

УТВЕРЖДЕН

ЖТЯИ.00101-02 30 01-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

«КриптоПро CSP»

Версия 5.0 R2 KC1

Исполнение 1-Base

Формуляр

ЖТЯИ.00101-02 30 01

Содержание

1 ОБЩИЕ УКАЗАНИЯ	3
2 ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ	5
3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ	6
4 КОМПЛЕКТНОСТЬ	14
5 АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ЗАЩИТЫ ОТ НСД	16
6 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ	17
7 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ	18
8 ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)	19
9 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ	20
10 СВЕДЕНИЯ О ХРАНЕНИИ	21
11 СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ	22
12 СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ	23
13 ОСОБЫЕ ОТМЕТКИ	24

1 ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие «Средство криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base» ЖТЯИ.00101-02 (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. Сертификаты открытых ключей (ключей проверки ЭП), используемые СКЗИ, должны быть выпущены 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 (далее — СФ) 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 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 России 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 СФ на СКЗИ с целью оценки обоснованности и достаточности мер, принятых для защиты информации, обрабатываемой СКЗИ.

В разделе 1 документа «ЖТЯИ.00101-02 95 01. Правила пользования» указаны программные продукты (СФ), проведение оценки влияния которых на СКЗИ не требуется.

В случае использования вызовов, не входящих в перечень Приложения 2 документа «ЖТЯИ.00101-02 95 01. Правила пользования», необходимо проводить разработку отдельного СКЗИ на базе «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base (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)).

Проведение тематических исследований программных продуктов и приложений, перечисленных в разделе 1 документа «ЖТЯИ.00101-02 95 01. Правила пользования», не требуется.

1.6. СКЗИ соответствует «Требованиям к средствам электронной подписи» (Приложение 1 к Приказу ФСБ России 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. СКЗИ соответствует требованиям Приказа Минкомсвязи России от 14.09.2020 № 472 «Об утверждении Формата электронной подписи, обязательного для реализации всеми средствами электронной подписи».

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

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

1.10. СКЗИ предназначено для использования как на территории Российской Федерации, так и за ее пределами. Использование СКЗИ в обычном или в экспортном варианте определяется лицензией.

2 ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ

При эксплуатации СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base 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. При создании защищенных с использованием шифровальных (криптографических) средств информационных систем необходимо на основании модели угроз и нарушителя на эту систему определить необходимость применения антивирусных средств (АВС). Если такая необходимость определена, должны применяться АВС, сертифицированные органом, ответственным за обеспечение информационной безопасности в создаваемой информационной системе.

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 платформах iOS/Android/Sailfish при обработке информации для конкретного мобильного устройства, работающего под управлением указанных ОС, 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 платформах iOS/Android/Sailfish при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации. Внос и использование мобильного устройства, работающего под управлением ОС iOS/Android/Sailfish, 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 (раздел 2 «ЖТЯИ.00101-02 95 01. Правила пользования»).

3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1. СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base может выступать как в качестве готового к применению средства, так и в качестве платформы для построения на его основе программных, программно-аппаратных и аппаратных решений в области обеспечения информационной безопасности, основанных на применении российских криптографических алгоритмов.

СКЗИ предназначено для выполнения следующих функций:

- 1) защищенное хранение пользовательских ключей в ключевом контейнере с использованием шифрования, имитозащиты и аутентификации доступа;
- 2) шифрование, вычисление имитовставки, хэширование, создание/проверка ЭП;
- 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 («КриптоПро TLS»);
- 5) аутентификация в домене Windows («КриптоПро Winlogon»);
- 6) защита IP-соединений («КриптоПро IPsec»);

3.2. СКЗИ функционирует в следующих программно-аппаратных средах:

Windows

Windows 7/8/8.1/10/Server 2008 (x86, x64)

Windows Server 2008 R2/2012/2012 R2/2016/2019 (x64)

LSB Linux

Дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x.

