АО «СИГНАЛ-КОМ»

УТВЕРЖДЕН
ШКНР.00064-01 30 01-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«Крипто-КОМ 3.5»

ФОРМУЛЯР
для вариантов исполнения 1, 2

ШКНР.00064-01 30 01
Листов 23

2023

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1. Перед эксплуатацией средства криптографической защиты информации (СКЗИ) «Крипто-КОМ 3.5» (далее – изделие) необходимо внимательно ознакомиться с формуляром и документами по эксплуатации СКЗИ, приведенными в разделе 3 «Комплектность».

1.2. Сотрудники допускаются к работе только после изучения документации (см. раздел 2 «Общие сведения об изделии»).

1.3. Формуляр входит в комплект поставки изделия.

1.4. Все записи в формуляре производятся отчетливо и аккуратно. Незаверенные исправления не допускаются.

2. ОБЩИЕ СВЕДЕНИЯ ОБ ИЗДЕЛИИ

2.1. Изделие: СКЗИ «Крипто-КОМ 3.5» ШКНР.00064-01.

2.2. Изготовитель: АО «СИГНАЛ-КОМ».

2.3. СКЗИ «Крипто-КОМ 3.5» предназначено для криптографической защиты открытой информации в информационных системах общего пользования (формирование/проверка электронной подписи) и обеспечения криптографической защиты конфиденциальной информации, не содержащей сведений, составляющих государственной тайны. Допускается использование СКЗИ «Крипто-КОМ 3.5» для криптографической защиты персональных данных.

2.4. СКЗИ «Крипто-КОМ 3.5» вариант исполнения 1 поставляется для следующих операционных систем (при условии их поддержки производителем):

- Windows Server 2016/2019/2022 (x86_64);
- Windows 10/11 (x86, x86_64);
- Oracle Linux 7/8 (x86_64);
- Red Hat Enterprise Linux 6/7/8 (x86, x86_64);
- CentOS 7 (x86, x86_64, ARM);
- SUSE Linux Enterprise Server 12/15 (x86_64);
- OpenMandriva Lx 5 (x86_64, ARM);
- openSUSE 15 (x86_64, ARM);
- Ubuntu 20/22 (x86_64, ARM);
- Debian 10/11/12 (x86, x86_64, ARM);
- Fedora 37/38 (x86, x86_64, ARM);
- Linux Mint 20/21 (x86, x86_64, ARM);
- Astra Linux Common Edition 2 (x86_64);
- Astra Linux Special Edition 1.6/1.7 (x86_64);
- ROSA Fresh/Enterprise Linux Desktop/Enterprise Linux Server (x86, x86_64);
- РОСА «КОБАЛЬТ» (x86_64);
- Альт Линукс 8/9 (x86, x86_64);
- РЕД ОС 7 (x86_64);
- macOS 11/12/13/14 (x86_64, ARM);
- iOS/iPadOS 12/13/14/15 (ARM).

Примечание. В скобках указаны аппаратные платформы.

2.5. СКЗИ «Крипто-КОМ 3.5» (вариант исполнения 2) поставляется для следующих операционных систем:

- Windows Server 2016/2019/2022 (x86_64);
- Windows 10/11 (x86, x86_64);
- Oracle Linux 7/8 (x86_64);
- Red Hat Enterprise Linux 6/7/8 (x86, x86_64);
- CentOS 7 (x86, x86_64);
- SUSE Linux Enterprise Server 12/15 (x86_64);
- OpenMandriva Lx 5 (x86_64);
- openSUSE 15 (x86_64);
- Ubuntu 20/22 (x86_64);
- Debian 10/11/12 (x86, x86_64);
- Fedora 37/38 (x86, x86_64);
- Linux Mint 20/21 (x86, x86_64);
- Astra Linux Common Edition 2 (x86_64);
- Astra Linux Special Edition 1.6/1.7 (x86_64);
- ROSA Fresh/Enterprise Linux Desktop/Enterprise Linux Server (x86, x86_64);
- РОСА «КОБАЛЬТ» (x86_64);
- Альт Линукс 8/9 (x86, x86_64);
- РЕД ОС 7 (x86_64).

