СОГЛАСОВАНО
Первый заместитель
руководителя Научно-
технической службы
ФСБ России

_____ А.М. Ивашко
«24» 01 2020

УТВЕРЖДАЮ
Заместитель Председателя
Банка России

_____ Д.Г. Скобелкин
«28» 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

СОДЕРЖАНИЕ

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящих требованиях применяются следующие термины с соответствующими определениями.

Термин/Сокращение	Определение
Платежное устройство с терминальным ядром (сокращенно – ПУ, Платежный терминал)	Программно-аппаратный комплекс (или его части), позволяющий считывать информацию с платежной карты и предназначенный для выполнения операций с использованием платежных карт, таких как осуществление переводов денежных средств, выдача и прием наличных денежных средств
Персональный идентификационный номер (сокращенно – ПИН)	**(PIN, personal identification number)** Секретный цифровой пароль, известный только пользователю платежной карты и платежной системе, используемый для аутентификации пользователя
PAN-код	(personal account number) Номер платежной карты, отображенный на ее лицевой стороне
PED	(PIN entry device) Платежное устройство с терминальным ядром, поддерживающее ввод ПИН
СВТ	Средство вычислительной техники, представляющее собой программно-аппаратный комплекс, способный функционировать самостоятельно или в составе других систем и предназначенный для обработки информации
Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
Вендор ПУ (терминальный вендор)	Юридическое лицо, ответственное за соответствие ПУ и (или) его компонентов установленным требованиям
Код верификации (CVV/CVC)	(Card Verification Value / Card Validation Code) Трехзначный числовой код проверки подлинности платежной карты
СКЗИ	Средство криптографической защиты информации

HSM	Аппаратный криптографический модуль (Hardware Security Module), криптографическое средство шифрования информации и управления ключами

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие требования разработаны и утверждены в рамках мероприятий федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»: 05.02.002.017.003 – «Определение порядка разработки, ответственных за поддержание в актуальном состоянии, а также разработка и опубликование функционально-технических требований к техническим средствам и программному обеспечению, реализующим СКЗИ (включая функциональные и эксплуатационные требования): аппаратный модуль безопасности (HSM-модули); платежные устройства с терминальным ядром; платежные карты (криптомодуль, приложение); интернет-браузеры и стандартные операционные системы и т.д.».

Настоящий документ определяет функционально-технические требования к техническим средствам и программному обеспечению, реализующим СКЗИ в платежных устройствах с терминальным ядром.

Требования к устройствам предъявляются в зависимости от данных платежных карт, которые они обрабатывают, хранят, передают. Классификация платежных устройств с терминальным ядром представлена в разделе 2.

Проведение тестирования технических средств на соответствие требованиям, представленным в настоящем документе, осуществляется с привлечением Центра тестирования технических средств и программного обеспечения в соответствии с регламентом и методиками проведения тестирования[1].

Подтверждение соответствия требованиям настоящего документа не исключает подтверждение соответствия требованиям, устанавливаемым платежными системами, а также требованиям по информационной безопасности ФСБ России.

---

[1] Регламент и методики проведения тестирования разрабатываются в рамках выполнения мероприятия 05.02.002.017.008 «Создание и обеспечение функционирования центра тестирования технических средств и программного обеспечения на соответствие функционально-техническим требованиям, включая разработку регламента и методики тестирования» паспорта федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», утвержденного президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 27 декабря 2018 № 6) / задача 1.22 «Обеспечение информационной безопасности, в том числе с использованием российских криптографических средств, в значимых платежных системах» паспорта федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», утвержденного президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 № 9, приложение 5 и приложение 8).

2. КЛАССИФИКАЦИЯ ПЛАТЕЖНЫХ УСТРОЙСТВ С ТЕРМИНАЛЬНЫМ ЯДРОМ

По авторизации платежные устройства делятся на следующие типы:

- с возможностью отложенной авторизации,
- только онлайн-авторизация.