CentOS 6 (x86, x64)

CentOS 7 (x86, x64, POWER, ARM, ARM64)

CentOS 8 (x64, POWER, ARM64)

ОСь (OS-RT) (x64)

ТД ОС АИС ФССП России (GosLinux) (x86, x64)

РЕД ОС, РЕД ОС 7.1/7.2 (x86, x64)

Fedora 28/29/30/31 (x86, x64, ARM, ARM64)

Oracle Linux 5/6 (x86, x64)

Oracle Linux 7 (x64)

Oracle Linux 8 (x64, ARM64)

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 5/6 (x86, x64)

Red Hat Enterprise Linux 7/8 (x64, POWER, ARM64)

Check Point GAIa (x86, x64)

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, ARM, ARM64)
Ubuntu 18.04/19.10/20.04 (x64, ARM, ARM64)
Halo OS (x64)
Linux Mint 18/19/20 (x86, x64)
Debian 8/9/10 (x86, x64, ARM, ARM64, MIPS)
Лотос (x86, x64)
Astra Linux Special Edition, Common Edition (x86, x64, ARM, ARM64, MIPS, Эльбрус)
МСВСфера 6.3 Сервер (x64, ARM64)
ThinLinux 2 (x64)
ЕМИАС 1.0 (x64)
Мурена 1.4 (ARM9)

Unix

ОС Эльбрус версия 3 (Эльбрус)
ALT Linux 7 (x86, x64, ARM)
Альт Сервер 9, Альт Рабочая станция 9, Альт Образование 9 (x86, x64, ARM64, MIPS, Эльбрус)
Альт 8 СП Сервер, Альт 8 СП Рабочая станция (x86, x64, Эльбрус)
Альт Сервер 8, Альт Рабочая станция 8, Альт Образование 8 (x86, x64)
ROSA Enterprise Desktop (RED X4) (x86, x64)
ROSA Enterprise Linux Desktop, Enterprise Linux Server (x64)
РОСА КОБАЛЬТ (x64)
FreeBSD 11/12, pfSense 2.x (x86, x64)
AIX 6/7 (POWER)
Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14/10.15 (x64)

Solaris

Solaris 10 (SPARC, x86, x64)
Solaris 11 (SPARC, x64)

Sailfish

Sailfish OS (Sailfish Mobile OS RUS) 2/3 (ОС «Аврора») (ARMv7)

iOS

Apple iOS 8/9/10/11/12/13/14 (ARMv7, ARM64)

Android

Android 8/9/10/11 (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 (x64)
VMWare WorkStation 11/12/14/15 (x86, x64)
VMWare WorkStation Player 12/14/15 (x86, x64)
VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7 (x64)
Oracle VirtualBox 5.2 (x86, x64)
RHEV 4 (x64)
ROSA Virtualization (x64)
Альт Сервер Виртуализации 9 (x64, ARM64)

Java-машины (для модуля «КриптоПро JavaCSP»)

Java-машины 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-машины 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

Примечание.

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

2. Необходимо использовать дистрибутивы указанных ОС, полученные у разработчика ОС, 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;
- ОС семейства Linux Server (Red Hat Enterprise Linux Server, SUSE Linux Enterprise Server, ROSA Enterprise Linux Server и др.);
- Серверные и сетевые ОС (AIX, FreeBSD, Solaris);
- Все платформы с серверной процессорной архитектурой (POWER, SPARC).

4. Для использования «КриптоПро IPsec» в среде серверных ОС необходимо приобретать лицензию на право использования «КриптоПро IPsec» на сервере. Указанная лицензия не входит в комплект поставки и поставляется отдельно по согласованию с Заказчиком.

5. Для использования протокола TLS в среде серверных ОС, отличных от Windows, необходимо приобретать лицензию на право использования СКЗИ «КриптоПро CSP» версии 5.0 R2 KC1 для TLS-сервера. Указанная лицензия не входит в комплект поставки и поставляется отдельно по согласованию с Заказчиком.



