ООО «КРИПТО-ПРО»

УТВЕРЖДЕН

ЖТЯИ.00101-03 30 01-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

«КриптоПро CSP»

Версия 5.0 R3 KC1

(исполнение 1-Base)

Формуляр

ЖТЯИ.00101-03 30 01

С учетом извещения об изменениях ЖТЯИ.00101-03.1-2024

2024

Содержание

1 ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие «Средство криптографической защиты информации «КриптоПро CSP» версия 5.0 R3 KC1 (исполнение 1-Base)» ЖТЯИ.00101-03 (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 зашиты информации (Положение ПКЗ-2005)».

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

1.4. Сертификаты открытых ключей (ключей проверки ЭП), используемые СКЗИ, следует выпускать Удостоверяющим центром, сертифицированным ФСБ России по классу защиты не ниже класса защиты используемого СКЗИ, с учетом модели угроз и нарушителя информационной системы, в которой применяется СКЗИ, а также с учетом нормативных документов, определяющих создание такой информационной системы.

1.5. Встраивание СКЗИ в аппаратные, программно-аппаратные и программные средства связи/системы и проведение исследований среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований должны выполняться в соответствии с требованиями раздела 4 документа «ЖТЯИ.00101-03 95 01. Правила пользования».

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

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

1.9. 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 R3 КС1 (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. Внос и использование мобильного устройства, работающего под управлением ОС iOS/Android/Аврора, в помещениях, в которых ведутся переговоры, содержащие сведения, составляющие государственную тайну, или проводятся работы секретного характера, без проведения его специальных исследований и специальной проверки запрещаются.

2.10. Эксплуатация СКЗИ может осуществляться только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации (раздел 2 «ЖТЯИ.00101-03 95 01. Правила пользования»).

3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1. СКЗИ «КриптоПро CSP» версия 5.0 R3 КС1 (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;

2) шифрование, вычисление имитовставки, хэширование, создание/проверка ЭП;

3) создание, управление и уничтожение ключевой информации (в т.ч. сессионных ключей, ключей обмена и ключей ЭП/ключей проверки ЭП);

4) идентификация, аутентификация, шифрование и имитозащита TLS-соединений;

5) аутентификация в домене Windows («КриптоПро Winlogon»);

6) защита IP-соединений («КриптоПро IPsec»);

7) использование в качестве клиентского компонента ПАКМ «КриптоПро HSM» версия 2.0 R3.

3.2. СКЗИ функционирует в следующих программно-аппаратных средах:

Windows

Windows 7*/8/8.1 (x86, x64)

Windows 10 (x86, x64, ARM64)

Windows 11 (x64, ARM64)

Windows Server 2008 (x86, x64)

Windows Server 2008 R2/2012/2012 R2/2016/2019/2022 (x64)

**Версия Embedded/Embedded POSReady*

LSB Linux

Дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base (LSB) ISO/IEC 23360

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

CentOS 8 (x64, POWER, ARM64)

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

РЕД ОС 7.1/7.2/7.3/8 (x86, x64, ARM64)

Oracle Linux 6 (x86, x64)

Oracle Linux 7 (x64)

Oracle Linux 8/9 (x64, ARM64)

OpenSUSE Leap 15 (x86, x64, ARM, ARM64)

AlterOS (x64)

SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64)

Red Hat Enterprise Linux 6 (x86, x64)

Red Hat Enterprise Linux 7/8/9 (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 (x64, ARM, ARM64)
Ubuntu 20.04/22.04 (x64, ARM, ARM64, RISC-V)
Halo OS (x64)
Linux Mint 20/21 (x86, x64)
Debian 8/9/10/11/12 (x86, x64, ARM, ARM64, MIPS)
Лотос (x86, x64)
Astra Linux Special Edition, Common Edition (x64, ARM, ARM64, MIPS, Эльбрус, подсистема x86)
МСВСфера 6.3 Сервер (x64, ARM64)
ThinLinux 2 (x64)
ЕМИАС 1.0 (x64)
Мурена 1.4 (ARM9)
ОС ОН «Стрелец» (x64)
ОС «Атлант» (x64)
ОСОН «ОСнова» 2.0 (x64)

