Модуль безопасности для систем платежных карт «SPB HSM PS base»

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

2023

Содержание

1 Назначение изделия

Модуль безопасности для систем платёжных карт (МБ СПК) предназначен для применения во внутренних системах банков и платёжных системах для обеспечения защиты персональных данных держателей карт в следующих процессах и механизмах систем платёжных карт:

– инициализация платёжных карт при их производстве;

– эмиссия платёжных карт, включая генерацию секретных величин, электрическую персонализацию и печать пин-конвертов;

– авторизация платёжных транзакций;

– эквайринг, обработка транзакций от платёжных устройств;

– 3D-Secure;

– поддержка режима работы национальной системы платежных карт (НСПК) в качестве операционного платежного клирингового вычислительного центра (ОПКЦ);

– генерация, смена, резервирование, экспорт локальных, зональных, терминальных, транспортных мастер ключей, которые используются в вышеперечисленных процессах.

МБ СПК является СКЗИ и соответствует следующим требованиям:

– «Требования к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу КВ;

– «Требования к средствам криптографической защиты информации в платёжных устройствах с терминальным ядром, серверных компонентах платёжных систем (HSM модулях), платёжных картах и иных технических средствах информационной инфраструктуры платёжной системы, используемых при осуществлении переводов денежных средств, указанных в п. 2.20 Положения Банка России от 9 июня 2012 г. № 382-П»;

– «Специальные требования к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений,

составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации» по уровню КВ;

– «Требования по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню защищенности КВ.

Изделие предназначено для непрерывной круглосуточной эксплуатации в закрытых постоянно отапливаемых помещениях.

2 Описание структуры, состояний и режимов работы изделия

2.1 Структура изделия

Структурно в состав единой конструкции МБ СПК входят два блока:

– блок ввода-вывода и управления (ВВиУ),

– криптоблок.

Блок ВВиУ обеспечивает:

– ввод-вывод и разбор формата команд, поступающих от прикладной хост-системы;

– взаимодействие с криптоблоком для выполнения критичных криптографических преобразований;

– предоставление функции удаленного управления устройством через защищённый TLS канал.

Криптоблок обеспечивает все операции по генерации, защищённому хранению, экспорту, созданию резервных локальных мастер ключей, а также расшифрование и зашифрование персональных данных владельцев карт (ключей, PIN, PIN-блоков) на локальных мастер ключах. Через криптоблок обеспечивается взаимодействие со смарт-картами.

2.2 Комплект поставки

В комплект поставки входят:

– МБ СПК с набором лицензий;

– три смарт-карты для хранения LMK;

– четыре USB-токена для администраторов безопасности и управления;

– монтажный комплект, шнур электропитания, сетевой кабель (RJ-45);

– комплект эксплуатационной документации.

При наличии лицензии «Удаленное управление» в комплект поставки дополнительно входит ПО «Терминал управления».

2.3 Состояния изделия

2.3.1 Поставочное состояние

Данное состояние характеризуется тем, что:

– изделие доставлено на объект эксплуатации;

– изделие не введено в эксплуатацию.

2.3.2 Рабочее состояние

Данное состояние характеризуется тем, что:

– изделие введено в эксплуатацию:

1) проведена Инициализация, в том числе созданы два идентификатора администраторов безопасности «АБ-1», «АБ-2»;
2) созданы два идентификатора администраторов управления с маркировкой «АУ-1», «АУ-2»;
3) осуществлена генерация или импорт LMKs.

– изделие в Авторизованном или Неавторизованном состояниях поддерживает работу:

1) в Основном режиме (Online);
2) в Автономном режиме (Offline);
3) в Безопасном режиме (Secure).

2.3.3 Деинициализированное состояние

Данное состояние характеризуется тем, что:

– изделие приведено в поставочный состояние (стерты идентификаторы администраторов, все настройки изделия по умолчанию);

– стёрта ключевая информация.

