ООО «КРИПТО-ПРО»

УТВЕРЖДЕН
ЖТЯИ.00096-02-2019-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КРИПТОГРАФИЧЕСКИЙ МОДУЛЬ «КриптоПро HSM» версия 2.0 (КОМПЛЕКТАЦИЯ 3)

Формуляр

ЖТЯИ.00096-02 30 01

Листов 34

С учетом извещения об изменениях
ЖТЯИ.00096-02-2019

2020 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0, ПАКМ ЖТЯИ.00096-02, является документом, удостоверяющим гарантированные изготовителем основные характеристики СКЗИ, определяющим комплект поставки, отражающим сведения о производимых изменениях в комплекте поставки и другие данные за весь период эксплуатации.

1.2. Эксплуатация ПАКМ ЖТЯИ.00096-02 должна проводиться в соответствии с эксплуатационной документацией, предусмотренной настоящим Формуляром, и в соответствии с разделом V «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств зашиты информации (Положение-2005)».

1.3. Порядок обеспечения информационной безопасности при использовании ПАКМ ЖТЯИ.00096-02 определяется руководителем эксплуатирующей организации на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ.

1.4. При эксплуатации ПАКМ ЖТЯИ.00096-02 должны использоваться сертификаты открытых ключей, выпущенные Удостоверяющим центром, сертифицированным ФСБ России по классу защиты не ниже класса защиты используемого СКЗИ.

1.5. При встраивании ПАКМ ЖТЯИ.00096-02 (собственно ПАКМ, клиентская компонента ПАКМ «КриптоПро HSM Client», «КриптоПро DSS») в прикладные системы необходимо по Техническому заданию, согласованному с 8 центром ФСБ России, проводить оценку влияния среды функционирования ПАКМ на выполнение предъявленных к ПАКМ требований в случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации защиты конфиденциальной информации, обрабатываемой СКЗИ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- при организации криптографической защиты конфиденциальной информации, обрабатываемой СКЗИ, в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд;
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;
- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;
- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

В указанных выше случаях, если встраивание СКЗИ производится в прикладные системы, в которых функции создания и/или проверки электронной подписи не являются автоматическими, в том числе необходимо проводить оценку соответствия прикладной системы п.п. 8 и/или 9 Приложения 1 к Приказу ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

В остальных случаях рекомендуется проводить установленным порядком оценку влияния среды функционирования на СКЗИ с целью оценки обоснованности и достаточности мер, принятых для защиты информации, обрабатываемой СКЗИ.

В разделе 13 документа «ЖТЯИ.00096-02 95 01. КриптоПро HSM. Правила пользования» указаны приложения, проведение оценки влияния которых на СКЗИ не требуется.

В случае использования вызовов, не входящих в перечень Приложений 1 и 2 документа «ЖТЯИ.00096-02 95 01. КриптоПро HSM. Правила пользования», необходимо производить разработку отдельного СКЗИ на базе ПАКМ «КриптоПро HSM» версия 2.0 (с проведением соответствующих тематических исследований) в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).

1.6. Формуляр входит в комплект поставки ПАКМ ЖТЯИ.00096-02 и должен постоянно храниться в органе (подразделении), ответственном за эксплуатацию ПАКМ, в печатном виде.

1.7. Все записи, вносимые в формуляр, должны быть заверены лицами, ответственными за эксплуатацию ПАКМ.

1.8. ПАКМ «КриптоПро HSM» версия 2.0 соответствует «Требованиям к средствам электронной подписи» (Приложение 1 к Приказу ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»).

1.9. ПАКМ «КриптоПро HSM» версия 2.0 предназначен для эксплуатации на территории Российской Федерации. Исполнения «myDSS SDK», «Сбербанк myDSS SDK» и «DSS Client SDK» Комплектации 3 ПАКМ могут эксплуатироваться в том числе за пределами Российской Федерации. Использование данных исполнений в обычном или в экспортном варианте определяется лицензией.

2. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ ПАКМ

При эксплуатации ПАКМ ЖТЯИ.00096-02 должны выполняться следующие требования:

2.1. Средствами ПАКМ не допускается обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

2.2. Допускается использование ПАКМ для криптографической защиты персональных данных.

2.3. Ключевая информация является конфиденциальной.

2.4. Срок действия ключа проверки ЭП – не более 15 лет после окончания срока действия соответствующего ключа ЭП.

2.5. Клиентские компоненты ПАКМ должны использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Если для программно-аппаратной платформы, под управлением которой функционирует клиентская компонента ПАКМ, отсутствует сертифицированное ФСБ России средство антивирусной защиты, необходимо использовать любое доступное для данной платформы средство антивирусной защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

2.6. Размещение компонент ПАКМ в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

2.7. При эксплуатации ПАКМ (ПАКМ, клиентские компоненты ПАКМ, DSS) необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).

2.8. Установка программных компонент может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации (в соответствии с п. 7 «ЖТЯИ.00096-02 90 02. КриптоПро HSM. Использование интерфейсных модулей»).

3. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1. ПАКМ ЖТЯИ.00096-02 предназначен для защиты информации, не содержащей сведений, составляющих государственную тайну, в информационных системах с выполнением следующих функций:

- создание/проверка электронной подписи;
- вычисление значения хэш-функции областей памяти и файлов;
- шифрование/расшифрование областей памяти и файлов;
- вычисление имитовставки областей памяти и файлов;
- генерация и хранение ключей, уничтожение ключей;
- сопряжение с устройством доступа по криптографически защищенным каналам «K»[1], «K2», «K2s»;
- удаленное выполнение операций создания/проверки электронной подписи и шифрования/расшифрования файлов.

Примечание 1: Канал «K» используется только в рамках Головного удостоверяющего центра.

3.2. Архитектура ПАКМ

В состав ПАКМ ЖТЯИ.00096-02 в зависимости от комплектации (см. разд. 4) могут входить следующие элементы:

1. ПАКМ «КриптоПро HSM» (аппаратный модуль, обеспечивающий выполнение криптографических операций);
2. «КриптоПро HSM Client»;
3. «КриптоПро DSS»;
4. СКЗИ «КриптоПро CSP»/«КриптоПро JCP»;
5. Апплет на SIM-карте;
6. Приложение «myDSS»/«AirKey Lite»;
7. Фреймворк «myDSS SDK»/«Сбербанк myDSS SDK»/«DSS Client SDK»

Порядок взаимодействия компонент ПАКМ изображен на рисунке 1.

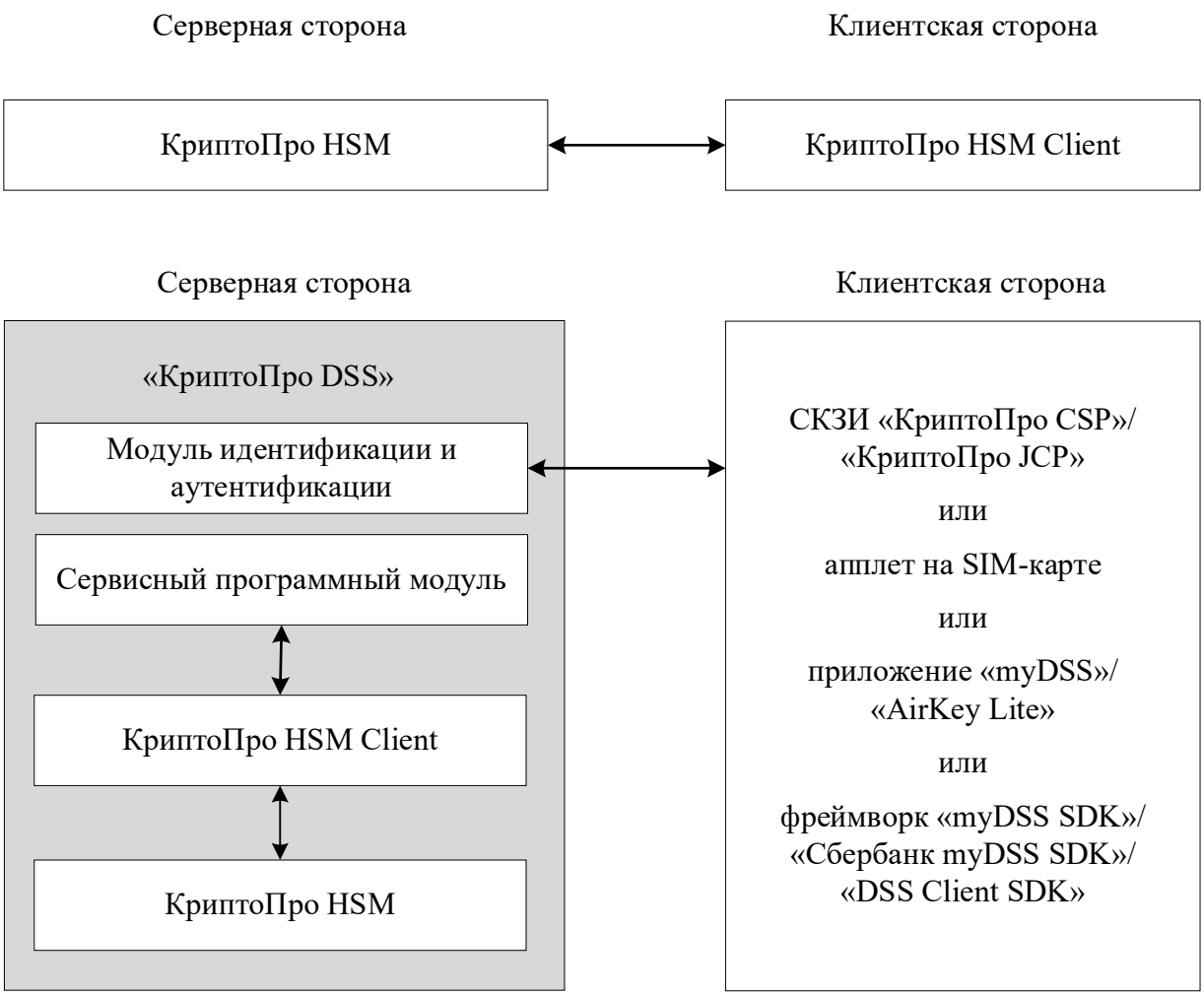

Рисунок 1 — Взаимодействие компонент ПАКМ ЖТЯИ.00096-02

Примечания:

