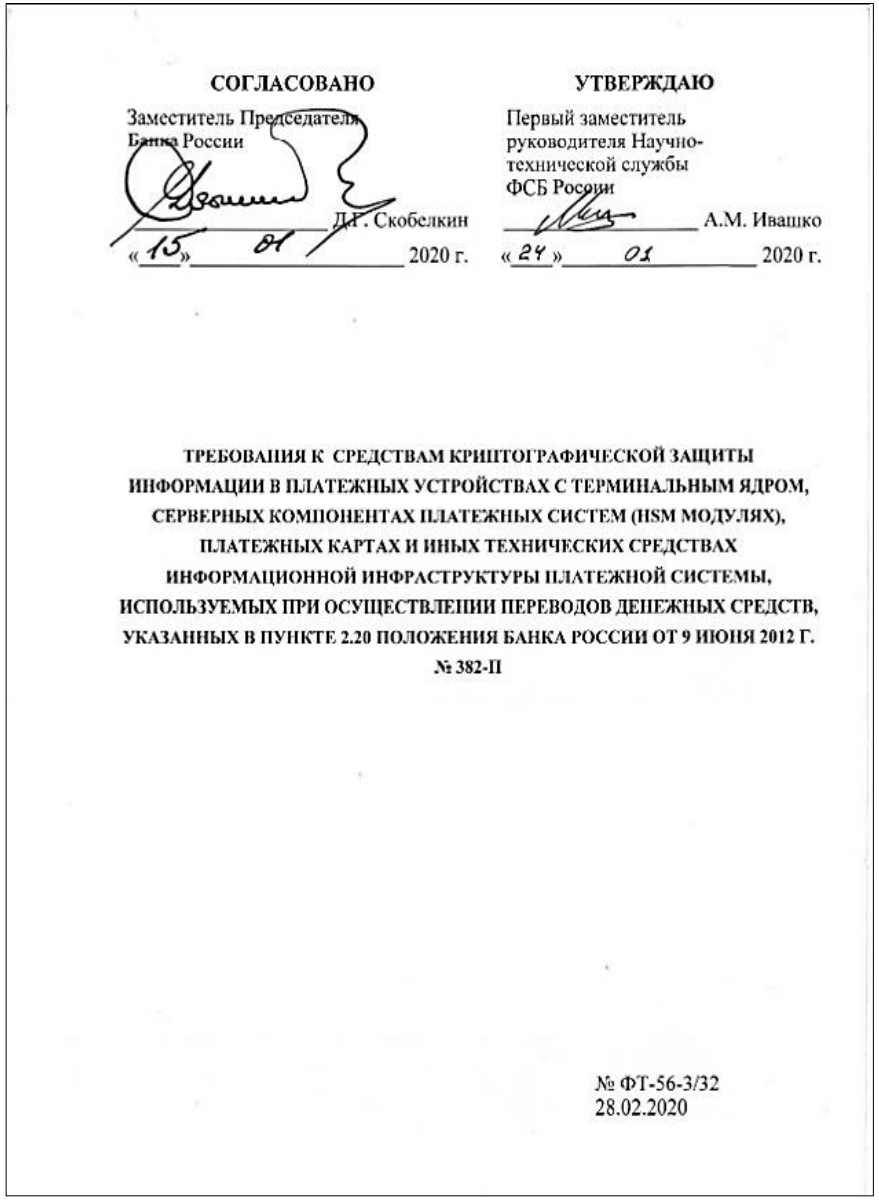
Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Требования к СКЗИ в информационной инфраструктуре значимых платежных систем

Елистратов Андрей

- Настоящие требования разработаны и утверждены в рамках мероприятий федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»
- http://www.cbr.ru/content/document/file/104755/ft_35.pdf



СОГЛАСОВАНО

Заместитель Председателя Банка России

_____ Д.Г. Скобелкин

«15» 01 2020 г.