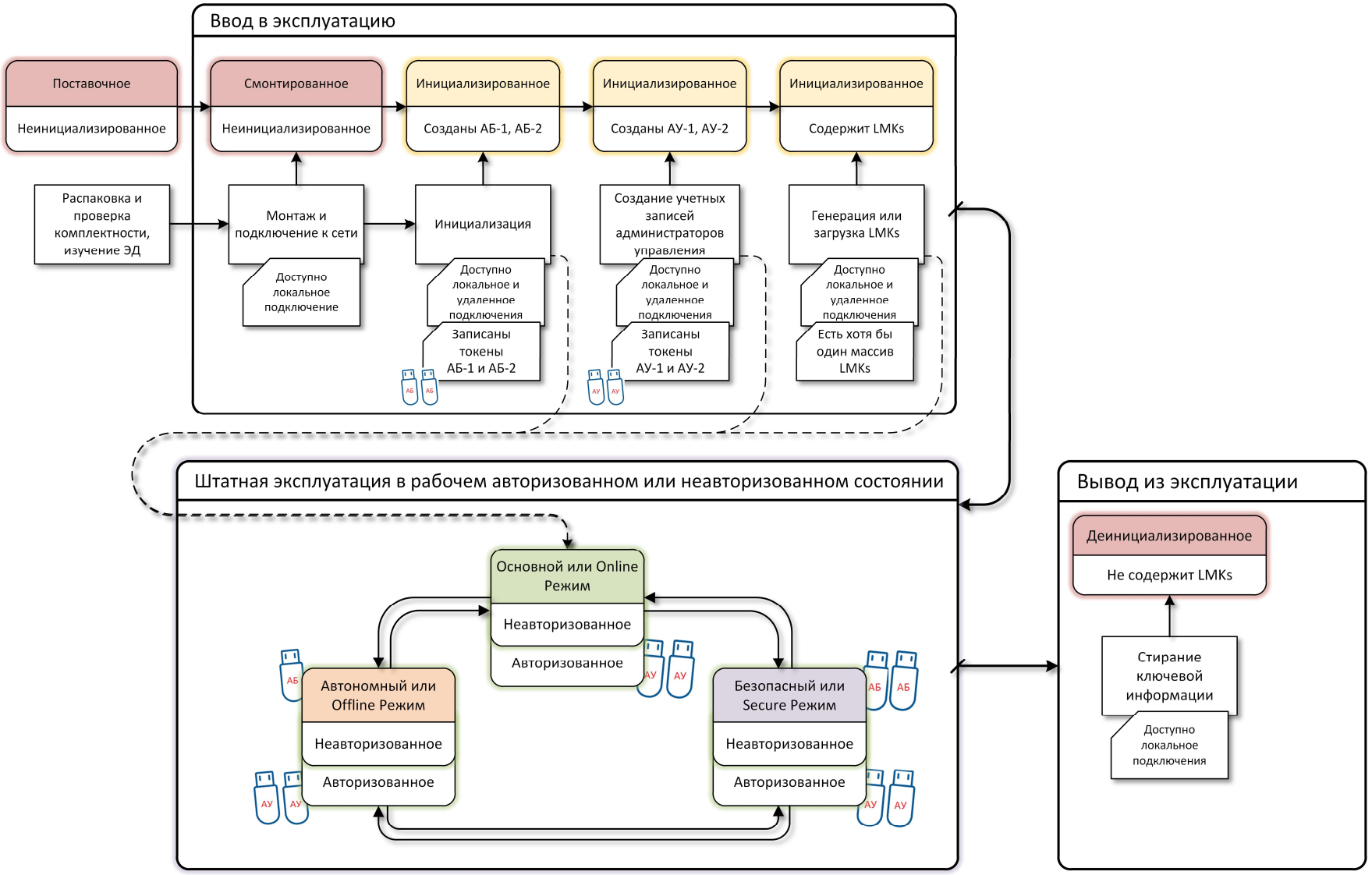


Рисунок 1 – Состояния изделия

2.4 Рабочие режимы изделия

МБ СПК в процессе штатной эксплуатации поддерживает работу в следующих режимах:

– Основной (Online) – режим работы по умолчанию, в котором выполняются платежные функции;

– Автономный (Offline) – режим работы, в котором доступны сетевые и системные настройки;

– Безопасный (Secure) – режим работы, в котором доступны команды управления массивами LMKs, а также настройки безопасности.

Рабочие режимы изделия доступны сразу после проведения Инициализации, при этом, если ключи LMK не загружены, то предоставляется возможность выполнять отдельные режимы управления изделием.

На рисунке 2, представлена схема переходов между рабочими режимами, с применением идентификаторов администраторов безопасности.