1. Каждое исполнение, представленное в Таблицах 4.5-4.12 раздела 4, является совокупностью двух изделий: «КриптоПро DSS» и СКЗИ «КриптоПро CSP», установленного на клиентской стороне;

2. Исполнение, представленное в Таблице 4.13 раздела 4, является совокупностью двух изделий: «КриптоПро DSS» и СКЗИ «КриптоПро JCP», установленного на клиентской стороне;

3. Каждое исполнение, представленное в Таблицах 4.14-4.15 раздела 4, является совокупностью двух изделий: «КриптоПро DSS» и апплета на SIM-карте;

4. Каждое исполнение, представленное в Таблицах 4.16-4.17 раздела 4, является совокупностью двух изделий: «КриптоПро DSS» и мобильного приложения, установленного на клиентской стороне;

5. Каждое исполнение, представленное в Таблицах 4.18-4.20 раздела 4, включает фреймворк для разработки мобильного приложения.

6. Допускается подключение различных клиентских компонент к единому набору серверных компонент. При этом используемое исполнение определяется типом используемой клиентской компоненты.

7. Уровень защиты при подключении по протоколу TLS к серверной стороне с двусторонней аутентификацией определяется уровнем защиты клиентской компоненты

(СКЗИ «КриптоПро CSP»/«КриптоПро JCP»/апплет на SIM-карте/приложение «myDSS»/ «AirKey Lite»/фреймворк «myDSS SDK»/«Сбербанк myDSS SDK»/«DSS Client SDK» для «КриптоПро DSS»), но не выше уровня КВ/КВ2 в случае использования оборудования, соответствующего Комплектации 1 Исполнению 1 ПАКМ «КриптоПро HSM» версия 2.0, и не выше уровня КС3 в случае использования оборудования, соответствующего Комплектации 1 Исполнениям 2-5 ПАКМ «КриптоПро HSM» версия 2.0.

8. При использовании компоненты «КриптоПро DSS» с подключением по протоколу TLS с односторонней аутентификацией обеспечивается уровень защиты КС1 (п. 11 «ЖТЯИ.00096-02 95 01. КриптоПро HSM. Правила пользования»). При этом для исполнений отличных от «DSS + myDSS», «DSS + AirKey Lite», «DSS + SIM (QES)», «myDSS SDK», «Сбербанк myDSS SDK», «DSS Client SDK» обязательно отсутствие подключений (прямых или опосредованных) компонент к сетям общего пользования.

9. Дистрибутивы СКЗИ «КриптоПро CSP»/«КриптоПро JCP», мобильные приложения, апплет на SIM-карте, фреймворки могут поставляться отдельно от «КриптоПро DSS».

10. Название используемой комплектации необходимо указывать в сертификате ключа проверки электронной подписи.

11. Комплектации 1 и 2 определяются формуляром ЖТЯИ.00096-01 30 01 и сопутствующим ему комплектом документации. При использовании программных и аппаратных средств комплектаций 1 и 2 в составе Комплектации 3 следует руководствоваться настоящим формуляром ЖТЯИ.00096-02 30 02 и формуляром ЖТЯИ.00096-01 30 01.

12. В случаях аутентификации по логину и паролю и аутентификации по сертификату требуется установка TLS-соединения с использованием алгоритмов п. 3.7.

3.3. «КриптоПро DSS» (Комплектация 3) поставляется в следующих исполнениях, отличающихся обеспечиваемым уровнем защиты:

- DSS + CSP версия 4.0 Исполнение 1-Base;
- DSS + CSP версия 4.0 Исполнение 2-Base;
- DSS + CSP версия 4.0 Исполнение 3-Base;
- DSS + CSP версия 4.0 Исполнение 1-Lic;
- DSS + CSP версия 4.0 Исполнение 2-Lic;
- DSS + CSP версия 5.0 КС1 Исполнение 1-Base;
- DSS + CSP версия 5.0 КС2 Исполнение 2-Base;
- DSS + CSP версия 5.0 КС3 Исполнение 3-Base;
- DSS + JCP версия 2.0 Исполнение 2;
- DSS + SIM (QES);
- DSS + SIM (M2M);
- DSS + myDSS;
- DSS + AirKey Lite;
- myDSS SDK;
- Сбербанк myDSS SDK;
- DSS Client SDK.

Примечание: Исполнения и обеспечиваемый уровень защиты описаны в разд. 4. Каждое из исполнений Комплектации 3 допустимо использовать с аппаратной частью каждого из исполнений Комплектации 1.