Для использования двусторонней аутентификации в протоколе TLS в среде клиентских ОС (при отсутствии лицензии на «КриптоПро CSP»), необходимо приобретать лицензию на право использования СКЗИ «КриптоПро CSP» версии 5.0 R2 KC1 для TLS-аутентификации на одном рабочем месте. Указанная лицензия не входит в комплект поставки и поставляется отдельно по согласованию с Заказчиком.

6. Для использования «КриптоПро JavaCSP» в среде серверных ОС необходимо приобретать лицензию на право использования «КриптоПро JavaCSP» на сервере. Указанная лицензия не входит в комплект поставки и поставляется отдельно по согласованию с Заказчиком. В клиентских ОС отдельная лицензия на использование «КриптоПро JavaCSP» не требуется при условии наличия клиентской лицензии на «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base.

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 Р 34.12-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Блочные шифры», ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018) «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

3.4. Алгоритмы формирования и проверки электронной подписи реализованы в соответствии с ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», 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 создания электронной подписи после 31 декабря 2019 года не допускается.

3.5. Алгоритмы выработки значения хэш-функции реализованы в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования», ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018) «Информационная технология. Криптографическая защита информации. Функция хэширования».

3.6. Сетевая аутентификация на базе протокола TLS 1.0, 1.1, 1.2 с использованием алгоритмов п.п. 3.3.–3.5. реализована в соответствии с методическими рекомендациями МР 26.2.001-2013 «Информационная технология. Криптографическая защита информации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)» и рекомендациями по стандартизации Р 1323565.1.020-2018 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».

3.7. Сетевая аутентификация, шифрование и обеспечение целостности соединений на базе протоколов IPSEC с использованием алгоритмов п.п. 3.3-3.5 реализованы в соответствии с техническими спецификациями, разработанными Техническим комитетом по стандартизации «Криптографическая защита информации» (ТК 26):

- ТС 26.2.002-2013 «Информационная технология. Криптографическая защита информации. Использование ГОСТ Р 34.11-94 при обеспечении целостности в протоколах IPSEC и ESP»;
- ТС 26.2.001-2015 «Информационная технология. Криптографическая защита информации. Использование ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 в протоколах обмена ключами IKE и ISAKMP»;
- ТС 26.2.001-2013 «Информационная технология. Криптографическая защита информации. Использование ГОСТ 28147-89 и ГОСТ Р 34.10-2001 при согласовании ключей в протоколах IKE и ISAKMP»;

– ТС 26.2.002-2014 «Информационная технология. Криптографическая защита информации. Использование ГОСТ 28147-89 при шифровании вложений в протоколах IPSEC ESP».

3.8. Формирование защищенных сообщений в формате CMS с использованием алгоритмов п.п. 3.3.–3.5. реализовано в соответствии с методическими рекомендациями МР 26.2.002- 2013. «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10 и ГОСТ Р 34.11 в криптографических сообщениях формата CMS» и рекомендациями по стандартизации Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами».

3.9. 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.

3.10. Варианты возможных носителей для хранения ключей ЭП (закрытых ключей) в зависимости от используемой ОС отражены в Таблице 3.2.

Таблица 3.2. Использование ключевых носителей в зависимости от программно-аппаратной платформы

Носители/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Sailfish
Функциональные ключевые носители (ФКН) с поддержкой SESPAAKE ¹									
Рутокен ЭЦП 2.0 3000 (USB, Type-C, micro)	+	+	+	–	–	+	–	+	+
Смарт-карта Рутокен ЭЦП 3.0	+	+	+	–	–	+	+	+	+
InfoCrypt Токен++	+	+	+	–	–	+	–	–	+
Форос 2. Базис	+	+	+	–	–	+	–	–	+
Функциональные ключевые носители (ФКН) без поддержки SESPAAKE ²									
Aladdin R.D. JaCarta-2 ГОСТ, JaCarta SF/ГОСТ	+	+	–	–	–	+	+	+	+
Aladdin R.D. JaCarta-2 SE/PKI/ГОСТ	–	–	–	–	–	–	–	+	–
Рутокен ЭЦП 2.0 (USB, micro, Flash, Touch) Рутокен ЭЦП 2.0 2100 (USB, Type-C, micro) Рутокен ЭЦП PKI (USB, Type-C, micro) Рутокен ЭЦП (USB, micro, Flash) Рутокен ЭЦП 2.0 2151	+	+	+	–	–	+	–	+	+
Смарт-карты Рутокен ЭЦП SC, Рутокен ЭЦП 2.0 2100, Рутокен ЭЦП 2.0 2151	+	+	+	–	–	+	–	–	–
Рутокен ЭЦП Bluetooth ⁴	+	+	+	–	–	+	+	+	–
Рутокен PINPad	+	+	+	–	–	+	–	–	–
Рутокен TLS (исполнение 1)	+	+	–	–	–	+	–	–	–
InfoCrypt VPN-Key-TLS, Токен++ TLS	+	+	+	–	–	+	–	–	+
ESMART Token ГОСТ	+	+	–	–	–	+	–	–	–
еDoc (УЛГ)	+	+	+	–	–	+	–	–	–