2.1. Терминалы точек обслуживания (PED-устройства)

PED-терминал – это программно-аппаратный комплекс, используемый при расчетах с помощью платежных карт с вводом ПИН.

PED-терминал позволяет проводить расчеты с использованием различных методов проверки держателя карты, включая подпись, проверку ПИН-кода, проверку «на устройстве», биометрические методы проверки.

PED-терминал должен быть оборудован дисплеем и клавиатурой, в случае если для проверки держателя карты требуется ввести ПИН-код, и устройством печати или сенсорным экраном, в случае если требуется подпись держателя карты.

Допускается встраивание PED-терминалов в терминалы самообслуживания.

2.2. Терминалы точек обслуживания без ввода ПИН (Non-PED)

Non-PED-терминал – это программно-аппаратный комплекс, используемый при расчетах с помощью платежных карт, который не позволяет проводить авторизацию платежа по ПИН. Non-PED-терминал позволяет проводить расчеты только без ввода ПИН. Non-PED-терминал не может запрашивать ПИН при осуществлении операций.

2.3. Терминалы для использования в устройствах самообслуживания (UPT-устройства)

UPT-устройства предназначены для чтения, фиксации и передачи данных платежной карты в устройствах самообслуживания (вендинговые автоматы, билетные машины и т.п.).

2.4. Зависимые терминалы для использования в устройствах самообслуживания (EPP-устройства)

EPP-устройства предназначены для обеспечения ввода и обработки ПИН, использования в устройствах самообслуживания под управлением процессора устройства самообслуживания.

2.5. Защищенный считыватель карт (SCR-устройство)

SCR-устройство – это защищенный считыватель карт, который может использоваться для подключения к незащищенным устройствам или использоваться как OEM-продукт для встраивания в платежное устройство или банкомат. Тип считывателя карт может быть гибридным, считывателем магнитной полосы, считывателем карт с чипом и бесконтактным.

2.6. Защищенный считыватель карт для пользовательских устройств (SCRP-устройство)

SCRP-устройство – это защищенный считыватель карт для использования с пользовательскими устройствами, такими как мобильный телефон или планшет. Тип считывателя: для карт с чипом и/или бесконтактных карт.

3. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

3.1. Нормы и стандарты, которым должны соответствовать платежные устройства с терминальным ядром

Функциональные требования к считывателю магнитной полосы

Требования к считывателю магнитной полосы описаны в ISO/IEC 7813.

3.1.1. Функциональные требования к считывателю смарт-карт

Требования к считывателю смарт-карт определены в документе «EMV Integrated Circuit Card Specification for Payment System. Book 1. Application Independent ICC to Terminal Interface Requirements».

3.1.2. Функциональные требования к считывателю бесконтактных карт

Требования к считывателю бесконтактных карт определены в документе «EMV. Level 1 Specification for Payment System. EMV Contactless Interface Specification. Version 3.0».

Требования к протоколу обмена между платежным устройством и смарт-картой

– «EMV Integrated Circuit Card Specification for Payment System. Book 2. Security and Key Management»;

– «EMV Integrated Circuit Card Specification for Payment System. Book 3. Application Specification»;

– «EMV Integrated Circuit Card Specification for Payment System. Book 4. Cardholder, Attendant, and Acquirer Interface Requirements».

3.1.5. Требования к протоколу обмена между ПУ и бесконтактной картой

– «EMV Contactless Specifications for Payment Systems. Book B. Entry Point Specification»;

– «EMV Contactless Specifications for Payment Systems. Book A. Architecture and General Requirements»;

– «EMV Contactless Specifications for Payment Systems. Book C-2. Kernel 2 Specification»;

– «EMV Contactless Specifications for Payment Systems. Book C-3. Kernel 3 Specification»;

– «EMV Contactless Specifications for Payment Systems. Book C-4. Kernel 4 Specification»;

– «EMV Contactless Specifications for Payment Systems. Book C-5. Kernel 5 Specification»;

– «EMV Contactless Specifications for Payment Systems. Book C-6. Kernel 6 Specification»;

– «EMV Contactless Specifications for Payment Systems. Book C-7. Kernel 7 Specification».