3.4. ПАКМ «КриптоПро HSM» обеспечивает:

- реализацию криптографических функций и интерфейса взаимодействия ПАКМ с серверами и клиентскими компонентами ПАКМ пользователей;
- хранение более 500 000 ключевых контейнеров пользователей в зашифрованном виде;
- интерфейс к прикладным криптографическим функциям в соответствии со спецификацией интерфейса СКЗИ «КриптоПро CSP» версии 4.0/5.0;
- возможность использования функций ПАКМ через интерфейсы Microsoft CryptoAPI;
- возможность использования функций ПАКМ через интерфейс PKCS#11;
- идентификацию и аутентификацию пользователей при локальном и удаленном доступе к ПАКМ;
- проверку целостности критичного к безопасному функционированию ПО при инициализации ПАКМ;
- генерацию случайных чисел с использованием аппаратного ДСЧ;
- генерацию закрытого ключа/ключа ЭП с использованием исходного материала, предоставленного уполномоченной организацией;
- сопряжение ПАКМ с сервером/группой серверов по отдельному сегменту Ethernet;
- сопряжение ПАКМ с удаленным рабочим местом Web администрирования ПАКМ;
- ввод закрытого разделенного ключа активации ПАКМ с ключевых носителей на интеллектуальных картах;
- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), вычисление хэш-функции согласно ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2012 (ГОСТ 34.11-2018);
- шифрование и имитозащита согласно ГОСТ 28147-89;
- возможность встречной работы ПАКМ «КриптоПро HSM» с СКЗИ «КриптоПро CSP».

3.5. При встраивании ПАКМ уровень защиты данных, обрабатываемых результирующей системой с применением ПАКМ, определяется в рамках оценки влияния (см. п.1.5) среды функционирования ПАКМ на выполнение предъявленных к ПАКМ требований по классу не выше КВ/КВ2 (при встраивании аппаратного модуля в соответствии с Комплектацией 1 Исполнением 1) или КС3 (при встраивании аппаратного модуля в соответствии с Комплектацией 1 Исполнениями 2-5).

3.6. Срок действия ключей ЭП, являющихся неэкспортируемыми, составляет не более 3-х лет. Максимальный срок действия ключа проверки ЭП — 15 лет после окончания срока действия соответствующего ключа ЭП. Максимальный срок действия открытых ключей обмена — не более 3-х лет. Максимальный срок действия неэкспортируемых закрытых ключей обмена составляет не более 3-х лет. Срок действия иных ключей не превышает 1 года 3 месяцев.

Примечание. Сроки действия ключей ЭП и закрытых ключей обмена могут уточняться при проведении работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПАКМ, на выполнение предъявленных к ПАКМ требований по ТЗ, согласованному с 8 Центром ФСБ России.

3.7. В ПАКМ «КриптоПро HSM» реализованы следующие российские криптографические алгоритмы:

- Алгоритм зашифрования/расшифрования данных и вычисления имитовставки реализован в соответствии с документом «ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

• Алгоритмы формирования и проверки ЭП реализованы в соответствии с документами ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2019 года не допускается.

• Алгоритм выработки значения хэш-функции реализован в соответствии с документами ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018) «Информационная технология. Криптографическая защита информации. Функция хэширования».

3.8. В ПАКМ «КриптоПро HSM» обеспечена возможность использования криптографических алгоритмов SHA1, RSA, 3DES.

3.9. Сетевая аутентификация реализована на базе протокола TLS v.1.0 (RFC 2246) с использованием алгоритмов п. 3.7 в соответствии с документом «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS). Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)».

4. КОМПЛЕКТНОСТЬ

Таблица 4.1 — Комплектация 1 «ПАКМ» Исполнение 1 (уровень защиты КВ/КВ2), Исполнения 2, 3, 4, 5 (уровень защиты КС3)

Наименование	Количество, децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM». Системный блок	1 В соответствии с приложениями А1-А5 ЖТЯИ.00096-01 ТУ
Ключи электронного замка ПАКМ - идентификаторы Touch Memory. Один идентификатор (с маркировкой «А»), предназначен для проведения технического обслуживания предприятием-изготовителем; остальные служат для активации ПАКМ.	
Ключевой носитель – смарт-карта	16
Кабель электропитания	1
Считыватель смарт-карт	Опционально
Сетевой адаптер с оптическим интерфейсом SC	Опционально
Соединительный оптический патч-корд SC-LC, 3 м	Опционально
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули	ЖТЯИ.00096-01 99 01
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-01 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-01 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-01 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-01 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-01 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-01 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-01 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-01 ТУ
Заверенная копия сертификата	

Таблица 4.2 — Комплектация 2 Исполнение 1 — «ПАКМ» и «КриптоПро HSM Client» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1
Программные компоненты	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02