УТВЕРЖДАЮ

Первый заместитель руководителя Научно-технической службы ФСБ России

_____ А.М. Ивашко

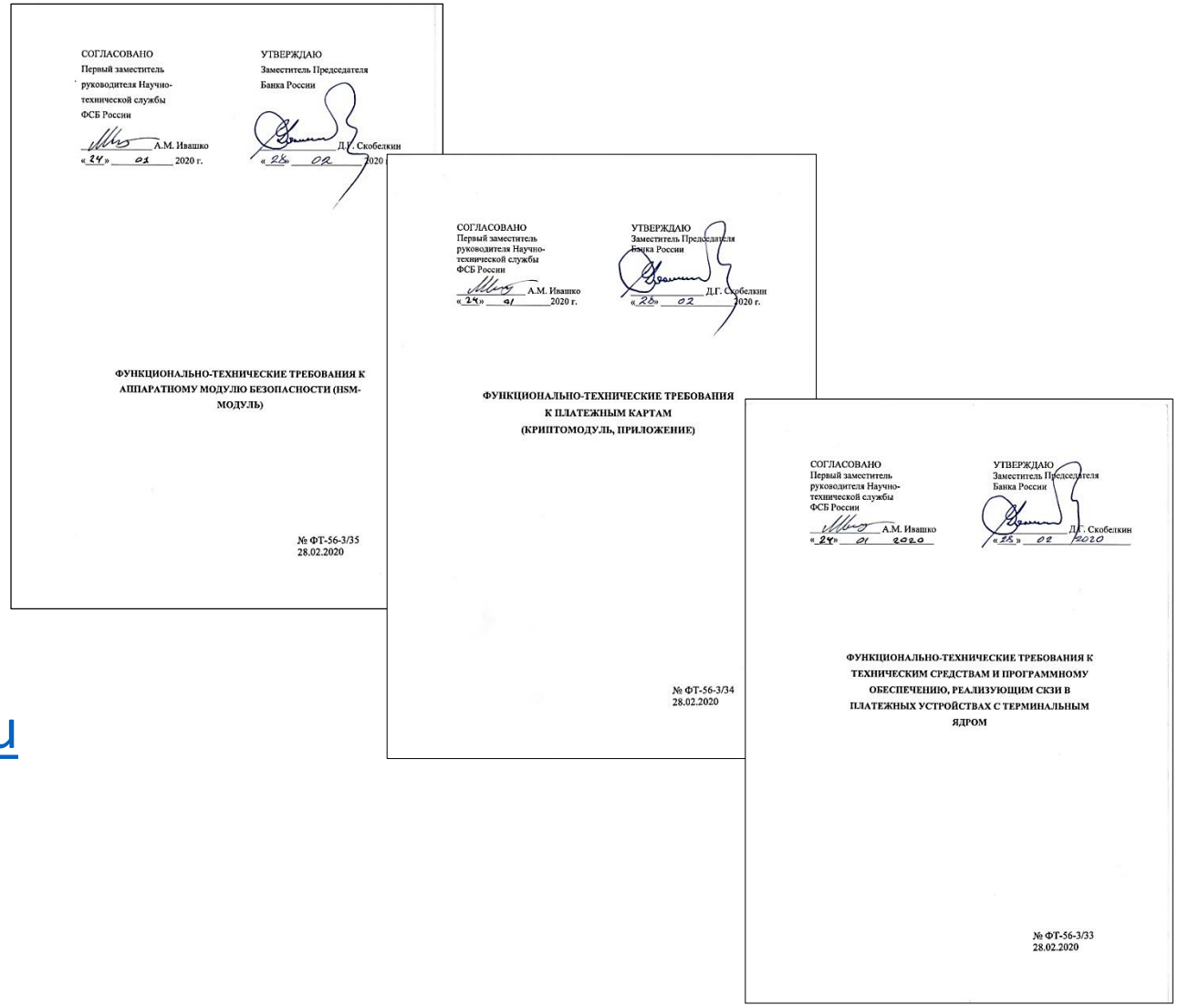
«24» 01 2020 г.

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

- Функционально-технические требования к:
- HSM-модулю
- Платежным картам
- Терминалам

- http://www.cbr.ru/information_security/



СОГЛАСОВАНО
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

УТВЕРЖДАЮ
Заместитель Председателя Банка России
Д.Г. Скобелкин
«25» 02 2020 г.

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

№ ФТ-56-3/35
28.02.2020

СОГЛАСОВАНО
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

УТВЕРЖДАЮ
Заместитель Председателя Банка России
Д.Г. Скобелкин
«25» 02 2020 г.

ФУНКЦИОНАЛЬНО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ПЛАТЕЖНЫМ КАРТАМ (КРИПТОМОДУЛЬ, ПРИЛОЖЕНИЕ)

№ ФТ-56-3/34
28.02.2020

СОГЛАСОВАНО
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020

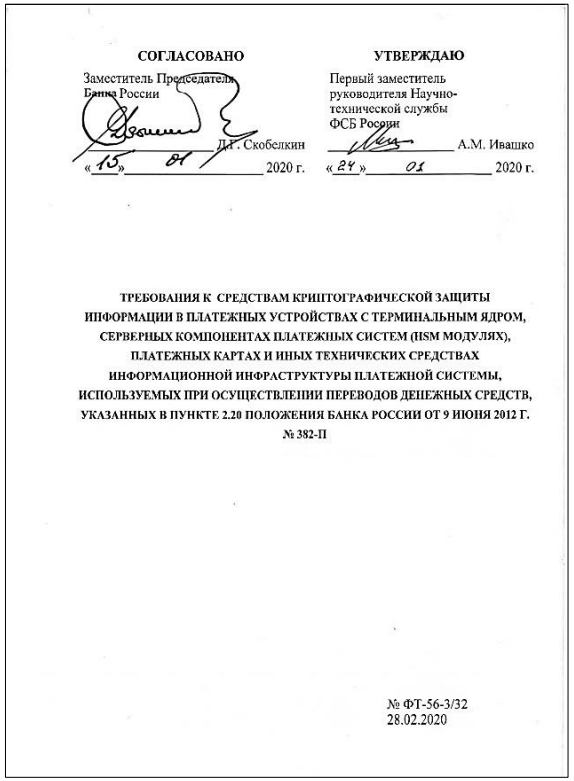
УТВЕРЖДАЮ
Заместитель Председателя Банка России
Д.Г. Скобелкин
«25» 02 2020

