Александр Иванович

bondarenko_ai@tc26.ru

Технический комитет по стандартизации «Криптографическая защита и информации»

Цифровая экономика Российской Федерации

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 28 июля 2017 г. № 1632-р

МОСКВА

Утвердить прилагаемую программу "Цифровая экономика Российской Федерации".

Председатель Правительства
Российской Федерации Д.Медведев

Основополагающие принципы информационной безопасности:

- использование российских технологий обеспечения целостности, конфиденциальности, аутентификации и доступности передаваемой информации и процессов ее обработки;
- преимущественное использование отечественного программного обеспечения и оборудования;
- применение технологий защиты информации с использованием российских криптографических стандартов.

План мероприятий по направлению «Информационная безопасность»

- 05.02.009.004.001
- Разработка технических требований по безопасности к компонентам платежной инфраструктуры (изделиям микроэлектроники, а также всему комплексу средств ИТ и ИБ) на основании гармонизации зарубежных и национальных требований по безопасности
- С января 2018 года по июль 2019 года
- Исполнители:
  - Минпромторг России (ответственный исполнитель)
  - Минкомсвязи России
  - ФСТЭК России
  - ФСБ России
  - Банк России

Указание Банка России от 25 июля 2014 года № 3342-У

Требования можно логически разделить на следующие группы:

- к разработчикам программных средств;
- к материальным носителям платежных карт;
- к криптографическим модулям, используемым в интегральных схемах платежных карт;
- к процессу изготовления (сборки) платежных карт;
- к значению качественной оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Компоненты платежной инфраструктуры

- платежные карты

- POS-терминалы (Point-of-Sale)

- аппаратные модули защиты (Hardware Security Modules –HSM)

Payment Card Industry (PCI)

PIN Transaction Security (PTS) Hardware Security Module (HSM)

Modular Security Requirements

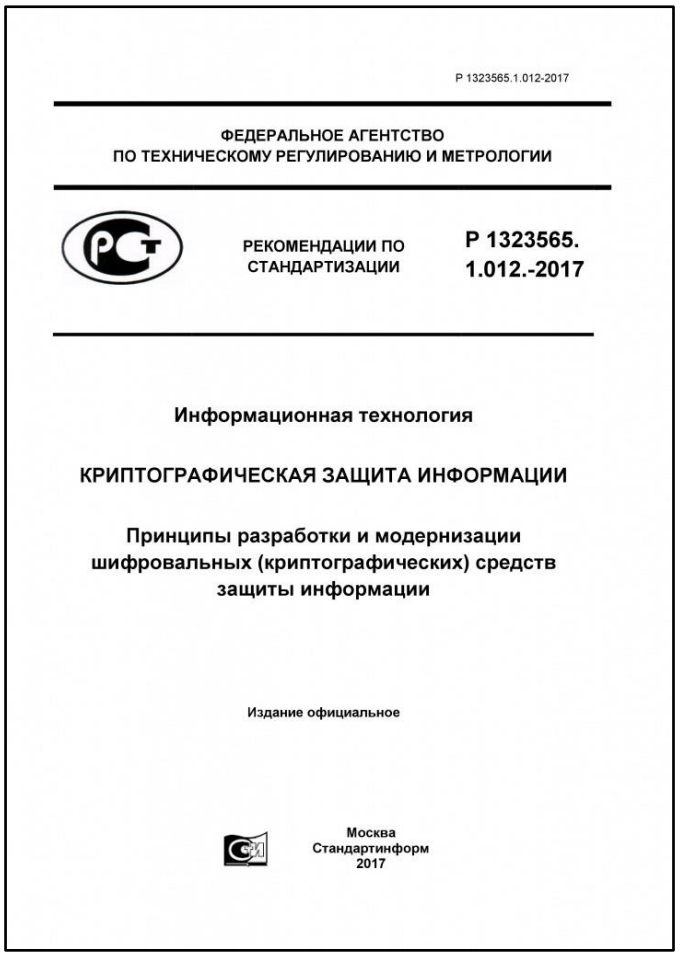
Version 3.0

June 2016

Payment Card Industry (PCI)

PIN Transaction Security (PTS) Hardware Security Module (HSM)

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации



Р 1323565.1.012-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва
Стандартинформ
2017

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(Росстандарт)

ПРИКАЗ

22 декабря 2017 г. № 2068-ст

Москва

Об утверждении рекомендаций по стандартизации

В соответствии со статьей 9 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации» п р и к а з ы в а ю:

1. Утвердить рекомендации по стандартизации Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации» с датой введения в действие 1 мая 2018 г.

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Принципы позволяют сориентироваться и ознакомиться с:

- проблемами, возникающими при разработке (модернизации) и эксплуатации СКЗИ;
- правилами классификации классов разрабатываемых СКЗИ, а также совокупностями возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак, для каждого класса защищенности;
- перечнем необходимых для создания и/или модернизации СКЗИ работ.

FIPS PUB 140-2: Security Requirements for Cryptographic Modules

- Некоторые требования, определенные Modular Security Requirements, основаны на американских требованиях FIPS PUB 140-2: Security Requirements for Cryptographic Modules (A1, B1, B5, B7-B10, …)

Структура Modular Security Requirements

Средства криптографической защиты информации разделяются на:

- средства, реализующие функции имитозащиты (подраздел F);
- средства, реализующие функции электронной цифровой подписи (подраздел H);
- средства, реализующие генерации ключей (подраздел G).

ПКЗ-2005 определяет:

- …
- средства имитозащиты;
- средства изготовления ключевых документов;
- средства электронной цифровой подписи;
- …

Evaluation Module 3: Remote Administration .....

E – Logical Security .....

F – Devices with Message Authentication Functionality ..

G – Devices with Key-Generation Functionality .....

