ООО "КРИПТО-ПРО"

УТВЕРЖДЕН
ЖТЯИ.00046-01 30 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КРИПТОГРАФИЧЕСКИЙ МОДУЛЬ "КриптоПро HSM" v. 1.0

Формуляр

ЖТЯИ.00046-01 30 01

Листов 20

2013

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие Программно-аппаратный криптографический модуль "КриптоПро HSM" v. 1.0, ПАКМ ЖТЯИ.00046-01, 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.00046-01 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.00046-01 определяется руководителем эксплуатирующей организации на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ.

1.4. При эксплуатации ПАКМ ЖТЯИ.00046-01 должны использоваться сертификаты открытых ключей, выпущенные Удостоверяющим центром, сертифицированным по классу защиты не ниже класса защиты используемого СКЗИ.

1.5. При встраивании ПАКМ ЖТЯИ.00046-01 (собственно ПАКМ, клиентские компоненты ПАКМ - "КриптоПро HSM Client". "КриптоПро HSM Client A") в прикладные системы необходимо проводить оценку 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 классам защиты КС3 и КВ2 – во всех случаях;

- по классам защиты КС1 и КС2 - в следующих случаях:

1) если информация, обрабатываемая ПАКМ, подлежит защите в соответствии с законодательством Российской Федерации;

2) при организации защиты информации, обрабатываемой ПАКМ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;

3) при организации криптографической защиты информации, обрабатываемой ПАКМ, 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.

Указанную оценку необходимо проводить по ТЗ, согласованному с 8 Центром ФСБ России.

1.6. Формуляр входит в комплект поставки ПАКМ ЖТЯИ.00046-01 и должен постоянно храниться в органе (подразделении), ответственном за эксплуатацию ПАКМ.

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

2. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ ПАКМ

При эксплуатации ПАКМ ЖТЯИ.00046-01 должны выполняться следующие требования:

1. Средствами ПАКМ **НЕ ДОПУСКАЕТСЯ** обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

   ДОПУСКАЕТСЯ использование ПАКМ для криптографической защиты персональных данных.

2. Ключевая информация является **конфиденциальной**.
3. Для клиентских компонент ПАКМ классов защиты КС1, КС2 и КС3, базирующихся на базе СКЗИ "КриптоПро CSP", должны выполняться требования к эксплуатации соответствующей СКЗИ.
4. Клиентские компоненты ПАКМ должны использоваться со средствами антивирусной защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.
5. Размещение ПАКМ (ПАКМ, клиентские компоненты ПАКМ) в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.
6. В случае, если в модели угроз, которым должно противостоять ПАКМ в информационной системе заказчика, признана опасной утечка по техническим каналам, ПЭВМ, на которых устанавливаются клиентские компоненты ПАКМ, должны быть допущены для обработки информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).
7. Инсталляция клиентских компонент ПАКМ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

3. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1. ПАКМ ЖТЯИ.00046-01 (в составе собственно ПАКМ, клиентских компонент ПАКМ) предназначено для защиты открытой информации в информационных системах общего пользования (вычисление/проверка электронной подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в информационных системах с выполнением функций:

- генерация/проверка электронной подписи областей памяти и файлов;
- вычисление хэш-функции областей памяти и файлов;
- шифрование/расшифрование областей памяти и файлов;
- вычисление имитовставки областей памяти и файлов;
- генерация ключей;
- уничтожение ключей;
- сопряжение с устройством доступа по криптографически защищенным каналам «К», «К2»;
- управления ключами в системе ЕПСС ОАО "УЭК":
  - при работе с российскими криптографическими алгоритмами;
  - при работе с алгоритмами SHA1, RSA, 3DES.

3.2. ПАКМ «КриптоПро HSM» обеспечивает:

- реализацию криптографических функций и интерфейс взаимодействия ПАКМ с серверами и клиентскими компонентами ПАКМ пользователей;
- хранение ключей до 10000 пользователей в зашифрованном виде;
- интерфейс к прикладным криптографическим функциям в соответствии со спецификацией интерфейса СКЗИ "Крипто-Про CSP" v.3.6.1;
- 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 с использованием исходного материала, предоставленного уполномоченной организацией;
- срок действия ключей ЭП, являющихся неизвлекаемыми, составляет не более 3-х лет. Максимальный срок действия ключей проверки ЭП - 15 лет. Максимальный срок действия открытых ключей обмена – не более 3-х лет. Максимальный срок действия неизвлекаемых закрытых ключей обмена составляет не более 3-х лет. Срок действия иных ключей не превышает 1 года 3 месяцев.
- сопряжение ПАКМ с сервером/группой серверов по отдельному сегменту Ethernet;
- сопряжение ПАКМ с удаленным рабочим местом Web администрирования ПАКМ по отдельному сегменту Ethernet;
- 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, вычисление хэш-функции согласно ГОСТ Р 34.11-94;
- шифрование и имитозащита согласно ГОСТ 28147-89;

- возможность встречной работы ПАКМ «КриптоПро HSM» с СКЗИ "КриптоПро CSP";

- Уровень защиты ПАКМ при взаимодействии с устройствами доступа (клиентская компонента ПАКМ, СКЗИ"КриптоПро CSP") определяется уровнем защиты устройства доступа, но не выше уровня КВ2.