ФУНКЦИОНАЛЬНО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ СРЕДСТВАМ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ, РЕАЛИЗУЮЩИМ СКЗИ В ПЛАТЕЖНЫХ УСТРОЙСТВАХ С ТЕРМИНАЛЬНЫМ ЯДРОМ

№ ФТ-56-3/33
28.02.2020

Положение Банка России № 382-П

- Положение Банка России от 9 июня 2012 г. № 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»
- П. 2.20



СОГЛАСОВАНО

Заместитель Председателя Банка России

Д.Г. Скобелкин

«15» 01 2020 г.

УТВЕРЖДАЮ

Первый заместитель руководителя Научно-технической службы ФСБ России

А.М. Ивашко

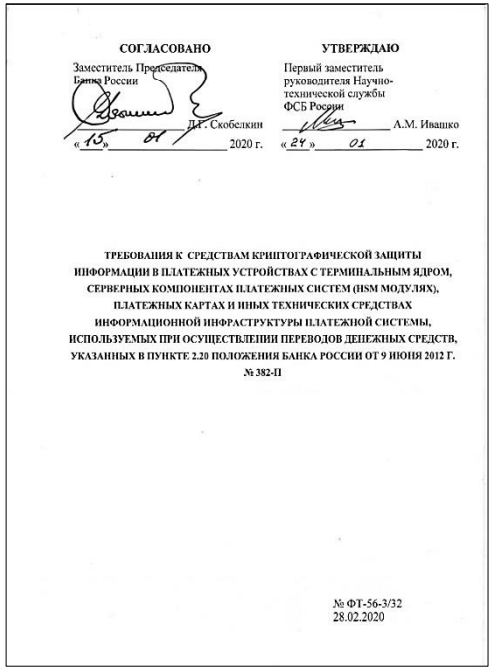
«24» 01 2020 г.

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

Положение Банка России № 719-П

- В замен 382-П с 1 января 2022 г.
- Положение Банка России от 4 июня 2020 г. № 719-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»
- П. 5.5



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 04 2020 г.

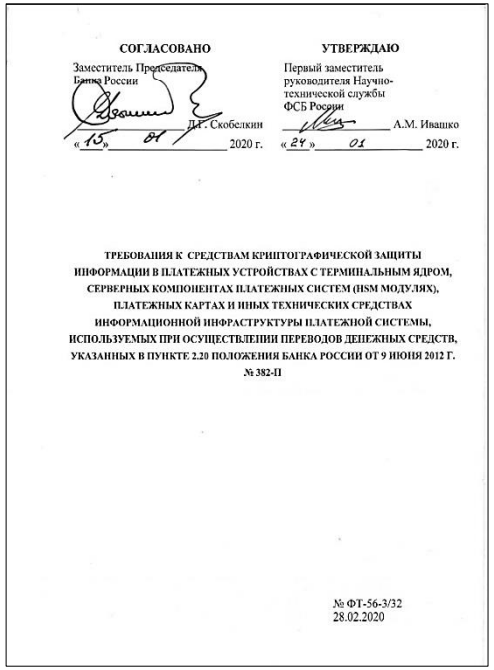
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Положение Банка России № 382-П
Положение Банка России № 719-П

- с **01.01.2024г.**
- **СКЗИ**, реализующих криптографические алгоритмы, **не определенные** национальными стандартами Российской Федерации, **имеющих подтверждение соответствия требованиям**, установленным **федеральным органом исполнительной власти в области обеспечения безопасности**



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 04 2020 г.

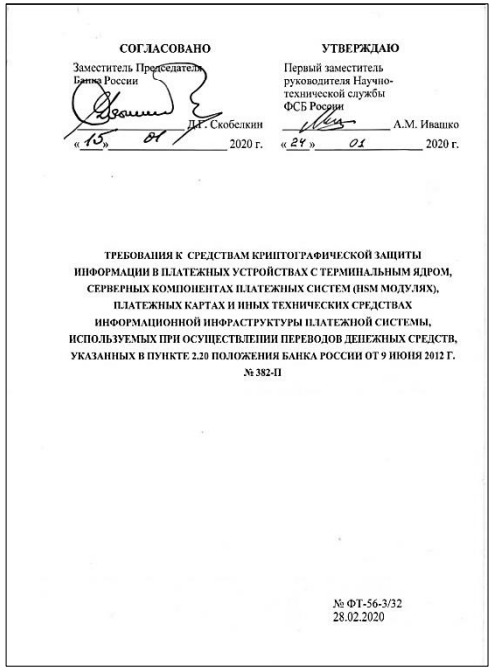
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Положение Банка России № 382-П
Положение Банка России № 719-П

- с **01.01.2031г.**
- **СКЗИ**, реализующих иностранные криптографические алгоритмы **и криптографические алгоритмы Российской Федерации, имеющих подтверждение соответствия требованиям**, установленным **федеральным органом исполнительной власти в области обеспечения безопасности**



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 01 2020 г.

