

ООО «КРИПТО-ПРО»

УТВЕРЖДЕН
ЖТЯИ.000101-01 30 01 ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

«КриптоПро CSP»

Версия 5.0 КС1

ФОРМУЛЯР

ЖТЯИ.00101-01 30 01

2018 г.

СОДЕРЖАНИЕ

1.	Общие указания	3
2.	Требования к эксплуатации СКЗИ	5
3.	Общие сведения и Основные технические данные.....	6
4.	Комплектность.....	11
5.	Аппаратно-программное средство защиты от НСД.....	12
6.	Свидетельство о приемке	13
7.	Свидетельство об упаковке	14
8.	Гарантии изготовителя (поставщика)	15
9.	Сведения о рекламациях	16
10.	Сведения о хранении	17
11.	Сведения о закреплении изделия при эксплуатации	18
12.	Сведения об изменениях	19
13.	Особые отметки.....	20

1. ОБЩИЕ УКАЗАНИЯ

1.1 Формуляр на изделие «Средство криптографической защиты информации «КриптоПро CSP» версия 5.0 KC1» ЖТЯИ.00101-01 (далее — СКЗИ), 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 СКЗИ 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 защиты информации (Положение ПКЗ-2005)».

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

1.4 При эксплуатации СКЗИ должны использоваться сертификаты ключей электронной подписи (сертификаты открытых ключей), выпущенные Удостоверяющим центром, сертифицированным ФСБ России по классу защиты не ниже класса защиты используемого СКЗИ.

1.5 При встраивании СКЗИ в прикладные системы необходимо по Техническому заданию, согласованному с 8 Центром ФСБ России, проводить оценку влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ 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 обработке 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 обработке 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 остальных случаях рекомендуется проводить установленным порядком проверку корректности встраивания СКЗИ в прикладные системы с целью оценки обоснованности и достаточности мер, принятых для защиты информации, обрабатываемой СКЗИ.

Проведение оценки влияния приложений, перечисленных в п.2 Правил пользования ЖТЯИ.00101-01 95 01, не требуется.

В случае использования вызовов, не входящих в перечень Приложения 2 документа ЖТЯИ.00101-01 95 01. Правила пользования, необходимо производить разработку отдельного СКЗИ на базе «КриптоПро CSP версия 5.0 KC1» 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 СКЗИ 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») при использовании в системах с автоматическим созданием и (или) автоматической проверкой электронной подписи.

1.7 Формуляр входит в комплект поставки СКЗИ и должен постоянно храниться в органе (подразделении), ответственном за эксплуатацию СКЗИ.

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

2. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ

При эксплуатации СКЗИ должны выполняться следующие требования:

2.1 С помощью СКЗИ **не допускается** обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

2.2 Допускается использование СКЗИ 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 Внешняя гамма, используемая для инициализации состояния программного ДСЧ, является конфиденциальной.

2.6 СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. В случае их отсутствия рекомендуется по возможности использовать существующие антивирусные средства защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

2.7 Размещение СКЗИ в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

2.8 При эксплуатации СКЗИ необходимо руководствоваться Положением ПКЗ-2005.

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

При эксплуатации СКЗИ на платформе iOS/Android при обработке конфиденциальной информации для конкретного мобильного устройства, работающего под управлением ОС iOS/Android производства компании Apple/Google, должны выполняться действующие в Российской Федерации требования по защите открытой (конфиденциальной) информации от утечки по техническим каналам. Данное требование не предъявляется в случае эксплуатации СКЗИ на платформе iOS/Android при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации. Внос и использование мобильного устройства, работающего под управлением ОС iOS/Android производства компании Apple/Google, в помещениях, в которых ведутся переговоры секретного содержания или проводятся работы секретного характера, без проведения его специальных исследований и специальной проверки запрещаются.

2.10 Установка СКЗИ на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации (п. 2 ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть).

3. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1 СКЗИ 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 корпоративных информационных системах с выполнением следующих функций:

- 1) защищенное хранение пользовательских ключей в ключевом контейнере с использованием шифрования, имитозащиты и аутентификации доступа;
- 2) шифрование, вычисление имитовставки, хэширование, создание/проверка электронной подписи;
- 3) формирование сессионных ключей, ключей обмена и ключей создания/проверки ЭП, их импорт/экспорт из/в ключевой контейнер;
- 4) идентификация, аутентификация, шифрование и имитозащита TLS-соединений;
- 5) аутентификация в домене Windows с использованием «КриптоПро Winlogon».