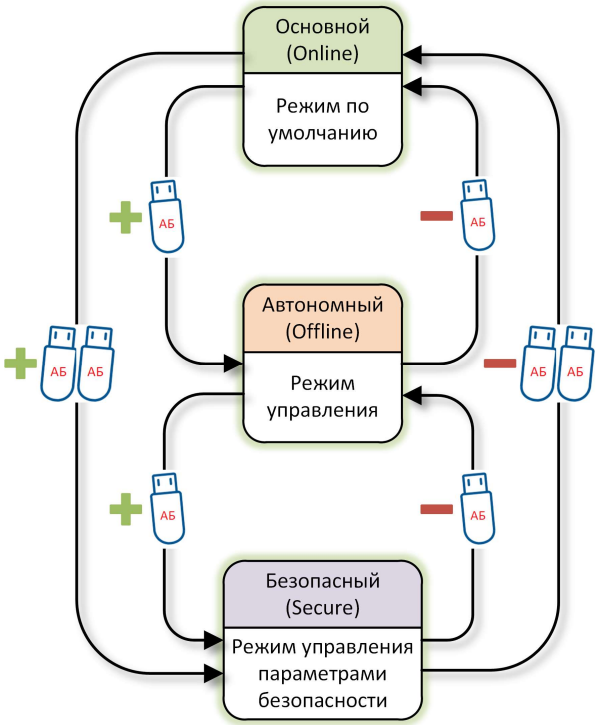


Рисунок 2 – Схема перехода между режимами

Режим работы Основной (Online) активируется автоматически после инициализации, а также после включения питания/перезагрузки изделия.

Для перехода в Автономный (Offline) режим работы необходимо провести аутентификацию одного администратора безопасности с помощью USB-токена. После перехода в данный режим производится автоматическая блокировка обработки хост-команд. После изъятия идентификатора АБ, МБ СПК возвращается в Основной (Online) режим.

Если в режиме Автономный (Offline) провести аутентификацию второго администратора безопасности с помощью USB-токена, то МБ СПК перейдет в Безопасный (Secure) режим. В данном режиме также производится автоматическая блокировка обработки хост-команд. После изъятия любого из USB-токенов АБ, МБ СПК переходит в Автономный режим (Offline). В случае изъятия сразу обоих USB-токенов АБ, МБ СПК переходит в Основной режим (Online).

Также при наличии в МБ СПК сгенерированных или загруженных LMKs, возможен перевод МБ СПК в авторизованное состояние. Для установки состояния Авторизован, требуется аутентификация двух администраторов управления. МБ СПК в авторизованном состоянии расширяет доступные функции в каждом рабочем режиме.

Функциональность МБ СПК зависит от режима, в котором находится: Online, Offline, Secure. А также от состояния: Авторизован, Неавторизован.

3 Описание конструкции изделия

МБ СПК выполнен в виде моноблока, разработанного в соответствии с 19″ стандартом МЭК 297-3-100-2008, имеет высоту 2U.

МБ СПК, торговая марка SPB HSM PS base, как аппаратная платформа выпускается в следующем исполнении:

Рисунок 3 – МБ СПК «SPB HSM PS base»

На передней и задней панелях МБ СПК «SPB HSM PS base» расположены (см. Рисунок 4 и Рисунок 5):

– индикаторы «I – Initialization», «K – Keys», «A – Attention», предназначенные для отображения состояния работы изделия (1);

– индикатор «CHARGE STATUS», предназначенный для отображения минимального уровня заряда элемента питания типа AA, установленного в отсек «BAT» (2);

– QR-код, предназначенный для отображения подробной информации об изделии (3);

– кнопка открытия экранирующей сдвижной крышки считывателя «READER», оснащенной датчиком положения (закрыт) (4);

– считыватель «READER», предназначенный для считывания носителей ключевых документов форм-фактора смарт-карта (5);

– два разъема «USB1», «USB2», предназначенные для записи идентификаторов администраторов или подключения принтера для печати PIN-конвертов (6);

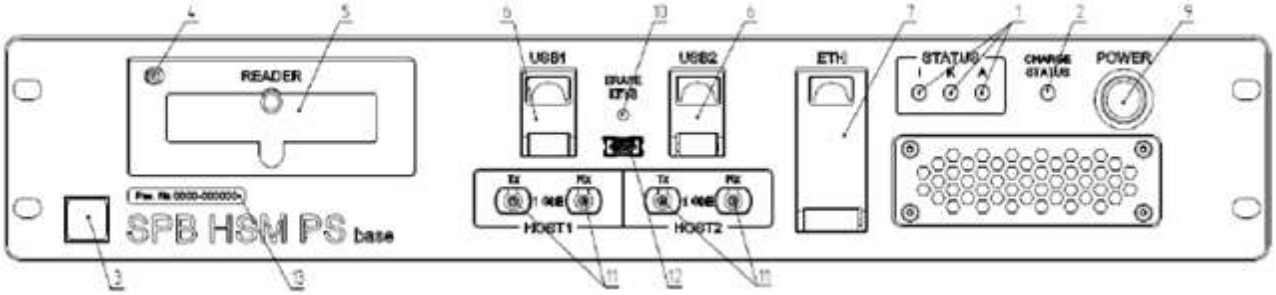
– разъем «ETH», предназначенный для подключения терминала локального управления, тип разъема RJ45 (7);