Примечание. В скобках указаны аппаратные платформы.

2.6. СКЗИ «Крипто-КОМ 3.5» (вариант исполнения 1) может использоваться на перечисленных выше операционных системах, выполняемых в среде следующих виртуальных машин (гипервизоров):

- Microsoft Hyper-V в составе Windows Server 2016/2019;
- Microsoft Hyper-V в составе Windows 10/11;
- Citrix XenServer 8.2;
- VMWare Workstation 17;
- VMWare Workstation Player 17;
- VMWare vSphere ESXi/Hypervisor 7.0/8.0;
- Oracle VM VirtualBox 6.1/7.0;
- RHEV 4.3/4.4;
- ROSA Virtualization 2;
- Альт Сервер Виртуализации 9.

2.7. Порядок эксплуатации СКЗИ «Крипто-КОМ 3.5» должен проводиться в соответствии с разделом V «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств зашиты информации (Положение ПКЗ-2005)».

2.8. При встраивании СКЗИ «Крипто-КОМ 3.5» в прикладные системы необходимо проводить оценку влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к СКЗИ требований в следующих случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- при организации криптографической защиты информации 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 ФСБ России.

В рамках работ по оценке влияния необходимо проводить в том числе следующие исследования: проверку выполнения требований и рекомендаций, указанных в документации на СКЗИ; проверку невлияния на инженерно-криптографические качества СКЗИ; проверку выполнения требований контроля целостности; анализ документации на прикладное программное обеспечение, используемое с СКЗИ; проверку соответствия пунктам 8, 9 «Требований к средствам электронной подписи»; проверку программного обеспечения BIOS ПЭВМ, на которой функционирует СКЗИ; и др.

Подтверждение соответствия сред функционирования, в составе которых используется СКЗИ «Message-PRO 5.0» (варианты исполнения 1, 2) требованиям к средствам ЭП, установленным частями 2 и 3 статьи 12 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», а также пунктами 8 и 9 «Требований к средствам электронной подписи» (приложение № 1 к приказу ФСБ России от 27.12.2011 № 796), должно проводиться в случае их использования для создания и проверки квалифицированных ЭП, создания ключей квалифицированных ЭП и ключей их проверки.

Указанное подтверждение соответствия необходимо проводить по ТЗ, согласованному с ФСБ России.

В случае использования СКЗИ «Message-PRO 5.0» (варианты исполнения 1, 2) для создания и проверки неквалифицированной ЭП, а также для создания ключей неквалифицированной ЭП, указанная проверка не требуется, но рекомендуется.

При использовании СКЗИ «Message-PRO 5.0» (варианты исполнения 1, 2) для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе, требования к средствам ЭП, установленные частями 2 и 3 статьи 12 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», а также пунктами 8 и 9 «Требований к средствам электронной подписи» (приложение № 1 к приказу ФСБ России от 27.12.2011 № 796), не применяются.

2.9. СКЗИ «Крипто-КОМ 3.5» состоит из следующих модулей:

Таблица 1

Код	Обозначение	Наименование
А1	ШКНР.00064-01 94 01	СКЗИ «Крипто-КОМ 3.5». Библиотека криптографических преобразований для вариантов исполнения 1, 2 (для разработчика).
А2	ШКНР.00064-01 94 02	СКЗИ «Крипто-КОМ 3.5». Библиотека криптографических преобразований для вариантов исполнения 1, 2 (для конечного пользователя).
А3	ШКНР.00064-01 94 05	СКЗИ «Крипто-КОМ 3.5». Программное обеспечение контроля целостности.
А4	ШКНР.00064-01 94 06	СКЗИ «Крипто-КОМ 3.5». Утилита удаления файлов.
А5	ШКНР.00064-01 94 07	СКЗИ «Крипто-КОМ 3.5». Программное обеспечение регламентного контроля ДСЧ.
А6[1]		Программно-аппаратные модули доверенной загрузки ЭВМ: - ПАК «Соболь». Версия 3.0 (версии кода расширения BIOS 1.0.280, 1.0.991); - АПМДЗ «КРИПТОН-ЗАМОК/К» (М-526А); - АПМДЗ «КРИПТОН-ЗАМОК/У» (М-526Б). Другие сертифицированные ФСБ России модули доверенной загрузки ЭВМ могут использоваться по согласованию с ФСБРоссии.