3.2 СКЗИ функционирует в следующих программно-аппаратных средах:

Windows

Включает программно-аппаратные среды:

- Windows 7/8.1/10/Server 2003/2008 (x86, x64);
- Windows Server 2008 R2/2012/2012 R2/2016 (x64).

LSB Linux

Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x:

- CentOS 4/5/6 (x86, x64);
- CentOS 7 (x86, x64, POWER, ARM, ARM64);
- Ось (OS-RT) (x64);
- ТД ОС АИС ФССП России (GosLinux) (x86, x64);
- Red OS (x86, x64);
- Fedora 27/28 (x86, x64, ARM);
- Oracle Linux 4/5/6 (x86, x64);
- Oracle Linux 7 (x64);
- OpenSUSE Leap 42, 15 (x86, x64, ARM, ARM64);
- AlterOS (x64);
- SUSE Linux Enterprise Server 11SP4 (x86, x64);
- SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64);
- Red Hat Enterprise Linux 4/5/6 (x86, x64);
- Red Hat Enterprise Linux 7 (x64, POWER, ARM64);
- Синтез-ОС.РС (x86, x64);
- ПК «СинтезМ-Клиент» в составе КП «ЗОС «СинтезМ» (x64);
- ПК «СинтезМ-Сервер» в составе КП «ЗОС «СинтезМ» (x64);
- КП «ОС «СинтезМ-К» (x64);
- Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64);
- Ubuntu 18.04 (x86, x64);
- Linux Mint 17/18/19 (x86, x64);
- Debian 7/8/9 (x86, x64, POWER, ARM, ARM64, MIPS);
- ОС Лотос (x86, x64);
- Astra Linux Special Edition, Common Edition (x64, MIPS, Эльбрус);
- MCBCСфера 6.3 Сервер (x64, ARM64).

Unix

Включает программно-аппаратные среды:

- ОС Эльбрус версия 3 (Эльбрус);
- ALT Linux 6/7 (x86, x64, ARM);
- Альт Сервер 8, Альт Рабочая станция 8, Альт Рабочая станция К 8 (x86, x64, ARM, ARM64);

ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64);
РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);
FreeBSD 9/10/11, pfSense 2.x (x86, x64);
AIX 5/6/7 (POWER);
Mac OS X 10.9/10.10/10.11/10.12 (x64).

Solaris

Включает программно-аппаратные среды:
Solaris 10 (sparc, x86, x64);
Solaris 11 (sparc, x64).

Sailfish

Включает программно-аппаратную среду:
SailfishOS 2.1.1.12 (ARMv7).

iOS

Включает программно-аппаратные среды:
Apple iOS 8.0 и выше (ARMv7, ARM64).

Android

Включает программно-аппаратные среды:
Android 7.0 и выше (ARMv7, ARM64).

Виртуальные среды

Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);
Microsoft Hyper-V 8/8.1/10 (x64);
Citrix XenServer 7.1/7.2 (x64);
VMWare WorkStation 11/12 (x86-64);
VMWare Player 7/12 (x86, x64);
VMWare Sphere ESXi 5.5/6.0 (x64);
Virtual Box 3.2/4.0/4.1/4.2/4.3/5.0/5.1 (x86, x64);
RHEV 3.4/3.5/3.6/4.0 (x64).

Примечания:

1. При эксплуатации СКЗИ необходимо учитывать, что порядок и сроки эксплуатации операционных систем, в среде которых функционирует СКЗИ, определяются производителями операционных систем. Использование операционных систем, поддержка которых остановлена производителем, не допускается.

2. Необходимо использовать дистрибутивы указанных операционных систем, полученные у разработчика операционной системы, и их штатные репозитории с пакетами. Использование прочих сборок ОС не допускается.