Unix

ОС Эльбрус версия 3 (Эльбрус)
ALT Linux 7 (x86, x64, ARM)
Альт 8 СП Сервер, Альт 8 СП Рабочая станция (x86, x64, Эльбрус)
Альт Сервер 8, Альт Рабочая станция 8, Альт Образование 8 (x86, x64)
Альт Сервер 9, Альт Рабочая станция 9, Альт Образование 9 (x86, x64, ARM64, MIPS, Эльбрус)
Альт Сервер 10, Альт Рабочая станция 10, Альт Образование 10 (x86, x64, ARM64, Эльбрус)
Альт СП релиз 10 Сервер, Альт СП релиз 10 Рабочая станция (x64, ARM64)
ROSA Enterprise Desktop (RED X4) (x86, x64)
ROSA Enterprise Linux Desktop, Enterprise Linux Server (x64)
РОСА «КОБАЛЬТ», РОСА «НИКЕЛЬ» (x64)
FreeBSD 12/13, pfSense 2.x (x86, x64)
AIX 7 (POWER)
Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14/10.15/11/12/13/14 (x64, ARM64)

Solaris

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

Аврора

ОС «Аврора» 4.0/4.1 (ARMv7)

iOS

Apple iOS (включая iPadOS) 12/13/14/15/16/17 (ARM64)

Android

Android 8/9/10/11/12/13/14 (ARMv7, ARM64, x86, x64)

Виртуальные среды

Программно-аппаратные виртуальные среды:

Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016/2019 (x64)

Microsoft Hyper-V 8/8.1/10 (x64)

Citrix XenServer 7 (x64)

Citrix Hypervisor 8.0/8.1/8.2 (x64)

VMWare WorkStation 11/12/14/15/16 (x86, x64)

VMWare WorkStation Player 12/14/15 (x86, x64)

VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7/7.0 (x64)

Oracle VirtualBox 5.2/6.0/6.1/7.0 (x86, x64)

RHEV 4 (x64)

ROSA Virtualization (x64)

Альт Сервер Виртуализации 9 (x64, ARM64)

ПК «Средства виртуализации «БРЕСТ» в составе ОС «Astra Linux Special Edition»

KVM из состава поддерживаемых ОС (x64), в т.ч. совместно с Libvirt 6/7/8 (x64)

QEMU 4.2/5.2/6.2/7 (x64)

Yandex KVM YC 5.10 (x64)

Yandex QEMU YC 5.0.1 (x64)

Proxmox VE 7 (x64) в режиме администрирования ВМ

Программные виртуальные среды (средства контейнеризации):

Docker Engine 20.10 (x64, ARM)

Kubernetes 1.24, 1.25 (x64)

OpenShift Container Platform 4.10, 4.11 (x64)

Java-машины (для модуля «КриптоПро JavaCSP»)

Java-машины производства Oracle на 32-битной и 64-битной платформе:

«Java™ 8 Runtime Environment, Standard Edition» версии 1.8

Java-машины производства Oracle на 64-битной платформе:

«Java™ 11 Runtime Environment, Standard Edition» версии 11

«Java™ 17 Runtime Environment, Standard Edition» версии 17

Java-машины J9VM производства IBM на 32-битной и 64-битной платформе:

«Java™ 8 Runtime Environment, Standard Edition» версии 1.8

Java-машина J9VM производства IBM на 64-битной платформе:

«IBM® Semeru Runtime™ Certified Edition» версии 11

Java-машины «OpenJDK» версии 8 на 32-битной и 64-битной платформе

Java-машины «OpenJDK» версий 11/17 на 64-битной платформе

Java-машины «Axiom» версий 8/11/17 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. Использование СКЗИ в конкретной программно-аппаратной среде ограничивается лицензией.
4. 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).