Примечание. Сроки действия ключей электронной подписи и закрытых ключей обмена могут уточняться при проведении работ по встраиванию ПАКМ «КриптоПро HSM» в системы по ТЗ, согласованным с 8 Центром ФСБ России.

3.3. В ПАКМ "КриптоПро HSM" реализованы российские криптографические алгоритмы:

- Алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализован в соответствии с ГОСТ 28147-89 "СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ";

- Алгоритм формирования и проверки ЭП реализован в соответствии с ГОСТ Р 34.10-2001. "ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ";

- Алгоритм выработки значения хэш-функции реализован в соответствии с ГОСТ Р 34.11-94 "ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ФУНКЦИЯ ХЭШИРОВАНИЯ".

3.4. В ПАКМ "КриптоПро HSM" обеспечена возможность использования криптографических алгоритмов SHA1, RSA, 3DES.

3.5. Сетевая аутентификация реализована на базе протокола TLS v.1.0 (RFC 2246) с использованием алгоритмов п. 3.3.

4. КОМПЛЕКТНОСТЬ

Комплектация "ПАКМ"

Наименование	Количество, децимальный номер
Аппаратные компоненты	
ПАКМ «КриптоПро HSM». Системный блок	1
Ключи электронного замка ПАКМ - идентификаторы Touch Memory. Один идентификатор (с маркировкой «А»),предназначен для проведения технического обслуживания предприятием-изготовителем; остальные - служат для активации ПАКМ.	
Карта канала К/К2	4
Ключевой носитель – смарт-карта	16
Кабель электропитания	1
Считыватель смарт-карт	Опционально
Сетевой адаптер с оптическим интерфейсом SC	Опционально
Соединительный оптический патч-корд SC-SC, 3 м	Опционально
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 01
ПАКМ «КриптоПро HSM». Интерфейсные программные модули.	ЖТЯИ.00046-01 99 02
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Заверенная копия сертификата	

Комплектация "КриптоПро HSM Client", уровень защиты КС1

Наименование	Децимальный номер
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 03
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03

Наименование	Децимальный номер
Программные компоненты	
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя»	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Заверенная копия сертификата	

Комплектация "КриптоПро HSM Client", уровень защиты КС2

Наименование	Децимальный номер
Аппаратные компоненты	
Средство защиты от несанкционированного доступа	См. Примечание п. 4
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 04
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Заверенная копия сертификата	

Комплектация "КриптоПро HSM Client", уровень защиты КС3

Наименование	децимальный номер
Аппаратные компоненты	
Средство защиты от несанкционированного доступа	См. Примечание п. 4
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 05
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07

Наименование	децимальный номер
Аппаратные компоненты	
Средство защиты от несанкционированного доступа	См. Примечание п. 4
Программные компоненты	
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Secure Pack Rus версия 3.0. Формуляр.	ЕАРМ.5090005.032-01 30 01
Заверенная копия сертификата	

Комплектация "КриптоПро HSM Client", уровень защиты КВ2

Наименование	Децимальный номер
Аппаратные компоненты	
Средство защиты от несанкционированного доступа	См. Примечание п. 4
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 06
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя»	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Заверенная копия сертификата	

Комплектация "КриптоПро HSM Client A", уровень защиты КС1

Наименование	Децимальный номер
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 07
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя»	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Заверенная копия сертификата	

Комплектация "КриптоПро HSM Client A", уровень защиты КС2

Наименование	Децимальный номер
Аппаратные компоненты	
Средство защиты от несанкционированного доступа	См. Примечание п. 4
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 08
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя»	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Заверенная копия сертификата	

Комплектация "КриптоПро HSM Client A", уровень защиты КС3

Наименование	Децимальный номер
Аппаратные компоненты	
Средство защиты от несанкционированного доступа	См. Примечание п. 4
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 09
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя»	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Secure Pack Rus версия 3.0. Формуляр.	ЕАРМ.5090005.032-01 30 01
Заверенная копия сертификата	