– отсек «BAT», предназначенный для установки элемента питания типа AA, располагающийся на задней панели изделия (см. Рисунок 5);

– кнопка «POWER», предназначенная для включения/отключения электропитания изделия, оснащенная подсветкой (9);

– кнопка «ERASE KEYS», предназначенная для экстренного стирания LMK, сброса настроек изделия по умолчанию (утоплена относительно лицевой панели, во избежание случайного нажатия. Для нажатия используется специальный стилус, входящий в комплект поставки) (10);

– оптические разъемы «Tx» и «Rx», предназначенные для подключения хост-системы и терминала удаленного управления, тип разъемов LC (11).



1 – индикаторы «I», «K», «A» процессов работы изделия,

2 – индикатор «CHARGE STATUS» уровня заряда элемента питания типа AA,

3 – идентифицирующий QR-код, 4 – кнопка открытия крышки считывателя,

5 – считыватель «READER» ключевых документов,

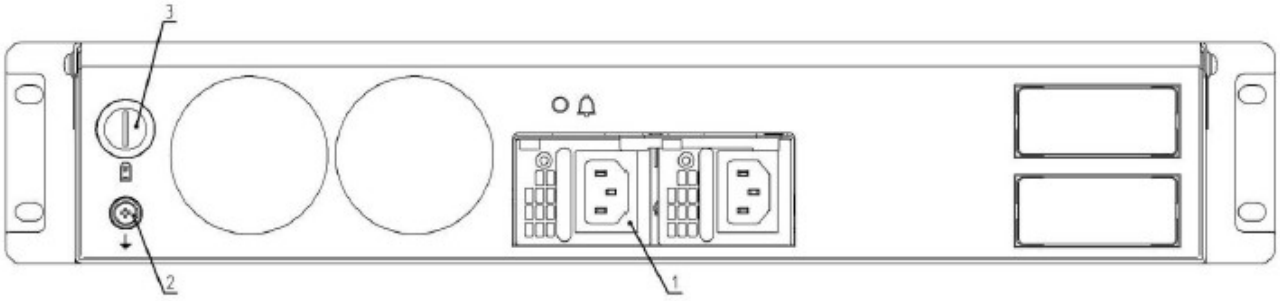
6 – разъемы «USB 1», «USB 2», 7 – разъем «ETH» управления,

9 – кнопка «POWER» включения/отключения электропитания изделия,

10 – кнопка «ERASE KEYS» экстренного стирания ключей LMK,

11 – разъемы «Tx» и «Rx» для подключения к HOST системе

Рисунок 4 – Передняя панель МБ СПК «SPB HSM PS base»



1 – блок питания, 2 – узел заземления, 3 – отсек BAT для элемента питания типа AA

Рисунок 5 – Задняя панель МБ СПК «SPB HSM PS base»

Конструктивной особенностью изделия является система охлаждения, принцип которой заключается в заборе воздуха с лицевой панели изделия и отводе нагретого воздуха через заднюю стенку изделия.

Вентиляторы, использующиеся в системе охлаждения, выбраны со временем наработки на отказ, превышающим срок службы изделия (7 лет). В случае выхода из строя вентилятора, его замена осуществляется в рамках технической поддержки.

Очистка противопылевого фильтра возможна на объекте эксплуатации без выключения электропитания изделия.

Монтаж МБ СПК «SPB HSM PS base» осуществляется на опоры раздвижные, входящие в комплект поставки. При этом над изделием не требуется свободное пространство в стойке.

На задней стенке МБ СПК «SPB HSM PS base» расположен блок питания с резервированием, позволяющим производить «горячую» замену модулей питания. Также на задней стенке изделия размещён узел заземления изделия (см. Рисунок 5).

Для защиты от несанкционированного подключения к неиспользуемым разъёмам на лицевой панели предусмотрены опечатываемые откидные крышки.