Носители/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Sailfish
КриптоПро Cloud CSP (модуль взаимодействия с DSS)	+	+	+	-	-	+	-	-	-
Пассивные ключевые носители ³									
ГМД 3,5", USB-флэш-накопители	+	+	+	+	-	+	-	-	-
Gemalto MPCOS (Optelio, Native)	+	+	+	-	-	+	-	-	-
SafeNet eToken	+	-	-	-	-	-	-	-	-
Aladdin R.D. JaCarta LT/PKI/PRO/BIO/ГОСТ	+	+	-	-	-	+	+	+	+
USB-токены Рутокен Lite, Рутокен S, Рутокен КП, смарт-карты Рутокен Lite SC	+	+	+	-	-	+	-	+	+
Рутокен Lite microSD	-	-	-	-	-	-	-	+	-
Novacard	+	+	+	-	-	+	-	-	-
ОСКАР, Форос, Форос 2, R301 Форос	+	+	+	-	-	+	+	-	+
InfoCrypt Token++ Lite	+	+	+	-	-	+	-	-	+
MorphoKST	+	+	+	-	-	+	-	-	-
Multisoft MS_Key K	+	+	+	-	-	+	-	-	+
ESMART Token	+	+	+	-	-	+	-	-	-
Alioth INPASPOТ, SCOne	+	+	+	-	-	+	-	-	-
Rosan	+	+	+	-	-	+	-	-	-
Dallas Touch Memory (iButton) DS199x	+	-	-	-	-	-	-	-	-
Реестр ⁵	+	-	-	-	-	-	-	-	-
Раздел HDD/SSD ПЭВМ / устройство Apple iOS / устройство Android / устройство Sailfish ⁵	+	+	+	+	+	+	+	+	+

Примечание.

1. Работа с данными носителями поддерживается в режиме активного вычислителя с защитой канала между носителем и СКЗИ по протоколу SESPake (ФКН с поддержкой SESPake). Необходимо наличие положительного заключения ФСБ России на указанные носители.



2. Работа с данными носителями поддерживается в режиме активного вычислителя без защиты канала между носителем и СКЗИ по протоколу SESPake (ФКН без поддержки SESPake). Требуется применение дополнительных организационно-технических мер защиты. Необходимо наличие положительного заключения ФСБ России на указанные носители.

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

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

5. Хранение закрытых ключей на несъемных носителях (в реестре ОС Windows, в разделе HDD/SSD ПЭВМ, на устройствах Apple iOS/Android/Sailfish и т.п.) допускается только при условии распространения на носитель требований по обращению с ключевыми носителями (раздел 3 «ЖТЯИ.00101-02 95 01. Правила пользования»).
6. Использование других носителей — только по согласованию с ФСБ России.
7. Описание типов носителей, технологий работы с ключами и правила обеспечения безопасности при работе с ними приведены в разделе 3.3 документа «ЖТЯИ.00101-02 95 01. Правила пользования».

3.11. Формирование закрытых ключей (ключей ЭП) производится с использованием следующих типов считывателей, указанных в Таблице 3.4.