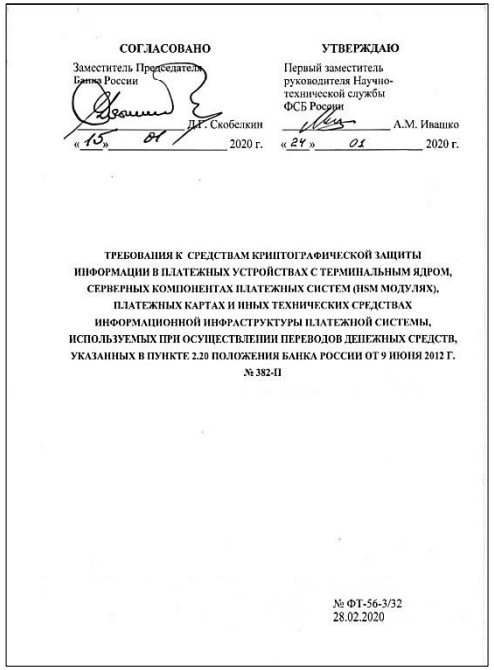
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Требования к СКЗИ в информационной инфраструктуре значимых платежных систем

- платежные устройства с терминальным ядром (терминалы и банкоматы)
- серверные компоненты платежных систем (HSM модули),
- платежные карты,
- иные технические средства информационной инфраструктуры платежной 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

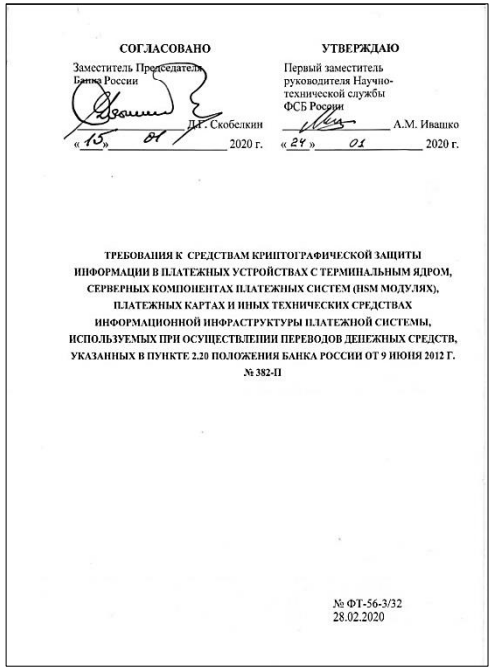
«24» 01 2020 г.

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

Требования к СКЗИ в информационной инфраструктуре значимых платежных систем

- Описание модели нарушителя для СКЗИ используемых при осуществлении переводов денежных средств.
- Общие принципы построения СКЗИ в технических средствах информационной инфраструктуры платежной системы
- Принципы применения криптографических механизмов защиты
- Принципы применения инженерно-криптографических механизмов защиты



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 01 2020 г.

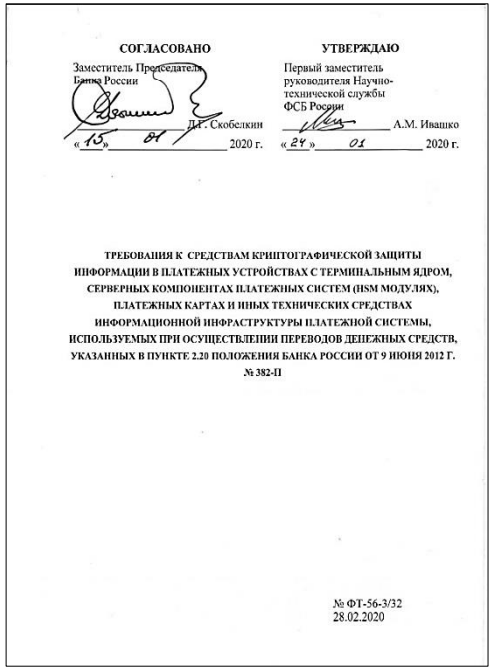
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Модель нарушителя для СКЗИ используемых при осуществлении переводов денежных средств

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



СОГЛАСОВАНО

Заместитель Председателя Банка России

Д.Г. Скобелкин

«15» 01 2020 г.