Наименование	Децимальный номер
СКЗИ «КриптоПро CSP» версии 4.0 Исполнение 1-Base / «КриптоПро CSP» версии 5.0 КС1 Исполнение 1-Base	ЖТЯИ.00087 / ЖТЯИ.00101
ПО «КриптоПро JavaCSP»	ЖТЯИ.00096-01 99 12
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-01 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-01 90 02
«КриптоПро HSM». Инструкция по использованию. JavaCSP	ЖТЯИ.00096-01 90 03
«КриптоПро HSM». Инструкция по использованию. JavaTLS	ЖТЯИ.00096-01 90 04
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-01 91 01
«КриптоПро HSM». Руководство администратора безопасности. JavaCSP и JavaTLS	ЖТЯИ.00096-01 91 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство программиста. JavaCSP	ЖТЯИ.00096-01 92 02
«КриптоПро HSM». Руководство программиста. JavaTLS	ЖТЯИ.00096-01 92 03
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-01 93 01
«КриптоПро HSM». Приложение командной строки для подписи и шифрования файлов	ЖТЯИ.00096-01 93 03
«КриптоПро HSM». Приложение командной строки для работы с сертификатами	ЖТЯИ.00096-01 93 04
«КриптоПро HSM». Приложение для создания TLS-туннеля	ЖТЯИ.00096-01 93 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-01 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-01 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-01 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-01 ТУ
Заверенная копия сертификата	

Таблица 4.3 — Комплектация 2 Исполнение 2 — «ПАКМ» и «КриптоПро HSM Client» (уровень защиты КС2)

Наименование	Децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1
Средство защиты от несанкционированного доступа	См. Примечания п. 1
Программные компоненты	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
СКЗИ «КриптоПро CSP» версии 4.0 Исполнение 2-Base / «КриптоПро CSP» версии 5.0 КС2 Исполнение 2-Base	ЖТЯИ.00088 / ЖТЯИ.00102
ПО «КриптоПро JavaCSP»	ЖТЯИ.00096-01 99 12
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-01 90 01

Наименование	Децимальный номер
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-01 90 02
«КриптоПро HSM». Инструкция по использованию. JavaCSP	ЖТЯИ.00096-01 90 03
«КриптоПро HSM». Инструкция по использованию. JavaTLS	ЖТЯИ.00096-01 90 04
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-01 91 01
«КриптоПро HSM». Руководство администратора безопасности. JavaCSP и JavaTLS	ЖТЯИ.00096-01 91 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство программиста. JavaCSP	ЖТЯИ.00096-01 92 02
«КриптоПро HSM». Руководство программиста. JavaTLS	ЖТЯИ.00096-01 92 03
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-01 93 01
«КриптоПро HSM». Приложение командной строки для подписи и шифрования файлов	ЖТЯИ.00096-01 93 03
«КриптоПро HSM». Приложение командной строки для работы с сертификатами	ЖТЯИ.00096-01 93 04
«КриптоПро HSM». Приложение для создания TLS-туннеля	ЖТЯИ.00096-01 93 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-01 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-01 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-01 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-01 ТУ
Заверенная копия сертификата	

Таблица 4.4 — Комплектация 2 Исполнение 3 — «ПАКМ» и «КриптоПро HSM Client» (уровень защиты КС3)

Наименование	Децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1
Средство защиты от несанкционированного доступа	См. Примечания п. 1
Программные компоненты	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
СКЗИ «КриптоПро CSP» версии 4.0 Исполнение 3-Base / «КриптоПро CSP» версии 5.0 КС3 Исполнение 3-Base	ЖТЯИ.00089 / ЖТЯИ.00103
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-01 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-01 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-01 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-01 93 01
«КриптоПро HSM». Приложение командной строки для подписи и шифрования файлов	ЖТЯИ.00096-01 93 03
«КриптоПро HSM». Приложение командной строки для работы с сертификатами	ЖТЯИ.00096-01 93 04

Наименование	Децимальный номер
«КриптоПро HSM». Приложение для создания TLS-туннеля	ЖТЯИ.00096-01 93 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-01 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-01 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-01 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-01 ТУ
Secure Pack Rus версия 3.0.	ЕАРМ.5090005.032-03 (ЖТЯИ.00106-01)
Secure Pack Rus версия 3.0. Формуляр.	ЕАРМ.5090005.032-03 30 01 (ЖТЯИ.00106-01 30 01)
Заверенная копия сертификата	

Таблица 4.5 — Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 1-Base» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Программные компоненты клиентской стороны	
СКЗИ «КриптоПро CSP» версия 4.0 Исполнение 1-Base	ЖТЯИ.00087
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.6 — Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 2-Base» (уровень защиты КС2)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Аппаратные компоненты клиентской стороны	
Средство защиты от несанкционированного доступа	См. Примечания п. 1
Программные компоненты клиентской стороны	
СКЗИ «КриптоПро CSP» версия 4.0 Исполнение 2-Base	ЖТЯИ.00088
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.7 — Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 3-Base» (уровень защиты КС3)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Аппаратные компоненты клиентской стороны	

