

Ежегодная международная научно-практическая конференция

# «РусКрипто'2022»

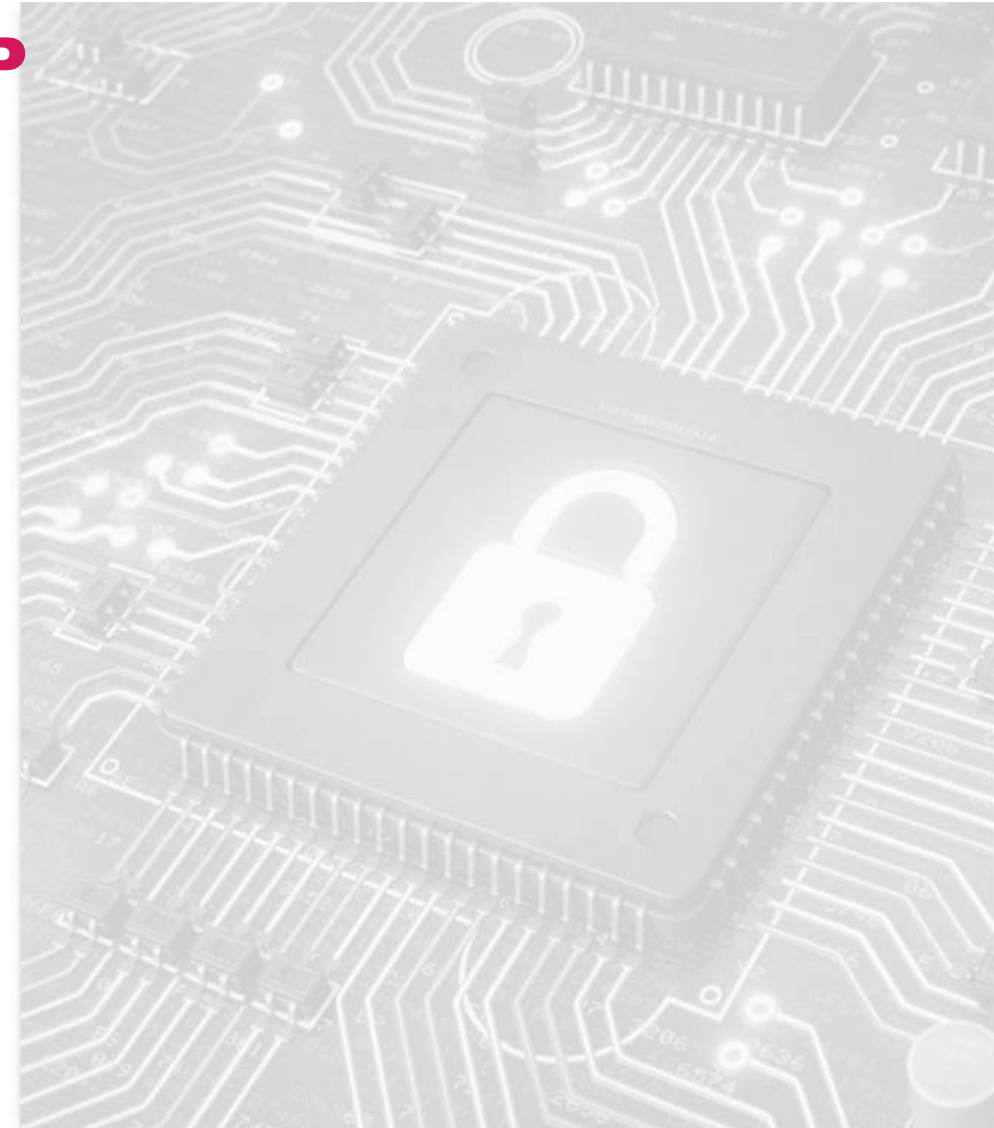
## О мероприятиях по импортозамещению в банковской сфере

**Зинюк Б.Ф.,**  
Академия криптографии  
Российской Федерации

# Информационная безопасность платежных систем

Федеральный закон от 27.06.2011 № 161  
«О национальной платежной системе»:

- Статья 27
- Статья 28 (часть 3.11)



# Информационная безопасность платежных систем

Ключевым регулятором в отрасли является  
Центральный Банк Российской Федерации



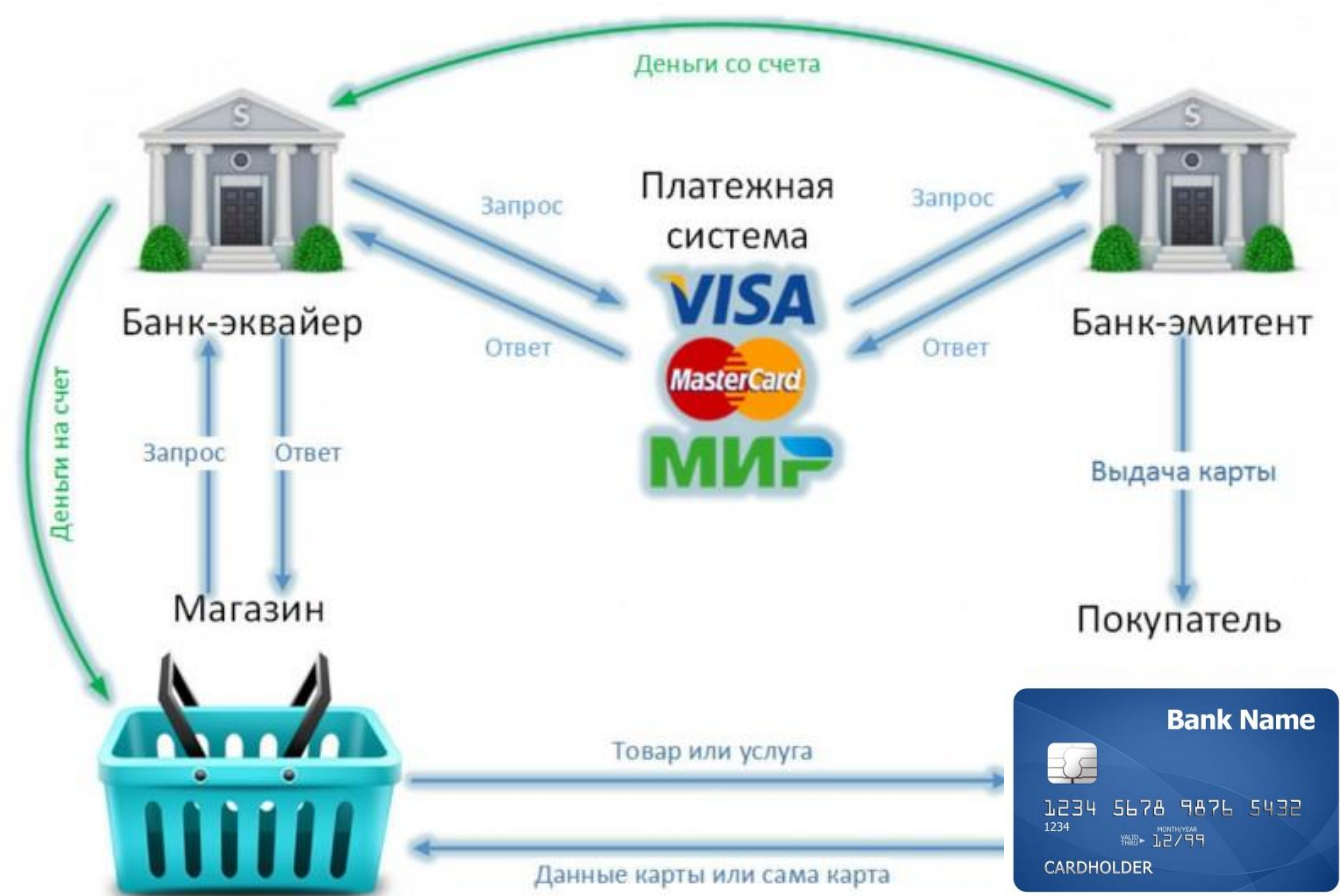
ФСБ России



ФСТЭК России



# Информационная безопасность платежных систем



# Информационная безопасность платежных систем



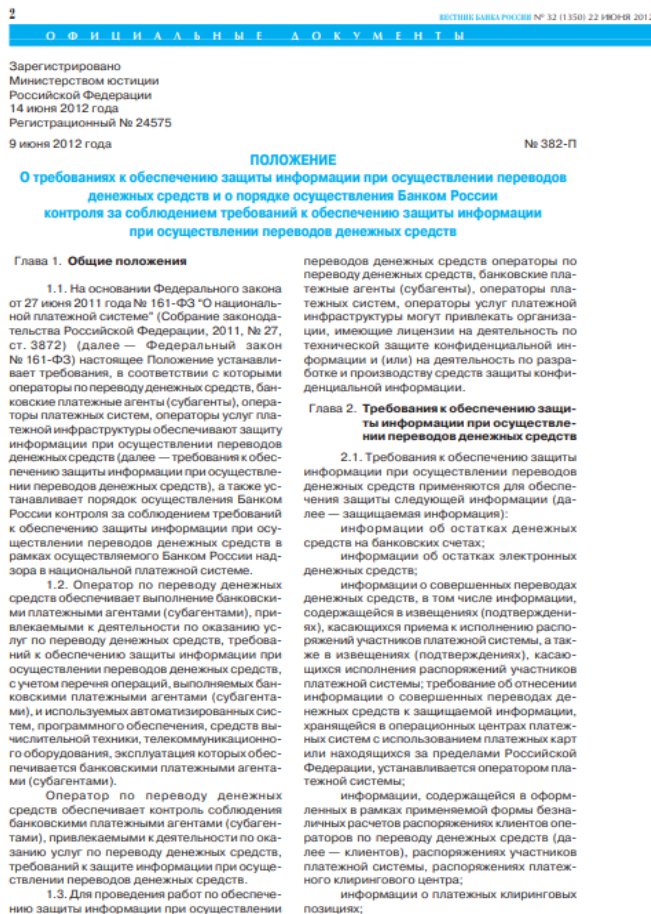
# Информационная безопасность платежных систем



## Регуляторы платежных систем:

- Payment Card Industry Data Security Standard (**PCI DSS**) - это стандарт безопасности данных индустрии платёжных карт, разработанный Советом по стандартам безопасности индустрии платёжных карт (Payment Card Industry Security Standards Council, PCI SSC), учреждённым международными платёжными системами Visa, MasterCard, American Express, JCB и Discover
- **EMVCo** - организация, созданная международными платёжными системами с целью разработки международных стандартов для чиповых карт и операций с ними. Учредителями организации **EMVCo** являются международные платёжные системы American Express, Discover, JCB, MasterCard, UnionPay и Visa

# 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

# Положение Банка России № 719-П

Зарегистрировано Министерством юстиции  
Российской Федерации 23 сентября 2020 года  
Регистрационный № 59991

4 июня 2020 года

№ 719-П

## ПОЛОЖЕНИЕ

### 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

Настоящее Положение на основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ "О национальной платежной системе" (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) устанавливает требования к обеспечению операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, поставщиками платежных приложений, операторами платежных систем, операторами услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств, а также порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

#### Глава 1. Общие положения

1.1. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры в части требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается при осуществлении переводов денежных средств операторами по переводу денежных средств (далее — объекты информационной инфраструктуры), должны обеспечивать реализацию установленных настоящим Положением уровней защиты информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения информации, указанной в абзаце первом пункта 1.3 настоящего Положения, в целях осуществления переводов денежных средств, определенных

национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер", утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст "Об утверждении национального стандарта Российской Федерации" (М., ФГУП "Стандартинформ", 2017) (далее — ГОСТ Р 57580.1-2017); ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры с учетом особенностей, предусмотренных пунктами 3.8 и 3.9 настоящего Положения;

проведение оценки соответствия уровням защиты информации, установленным настоящим Положением (далее — оценка соответствия защиты информации), в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия", утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст "Об утверждении национального стандарта Российской Федерации" (М., ФГУП "Стандартинформ", 2018) (далее — ГОСТ Р 57580.2-2018), с учетом особенностей, предусмотренных пунктами 2.3, 2.4, 3.6—3.9, 4.4, 4.5, 6.7 и 6.8 настоящего Положения.