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 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 с использованием алгоритмов п.п. 3.3.–3.5. реализована в соответствии с методическими рекомендациями и рекомендациями по стандартизации, разработанными Техническим комитетом по стандартизации «Криптографическая защита информации» (ТК 26):

– 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)»;

– Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»;

– Р 1323565.1.030-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)».

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 3.1.

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

Носители/ОС	**Windows**	**Linux**	**FreeBSD**	**Solaris**	**AIX**	**Mac OS X**	**Apple iOS**	**Android**	**Аврора**
Функциональные ключевые носители (ФКН) с поддержкой SESPAKE[1]									
Рутокен ЭЦП 2.0 3000 (USB, Type-C, micro)	+	+	+	–	–	+	+	+	+
Рутокен ЭЦП 3.0 (форм-факторы указаны в формуляре на Рутокен ЭЦП 3.0)	+	+	+	–	–	+	+	+	+
InfoCrypt Токен++	+	+	+	–	–	+	–	–	–
СмартПарк Форос 2. Базис	+	+	+	–	–	+	–	–	+
СмартПарк Форос 3. Базис	+	+	+	–	–	+	–	–	–
Функциональные ключевые носители (ФКН) без поддержки SESPAKE[2]									
Aladdin R.D. JaCarta-2 ГОСТ, JaCarta-2 SE, JaCarta-2 PKI/ГОСТ	+	+	–	–	–	+	+	+	+
Aladdin R.D. JaCarta SF/ГОСТ	+	+	–	–	–	+	+	+	–

Носители/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Аврора
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[6]	+	+	+	–	–	+	+	+	–
Рутокен PINPad	+	+	+	–	–	+	–	–	–
Рутокен TLS (исполнение 1)	+	+	–	–	–	+	–	–	–
InfoCrypt VPN-Key-TLS, Токен++ TLS	+	+	+	–	–	+	–	–	–
ESMART Token ГОСТ	+	+	–	–	–	+	–	–	–
MultiSoft «MS_KEY K» — «АНГАРА» (ESMART), исполнения 8.1.1, 8.2.1, 8.2.3	+	+	+	–	–	+	–	–	–
КриптоПро Cloud CSP (облачный токен)[3]	+	+	+	–	–	+	–	–	–
ПАКМ «КриптоПро HSM» версия 2.0 R3[4]	+	+	+	+	+	+	–	–	–
Пассивные ключевые носители[5]									
ГМД 3,5", USB-флэш-накопители	+	+	+	+	–	+	–	–	–
Gemalto MPCOS (Optelio, Native)	+	+	+	–	–	+	–	–	–
SafeNet eToken	+	–	–	–	–	–	–	–	–
Смарт-карты Aladdin R.D. JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO	+	+	+	–	–	+	+	+	+
USB-токены Aladdin R.D. JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT	+	+	+	–	–	+	–	+	+
USB-токены Рутокен Lite, Рутокен S, Рутокен КП, смарт-карты Рутокен Lite SC	+	+	+	–	–	+	–	+	+
Рутокен Lite microSD	–	–	–	–	–	–	–	+	–
eDoc (УЛГ)	+	+	+	–	–	+	–	–	–
Novacard	+	+	+	–	–	+	–	–	–
ОСКАР, Форос, Форос 2, Форос 3, R301 Форос, ПЭК-М	+	+	+	–	–	+	+	–	+

Носители/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Аврора
InfoCrypt Токен++ Lite	+	+	+	–	–	+	–	–	–
MorphoKST	+	+	+	–	–	+	–	–	–
Multisoft MS_Key K	+	+	+	–	–	+	–	–	+
ESMART Token	+	+	–	–	–	+	–	–	–
Alioth INPASPOT, SCOne	+	+	+	–	–	+	–	–	–
Rosan	+	+	+	–	–	+	–	–	–
Dallas Touch Memory (iButton) DS199x	+	+	–	–	–	–	–	–	–
USB-флэш-накопитель «Аметист»	+	+	–	–	–	+	–	–	–
Реестр[7]	+	–	–	–	–	–	–	–	–
Раздел HDD/SSD ПЭВМ / устройство Apple iOS / устройство Android / устройство Аврора[7]	+	+	+	+	+	+	+	+	+

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. Необходимо наличие положительного заключения ФСБ России.