Таблица 3.4. Использование считывателей в зависимости от программно-аппаратной платформы

Считыватели/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Sailfish
Дисковод/USB-порт	+	+	+	+	–	+	–	–	–
PC/SC совместимый считыватель смарт-карт	+	+	–	+	–	–	+	–	–
ПАК «Соболь». Версия 3.0. RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180)	+	+	+	–	–	–	–	–	–
ПАК «Соболь». Версия 3.1. RU.88338853.501410.020 (исполнения 1, 2)	+	+	+	–	–	–	–	–	–
ПАК «Соболь». Версия 3.2. RU.88338853.501410.021 (исполнения 1, 2)	+	+	+	–	–	–	–	–	–
ПАК «Соболь». Версия 4. RU.88338853.501410.019	+	+	+	–	–	–	–	–	–
СЗИ НСД «Аккорд-АМД3» ТУ 4012-006-11443195-2005, ТУ 4012-038-11443195-2011, ТУ 4012-054-11443195-2013, ТУ 26.20.40.140-079-37222406-2019	+	+	–	–	–	–	–	–	–
Раздел HDD/SSD ПЭВМ, реестр	+	+	+	+	+	+	–	–	–
Устройство Apple iOS	–	–	–	–	–	–	+	–	–
Устройство Android	–	–	–	–	–	–	–	+	–
Устройство Sailfish	–	–	–	–	–	–	–	–	+



Примечание. Списки версий программно-аппаратных сред, в которых функционируют перечисленные изделия, приведены в документации на соответствующее изделие.

3.12. Формирование случайной последовательности производится с использованием ДСЧ, указанных в Таблице 3.5.

Таблица 3.5. Использование ДСЧ в зависимости от программно-аппаратной платформы

ДСЧ/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Sailfish
Биологический ДСЧ	+	+	+	+	+	+	+	+	–
Физический ДСЧ в составе ПАК «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180)	+	+	+	–	–	–	–	–	–
Физический ДСЧ в составе ПАК «Соболь». Версия 3.1. RU.88338853.501410.020 (исполнения 1, 2)	+	+	+	–	–	–	–	–	–
Физический ДСЧ в составе ПАК «Соболь». Версия 3.2. RU.88338853.501410.021 (исполнения 1, 2)	+	+	+	–	–	–	–	–	–
Физический ДСЧ в составе ПАК «Соболь». Версия 4. RU.88338853.501410.019	+	+	+	–	–	–	–	–	–
Физический ДСЧ в составе СЗИ НСД «Аккорд-АМДЗ» ТУ 4012-006-11443195-2005, ТУ 4012-038-11443195-2011, ТУ 4012-054-11443195-2013, ТУ 26.20.40.140-079-37222406-2019	+	+	–	–	–	–	–	–	–
Физический ДСЧ в составе АПМДЗ «КРИПТОН-ЗАМОК/У» (М-526Б) КБДЖ.468243.067 ТУ, АПМДЗ «КРИПТОН-ЗАМОК/Е» (М-526Е1) КБДЖ.468243.090 ТУ	+	+	–	–	–	–	–	–	–
Физический ДСЧ в составе АПМДЗ «Максим-М1»	+	+	–	–	–	–	–	–	–
Физический ДСЧ «КРИПТОН-ССК/ДСЧ»	+	+	–	–	–	–	–	–	–
Физический ДСЧ «КРИПТОН USB-ДСЧ»	+	+	–	–	–	–	–	–	–
Физический ДСЧ в составе АПМДЗ «Витязь-А»	+	+	–	–	–	–	–	–	–
Внешняя гамма	+	+	+	+	+	+	–	–	+



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

4 КОМПЛЕКТНОСТЬ

Таблица 4.1. Комплектация «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base