Наименование	Децимальный номер
Средство защиты от несанкционированного доступа	См. Примечания п. 1
Программные компоненты клиентской стороны	
СКЗИ «КриптоПро CSP» версия 4.0 Исполнение 3-Base	ЖТЯИ.00089
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.8 — Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 1-Lic» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Программные компоненты клиентской стороны	
СКЗИ «КриптоПро CSP» версия 4.0 Исполнение 1-Lic	ЖТЯИ.00087
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01

Наименование	Децимальный номер
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.9 — Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 2-Lic» (уровень защиты КС2)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Аппаратные компоненты клиентской стороны	
Средство защиты от несанкционированного доступа	См. Примечания п. 1
Программные компоненты клиентской стороны	
СКЗИ «КриптоПро CSP» версия 4.0 Исполнение 2-Lic	ЖТЯИ.00088
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.10 — Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС1 Исполнение 1-Base» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Программные компоненты клиентской стороны	
СКЗИ «КриптоПро CSP» версия 5.0 КС1 Исполнение 1-Base	ЖТЯИ.00101
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.11 — Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС2 Исполнение 2-Base» (уровень защиты КС2)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Аппаратные компоненты клиентской стороны	
Средство защиты от несанкционированного доступа	См. Примечания п. 1
Программные компоненты клиентской стороны	

Наименование	Децимальный номер
СКЗИ «КриптоПро CSP» версия 5.0 КС2 Исполнение 2-Base	ЖТЯИ.00102
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.12 — Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС3 Исполнение 3-Base» (уровень защиты КС3)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Аппаратные компоненты клиентской стороны	
Средство защиты от несанкционированного доступа	См. Примечания п. 1
Программные компоненты клиентской стороны	
СКЗИ «КриптоПро CSP» версия 5.0 КС3 Исполнение 3-Base	ЖТЯИ.00103
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01

Наименование	Децимальный номер
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.13 — Комплектация 3 Исполнение «DSS + JCP версия 2.0 Исполнение 2» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Программные компоненты клиентской стороны	
СКЗИ КриптоПро JCP версия 2.0 Исполнение 2	ЖТЯИ.00091
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.14 — Комплектация 3 Исполнение «DSS + SIM (QES)» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Программные компоненты клиентской стороны	
Апплет на SIM-карте (QES)	ЖТЯИ.00096-02 99 06
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
«КриптоПро DSS». Технические условия для записи апплета на SIM-карту	ЖТЯИ.00096-02 98 02
Заверенная копия сертификата	

Таблица 4.15 — Комплектация 3 Исполнение «DSS + SIM (M2M)» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05

Наименование	Децимальный номер
Программные компоненты клиентской стороны	
Апплет на SIM-карте (M2M)	ЖТЯИ.00096-02 99 06
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
«КриптоПро DSS». Технические условия для записи апплета на SIM-карту	ЖТЯИ.00096-02 98 02
Заверенная копия сертификата	

Таблица 4.16 — Комплектация 3 Исполнение «DSS + myDSS» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Программные компоненты клиентской стороны	
Мобильное приложение myDSS	ЖТЯИ.00096-02 99 07
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01

Наименование	Децимальный номер
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.17 — Комплектация 3 Исполнение «DSS + AirKey Lite» (уровень защиты КС1)

Наименование	Децимальный номер
Аппаратные компоненты серверной стороны	
ПАКМ «КриптоПро HSM»	В соответствии с табл. 4.1, 4.4
Программные компоненты серверной стороны	
ПО «КриптоПро HSM Client». Интерфейсные программные модули	ЖТЯИ.00096-01 99 02
«КриптоПро DSS». Модуль идентификации и аутентификации пользователей.	ЖТЯИ.00096-02 99 04
«КриптоПро DSS». Сервисный программный модуль	ЖТЯИ.00096-02 99 05
Программные компоненты клиентской стороны	
Мобильное приложение AirKey Lite	ЖТЯИ.00096-02 99 08
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
Заверенная копия сертификата	

Таблица 4.18 — Комплектация 3 Исполнение «myDSS SDK» (уровень защиты КС1)

Наименование	Децимальный номер
Программные компоненты клиентской стороны	
Фреймворк myDSS SDK	ЖТЯИ.00096-02 99 09
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
«КриптоПро DSS». myDSS SDK. Руководство разработчика. IOS	ЖТЯИ.00096-02 97 02-01
«КриптоПро DSS». myDSS SDK. Руководство разработчика. Android	ЖТЯИ.00096-02 97 02-02
Заверенная копия сертификата	

Таблица 4.19 — Комплектация 3 Исполнение «Сбербанк myDSS SDK» (уровень защиты КС1)

Наименование	Децимальный номер
Программные компоненты клиентской стороны	
Фреймворк Сбербанк myDSS SDK	ЖТЯИ.00096-02 99 10
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро DSS». Конкретизированные правила изготовления и использования векторов аутентификации и пользовательских ключей	ЖТЯИ.00096-02 93 02
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01

Наименование	Децимальный номер
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
«КриптоПро DSS». myDSS SDK. Руководство разработчика. IOS	ЖТЯИ.00096-02 97 02-01
«КриптоПро DSS». myDSS SDK. Руководство разработчика. Android	ЖТЯИ.00096-02 97 02-02
Заверенная копия сертификата	