3. Для серверного применения СКЗИ (массовое обслуживание) необходима серверная лицензия. Серверными считаются:

- ОС семейства Windows Server (2003/2008/2008R2/2012/2012R2/2016);
- ОС семейства Linux Server (Red Hat Enterprise Linux Server, SuSE Linux Server, Ubuntu Server, Mandriva Enterprise Server 5, Business Server 1, ROSA Enterprise Linux Server);
- Серверные и сетевые ОС (AIX, FreeBSD, Solaris);
- Все платформы с серверной процессорной архитектурой (PowerPC, Sparc).

3.3 Алгоритмы зашифрования/расшифрования данных и вычисления имитовставки реализованы в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», ГОСТ 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» и ГОСТ 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

3.4 Алгоритмы формирования и проверки электронной подписи реализованы в соответствии с ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ Р 34.10-2001 «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.

3.5 Алгоритмы выработки значения хэш-функции реализованы в соответствии с ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

3.6 Сетевая аутентификация реализована на базе протокола TLS v.1.0 с использованием алгоритмов п.п. 3.3-3.5 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)»;

3.7 Ключевая система СКЗИ обеспечивает возможность парно-выборочной связи абонентов сети (по типу «каждый с каждым») с использованием для каждой пары абонентов уникальных ключей, создаваемых на основе принципа открытого распределения ключей.

3.8 Варианты возможных носителей для хранения ключей ЭП (закрытых ключей) в зависимости от используемой ОС отражены в Таблице 3.1.

Таблица 3.1 — Использование ключевых носителей в зависимости от программно-аппаратной платформы

Носитель/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Sailfish OS
ГМД 3,5", USB диски	+	+	+	+	-	+	-	-	-
Gemalto MPCOS (Optelio, Native)	+	+	+	-	-	+	-	-	-
SafeNet eToken	+	-	-	-	-	-	-	-	-
Aladdin R.D. JaCarta LT/PKI/PRO/BIO	+	+	-	-	-	-	-	-	-
Aladdin R.D. JaCarta ГОСТ, JaCarta-2 ГОСТ ¹	+	+	-	-	-	-	-	-	-
Aladdin R.D. JaCarta ФКН ²	+	+	-	-	-	-	-	-	-
USB-токены Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 (micro, Flash, Touch, 2100, micro 2100), Рутокен ЭЦП PKI, Рутокен ЭЦП (micro, Flash), Рутокен ЭЦП 2.0 2151, Рутокен Lite ¹	+	+	+	-	-	+	-	-	-
Рутокен ЭЦП Bluetooth ⁴	+	+	+	-	-	+	-	+	-
Смарткарты Рутокен Lite SC, Рутокен ЭЦП SC, Рутокен ЭЦП 2.0 2100, Рутокен ЭЦП 2.0 2151 ¹	+	+	+	-	-	+	-	-	-
Рутокен S	+	+	+	-	-	+	-	-	-
Рутокен PINPad ¹	+	+	+	-	-	+	-	-	-
Рутокен ФКН ²	+	+	+	+	-	+	-	-	-
Novacard	+	+	+	+	-	+	-	-	-
РИК, ОСКАР, Магистра	+	+	+	+	-	+	-	-	-
СмартПарк ФКН ²	+	+	+	+	-	+	-	-	-
InfoCrypt Token++ Lite	+	+	+	-	-	+	-	-	-
InfoCrypt Token++ ²	+	+	+	-	-	+	-	-	-
InfoCrypt VPN-Key-TLS, Token++ TLS ¹	+	+	+	-	-	+	-	-	-
MorphoKST	+	+	-	-	-	-	-	-	-
Multisoft MS_Key K	+	+	-	-	-	+	-	-	-
ESMART Token	+	+	-	-	-	+	-	-	-
ESMART Token ГОСТ ¹	+	+	-	-	-	+	-	-	-

Alioth INPASPOT, SCONe	+	+	-	-	-	-	-	-	-
Rosan	+	+	+	+	-	+	-	-	-
Модуль взаимодействия с DSS (Cloud)	+	+	+	-	-	+	-	-	-
Реестр	+	-	-	-	-	-	-	-	-
Раздел HDD ПЭВМ/устройство Apple iOS/устройство Android/устройство SailfishOS	+	+	+	+	+	+	+	+	+

Примечания:

1. Необходимо положительное заключение ФСБ России.