4 Технические характеристики

Основные технические характеристики МБ СПК «SPB HSM PS base» с учётом исполнений приведены в таблице:

Характеристики	Параметры
	SPB HSM PS base
Интерфейс для подключения к хост-системе и для удаленного управления, GbE	1
Тип разъёма подключения к хост-системе и для удаленного управления[1)]	4 × LC, 10 км (SMF), ʎc 1310 нм
Протокол взаимодействия с хост-системой и для удаленного управления	UDP, TCP/IP
Производительность[2)], tps	1 000
API с ПО хост-системы	Режим команда-ответ
Протокол взаимодействия для удаленного управления	Р 1323565.1.020-2018 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»
Интерфейс локального подключения, GbE	1
Тип разъема для подключения идентификаторов АБ или АУ	2 × USB
Лицензии	Предусмотрены следующие лицензии: – «Core» – основная; – «Legacy» – обеспечивающая совместимость с устаревшими командами и командами прошивки Р3; – «Загрузка LMK с внешнего носителя»; – «Удаленное управление».
Режимы работы	Поддерживаются следующие режимы: – Основной режим (Online); – Автономный режим (Offline); – Безопасный режим (Secure). Поддерживаются следующие состояния: – Авторизованное; – Неавторизованное.

Характеристики	Параметры
	SPB HSM PS base
Международные криптографические алгоритмы и механизмы	Криптографические алгоритмы: – DES/3DES – NIST FIPS 46-3 SP 800-67 и ISO 10116; – AES – NIST FIPS 197; – RSA – RFC 3447 NIST FIPS 186-4; – SHA-1 – RFC 3174 и NIST FIPS 180-4; – SHA-224, SHA-256, SHA-512 – ISO/IEC 10118-2 и NIST 180-4; – MAC – ISO 9797 и NIST FIPS 198-1; – HMAC – ISO/IEC 9797-2. Поддерживаемые механизмы: – Global Platform v.2.2.1; – EMV CPS 1.1; – EMV3.1.1, EMV 4.1, EMV 4.3 (ARQC/ARPC/AAC), IDN; – Union Pay (ARQC/ARPC); – CVP/iCVP/CVP2; – CVC/CVV/CVC3; – PVV; – MST; – MasterCard CAP; – CAVV; – PIN Block (ISO 9564-1) – в том числе ISO-0, ISO-3, ISO-4; – IBM 3624; – ANSI X9-24 (DUKPT).
Российские криптографические алгоритмы (РКА)	Блочный шифр «Кузнечик» ГОСТ Р 34.12-2015 в режимах ГОСТ Р 34.13-2015, хэш функция ГОСТ Р 34.11-2012
Совместимость с банковским ПО	БПЦ – SmartVista, OpenWay – Way4, CompasPlus – TranzWare
Форм-фактор	19″ моноблок 2U
Электропитание (с резервированием)	220 В, 50 Гц
Потребляемая мощность, Вт, не более	150
Габариты, В×Ш×Д, мм, не более	84×483×559
Масса, кг, не более	15
Направление воздушного охлаждения	Front-to-back
Срок службы	7 лет

Характеристики	Параметры
	SPB HSM PS base
Условия монтажа	19″ телекоммуникационный шкаф/стойка глубиной 800-1200 мм[3)]
Условия эксплуатации	ГОСТ 15150 4 группа климатического исполнения УХЛ с уточнениями: – температура окружающего воздуха от + 5 до + 30°С; – относительная влажность воздуха до 80% при температуре + 25°С; – атмосферное давление от 84 до 106,7 кПа (от 630 до 800 мм рт. ст.).
Физическая безопасность	Конструкция, обеспечивающая защиту от НСД, использование различных систем обнаружения НСД и датчиков вскрытия – механические микропереключатели, датчик объема
Методы генерации, защиты и использования локальных мастер ключей	Совместное использование ФДСЧ и ПДСЧ для генерации, хранение в зашифрованном виде на РКА во внутренней памяти криптоблока, гарантированное стирание при обнаружении попытки НСД. Поддерживается два способа использования LMK: – Variant LMK; – Keyblock LMK.
Поддерживаемые форматы ключевых контейнеров для экспорта	ASC X9 TR-31-2018 (в том числе TR-31-TK26 MAGMA/KUZNECHIK), Thales Variant Scheme (ANSI X9.17), PKCS #1 v1.5
Резервирование локальных мастер-ключей	В виде компонент на смарт-картах непосредственно из криптоблока с применением алгоритмических мер защиты от ПЭМИН
Совместимые принтеры[4)]	OKI Microline 5100FB eco
Совместимые медиаконвертеры[4)]	tp-link MC210CS, SNR-CVT-1000SFP-V2

1) Для подключения необходимо использовать одномодовый оптический кабель;
2) Производительность измеряется по методике, эквивалентной методике НСПК – число перешифрований PIN-блока с одного зонального ключа на другой;
3) В комплект поставки изделия входят опоры раздвижные. Рекомендуется использовать воздушное охлаждение шкафа/стойки Front-to-Back;
4) Полный актуальный список совместимого оборудования размещен на сайте предприятия-изготовителя изделия.