Таблица 4.20 — Комплектация 3 Исполнение «DSS Client SDK» (уровень защиты КС1)

Наименование	Децимальный номер
Программные компоненты клиентской стороны	
Фреймворк DSS Client SDK	ЖТЯИ.00096-02 99 11
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00096-02 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00096-02 90 01
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00096-02 90 02
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00096-02 91 01
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00096-01 92 01
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00096-02 93 01
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00096-02 94 01
«КриптоПро HSM». Правила пользования	ЖТЯИ.00096-02 95 01
«КриптоПро HSM». Описание реализации	ЖТЯИ.00096-02 96 01
«КриптоПро HSM». ТУ	ЖТЯИ.00096-02 ТУ
«КриптоПро DSS». Общее описание	ЖТЯИ.00096-02 96 02
«КриптоПро DSS». Руководство разработчика	ЖТЯИ.00096-02 97 01
«КриптоПро DSS». Руководство администратора	ЖТЯИ.00096-02 91 02
«КриптоПро DSS». DSS Client SDK. Руководство разработчика. IOS	ЖТЯИ.00096-02 97 03-01
«КриптоПро DSS». DSS Client SDK. Руководство разработчика. Android	ЖТЯИ.00096-02 97 03-02
Заверенная копия сертификата	

Примечания:

1. При использовании «КриптоПро HSM Client» необходимо выполнять требования к среде функционирования (в т.ч. к СЗИ от НСД/АПМДЗ) в соответствии с документацией на входящее в состав «КриптоПро HSM Client» СКЗИ «КриптоПро CSP».

2. СКЗИ «КриптоПро CSP» и «КриптоПро JCP», используемые на клиентской стороне «КриптоПро DSS», функционируют в программно-аппаратных средах, указанных в формуляре на используемую версию СКЗИ.

3. «КриптоПро JavaCSP» функционирует под управлением следующих Java-машин:

- *Java-машина производства Oracle «Java(TM) 7 Runtime Environment, Standard Edition» версии 1.7 и «Java(TM) 8 Runtime Environment, Standard Edition» версии 1.8 на 32-битной и 64-битной платформе.*
- *Java-машина производства Oracle «Java(TM) 10 Runtime Environment, Standard*

Edition» версии 10 и «Java(TM) 11 Runtime Environment, Standard Edition» версии 11 на 64-битной платформе.

- *Java-машины J9VM производства IBM «Java(TM) 7 Runtime Environment, Standard Edition» версии 1.7 и «Java(TM) 8 Runtime Environment, Standard Edition» версии 1.8 на 32-битной и 64-битной платформе.*
- *Java-машины «OpenJDK» версий 7, 8, 10, 11 на 32-битной и 64-битной платформе.*
- *Java-машины «Liberica» версий 8, 10, 11 на 32-битной и 64-битной платформе.*

4. Программные компоненты серверной стороны «КриптоПро DSS» функционируют в следующих программно-аппаратных средах: Windows Server 2008 R2/2012/2012R2/ 2016 (x64).

5. Программные компоненты клиентской стороны «DSS + SIM (QES)» и «DSS + SIM (M2M)» функционируют в среде SIM-карт, удовлетворяющих стандарту JavaCard версии 2.2.2 и выше.

6. Программные компоненты клиентской стороны «DSS + myDSS», «DSS + AirKey Lite», «myDSS SDK», «Сбербанк myDSS SDK», «DSS Client SDK» функционируют в следующих операционных системах:

iOS 8/9/10/11/12/13;
Android 7.0 и выше.

7. При использовании компоненты «КриптоПро DSS» с подключением по протоколу TLS с односторонней аутентификацией обеспечивается уровень защиты КС1 (п. 11 «ЖТЯИ.00096-02 95 01. КриптоПро HSM. Правила пользования»). При этом для исполнений, отличных от «DSS + myDSS», «DSS + AirKey Lite», «DSS + SIM (QES)», «myDSS SDK», «Сбербанк myDSS SDK», «DSS Client SDK» обязательно отсутствие подключений серверных компонент к сетям общего пользования (прямого или опосредованного).

8. Комплект документации предназначен администраторам безопасности и разработчикам прикладного программного обеспечения, использующего СКЗИ.

9. Программное обеспечение и документация в электронном виде в формате PDF (Adobe Acrobat Reader) на CD-ROM для всех исполнений СКЗИ поставляется единым дистрибутивом, формуляр и копия сертификата, заверенная ООО «КРИПТО-ПРО», — в печатном виде.

10. Использование СКЗИ в конкретной программно-аппаратной среде ограничивается лицензией.

11. СКЗИ «КриптоПро CSP»/«КриптоПро JCP», используемые на клиентской стороне «КриптоПро DSS», должны использоваться с учетом документации на используемую версию СКЗИ и действующего на эту версию СКЗИ Извещения об изменениях, а также должны иметь действующий сертификат соответствия ФСБ России.