Оценка соответствия защиты информации должна осуществляться с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 "О лицензировании

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



# Положение Банка России № 719-П

Зарегистрировано Министерством юстиции  
Российской Федерации 23 сентября 2020 года  
Регистрационный № 59991

4 июня 2020 года

№ 719-П

## ПОЛОЖЕНИЕ

**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**

Настоящее Положение на основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ "О национальной платежной системе" (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) устанавливает требования к обеспечению операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, поставщиками платежных приложений, операторами платежных систем, операторами услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств, а также порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

### Глава 1. Общие положения

1.1. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры в части требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается при осуществлении переводов денежных средств операторами по переводу денежных средств (далее — объекты информационной инфраструктуры), должны обеспечивать реализацию установленных настоящим Положением уровней защиты информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения информации, указанной в абзаце первом пункта 1.3 настоящего Положения, в целях осуществления переводов денежных средств, определенных

национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер", утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст "Об утверждении национального стандарта Российской Федерации" (М., ФГУП "Стандартинформ", 2017) (далее — ГОСТ Р 57580.1-2017);

ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры с учетом особенностей, предусмотренных пунктами 3.8 и 3.9 настоящего Положения;

проведение оценки соответствия уровням защиты информации, установленным настоящим Положением (далее — оценка соответствия защиты информации), в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия", утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст "Об утверждении национального стандарта Российской Федерации" (М., ФГУП "Стандартинформ", 2018) (далее — ГОСТ Р 57580.2-2018), с учетом особенностей, предусмотренных пунктами 2.3, 2.4, 3.6—3.9, 4.4, 4.5, 6.7 и 6.8 настоящего Положения.

Оценка соответствия защиты информации должна осуществляться с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 "О лицензировании

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

# Положение Банка России № 719-П

Зарегистрировано Министерством юстиции  
Российской Федерации 23 сентября 2020 года  
Регистрационный № 59991

4 июня 2020 года

№ 719-П

## ПОЛОЖЕНИЕ

**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**

Настоящее Положение на основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ "О национальной платежной системе" (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) устанавливает требования к обеспечению операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, поставщиками платежных приложений, операторами платежных систем, операторами услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств, а также порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

### Глава 1. Общие положения

1.1. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, операторы услуг платежной инфраструктуры в части требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается при осуществлении переводов денежных средств операторами по переводу денежных средств (далее — объекты информационной инфраструктуры), должны обеспечивать реализацию установленных настоящим Положением уровней защиты информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения информации, указанной в абзаце первом пункта 1.3 настоящего Положения, в целях осуществления переводов денежных средств, определенных

национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер", утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст "Об утверждении национального стандарта Российской Федерации" (М., ФГУП "Стандартинформ", 2017) (далее — ГОСТ Р 57580.1-2017);

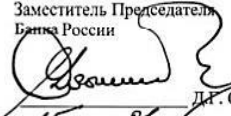
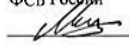
ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры с учетом особенностей, предусмотренных пунктами 3.8 и 3.9 настоящего Положения;

проведение оценки соответствия уровням защиты информации, установленным настоящим Положением (далее — оценка соответствия защиты информации), в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия", утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст "Об утверждении национального стандарта Российской Федерации" (М., ФГУП "Стандартинформ", 2018) (далее — ГОСТ Р 57580.2-2018), с учетом особенностей, предусмотренных пунктами 2.3, 2.4, 3.6—3.9, 4.4, 4.5, 6.7 и 6.8 настоящего Положения.