УТВЕРЖДАЮ

Первый заместитель руководителя Научно-технической службы ФСБ России

А.М. Ивашко

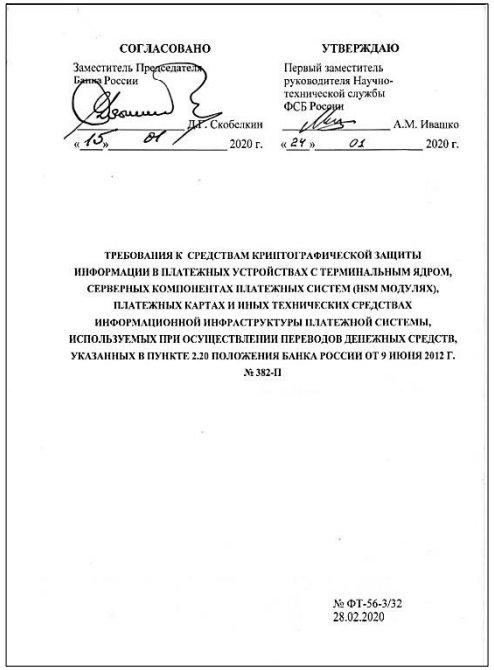
«24» 01 2020 г.

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

Модель нарушителя для СКЗИ используемых при осуществлении переводов денежных средств

- СКЗИ должны противостоять атакам, проводящимся нарушителем, имеющим непосредственный доступ к техническим средствам информационной инфраструктуры платежной системы, посредством попыток несанкционированного доступа, в том числе с использованием методов инженерного проникновения, с целью …
- Для платежных серверов необходимо обеспечить защиту ключевой информации пользователей от администратора (привилегированного пользователя)



СОГЛАСОВАНО

Заместитель Председателя Банка России

Д.Г. Скобелкин

«15» 01 2020 г.

УТВЕРЖДАЮ

Первый заместитель руководителя Научно-технической службы ФСБ России

А.М. Ивашко

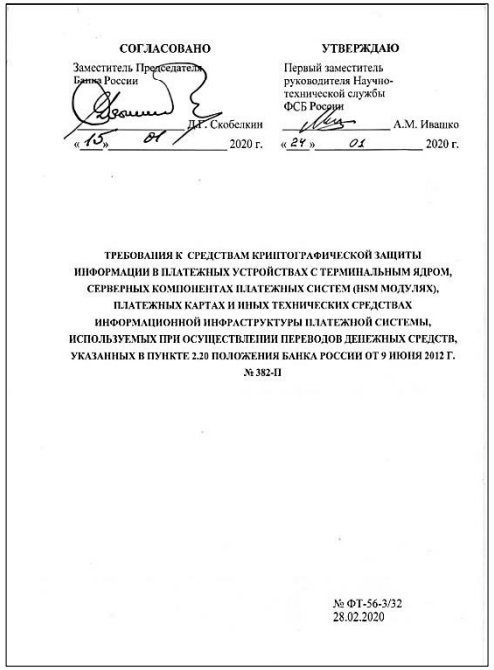
«24» 01 2020 г.

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

Общие принципы построения СКЗИ

- К конфиденциальным данным относятся: PIN-код, код верификации (CVV/CVC), ключи шифрования, ключи аутентификации, закрытые ключи, а также в некоторых случаях PAN
- Если используется дистанционное распределение ключей, то устройство должно поддерживать взаимную аутентификацию между отправляющим хостом распространения ключей и принимающим устройством.



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 01 2020 г.

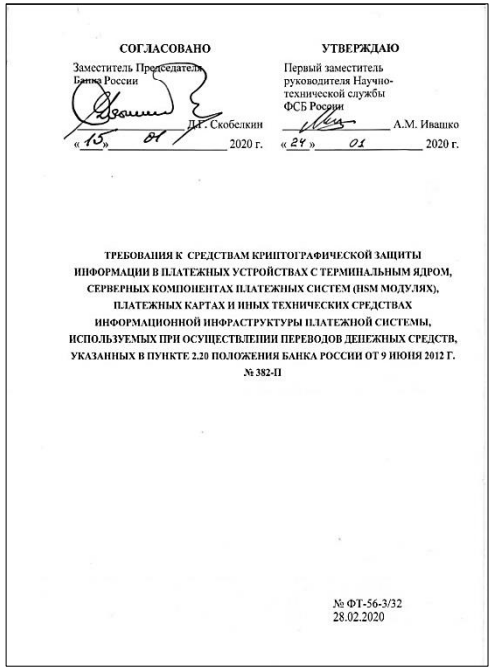
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Общие принципы построения СКЗИ

- Симметричные и закрытые ключи, которые находятся внутри устройства для обеспечения шифрования данных учетной записи, должны быть уникальными для каждого устройства.
- СКЗИ считается прошедшим оценку соответствия требованиям, если для ввода СКЗИ в эксплуатацию не требуется проведение дополнительных тематических исследований СКЗИ после утверждения положительного заключения ФСБ России о соответствии СКЗИ всем предъявляемым к нему требованиям.



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 01 2020 г.