3.2. Требования по функциональности

3.2.1. Интерфейсы для чтения и обработки данных карт

ПУ должно обеспечивать чтение и обработку данных карт через как минимум один из интерфейсов: контактный интерфейс, бесконтактный интерфейс.

В случае если ПУ поддерживает контактный интерфейс, оно может дополнительно поддерживать возможность чтения магнитной полосы карты. Контактный интерфейс ПУ должен удовлетворять требованиям спецификации «EMV Integrated Circuit Card Specification for Payment System. Book 1. Application Independent ICC to Terminal Interface Requirements».

Бесконтактный интерфейс ПУ должен удовлетворять требованиям спецификации «EMV. Level 1 Specification for Payment System. EMV Contactless Interface Specification. Version 3.0». Устройство чтения магнитной полосы должно удовлетворять требованиям ISO/IEC 7813.

Процедура обработки транзакции в ПУ должна выполняться в соответствии со спецификациями Level 2 платежных систем.

ПУ с бесконтактным интерфейсом должно поддерживать как минимум протоколы ‘01’ и ‘02’, описанные в спецификации ядра бесконтактного ридера платежной системы «Мир».

3.2.2. Авторизация и процессинг

ПУ должно обеспечивать безопасное подключение к процессингу для передачи сообщений, необходимых для выполнения финансовых и управляющих операций. ПУ должно:

- поддерживать протокол обмена сообщениями, используемый процессингом,
- синхронизировать финансовую и управляющую информацию с процессингом,
- передавать процессингу достоверную информацию, полученную в процессе обработки данных карты,
- корректно обрабатывать ответ процессинга, содержащий код авторизации, данные аутентификации и скрипты,
- представлять результат транзакции на дисплее, в чеке или с помощью световой или звуковой индикации,
- корректно обрабатывать ошибки обмена данными с процессингом.

3.2.2.1. Финансовые и административные операции

ПУ должно поддерживать подмножество административных и финансовых операций, указанных в спецификации ISO-8583. Точный набор операций, который должен реализовать терминал, определяется требованиями процессинга и используемым в процессинге протоколом взаимодействия. Обязательно требуется реализовать операцию (echo test), которая позволяет проверить соединение с процессингом. Рекомендуется как минимум реализовать следующие финансовые операции: Оплата, Возврат и Отмена, а также административные операции загрузки рабочих ключей. ПУ должно поддерживать процедуру автоотмены, которая выполняется в случае, если терминал не получил подтверждения завершения финансовой операции. Автоотмена используется для того, чтобы синхронизировать данные ПУ и процессинга в случае ошибок, вызванных нарушениями связи. Процедура автоотмены регламентируется выбранным протоколом обмена данными с процессингом (например, ISO-8583). ПУ должно обеспечивать возможность настройки количества повторов операции авто-отмены и таймаутов ожидания ответа от хоста процессинга.

3.2.2.2. Протоколы обмена данными с банковским сервером.

ПУ должно поддерживать протокол обмена сообщениями с процессингом ISO-8583. ПУ может реализовывать часть требований любого другого протокола взаимодействия по согласованию с процессингом.

3.2.2.3. Шифрование ПИН-блока

В случае если ПУ поддерживает проверку держателя карты с помощью ПИН-кода онлайн, ПУ должно обеспечивать шифрование ПИН-блока, а также передачу зашифрованного ПИН-блока в авторизационных сообщениях, направляемых процессингу. Следует заполнить память, в которой в процессе вычисления ПИН-блока хранилось значение ПИН-кода, случайными значениями непосредственно после окончания вычисления ПИН-блока.

Метод шифрования ПИН должен соответствовать ISO 9564.

Стандарт: IETF RFC 1851, P 1323565.1.011-2017.

3.2.2.4. Генерация и проверка MAC

В случае если вычисление MAC требуется процессингом, ПУ должно вычислять MAC для проверки входящих и подписи исходящих сообщений, пересылаемых между сервером процессинга и терминалом.