Оценка соответствия защиты информации должна осуществляться с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 "О лицензировании

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

# Требования к СКЗИ в информационной инфраструктуре значимых платежных систем

<b>СОГЛАСОВАНО</b> Заместитель Председателя Банка России  Д.И. Скобелкин « 15 » 01 2020 г.	<b>УТВЕРЖДАЮ</b> Первый заместитель руководителя Научно- технической службы ФСБ России  А.М. Ивашко « 24 » 01 2020 г.
--	--

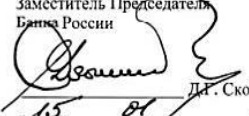
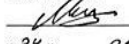
ТРЕБОВАНИЯ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ  
ИНФОРМАЦИИ В ПЛАТЕЖНЫХ УСТРОЙСТВАХ С ТЕРМИНАЛЬНЫМ ЯДРОМ,  
СЕРВЕРНЫХ КОМПОНЕНТАХ ПЛАТЕЖНЫХ СИСТЕМ (НСМ МОДУЛЯХ),  
ПЛАТЕЖНЫХ КАРТАХ И ИНЫХ ТЕХНИЧЕСКИХ СРЕДСТВАХ  
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПЛАТЕЖНОЙ СИСТЕМЫ,  
ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ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

№ ФТ-56-3/32  
28.02.2020

- 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/104752/ft\\_32.pdf](http://www.cbr.ru/content/document/file/104752/ft_32.pdf)

# Требования к СКЗИ в информационной инфраструктуре значимых платежных систем

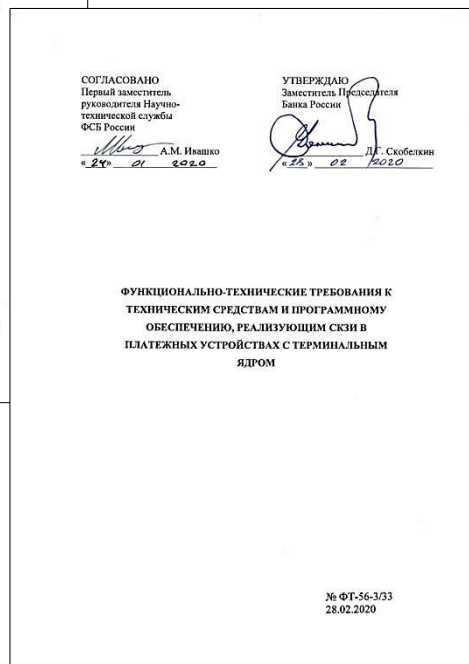
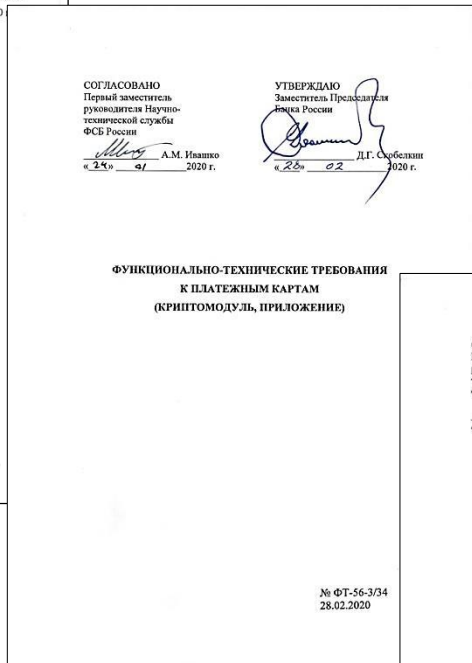
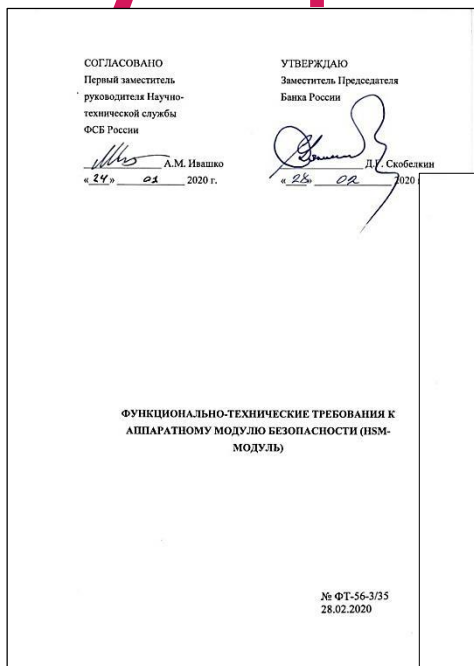
СОГЛАСОВАНО	УТВЕРЖДАЮ
Заместитель Председателя Банка России	Первый заместитель руководителя Научно- технической службы ФСБ России
	
Д.Г. Скобелкин	А.М. Ивашко
« 15 » 01 2020 г.	« 24 » 01 2020 г.