5 Лицензии

5.1 Лицензия «Core»

Перечень поддерживаемых команд:

Команда (ответ)	Описание	Примечание, авторизация
Команды управления ключами		
Команды генерации ключей		
A0 (A1)	Генерация ключа	+, A
A2 (A3, AZ)	Генерация и печать компонент	+, A
NE (NF, NZ)	Генерация ключа и печать в виде отдельных компонент	+
A4 (A5)	Формирования ключа из зашифрованных компонент	+, A
A6 (A7)	Импорт ключа	+, A
A8 (A9)	Экспорт ключа	+, A
BY (BZ)	Перешифрование ZMK из-под ZMK под LMK	+, A
Команды перешифрования из-под «старого» LMK под «новый»		
BG (BH)	Перешифрование PIN из-под «старого» LMK под «новый»	+
BW (BX)	Перешифрование ключа из-под «старого» LMK под «новый»	+
Команды управления ключами EMV		
KI (KJ)	Генерация мастер-ключей карты	+
K8 (K9)	Экспорт ключа под KEK	+
L6 (L7)	Импорт секретного ключа RSA	+
L8 (L9)	Экспорт секретного ключа RSA	+
Команды управления ключами MasterCard (OBKM)		
JO (JP)	Проверка самоподписанного сертификата корневого УЦ (MasterCard)	+, A
Команды управления Ассиметричными ключами		
EI (EJ)	Генерация пары секретный/открытый ключ RSA	+, A
EK (EL)	Загрузка секретного ключа RSA	+
EM (EN)	Перешифрование секретного ключа RSA	+
EO (EP)	Импорт открытого ключа RSA	+, A
EQ (ER)	Проверка открытого ключа RSA	+
ES (ET)	Проверка сертификата и импорт открытого ключа RSA	+
EU (EV)	Пересчет MAC за открытый ключ RSA	+
GI (GJ)	Импорт ключа DES на открытом ключе RSA	+
GK (GL)	Экспорт ключа DES на открытом ключе RSA	+
Команды эмиссии магнитной полосы		
Команды генерации PIN и Offset		
EE (EF)	Получение PIN методом IBM Offset	+
JA (JB)	Генерация случайного PIN	+

Команда (ответ)	Описание	Примечание, авторизация
DE (DF)	Генерация PIN-offset IBM-методом для PIN, зашифрованного под LMK	+
BK (BL)	Генерация PIN-offset IBM-методом для PIN, выбранного пользователем	+
DG (DH)	Генерация ABA PVV (PIN Verification Value) для PIN, зашифрованного под LMK	+
FW (FX)	Генерация ABA PVV (PIN Verification Value) для PIN, выбранного пользователем	+
BM (BN)	Загрузка таблицы PIN для проверки «слабых» PIN	+
Команды печати PIN конвертов		
PE (PF, PZ)	Печать PIN	+, A
OA (OB, OZ)	Печать данных	+, A
Команды управления форматом печати		
PA (PB)	Загрузка шаблонов печати PIN	+
Команды работы с чистым PIN		
BA (BB)	Зашифрование чистого PIN	+, A
NG (NH)	Расшифрование зашифрованного PIN	+, A
Команды генерации и проверки Card Verification Code/Value		
CW (CX)	Генерация Card Verification Code/Value (CVC/CVV)	+
CY (CZ)	Проверка Card Verification Code/Value (CVC/CVV)	+
RY (RZ)	Вычисление Card Security Codes (CSC), режим 3	+
Обработка транзакций магнитной полосы		
Команды смены PIN		
DU (DV)	Генерация и проверка PIN-offset IBM-методом для нового PIN, выбранного пользователем	+
CU (CV)	Генерация и проверка ABA PVV, для PIN выбранного пользователем	+
Команды проверки PIN		
DA (DB)	Проверка терминального PIN методом IBM Offset	+
EA (EB)	Проверка PIN методом IBM Offset	+
DC (DD)	Проверка терминального PIN методом ABA PVV	+
EC (ED)	Проверка PIN методом ABA PVV	+
BC (BD)	Проверка терминального PIN методом сравнения	+
BE (BF)	Проверка PIN методом сравнения	+
Команды перешифрования PIN		
CC (CD)	Перешифрование PIN из-под одного ZPK под другой	+
CA (CB)	Перешифрование PIN из-под TPK под ZPK/BDK (3DES DUKPT)	+
JE (JF)	Перешифрование PIN из-под ZPK под LMK	+
JC (JD)	Перешифрование PIN из-под TPK под LMK	+
JG (JH)	Перешифрование PIN из-под LMK под ZPK	+