4. СКЗИ возможно использовать в качестве клиентского компонента ПАКМ «КриптоПро HSM» версия 2.0 R3.
В случае приобретения экспортной лицензии на СКЗИ «КриптоПро CSP» при необходимости использования ключевого носителя лицензия на ПАКМ «КриптоПро HSM» также должна быть экспортной.
При использовании ключевого носителя ПАКМ «КриптоПро HSM» необходимо выполнять требования, изложенные в документации на данный ПАКМ.

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

6. В качестве пассивного хранилища ключевой информации с передачей данных по бесконтактному интерфейсу допускается использование только Рутокен ЭЦП Bluetooth (при наличии заключения ФСБ России).

7. Хранение закрытых ключей на несъемных носителях (в реестре ОС Windows, в разделе HDD/SSD ПЭВМ, на мобильных устройствах с ОС Apple iOS/Android/Аврора и т.п.) допускается только при условии распространения на носитель требований по обращению с ключевыми носителями (раздел 3 «ЖТЯИ.00101-03 95 01. Правила пользования»).

8. Использование других носителей — только по согласованию с ФСБ России.

9. Описание типов носителей, технологий работы с ключами и правила обеспечения безопасности при работе с ними приведены в разделе 3.3 документа «ЖТЯИ.00101-03 95 01. Правила пользования».

3.11. Формирование закрытых ключей (ключей ЭП) 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	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Аврора
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-АМДЗ» ТУ 4012-006-11443195-2005, ТУ 4012-054-11443195-2013, ТУ 26.20.40.140-108-37222406-2022	+	+	–	–	–	–	–	–	–
Раздел HDD/SSD ПЭВМ, реестр	+	+	+	+	+	+	–	–	–

Считыватели/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Аврора
Устройство Apple iOS	–	–	–	–	–	–	+	–	–
Устройство Android	–	–	–	–	–	–	–	+	–
Устройство Аврора	–	–	–	–	–	–	–	–	+

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 3.3.

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

ДСЧ/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Аврора
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 4012-054-11443195-2013, ТУ 26.20.40.140-108-37222406-2022	+	+	–	–	–	–	–	–	–
Физический ДСЧ в составе АПМДЗ «КРИПТОН-ЗАМОК/У» (М-526Б) КБДЖ.468243.067 ТУ, АПМДЗ «КРИПТОН-ЗАМОК/Е» (М-526Е1) КБДЖ.468243.090 ТУ, АПМДЗ-УМ2 исполнение 1 (М-526Е3) КБДЖ.468243.183-01 ТУ	+	+	–	–	–	–	–	–	–
Физический ДСЧ в составе АПМДЗ «Максим-М1»	+	+	–	–	–	–	–	–	–
Физический ДСЧ «КРИПТОН USB-ДСЧ»	+	+	–	–	–	–	–	–	–

ДСЧ/ОС	Windows	Linux	FreeBSD	Solaris	AIX	Mac OS X	Apple iOS	Android	Аврора
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 СКЗИ «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base)