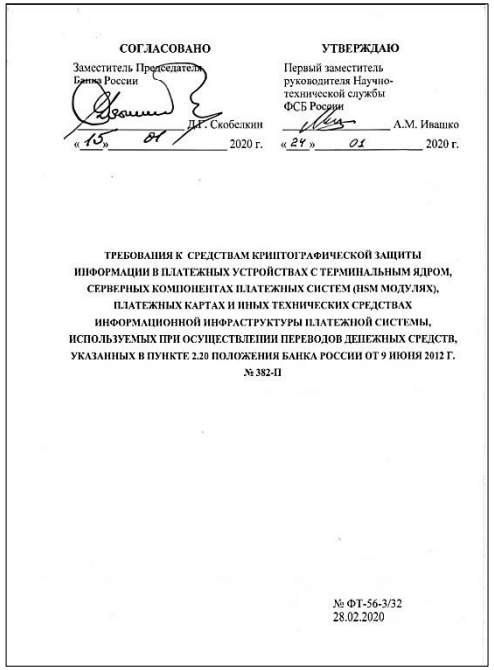
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Принципы применения криптографических механизмов защиты СКЗИ

- Применение криптографических механизмов.
- Применение датчиков случайных чисел.
- Выработка ключевой информации.
- Использование ключевой информации.
- Аутентификация субъектов доступа.
- Имитозащита.



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 01 2020 г.

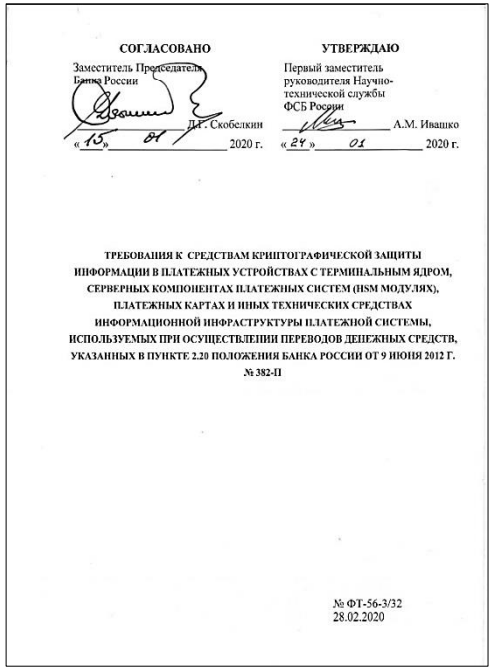
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Принципы применения криптографических механизмов защиты СКЗИ

- должны использоваться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта
- с целью обеспечения совместимости с действующими криптографическими решениями должны использоваться криптографические механизмы, отвечающие международным стандартам (ISO)



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

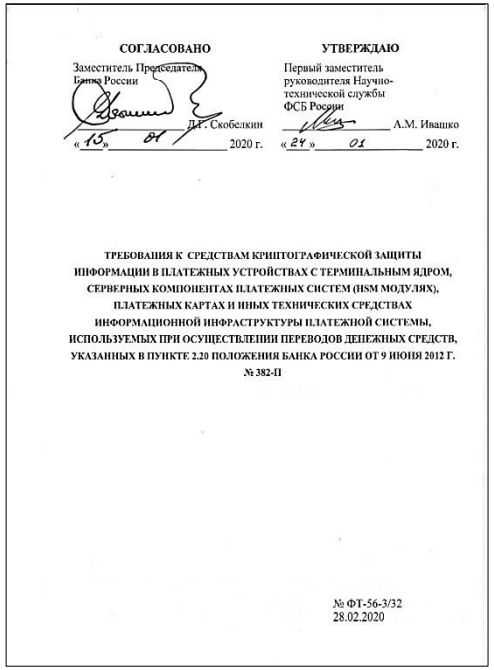
№ ФТ-56-3/32
28.02.2020

Принципы применения криптографических механизмов защиты СКЗИ

- Применение датчиков случайных чисел в СКЗИ основывается на следующих принципах:

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

ПДСЧ должен использовать криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта.



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 04 2020 г.

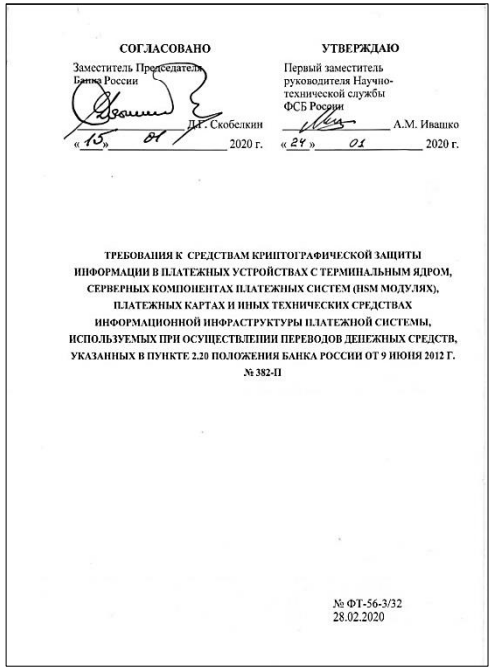
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Принципы применения криптографических механизмов защиты СКЗИ

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



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.