Стандарты: ISO 9797-1, X9-19 (Retail Mac).

3.2.3. Аутентификация данных карты

ПУ должно поддерживать следующие три алгоритма аутентификации данных контактной/бесконтактной карты:

a) Static Data Authentication (SDA),

b) Dynamic Data Authentication (DDA),

c) Combined Data Authentication (CDA).

Дополнительно должны быть поддержаны требования к алгоритму аутентификации CDA, указанные в спецификациях бесконтактных ядер L2 qVSDC (VISA) и платежной системы «Мир» (fDDA).

Стандарт: EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management, P 1323565.1.016-2018.

3.2.4. Управление ключами и сертификатами

ПУ должно поддерживать импорт и генерацию ключей.

В случае если ПУ имеет дисплей и клавиатуру, ПУ должно поддерживать режим ручного ввода компонентов ключей с клавиатуры. ПУ должно обеспечить безопасный ввод ключей и компонентов ключей с клавиатуры в соответствии с положениями спецификации PCI.

3.2.4.1. Безопасное хранение ключей

Ключи, используемые ПУ, должны храниться в зашифрованном виде. Обработка ключей в открытом виде допускается только при проведении криптографических операций, в которых задействованы эти ключи. Внешний доступ к хранимым в ПУ ключам в открытом виде должен быть запрещен. Следует заполнить память, в которой хранились значения ключей или компонентов ключей, случайными значениями сразу после использования ключа. Не допускается шифрование ключом, который имеет более низкую криптостойкость, чем ключ, который им шифруется. Значение каждого ключа, хранимого в ПУ, должно быть уникальным.

Стандарты: NIST FIPS 197, IETF RFC 1851, ISO 11568 (ANSI X9.24).

3.2.4.2. Генерация ключей

ПУ должно генерировать ключи для локального применения. Эти ключи не должны экспортироваться из терминала в открытом или защищенном виде и должны быть стерты из памяти в случае нарушения защиты ПУ.

Стандарты:

NIST FIPS 46-3/NIST Special Publication 800-67, ISO/IEC 10116 (ECB, CBC), ISO 11568.

3.2.4.3. Импорт ключей

Импорт ключей обеспечивает загрузку ключей в ПУ, в том числе удаленную загрузку в сетевой инфраструктуре с публичным доступом. Импортируемые ключи используются для защиты соединений ПУ с банковскими серверами, серверами настроек и серверами распределения ключей.

Стандарты:

1. ANSI X9.17, ASC X9 TR 31-2018,

2. NIST Special Publication 800-38F.

3.2.4.4. Алгоритмы управления ключами DUKPT

Алгоритмы управления ключами DUKPT обеспечивают безопасное управление ключами, используемыми для защиты информации, передаваемой между ПУ и банковским сервером, в том числе защиты финансовых транзакций. DUKPT следует использовать для шифрования сообщений между ПУ и процессингом в случае, если он поддерживается процессингом.

Стандарт: ANSI-X9.24-2017 part 3 (DUPKT).

3.2.4.5. Расчет контрольного числа симметричного ключа

Контроль корректности введенных или импортированных значений ключей и компонентов ключей. ПУ должно отображать по запросу контрольные значения ключей симметричных алгоритмов (3DES, AES).

Стандарт: ISO/IEC 18033-3:2010: Part 3: Block ciphers.

3.2.4.6. Импорт сертификатов

ПУ должно иметь способность импортировать реквизиты, необходимые для установки безопасного соединения с внешними серверами (например, SSL-сертификатов), за исключением реквизитов сервера настроек. Реквизиты сервера настроек загружаются в ПУ в процессе активации терминала. ПУ должно обеспечить безопасное хранение импортируемых реквизитов и их аутентификацию во время импорта или в любое время после загрузки в ПУ по запросу.

Стандарт: ITU-T X.509.