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

- 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

# Функционально-технические требования



К HSM-модулю  
К платежным картам  
К терминалам


[http://www.cbr.ru/information\\_ security/](http://www.cbr.ru/information_security/)

# Центр тестирования технических средств и программного обеспечения, реализующих СКЗИ значимых платежных систем

## ЦТ СКЗИ предназначен для автоматизации выполнения следующих задач:

- предоставление возможности для российских производителей технических средств и программного обеспечения проводить проверку (тестирование) разработанных аппаратных модулей безопасности (HSM модулей), платежных устройств с терминальным ядром, платежных карт (крипто приложений), банковского программного обеспечения поддержки процессинга, эквайринга и персонализации платежных карт:
  - 1) на соответствие функционально-техническим требованиям;
  - 2) по оценке влияния банковского программного обеспечения поддержки процессинга, эквайринга и персонализации платежных карт на разрабатываемых СКЗИ, по методикам, согласованным с ФСБ России;
  - 3) на соответствие требованиям платежных систем;
- создание унифицированного канала взаимодействия с разработчиками;
- обеспечение безопасного механизма передачи пакетов модификаций, библиотек программного обеспечения, сборок и файлов синхронизации в контур тестирования ЦТ СКЗИ.

# ТЕХНОЛОГИЧЕСКИЕ КАРТЫ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ, ОПИСЫВАЮЩИЕ ИНФРАСТРУКТУРНЫЕ ПРОЦЕССЫ ДЕЙСТВУЮЩЕЙ СИСТЕМЫ ПРОВЕДЕНИЯ КАРТОЧНЫХ ПЛАТЕЖЕЙ И ЭМИССИИ КАРТ НА ТЕРРИТОРИИ РФ

УТВЕРЖДАЮ  
Заместитель Председателя  
Банка России  
 Г.А. Зубарев  
«22» 03 2022 г.

ТЕХНОЛОГИЧЕСКИЕ КАРТЫ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ  
ДЕНЕЖНЫХ СРЕДСТВ, ОПИСЫВАЮЩИЕ ИНФРАСТРУКТУРНЫЕ  
ПРОЦЕССЫ ДЕЙСТВУЮЩЕЙ СИСТЕМЫ ПРОВЕДЕНИЯ  
КАРТОЧНЫХ ПЛАТЕЖЕЙ И ЭМИССИИ КАРТ НА ТЕРРИТОРИИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Москва, 2022 г.

№ ТРД-56-5/603  
от 22.03.2022

- Систематизировать процессы, протекающие в значимых платежных системах и сформировать полный список используемых стандартов
- Своевременно отслеживать изменения используемых стандартов, функций и протоколов
- Расширить список обязательных тестов криптографического оборудования, предназначенного для использования в значимых платежных системах
- Классифицировать системы тестов и выбирать только те, которые соответствуют заявленным при тестировании процессам

# План работ на 2022 год Рабочей группы по использованию СКЗИ в значимых платежных системах

- Выбор процессов, описанных в «Технологических картах осуществления переводов денежных средств, описывающие инфраструктурные процессы действующей системы проведения карточных платежей и эмиссии карт на территории Российской Федерации» для которых необходимо сформировать детальные сценарии для тестирования в первую очередь
- Обсуждение проблемных вопросов сертификации российского оборудования по линии PCI SSC



Вопросы

???

# Контактная информация

## Электронная почта:

Ziniuk\_bf@tc26.ru

## Телефон:

+7 (926) 566 – 82 – 95