Комплектация "КриптоПро HSM Client A", уровень защиты КВ2

Наименование	Децимальный номер

Аппаратные компоненты	
Средство защиты от несанкционированного доступа	См. Примечание п. 4
Программные компоненты	
ПАКМ «КриптоПро HSM». Базовые программные модули.	ЖТЯИ.00046-01 99 10
Эксплуатационная документация	
«КриптоПро HSM». Формуляр	ЖТЯИ.00046-01 30 01
«КриптоПро HSM». Инструкция по использованию	ЖТЯИ.00046-01 90 02
«КриптоПро HSM». Использование интерфейсных модулей	ЖТЯИ.00046-01 90 02-01
«КриптоПро HSM». Руководство администратора безопасности	ЖТЯИ.00046-01 90 03
«КриптоПро HSM». Руководство программиста	ЖТЯИ.00046-01 90 04
«КриптоПро HSM». Руководство пользователя»	ЖТЯИ.00046-01 90 05
«КриптоПро HSM». Описание процедуры сборки	ЖТЯИ.00046-01 90 07
«КриптоПро HSM». Правила пользования	ЖТЯИ.00046-01 90 08
Заверенная копия сертификата	

Примечания.

1. Клиентские компоненты уровня защиты КС1 функционирует в программно-аппаратных средах:
   - Windows 2000 (ia32);
   - Windows XP/2003/Vista/2008/7/2008R2 (ia32, ia64, x64).
2. Клиентские компоненты уровня защиты КС2 функционирует в программно-аппаратных средах
   - Windows XP/2003/Vista/2008/7/2008R2 (ia32, ia64, x64).
   - Linux Standard Base ISO/IEC 23360 (ia32, x64), программно-аппаратные среды, удовлетворяющие стандарту LSB 4.x:
     Cent OS (ia32, x64)
     Fedora (ia32, x64)
     Linpus (ia32)
     Mandriva (ia32, x64)
     MontaVista Linux (ia32, x64)
     Oracle Enterprise Linux (ia32, x64)
     Open SUSE (ia32, x64)
     Red Hat Enterprise Linux (ia32, x64)
     SUSE Linux Enterprise (ia32, x64)
     SUSE LINUX (ia32)
     Ubuntu (ia32, x64)
     Xandros (ia32)
     ALT Linux (ia32, x64);
     Debian (ia32, x64);
     Trustverse Linux XP (ia32);
   - FreeBSD 7/8 (ia32, x64);
   - AIX 5/6/7 (Power PC);
3. Клиентские компоненты уровня защиты КС3 функционируют в программно-аппаратных средах

   Windows XP/2003/Vista/2008/7/2008R2 (ia32, ia64, x64)

   с пакетом Secure Pack Rus версия 3.0,

   или в программно-аппаратных средах

   ОС Windows 2000 (ia32), ОС Windows XP/2003 (ia32, x64)

   с СЗИ Secret Net 6.
4. ПАКМ и клиентские компоненты уровня защиты КВ2 функционируют в программно-аппаратных средах, согласованных с 8 центром ФСБ.
5. В качестве средства защиты от несанкционированного доступа используется Программно-аппаратный комплекс с физическим датчиком случайных чисел "Соболь" УВАЛ.00300-58-01 ТУ или RU.40308570.501410.001 ПС . В программно-аппаратных

средах с ОС Windows может использоваться также Программно-аппаратное средство "Аккорд-АМДЗ" 4012-006-11443195-2005 ТУ. Поставка - по согласованию с пользователем.

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

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

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

5. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие ПАКМ «КриптоПро HSM» ЖТЯИ.00046-01 версия _____

серийный № дистрибутива _____

вид носителя:

☐ CD-ROM _____ шт.

☐ CD-ROM _____ шт.

☐ _____ _____ шт.

соответствует эталону и признано годным для эксплуатации.

Дата выпуска: "_____"_____ 20__ г.

М.П. Генеральный директор

_____

6. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие ПАКМ «КриптоПро HSM» ЖТЯИ.00046-01 версия _____

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» и должен использовать его в соответствии с рекомендациями, изложенными в эксплуатационной документации.

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

В случае выявления в изделии дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения (в соответствии с требованиями, предъявляемыми изготовителем носителей информации), 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.

7.3. Гарантийный срок изделия — 12 (двенадцать) месяцев.

7.4. Начальной датой исчисления гарантийного срока изделия является дата приемки изделия Заказчиком (эксплуатирующей организацией) (см. пп. 6, 7).

7.5. Действие гарантийных обязательств прекращается при истечении гарантийного срока.

7.6. Изготовитель гарантирует авторское сопровождение ПАКМ «КриптоПро HSM» в течение 5 лет с момента приемки изделия Заказчиком (эксплуатирующей организацией).

7.7. Данные о поставке (продаже) изделия:

_____

_____

(наименование организации-поставщика (продавца) изделия)

Дата исчисления гарантийного срока: "_____" _____ _____г.

М.П.

_____

(подпись)

Примечание. При отсутствии данных о дате поставки изделия гарантийный срок отсчитывается от даты его выпуска, указанной в разделе 4 "Свидетельство о приемке".

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. 2.

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 об 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»

№ 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)