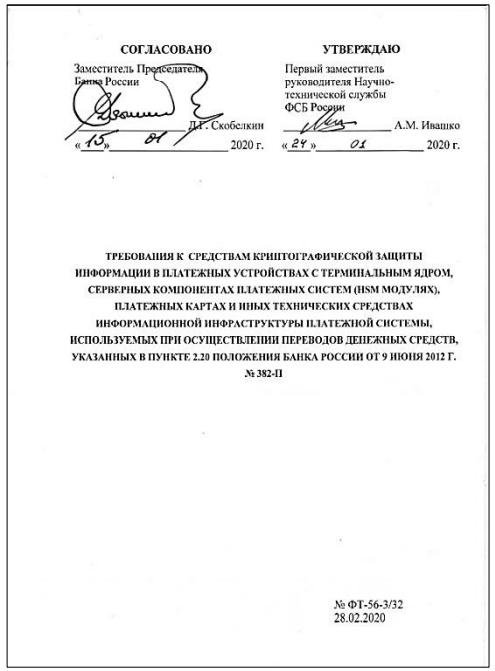
ТРЕБОВАНИЯ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНЫХ УСТРОЙСТВАХ С ТЕРМИНАЛЬНЫМ ЯДРОМ, СЕРВЕРНЫХ КОМПОНЕНТАХ ПЛАТЕЖНЫХ СИСТЕМ (HSM МОДУЛЯХ), ПЛАТЕЖНЫХ КАРТАХ И ИНЫХ ТЕХНИЧЕСКИХ СРЕДСТВАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПЛАТЕЖНОЙ СИСТЕМЫ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ, УКАЗАННЫХ В ПУНКТЕ 2.20 ПОЛОЖЕНИЯ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 Г. № 382-П

№ ФТ-56-3/32
28.02.2020

Принципы применения криптографических механизмов защиты СКЗИ

- Для обеспечения локальной аутентификации субъектов доступа должна быть реализована ролевая аутентификация субъектов доступа. При этом требуется поддержка следующих ролей:

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



СОГЛАСОВАНО

Заместитель Председателя Банка России

Д.Г. Скобелкин

«15» 01 2020 г.

УТВЕРЖДАЮ

Первый заместитель руководителя Научно-технической службы ФСБ России

А.М. Ивашко

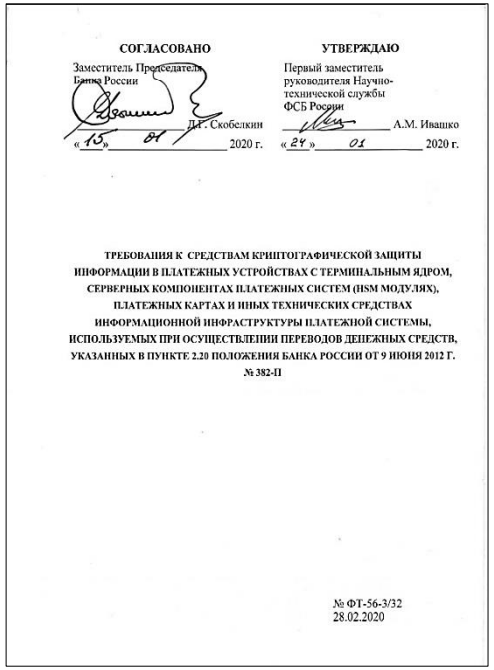
«24» 01 2020 г.

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

Принципы применения криптографических механизмов защиты СКЗИ

- Для всех классов СКЗИ для любого реализованного механизма аутентификации субъектов доступа должен быть реализован механизм ограничения числа следующих подряд неудачных попыток аутентификации одного субъекта доступа.
- При превышении числа следующих подряд неудачных попыток доступ этого субъекта доступа к СКЗИ следует блокировать на заданный промежуток времени.



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 01 2020 г.

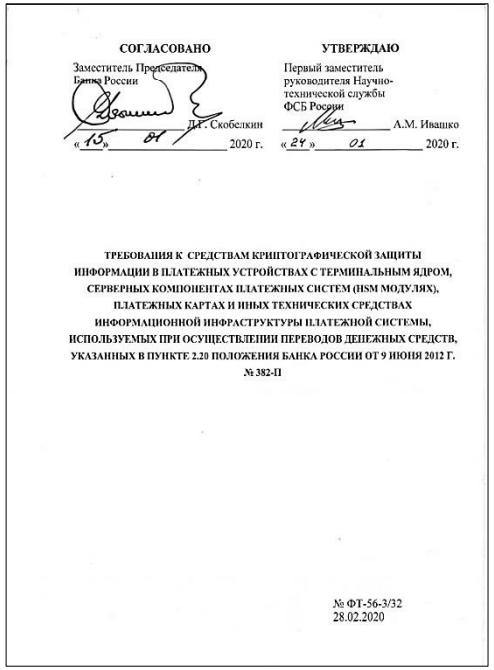
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Принципы применения инженерно-криптографических механизмов защиты

- 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.