Наименование		Обозначение
1	КриптоПро CSP. Базовые модули.	ЖТЯИ.00101-02
2	КриптоПро IPsec.	ЖТЯИ.00101-02 99 01
3	КриптоПро JavaCSP.	ЖТЯИ.00101-02 99 02
4	КриптоПро CSP Lite.	ЖТЯИ.00101-02 99 03
5	КриптоПро CSP. Формуляр.	ЖТЯИ.00101-02 30 01
6	КриптоПро CSP. Описание реализации.	ЖТЯИ.00101-02 90 01
7	КриптоПро CSP. Описание реализации IPsec.	ЖТЯИ.00101-02 90 02
8	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows.	ЖТЯИ.00101-02 91 02
9	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux.	ЖТЯИ.00101-02 91 03
10	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD.	ЖТЯИ.00101-02 91 04
11	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris.	ЖТЯИ.00101-02 91 05
12	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX.	ЖТЯИ.00101-02 91 06
13	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Mac OS X.	ЖТЯИ.00101-02 91 07
14	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС iOS.	ЖТЯИ.00101-02 91 08
15	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ в виртуальных средах.	ЖТЯИ.00101-02 91 09
16	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Sailfish.	ЖТЯИ.00101-02 91 10
17	КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Android.	ЖТЯИ.00101-02 91 11
18	КриптоПро CSP. Руководство администратора безопасности. Использование JavaCSP и JavaTLS.	ЖТЯИ.00101-02 91 12
19	КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС Windows.	ЖТЯИ.00101-02 92 01
20	КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС iOS.	ЖТЯИ.00101-02 92 02
21	КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС Android.	ЖТЯИ.00101-02 92 03
22	КриптоПро CSP. Инструкция по использованию JavaCSP.	ЖТЯИ.00101-02 92 04
23	КриптоПро CSP. Инструкция по использованию JavaTLS.	ЖТЯИ.00101-02 92 05
24	КриптоПро CSP. Инструкция по использованию графического приложения Инструменты КриптоПро.	ЖТЯИ.00101-02 92 06
25	КриптоПро CSP. Приложение командной строки cryptsp.	ЖТЯИ.00101-02 93 01

Наименование		Обозначение
26	КриптоПро CSP. Приложение командной строки для работы с сертификатами.	ЖТЯИ.00101-02 93 02
27	КриптоПро CSP. Приложения командной строки для создания TLS-туннеля.	ЖТЯИ.00101-02 93 03
28	КриптоПро CSP. АРМ выработки внешней гаммы.	ЖТЯИ.00101-02 94 01
29	КриптоПро CSP. Правила пользования.	ЖТЯИ.00101-02 95 01
30	КриптоПро CSP. Руководство программиста.	ЖТЯИ.00101-02 96 01
31	КриптоПро CSP. Руководство программиста JavaCSP.	ЖТЯИ.00101-02 96 02
32	КриптоПро CSP. Руководство программиста JavaTLS.	ЖТЯИ.00101-02 96 03
33	Сертификат СКЗИ (копия).	

**Примечание.**

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) поставляется на компакт-диске (CD-ROM, CD-RW, CD-R, DVD, DVD-R) 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 «КристоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base (ЖТЯИ.00101-02) укомплектовано аппаратно-программным средством защиты информации от несанкционированного доступа.

Наименование изделия, ТУ	Серийный номер, дата выпуска

М.П.

_____ / _____ /

"__" _____ 20 __ г.

6 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие «КристоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base (ЖТЯИ.00101-02)

серийный № дистрибутива _____

носители:

☐ компакт-диск _____ шт.

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

Дата выпуска: "___" _____ 20 __ г.

М.П. _____ / _____ /

7 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие «КристоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base (ЖТЯИ.00101-02)

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 разд. 6 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ.

8.5. Данные о поставке (продаже) изделия:

(наименование организации-поставщика (продавца) изделия)

Дата поставки: "___" _____ 20___ г.

М.П.

_____ / _____ /

9 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

127018, г. Москва, ул. Сущёвский 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 табл. 9.1.

Таблица 9.1. Сведения о рекламациях

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

10 СВЕДЕНИЯ О ХРАНЕНИИ

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

11 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

12 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

13 ОСОБЫЕ ОТМЕТКИ