2. Необходимо положительное заключение ФСБ России, возможно использование защищенного канала ПК-ФКН по протоколу SESPake.

Остальные носители используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене.

3. Использование носителей других типов — только по согласованию с ФСБ России.

4. Использование в качестве пассивного хранилища ключевой информации Рутокен ЭЦП Bluetooth возможно только при наличии сертификата соответствия ФСБ России на указанное устройство; для иных носителей использовать для передачи данных бесконтактный интерфейс запрещено.

3.9 Формирование закрытых ключей производится с использованием следующих типов считывателей, указанных в Таблице 3.2.

Таблица 3.2 — Использование считывателей в зависимости от программно-аппаратной платформы

Считыватели/ОС	Windows IA32	Windows x64	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Sailfish OS
Дисковод/USB дисковод	+	+	+	+	+	-	+	-	-	-
PS/SC совместимый считыватель смарт-карт	+	+	+	-	+	-	-	+	-	-
ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180)	+	+	+	+	-	-	-	-	-	-
ПАК защиты от НСД «Соболь». Версия 3.1. RU.88338853.501410.020 (исполнения 1, 2)	+	+	+	+	-	-	-	-	-	-
ПАК защиты от НСД «Соболь». Версия 3.2. RU.88338853.501410.021 (исполнения 1, 2)	+	+	+	+	-	-	-	-	-	-
СЗИ НСД «Аккорд-АМД3» ТУ 4012-054-11443195-2013, 4012-006-11443195-2005 ТУ	+	+	+	-	-	-	-	-	-	-
АПМДЗ-У М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ, М-526Е1 (КРИПТОН-ЗАМОК/Е) КБДЖ.468243.090 ТУ	+	+	+	-	-	-	-	-	-	-
Устройство чтения таблеток Touch-Memory Dallas: DS9097E, DS9097U, DS1410E	+	-	-	-	-	-	-	-	-	-
Раздел, реестр HDD ПЭВМ	+	+	+	+	+	+	+	-	-	-
Устройство Apple iOS	-	-	-	-	-	-	-	+	-	-
Устройство Android	-	-	-	-	-	-	-	-	+	-
Устройство Sailfish OS	-	-	-	-	-	-	-	-	-	+

3.10 Формирование случайной последовательности производится с использованием ДСЧ, указанных в Таблице 3.3.

Таблица 3.3 — Использование ДСЧ в зависимости от программно-аппаратной платформы

ДСЧ/ОС	Windows IA32	Windows x64	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Sailfish OS
Биологический ДСЧ	+	+	+	+	+	+	+	+	+	-
Физический ДСЧ в составе ПАК защиты от НСД «Соболь» RU.40308570.501410.001 ПС (версии кода расширения BIOS 1.0.99, 1.0.180)	+	+	+	+	-	-	-	-	-	-
Физический ДСЧ в составе ПАК защиты от НСД «Соболь». Версия 3.1. RU.88338853.501410.020 (исполнения 1, 2)	+	+	+	+	-	-	-	-	-	-
Физический ДСЧ в составе ПАК защиты от НСД «Соболь». Версия 3.2. RU.88338853.501410.021 (исполнения 1, 2)	+	+	+	+	-	-	-	-	-	-
Физический ДСЧ в составе СЗИ НСД «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013, 4012-006-11443195-2005 ТУ	+	+	+	-	-	-	-	-	-	-
Физический ДСЧ в составе АПМДЗ-У М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ, М-526Е1 (КРИПТОН-ЗАМОК/Е) КБДЖ.468243.090 ТУ	+	+	+	-	-	-	-	-	-	-
Физический ДСЧ в составе АПМДЗ «МАКСИМ-М1»	+	+	+	-	-	-	-	-	-	-
Физический ДСЧ «Криптон ССК/ДСЧ» в составе «АПМДЗ И1»	+	+	+	-	-	-	-	-	-	-
Внешняя гамма	+	+	+	+	+	+	+	-	-	+

Примечание: Списки версий программно-аппаратных сред, в которых функционируют перечисленные средства защиты от несанкционированного доступа, приведены в документации на соответствующее средства защиты от несанкционированного доступа.

Примечание: Использование других сертифицированных типов ДСЧ — только по согласованию с ФСБ России.