H – Devices with Digital Signature Functionality.....

Пересечения

Modular Security Requirements	Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации
B6. The device must automatically clear or reinitialize its internal buffers that hold sensitive information prior to reuse of the buffer.	6.1.11. В состав СКЗИ должны входить компоненты, обеспечивающие очистку областей памяти, используемых СКЗИ для хранения защищаемой, ключевой, исходной ключевой и криптографически опасной информации, при освобождении и/или перераспределении областей памяти, путем записи в области памяти случайной информации, вырабатываемой датчиком случайных чисел.
B10. The device uses accepted cryptographic algorithms, modes, and key sizes.	5.1.1 При разработке (модернизации) СКЗИ должны использоваться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта.

Пересечения

Modular Security Requirements	Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации
B13. The device ensures that each cryptographic key is only used for a single cryptographic function.	5.4.7. Для различных криптографических механизмов необходимо использовать различную ключевую информацию.
I2. The certified firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing lifecycle – e.g., using dual control or standartdized cryptographic authentication procedures.	6.1.9. Должен быть обеспечен контроль целостности СКЗИ на этапах хранения, транспортирования, ввода в эксплуатацию и эксплуатации всего жизненного цикла СКЗИ, а также контроль целостности среды функционирования СКЗИ на этапе эксплуатации СКЗИ. При этом для СКЗИ, начиная с класса КС3, рекомендуется использование криптографических механизмов контроля целостности.

Гармонизация

В отношении HSM процесс разработки технических требований по безопасности к ним возможно осуществлять на основании гармонизации:

- зарубежных требований - «Payment Card Industry. PIN Transaction Security. Hardware Security Module. Modular Security Requirements»;
- отечественных рекомендаций по стандартизации - «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации».

Рекомендации по стандартизации (утвержденные в 2017 году)

- алгоритмы блочного шифрования при формировании прикладных криптограмм в платежных системах;
- алгоритмы блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN;
- функции диверсификации для формирования производных ключей платежного приложения;
- режимы алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением;
- алгоритмы согласования ключа и блочного шифрования при офлайновой проверке PIN;
- режимы алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт.

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(Росстандарт)

П Р И К А З

19 декабря 2017 г. № 2019-ст

Москва

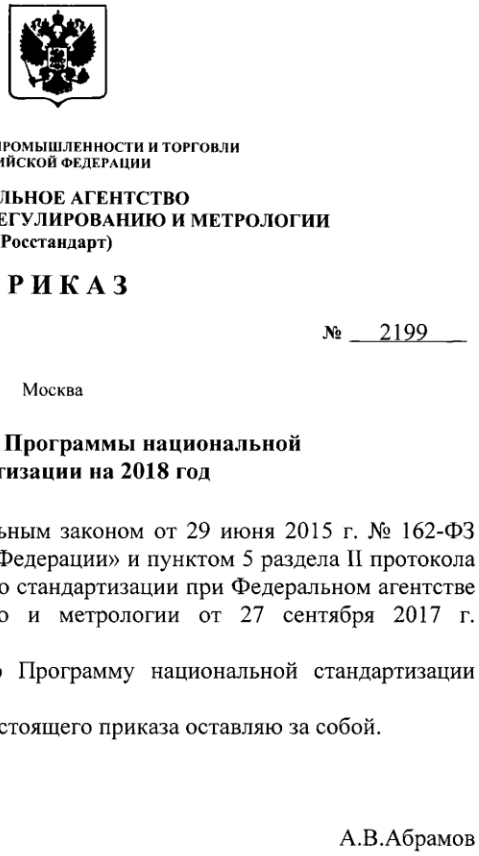
Об утверждении рекомендаций по стандартизации

В соответствии со статьей 9 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации» п р и к а з ы в а ю:

1. Утвердить рекомендации по стандартизации Р 1323565.1.011-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN» с датой введения в действие 1 июня 2018 г.

Рекомендации по стандартизации (планируемые в 2018 году)

- режимы алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре офлайновой аутентификации платежного приложения;
- параметры алгоритмов электронной подписи и функции хэширования в профиле сертификатов открытых ключей платёжных систем.



МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(Росстандарт)

П Р И К А З

23 октября 2017 г. № 2199

Москва

Об утверждении Программы национальной стандартизации на 2018 год

В соответствии с Федеральным законом от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации» и пунктом 5 раздела II протокола расширенного заседания Совета по стандартизации при Федеральном агентстве по техническому регулированию и метрологии от 27 сентября 2017 г. № АА-24пр п р и к а з ы в а ю:

1. Утвердить прилагаемую Программу национальной стандартизации на 2018 год.

2. Контроль исполнения настоящего приказа оставляю за собой.

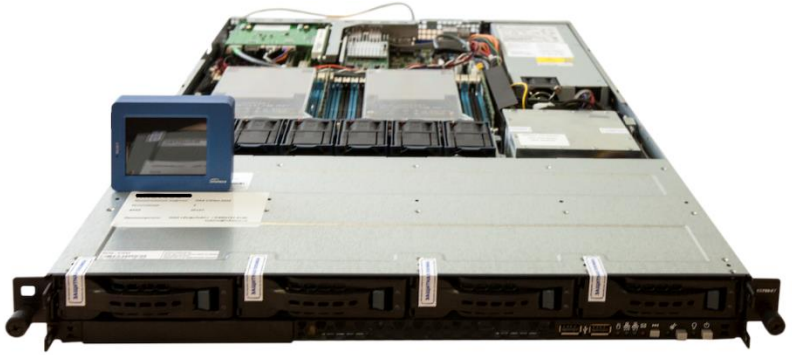
Руководитель А.В.Абрамов

Отечественные HSM

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ



Вопросы?!

Бондаренко Александр Иванович
bondarenko_ai@tc26.ru