3.2.4.7. Безопасное хранение сертификатов платежных систем

Сертификаты платежных систем должны храниться в ПУ и обрабатываться способом, исключающим их подмену. Следует использовать цифровую подпись для аутентификации сертификатов. Шифрование публичных сертификатов, хранимых в ПУ, не обязательно.

Стандарты: NIST FIPS 197, IETF RFC 1851.

3.2.5. Активация платежного терминала

Активация ПУ должна выполнятся в условиях, исключающих неавторизованный доступ к ПУ. Активация ПУ должна быть произведена перед его использованием по назначению. Неактивированное ПУ не должно выполнять функции, требующие доступ к ключам и сертификатам, кроме тех ключей и сертификатов, которые требуются для активации. Повторная активация ПУ удаляет данные, имеющиеся на терминале, включая настройки, ключи и сертификаты, кроме тех, которые требуются для повторной активации.

3.2.5.1. Генерация ключей, создание и передача в терминал сертификатов для связи с удаленными серверами

Активация ПУ включает загрузку реквизитов доверенного внешнего источника настроек ПУ, генерацию ключей и сертификатов, необходимых для установки соединения с доверенным внешним источником настроек.

Стандарты: IETF RFC 8017.

3.2.5.2. Генерация корневого ключа AES или 3DES для защиты данных на терминале

Активация ПУ включает генерацию локальных ключей для защиты и аутентификации данных, хранящихся в ПУ.

Стандарты: NIST FIPS 197, IETF RFC 1851.

3.2.6. Удаленная загрузка настроек платежного устройства с терминальным ядром

Настройки ПУ должны загружаться с доверенного источника настроек, который устанавливается в процессе активации. ПУ должно использовать взаимную аутентификацию и аутентифицировать источник. Для шифрования и подписи данных, передаваемых по защищенным каналам связи, следует использовать симметричные алгоритмы шифрования.

Рекомендуется для установки безопасного соединения между источником настроек и ПУ использовать протокол TLS 1.2 с взаимной аутентификацией. К настройкам терминала относятся:

идентификационные данные терминала, такие как номер терминала и клиентские сертификаты, использующиеся для установки безопасного соединения с различными удаленными сервисами, которые используются терминалом;

настройки контактного и бесконтактного ядра EMV. Эти настройки определяются спецификациями L2 платежных систем;

публичные сертификаты платежных систем;

черные списки банковских сертификатов и номеров карт;

дополнительные настройки функций терминала. Например, разрешение использования интерфейсов терминала, формат чека и пр.

ПУ должно обеспечивать проверку обновлений настроек и загрузку настроек в автоматическом режиме по установленному расписанию или при включении ПУ и по запросу оператора.

Стандарты: IETF RFC 5246, IETF RFC 8017, IETF RFC 1851, IETF RFC 6234.

3.2.7. Защита данных в платежном устройстве с терминальным ядром

Данные ПУ, включая настройки, содержащие конфиденциальную информацию и информацию о проведенных финансовых и административных операциях, следует хранить в зашифрованном виде, используя локально сгенерированные ключи для шифрования и аутентификации этих данных. Аутентификацию данных следует проводить при их загрузке в память перед использованием. Допускается выборочное шифрование данных.

Стандарты: NIST FIPS 197, IETF RFC 1851, IETF RFC 6234.

3.2.8. Обновление программного обеспечения

ПУ должно поддерживать функцию загрузки и установки обновлений программного обеспечения. ПУ должно проверять подлинность пакетов обновлений перед установкой. В случае если проверка подлинности завершается с ошибкой, установка обновления должна быть прервана, а файлы, содержащие обновление, должны быть удалены. Отмена обновлений (downgrade) возможна только в том случае, если имеется ясное обоснование того, что эта операция безопасна. Обновление программного обеспечения должно инициироваться автоматически в заданное время суток или через заданный интервал времени, или при включении терминала, или вручную администратором терминала. Следует проверять наличие новых обновлений не реже одного раза в сутки.