Программно-аппаратные модули[i]	
1	КриптоПро CSP. Базовые модули[1]
2	КриптоПро IPsec[2]
3	КриптоПро JavaCSP[3]
4	КриптоПро JavaTLS[4]
5	КриптоПро CSP Lite
6	Модуль Check[ii]
7	КриптоПро Мастер[5]
8	КриптоПро PKI SDK[6]
Эксплуатационная документация[iii]	
1	ЖТЯИ.00101-03 30 01. КриптоПро CSP. Формуляр
2	ЖТЯИ.00101-03 90 01. КриптоПро CSP. Описание реализации
3	ЖТЯИ.00101-03 90 02. КриптоПро CSP. Описание реализации IPsec
4	ЖТЯИ.00101-03 91 02. КриптоПро CSP. Руководство администратора безопасности. Windows
5	ЖТЯИ.00101-03 91 03. КриптоПро CSP. Руководство администратора безопасности. Linux
6	ЖТЯИ.00101-03 91 04. КриптоПро CSP. Руководство администратора безопасности. FreeBSD
7	ЖТЯИ.00101-03 91 05. КриптоПро CSP. Руководство администратора безопасности. Solaris
8	ЖТЯИ.00101-03 91 06. КриптоПро CSP. Руководство администратора безопасности. AIX
9	ЖТЯИ.00101-03 91 07. КриптоПро CSP. Руководство администратора безопасности. Mac OS
10	ЖТЯИ.00101-03 91 08. КриптоПро CSP. Руководство администратора безопасности. iOS
11	ЖТЯИ.00101-03 91 09. КриптоПро CSP. Руководство администратора безопасности. Виртуальные среды
12	ЖТЯИ.00101-03 91 10. КриптоПро CSP. Руководство администратора безопасности. Аврора
13	ЖТЯИ.00101-03 91 11. КриптоПро CSP. Руководство администратора безопасности. Android
14	ЖТЯИ.00101-03 91 12. КриптоПро CSP. Руководство администратора безопасности. JavaCSP и JavaTLS
15	ЖТЯИ.00101-03 92 01. КриптоПро CSP. Инструкция по использованию. Windows
16	ЖТЯИ.00101-03 92 02. КриптоПро CSP. Инструкция по использованию. iOS
17	ЖТЯИ.00101-03 92 03. КриптоПро CSP. Инструкция по использованию. Android
18	ЖТЯИ.00101-03 92 04. КриптоПро CSP. Инструкция по использованию. JavaCSP

19	ЖТЯИ.00101-03 92 05. КриптоПро CSP. Инструкция по использованию. JavaTLS
20	ЖТЯИ.00101-03 92 06. КриптоПро CSP. Инструкция по использованию. Инструменты КриптоПро
21	ЖТЯИ.00101-03 92 07. КриптоПро CSP. Инструкция по использованию. Аврора
22	ЖТЯИ.00101-03 93 01. КриптоПро CSP. Приложение командной строки cryptcp[7]
23	ЖТЯИ.00101-03 93 02. КриптоПро CSP. Приложение командной строки для работы с сертификатами
24	ЖТЯИ.00101-03 93 03. КриптоПро CSP. Приложения командной строки для создания TLS-туннеля
25	ЖТЯИ.00101-03 93 04. КриптоПро CSP. Приложение командной строки csptest
26	ЖТЯИ.00101-03 94 01. КриптоПро CSP. АРМ выработки внешней гаммы
27	ЖТЯИ.00101-03 95 01. КриптоПро CSP. Правила пользования
28	ЖТЯИ.00101-03 96 01. КриптоПро CSP. Руководство программиста
29	ЖТЯИ.00101-03 96 02. КриптоПро CSP. Руководство программиста. JavaCSP
30	ЖТЯИ.00101-03 96 03. КриптоПро CSP. Руководство программиста. JavaTLS
31	ЖТЯИ.00101-03 96 04. КриптоПро CSP. Руководство программиста. Check
32	Сертификат СКЗИ (копия, опционально)

Примечание.
i. Программное обеспечение и документация в электронном виде в формате PDF поставляется на компакт-диске (CD-ROM, CD-RW, CD-R, DVD, DVD-R) единым дистрибутивом, формуляр и заверенная копия сертификата — в печатном виде.
ii. Модуль представляет собой набор самостоятельных (не требующих установки базовых модулей КриптоПро CSP) программных компонентов, выполняющих функции расчета хэш-значения и проверки ЭП и предназначенных для эксплуатации под управлением ОС СН Astra Linux SE.
iii. Комплект документации предназначен для администраторов безопасности, разработчиков прикладного программного обеспечения и пользователей СКЗИ.