4. КОМПЛЕКТНОСТЬ

Таблица 4.1 — Комплектация СКЗИ «КриптоПро CSP» версии 5.0 КС1

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00101-01
КриптоПро CSP v. 5.0 КС1. Формуляр.	ЖТЯИ.00101-01 30 01
КриптоПро CSP. Описание реализации.	ЖТЯИ.00101-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00101-01 91 01
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows.	ЖТЯИ.00101-01 91 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux.	ЖТЯИ.00101-01 91 03
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD.	ЖТЯИ.00101-01 91 04
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris.	ЖТЯИ.00101-01 91 05
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX.	ЖТЯИ.00101-01 91 06
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Mac OS X.	ЖТЯИ.00101-01 91 07
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС iOS.	ЖТЯИ.00101-01 91 08
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ в виртуальных средах.	ЖТЯИ.00101-01 91 09
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС SailfishOS	ЖТЯИ.00101-01 91 10
КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС Windows.	ЖТЯИ.00101-01 92 01
КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС iOS.	ЖТЯИ.00101-01 92 02
КриптоПро CSP. Приложение командной строки для подписи и шифрования файлов.	ЖТЯИ.00101-01 93 01
КриптоПро CSP. Приложение командной строки для работы с сертификатами.	ЖТЯИ.00101-01 93 02
КриптоПро CSP. Приложение командной строки для создания TLS-туннеля.	ЖТЯИ.00101-01 93 03
КриптоПро CSP. АРМ выработки внешней гаммы.	ЖТЯИ.00101-01 94 01
КриптоПро CSP. Правила пользования.	ЖТЯИ.00101-01 95 01
КриптоПро CSP. Руководство программиста.	ЖТЯИ.00101-01 96 01
Сертификат СКЗИ (копия).	

Примечания:

1. Комплект документации предназначен для администраторов безопасности, разработчиков прикладного программного обеспечения и пользователей СКЗИ.

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

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

5. АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ЗАЩИТЫ ОТ НСД

Изделие «КриптоПро CSP» версия 5.0 КС1» ЖТЯИ.00101-01 укомплектовано аппаратно-программным средством защиты информации от несанкционированного доступа.

Наименование средства, ТУ	Серийный номер, дата выпуска

М.П.

/ _____ /
" ____ " _____ 20__ г.

6. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие «КриптоПро CSP» версия 5.0 КС1» ЖТЯИ.00101-01,
серийный № дистрибутива _____

носители:

CD-ROM _____ шт.

соответствует эталону, хранящемуся в ООО «КРИПТО-ПРО», и признано годным для эксплуатации.

Дата выпуска: " ____ " _____ 20__ г.

М.П.

_____ / _____ /

7. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие «КриптоПро CSP» версия 5.0 КС1» ЖТЯИ.00101-01,
серийный № дистрибутива _____

упаковано в

- бумажный конверт
- коробку
- пластиковый конверт
- _____

Дата упаковки: " ____ " _____ 20__ г.

М.П. Упаковку произвел _____ / _____ /

8. ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)

8.1 Пользователь приобретает изделие и несет ответственность за его использование в соответствии с рекомендациями, изложенными в эксплуатационной документации.

8.2 Предприятие-изготовитель гарантирует работоспособность изделия в соответствии с заявленными характеристиками.

8.3 В случае выявления в программном обеспечении дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения, изделие подлежит рекламации. 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 в последующих экземплярах изделия.

8.4 Гарантийный срок изделия — 12 месяцев с момента поставки при условии соблюдения пользователем требований эксплуатационной документации на изделие.

Примечание. При отсутствии данных о дате поставки изделия гарантийный срок отсчитывается от даты его выпуска, указанной в разделе 6 «Свидетельство о приемке».

8.5 Данные о поставке (продаже) изделия:

(наименование организации-поставщика (продавца) изделия)

Дата поставки: "___" _____ 20__г.

М.П.

(подпись)

9. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

127018, г. Москва, ул. Суцёвский Вал, д.18.

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

9.3 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.

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

9.5 Сведения о рекламациях фиксируются в таблице 9.1.

Таблица 9.1 — Сведения о рекламациях

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

13. ОСОБЫЕ ОТМЕТКИ