3.2.9. Информация о версии

ПУ должно по запросу возвращать информацию о версии операционной системы, включая версию ядра и загрузчика, если в системе имеются эти компоненты. Дополнительно ПУ должно возвращать версию программных компонентов системы, включая версии

библиотек L1 и L2, а также версию приложения, отвечающего за исполнение финансовых и административных операций, версию системы обновления и системы управления ключами, если они не встроены в операционную систему.

3.2.10. Пароль администратора

Управление ПУ должно быть защищено паролем, состоящим как минимум из восьми цифр. ПУ передается в эксплуатацию с установленным паролем по умолчанию, который должен быть изменен перед началом работы. ПУ должно автоматически предлагать сменить пароль администратора в случае, если установлен пароль по умолчанию, и переходить к работе только в случае смены пароля. Пароль на ПУ следует хранить в зашифрованном виде или вместо пароля хранить хэш (SHA-256) конкатенации пароля и случайной последовательности (salt) длиной 24 байта. Пароль администратора открывает доступ к вводу ключей с клавиатуры, запуску обновлений программного обеспечения или обновления настроек ПУ, отображению логов транзакций и отчетов, а также операций закрытия дня/смены и сверки итогов. ПУ должно обеспечивать возможность удаленной установки значения пароля по умолчанию через доверенный источник настроек. ПУ должно обеспечивать защиту от перебора пароля.

3.2.11. Индикация ошибок

В случае возникновения ошибок в процессе проверки или установки обновлений терминал должен фиксировать их в логе и информировать оператора, отображая ошибку на экране, печатая в чеке или передавая информацию об ошибке через программный интерфейс. Рекомендуется передавать вместе с кодами ошибок, которые могут быть использованы для машинной обработки, также текстовые пояснения.

3.2.12. Лог терминала

ПУ должен поддерживать ведение лога, в который помещаются информационные сообщения и сообщения об ошибках. Лог должен занимать такой объем пространства в памяти ПУ, который не оказывает негативного влияния на работу других программ. Лог не должен содержать информации, нарушающей безопасное использование данных ПУ, например значения ключей и их компонент (в открытом виде), ПИН-коды или номера карт. Номера карт следует маскировать, оставляя открытыми только четыре последние цифры номера. Каждая запись лога должна содержать метку типа «информационное сообщение»

или «сообщение об ошибке», дату и время внесения записи в лог с точностью до миллисекунды.

Стандарты: IETF RFC 1851.

3.3. Требования к средствам криптографической защиты информации, реализуемые в устройствах с терминальным ядром

Требования к средствам криптографической защиты информации, реализуемые в устройствах с терминальным ядром, устанавливаются ФСБ России в соответствии с требованиями к СКЗИ, разработанным согласно пункту № 05.02.002.017.004 федерального проекта «Информационная безопасность».

Средства криптографической защиты информации должны удовлетворять требованиям национальных стандартов, рекомендациям по стандартизации и методическим рекомендациям.

3.3.1. Национальные стандарты

Устройства с терминальным ядром могут поддерживать следующие национальные стандарты:

- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»;
- ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

3.3.2. Рекомендации по стандартизации

Устройства с терминальным ядром могут поддерживать следующие рекомендации по стандартизации:

- Р 1323565.1.026-2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование»;
- Р 1323565.1.009-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах»;
- Р 1323565.1.007-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN»;
- Р 1323565.1.010-2017 «Информационная технология. Криптографическая защита информации. Использование функции диверсификации для формирования производных ключей платежного приложения»;
- Р 1323565.1.008-2017 «Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением»;
- Р 132365.1.011-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN»;
- Р 132365.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт».

3.3.3. Методические рекомендации

Устройства с терминальным ядром могут поддерживать следующие методические рекомендации:

- МР 26.3.005-2017 «Использование функции диверсификации для формирования производных ключей платежного приложения»;
- МР 26.3.004-2017 «Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением»;

- МР 26.3.003-2017 «Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN»;
- МР 26.3.002-2017 «Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN»;
- МР 26.3.001-2017 «Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах».

4. ДОПОЛНИТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

4.1. Нефункциональные требования

4.1.1. Обновление ПО

Устройство ПУ должно предусматривать возможность обновления программного обеспечения *центрального процессора* с аутентификацией программного обеспечения. Если аутентификация программного обеспечения не подтверждается, обновление отменяется и удаляется с устройства.

4.1.2. Аутентификация приложений

Программное обеспечение процессора должно поддерживать аутентификацию приложений, загруженных на ПУ, в соответствии с п.4.1.13. Если ПУ разрешает обновления программного обеспечения и/или конфигурации, оно криптографически проверяет подлинность обновлений в соответствии с п.4.1.13.

4.1.3. Шифрование ПИН

Для ПУ с онлайн-проверкой ПИН введенный ПИН шифруется сразу после ввода пользователем платежной карты. Для ПУ с офлайн-проверкой ПИН введенный ПИН передается для верификации и не хранится в устройстве. Ввод ПИН считается оконченным после нажатия пользователем кнопки подтверждения (“enter”).

4.1.4. Лимиты работы защищаемых сервисов

Чтобы минимизировать риски от несанкционированного использования защищаемых сервисов, должно быть введено ограничение на количество действий, которые могут быть

выполнены, и наложен лимит времени, после которого устройство вынуждено вернуться в нормальный режим.

4.1.5. Требования к генератору случайных чисел

Если для защиты данных используются случайные числа, генерируемые платежным устройством, то должен использоваться генератор случайных чисел.

4.1.6. Политика безопасности

Вендор ПУ должен разработать и предоставлять пользователям ПУ политику безопасности, направленную на корректное использование ПУ с целью соблюдения требований, включая информацию об обязанностях управления ключами, административных обязанностях, функциональности ПУ, идентификации и требованиях к среде. Политика безопасности должна определять роли, поддерживаемые ПУ, и указывать сервисы, доступные для каждой роли, в определенном табличном формате. ПУ способно выполнять только свои предназначенные функции, т. е. скрытых функций нет. Единственными функциями, выполняемыми ПУ, являются те, которые разрешены политикой.

4.2. Технические требования к средствам криптографической защиты информации, реализованным в платежных устройствах с терминальным ядром

4.2.1. Требования к учету ключевой информации

Виды ключевой информации и ключевые носители

Ключевая информация и ключевые носители подразделяются на следующие виды:

- закрытый персональный ключ пользователя;
- открытый персональный ключ пользователя;
- закрытый симметричный ключ;
- закрытый корневой ключ;
- открытый корневой ключ.

Закрытые ключи должны храниться в зашифрованном виде в формате ключевого контейнера.

Открытые ключи должны храниться в открытом виде в соответствии с RFC5280, RFC4491.

Способы формирования ключевой информации должны быть описаны в эксплуатационных документах, входящих в состав комплекта поставки СКЗИ.

Для устройств с терминальным ядром, производимых на территории Российской Федерации, порядок изготовления ключевой информации определяется ФСБ России в соответствии с требованиями к СКЗИ, разработанным согласно пункту № 05.02.002.017.004 федерального проекта «Информационная безопасность».

Ключевая информация должна быть защищена от компрометации путем ее размещения в неизвлекаемые области памяти ПУ.

При отключении питания ПУ, перезагрузке ПУ или при ином аварийном сбое ПУ процедуры авторизации должны быть проведены автоматически.

4.2.2. Сроки действия ключей

Срок действия ключевой информации определяется в техническом задании на СКЗИ, производимые на территории Российской Федерации.

Допустимый срок действия закрытых ключей – не более 1 года 3 месяцев, открытых ключей – не более 15 лет.

Допустимый срок действия закрытых ключей – не более 3 лет при размещении ключевой информации в неизвлекаемые области памяти ПУ, а открытых ключей – не более 15 лет.

Контроль срока использования ключей должен обеспечиваться организационно-техническими мерами.

От ФСБ России

А.М. Шойтов

21/01/20

От Банка России

Директор Департамента
информационной безопасности

В.А. Уваров

22.01.2020 г

Васильев С.Н.