Порядок лицензирования СКЗИ.

1. Для использования СКЗИ «КриптоПро CSP» необходимо приобретать "Лицензию на право использования СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте/на сервере" или "Лицензию на обновление СКЗИ «КриптоПро CSP» до версии 5.0 на одном рабочем месте/на сервере".

Для использования протокола TLS в среде **серверных ОС, отличных от Windows**, необходимо приобретать "Лицензию на право использования СКЗИ «КриптоПро CSP» версии 5.0 для TLS-сервера". 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 для TLS-аутентификации на одном рабочем месте". Указанные лицензии не входят в комплект поставки и поставляются отдельно по согласованию с Заказчиком.

2. Для использования «КриптоПро IPsec» в среде **серверных ОС** необходимо приобретать "Лицензию на право использования «КриптоПро IPsec» из состава СКЗИ «КриптоПро CSP» версии 5.0 на сервере". Указанная лицензия не входит в комплект поставки и поставляется отдельно по согласованию с Заказчиком.

3. 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».

4. Для использования «КриптоПро JavaTLS» необходимо приобретать "Лицензию на право использования «КриптоПро JavaTLS» на сервере". Указанная лицензия не входит в комплект поставки и поставляется отдельно по согласованию с Заказчиком. В клиентских ОС отдельная лицензия на использование «КриптоПро JavaTLS» не требуется при условии наличия клиентской лицензии на «КриптоПро CSP».

5. КриптоПро Мастер представляет собой модуль управления установкой СКЗИ «КриптоПро CSP». Для использования КриптоПро Мастер необходимо приобретать "Лицензию на право использования ПО «Модуль управления установкой СКЗИ КриптоПро Мастер» из состава СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте/на сервере". Указанная лицензия не входит в комплект поставки и поставляется отдельно по согласованию с Заказчиком.

6. Для использования ПО «КриптоПро OCSP Client», входящего в состав «КриптоПро PKI SDK», необходимо приобретать "Лицензию на право использования ПО «КриптоПро OCSP Client» из состава СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте". Для использования ПО «КриптоПро TSP Client», входящего в состав «КриптоПро PKI SDK», необходимо приобретать "Лицензию на право использования ПО «КриптоПро TSP Client» из состава СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте". Для использования ПО «КриптоПро Revocation Provider», входящего в состав «КриптоПро PKI SDK», в среде ОС семейства Windows, необходимо приобретать "Лицензию на право использования ПО «КриптоПро Revocation Provider» из состава СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте". Данные лицензии поставляются отдельно по согласованию с Заказчиком.

7. Для использования приложения командной строки cryptcp в среде **ОС Windows** необходимо приобретать "Лицензию на право использования «Приложения командной строки cryptcp»". Указанная лицензия не входит в комплект поставки и поставляется отдельно по согласованию с Заказчиком.

Подробнее порядок получения прав на использование компонентов и модулей СКЗИ «КриптоПро CSP» описан в разделе 2 документа ЖТЯИ.00101-03 90 01. Описание реализации.

5 МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ

Изделие «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) (ЖТЯИ.00101-03) укомплектовано модулем доверенной загрузки (средством защиты информации от несанкционированного доступа).

Наименование изделия	Серийный номер, дата выпуска, ТУ (при наличии)

М.П. _____ / _____ /

"__"_____ 20 __ г.

6 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) (ЖТЯИ.00101-03)

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 «КриптоПро CSP» версия 5.0 R3 KC1 (исполнение 1-Base) (ЖТЯИ.00101-03)

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 требованиями и 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 и рекомендаций 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