СОГЛАСОВАНО

Заместитель Председателя Банка России

Д.Г. Скобелкин

«15» 01 2020 г.

УТВЕРЖДАЮ

Первый заместитель руководителя Научно-технической службы ФСБ России

А.М. Ивашко

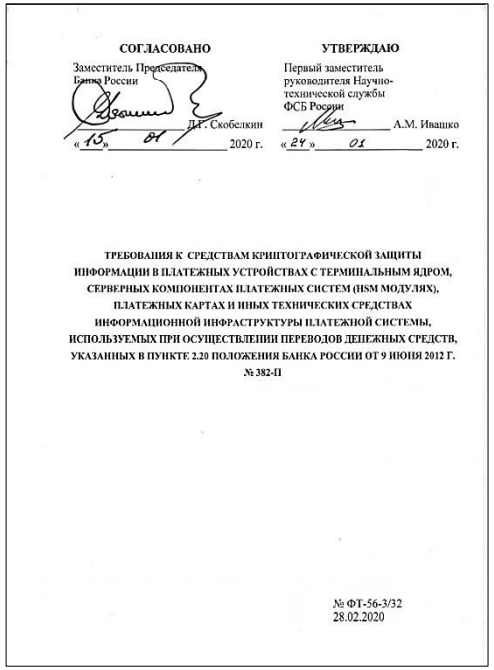
«24» 01 2020 г.

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

Принципы применения инженерно-криптографических механизмов защиты

- реализован контролирующий механизм, сигнализирующий или блокирующий работу СКЗИ при достижении предельных значений технических характеристик.
- контроль целостности на этапах хранения, транспортирования, ввода в эксплуатацию и эксплуатации .



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 01 2020 г.

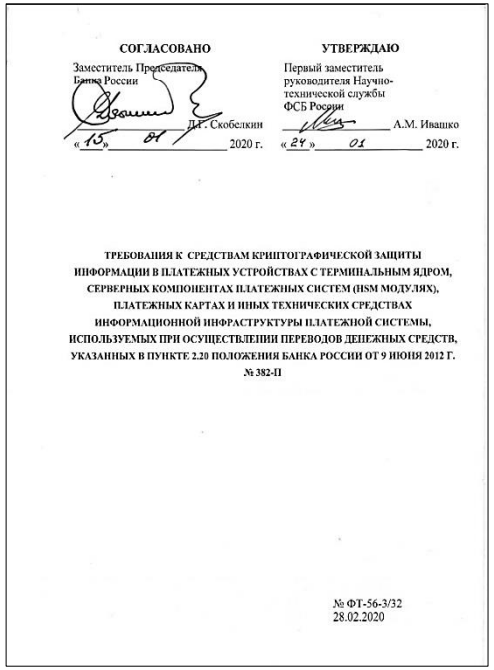
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Принципы применения инженерно-криптографических механизмов защиты

- 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
- механизм регистрации событий.



СОГЛАСОВАНО
Заместитель Председателя Банка России
Д.Г. Скобелкин
«15» 01 2020 г.

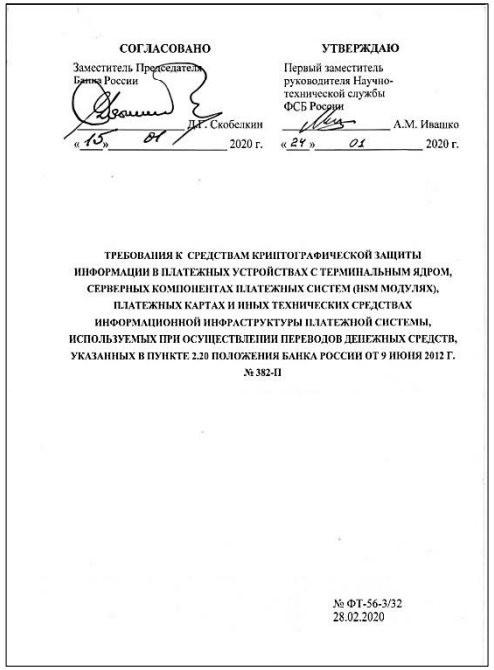
УТВЕРЖДАЮ
Первый заместитель руководителя Научно-технической службы ФСБ России
А.М. Ивашко
«24» 01 2020 г.

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

Принципы применения инженерно-криптографических механизмов защиты

- Положения по соответствию ПО СФ СКЗИ.
- Положения для аппаратных средств СКЗИ.
- Положения по физической защите СКЗИ и СФ СКЗИ.
- Дополнительные требования.
- Положения по обновлению ПО СФ СКЗИ.



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

Вопросы