Команда (ответ)	Описание	Примечание, авторизация
QK (QL)	Перешифрование PIN, зашифрованного под LMK, со сменой номера счета (Account Number)	+
AQ (AR)	Перешифрование PIN из-под RSA под ZPK или TPK	+
Команды проверки кода Card Verification Code/Value		
PM (PN)	Проверка кода Dynamic CVV/CVC	+
RY (RZ)	Проверка кода Card Security Codes (CSC), режим 4	+
Команды DUKPT (X9.24)		
G0 (G1)	Перешифрование PIN из-под BDK под BDK или ZPK (3DES & AES DUKPT)	+
GO (GP)	Проверка PIN методом IBM Offset (3DES & AES DUKPT)	+
GQ (GR)	Проверка PIN методом ABA PVV (3DES & AES DUKPT)	+
GU (GV)	Проверка PIN методом Encrypted PIN (3DES & AES DUKPT)	+
GW (GX)	Генерация/проверка MAC (3DES & AES DUKPT)	+
Команды защиты данных		
Команды контроля целостности		
M6 (M7)	Генерация MAC	+
M8 (M9)	Проверка MAC	+
EW (EX)	Генерация подписи RSA	+
EY (EZ)	Проверка подписи RSA	+
GM (GN)	Формирование Hash за блок данных	+
Команды шифрования данных		
M0 (M1)	Зашифрование блока данных	+
M2 (M3)	Расшифрование блока данных	+
M4 (M5)	Перешифрование блока данных	+
Команды расчета HMAC		
Расчет и проверка HMAC		
L0 (L1)	Генерация секретного ключа HMAC	+
LQ (LR)	Формирования HMAC за блок данных	+
LS (LT)	Проверка HMAC за блок данных	+
LU (LV)	Импорт ключа HMAC под ZMK	+
LW (LX)	Экспорт ключа HMAC на ZMK	+
LY (LZ)	Перешифрования HMAC Key из-под «старых» LMK под «новые»	+
Команды управления HSM		
Разные команды		
B2 (B3)	Команда «Эхо»	+, A
BU (BV)	Генерация проверочного значения за ключ	+
LO (LP)	Перешифрование таблицы децимализации из-под «старых» LMK под «новые»	+
NK (NL)	Формирование цепочки команд	+

Команда (ответ)	Описание	Примечание, авторизация
Команды диагностики		
NC (ND)	Выполнение диагностики HSM	+
NO (NP)	Получение статуса HSM	+
J2 (J3)	Загрузить HSM	+
J6 (J7)	Сброс статистики	+
JK (JL)	Запрос текущего состояния HSM	+
Команды обработки транзакций EMV		
Команды работы с EMV Chip Card		
KQ (KR)	Проверка ARQC и/или генерация ARPC (EMV 3.1.1)	+, A
KW (KX)	Проверка ARQC и/или генерация ARPC (EMV 4.x)	+, A
KU (KV)	Генерация секретного сообщения (Secure Message) (EMV 3.1.1)	+
KY (KZ)	Генерация секретного сообщения (EMV 4.x)	+
K2 (K3)	Проверка Truncated Application Cryptogram (MasterCard CAP)	+, A
KS (KT)	Проверка Data Authentication Code (DAC) и Dynamic Number (DN) (EMV 3.1.1)	+, A
K0 (K1)	Расшифрование зашифрованных счетчиков (EMV 4.x)	+
Команды эмиссии EMV и бесконтактных карт		
Подготовка данных бесконтактных карт		
NY (NZ)	Генерация IVCVC3 и CVC3	+
Подготовка данных EMV карт		
KE (KF)	Генерация пары секретный/открытый ключ RSA и сертификата эмитента	+, A
KG (KH)	Проверка сертификата открытого ключа эмитента	+
KM (KN)	Генерация подписи данных статической аутентификации (SDA)	+
KO (KP)	Генерация пары секретный/открытый ключ RSA и сертификата карты	+
KK (KL)	Проверка самоподписанного сертификата корневого УЦ	+, A
IK (IL)	Подпись EMV данных	+
IM (IN)	Проверка подписи EMV данных	+
Команды персонализации Chip Card		
IC (ID)	Установление защищенного соединения с чип-картой	+
IE (IF)	Подготовка защищенного сообщения для чип-карты	+

5.2 Лицензия «Legacy»

Перечень поддерживаемых команд:

Команда (ответ)	Описание	Примечание, авторизация
Команды управления ключами		
AA (AB)	Перешифрование TMK, TPK или PVK из-под «старых» LMK под «новые»	+
AC (AD)	Перешифрование TAK из-под «старых» LMK под «новые»	+
AE (AF)	Перешифрование TMK, TPK или PVK из-под LMK под другой TMK, TPK или PVK	+
AG (AH)	Перешифрование TAK из-под LMK под TMK	+
FA (FB)	Перешифрование ZPK из-под ZMK под LMK	+
FC (FD)	Перешифрование TMK, TPK или PVK из-под ZMK под LMK	+
FE (FF)	Перешифрование TMK, TPK или PVK из-под LMK под ZMK	+
FI (FJ)	Генерация ZEK/ZAK	+
FK (FL)	Перешифрование ZEK/ZAK из-под ZMK под LMK	+
FM (FN)	Перешифрование ZEK/ZAK из-под LMK под ZMK	+
FO (FP)	Генерация Watchword Key	+
FQ (FR)	Перешифрование Watchword Key из-под LMK под ZMK	+
FS (FT)	Перешифрование Watchword Key из-под ZMK под LMK	+
GC (GD)	Перешифрование ZPK из-под LMK под ZMK	+
GE (GF)	Перешифрование ZMK из-под «старых» LMK под «новые»	+
HA (HB)	Генерация TAK	+
HC (HD)	Генерация TMK, TPK, PVK	+
IA (IB)	Генерация ZPK	+
MG (MH)	Перешифрование TAK из-под LMK под ZMK	+
MI (MJ)	Перешифрование TAK из-под ZMK под LMK	+
KC (KD)	Перешифрование ZPK из-под «старых» LMK под «новые»	+
KA (KB)	Генерация проверочного значения за ключ	+
RW (RX)	Перешифрование величины KEYVAL	+
Команды контроля целостности		
MA (MB)	Генерация MAC за сообщение	+
MC (MD)	Проверка MAC за сообщение	+
ME (MF)	Проверка и переформирование MAC	+
MK (ML)	Генерация MAC за бинарные данные	+
MM (MN)	Проверка MAC за бинарные данные	+
MO (MP)	Проверка и переформирование MAC за бинарные данные	+
MQ (MR)	Генерация MAC (MAB) за большое бинарное сообщение	+
MS (MT)	Генерация MAC (MAB) за большое сообщение	+
Команды UnionPay		
JS (JT)	Проверка ARQC и генерация ARPC (UnionPay)	+

Команда (ответ)	Описание	Примечание, авторизация
JU (JV)	Генерация секретных сообщений с целостностью и опционально с зашифрованием (UnionPay)	+
Команды для сохранения совместимости с устаревшими версиями ПО		
HK (HL)	Генерация подписи данных статической аутентификации	+
IU (IV)	Генерация RSA пары (секретный/открытый ключ) эмитента (VISA)	+, A
IW (IX)	Проверка самоподписанного сертификата корневого УЦ (VISA)	+, A
IY (IZ)	Проверка сертификата открытого ключа эмитента (VISA)	+, A
JM (JN)	Генерация RSA пары (секретный/открытый ключ) эмитента (MasterCard)	+, A
JQ (JR)	Проверка сертификата открытого ключа эмитента (MasterCard)	+, A
P0 (P1)	Перешифрование блока секретных данных в специфичном формате карты	+
SI (SJ)	Диверсификация данных для записи на карту	+
XK (XL)	Зашифрование данных транзакции	+
YO (YP)	Генерация случайного числа	+
YS (YT)	Диверсификация ключа	+
YW (YX)	Экспорт ключа под KEK	+
YY (YZ)	Зашифрование данных	+
ZA (ZB)	Импорт ключа под KEK	+
ZC (ZD)	Расшифрование данных	+
ZE (ZF)	Перешифрование PIN	+
ZK (ZL)	Генерация или проверка MAC	+
ZU (ZV)	Сборка сертификата открытого ключа карты (ICC) из элементов	+
ZW (ZX)	Генерация ключевой пары карты (ICC)	+
ZY (ZZ)	Генерация производных ключей карты	+

5.3 Лицензия «Загрузка LMK с внешнего носителя»

Лицензия предоставляет возможность загружать LMK с внешнего носителя.

5.4 Лицензия «Удаленное управление»

Лицензия позволяет подключаться к изделию удаленно используя ПО «Терминал управления».

«Терминал управления» предназначен для выполнения следующих функций:

1) удаленное подключение к веб-интерфейсу управления изделием;
2) организация защищенного канала (TLS-туннель);
3) для удаленного использования идентификаторов администраторов безопасности и/или управления.

ПО «Терминал управления» может функционировать под управлением одной из операционных систем:

- Astra Linux Special Edition вер. 1.6;
- Windows 10 (x86/x64).