12. Комплектации 2 и 3 допустимо использовать с любой аппаратной компонентой (исполнением) Комплектации 1.

5. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие ПАКМ «КриптоПро HSM» версия 2.0 ЖТЯИ.00096-02

серийный № дистрибутива _____

вид носителя:

☐ CD-ROM _____ шт.

☐ CD-ROM _____ шт.

☐ _____ _____ шт.

соответствует эталону и признано годным для эксплуатации.

Дата производства: «_____» _____ 20__ г.

Дата модернизации: «_____» _____ 20__ г.

М.П.

Генеральный директор _____

(подпись)

6. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие ПАКМ «КриптоПро HSM» версия 2.0 ЖТЯИ.00096-02

серийный № дистрибутива _____

упаковано в

☐ коробку типа _____

☐ _____

Дата упаковки: "_____"_____ 20___ г.

М. П.

Упаковку произвел _____

(подпись)

7. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

7.1. Пользователь приобретает изделие ПАКМ «КриптоПро HSM» версия 2.0 и должен использовать его в соответствии с рекомендациями, изложенными в эксплуатационной документации.

7.2. Предприятие-изготовитель гарантирует работоспособность изделия в соответствии с объявленными характеристиками в течение Гарантийного срока при соблюдении пользователем требований эксплуатационной документации на изделие.

7.3. Гарантийный срок изделия — 12 (двенадцать) месяцев. Датой начала гарантийного срока является дата производства изделия (см. п. 5).

7.4. В случае выявления в изделии дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения (в соответствии с требованиями, предъявляемыми изготовителем носителей информации), в течение Гарантийного срока изделие подлежит рекламации, и предприятие-изготовитель обязуется по получении рекламации в возможно короткий срок устранить дефекты своими силами и средствами вплоть до поставки нового изделия, а также принять меры, исключающие эти дефекты во всех остальных экземплярах изделия.

7.5. Замена в изделии неисправных частей (деталей, узлов, сборочных единиц) в период гарантийного срока не ведет к установлению нового гарантийного срока на все изделие, либо на замененные части изделия. При этом гарантийный срок изделия продлевается на время, в течение которого изделие не использовалось из-за обнаруженных в нем недостатков.

7.6. Условия и порядок гарантийного обслуживания изделия приведены в Регламенте обслуживания оборудования, опубликованном на Интернет-сайте предприятия-изготовителя по адресу https://www.cryptopro.ru.

7.7. Действие гарантийных обязательств прекращается при истечении гарантийного срока.

7.8. Изготовитель предоставляет возможность продления сервисного обслуживания ПАКМ «КриптоПро HSM» версия 2.0 в течение не менее 5 лет с даты производства изделия (см. п. 5) в соответствии с Регламентом обслуживания оборудования, опубликованном на Интернет-сайте предприятия-изготовителя по адресу https://www.cryptopro.ru.

7.9. Данные о поставке (продаже) изделия:

_____

_____

(наименование организации-поставщика (продавца) изделия)

М.П.

_____

(подпись)

8. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

8.1. Рекламации, связанные с эксплуатацией изделия, должны направляться предприятию-изготовителю в письменном виде по адресу:

127018, Москва, ул. Сущёвский вал, д. 18.

8.2. Срок рассмотрения рекламации — 1 (один) месяц со дня получения рекламации.

8.3. При несоответствии поставляемого изделия, его тары, упаковки, консервации, маркировки и комплектности требованиям сопроводительной документации, пользователь обязан направить рекламацию предприятию-изготовителю в течении 60 дней со дня поставки изделия.

8.4. Предприятие-изготовитель принимает рекламацию, если не установлена вина получателя в возникновении дефекта в изделии.

8.5. Сведения о рекламациях представлены в табл. 1.

Таблица 1. Учет предъявленных рекламаций

Дата	**Содержание рекламации**	**Меры, принятые по рекламации**	**Подпись ответственного лица**

9. СВЕДЕНИЯ О ХРАНЕНИИ

Дата установки на хранение	Дата снятия с хранения	Условия хранения	Должность, фамилия и подпись отв. лица

10. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа о назначении	Номер и дата приказа об освобождении	Подпись ответственного лица

11. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

№ п/п	Основание (вх. № сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Должность, фамилия и подпись лица, ответственного за изменения	Подпись лица, ответственного за эксплуатацию изделия

12. ОСОБЫЕ ОТМЕТКИ

Учет документов ДСДР-001, используемых в ПАКМ «КриптоПро HSM» версия 2.0

№ п/п	Серийные номера	Номера экземпляров	Отметка о выдаче		Отметка об установке		Отметка об уничтожении ключевых документов		
			ФИО ответственного	Дата и расписка в выдаче	Ф.И.О. лиц произведших подключение (установку)	Дата установки, подписи лиц, произведших установку	Дата изъятия (уничтожения)	Ф.И.О. лиц производивших изъятие (уничтожение)	Номер акта или расписка об изъятии (уничтожении)