[1] АПМДЗ входят в состав СКЗИ, но не входят в комплект поставки СКЗИ.

2.10. Комплект документации СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) включает следующие документы:

Таблица 2

Код	Обозначение	Наименование
Д1	ШКНР.00064-01 30 01	СКЗИ «Крипто-КОМ 3.5». Формуляр.
Д2	ШКНР.00064-01 31 01	СКЗИ «Крипто-КОМ 3.5». Подсистема управления ключевой информацией. Общее описание.
Д3	ШКНР.00064-01 33 01	СКЗИ «Крипто-КОМ 3.5». Руководство программиста.
Д4	ШКНР.00064-01 90 02	СКЗИ «Крипто-КОМ 3.5». Правила пользования.
Д5	ШКНР.00064-01 34 01	СКЗИ «Крипто-КОМ 3.5». Программное обеспечение контроля целостности. Руководство оператора.
Д6	ШКНР.00064-01 34 02	СКЗИ «Крипто-КОМ 3.5». Утилита удаления файлов. Руководство оператора.
Д7	ШКНР.00064-01 34 03	СКЗИ «Крипто-КОМ 3.5». Программное обеспечение регламентного контроля ДСЧ. Руководство оператора.
КС		Сертификат соответствия ФСБ России (копия)

3. КОМПЛЕКТНОСТЬ

3.1. СКЗИ «Крипто-КОМ 3.5» поставляется в следующих вариантах исполнения:

Таблица 3

Вариант исполнения	Операционные системы	Аппаратная платформа	Комплектация 1 (для разработчика)	Комплектация 2 (для конечного пользователя)	Уровень защиты
1	Windows Server Windows	x86/x86_64	A1, A3, A4, A5 Д1, Д2, Д3, Д4, Д5, Д6, Д7, КС	A2, A3, A4, A5 Д1, Д2, Д4, Д5, Д6, Д7, КС	КС1
1	Oracle Linux Red Hat Enterprise Linux CentOS SUSE Linux Enterprise Server OpenMandriva Lx openSUSE Ubuntu Debian Fedora Linux Mint Astra Linux ROSA РОСА Альт Линукс РЕД ОС	x86/x86_64/ ARM	«	«	«
1	macOS	x86_64/ARM	«	«	«
1	iOS/iPadOS	ARM	«	«	«
2	Windows Server Windows	x86/x86_64	A1, A3, A4, A5, A6 Д1, Д2, Д3, Д4, Д5, Д6, Д7, КС	A2, A3, A4, A5, A6 Д1, Д2, Д4, Д5, Д6, Д7, КС	КС2
2	Oracle Linux Red Hat Enterprise Linux CentOS SUSE Linux Enterprise Server OpenMandriva Lx openSUSE Ubuntu Debian Fedora Linux Mint Astra Linux ROSA РОСА Альт Линукс РЕД ОС	x86/x86_64/ ARM	«	«	«

Примечания.

1. Расшифровка кодов A1, A2, A3, A4, A5, A6, Д1, Д2, Д3, Д4, Д5, Д6, Д7, КС приведена в таблицах 1, 2.
2. В комплектации 2 (для конечного пользователя) СКЗИ «Крипто-КОМ 3.5» поставляется в составе приложений, библиотек более высокого уровня и т.п.
3. Документация поставляется в электронном виде в формате PDF (Adobe Acrobat). Формуляр и копия сертификата поставляются в печатном виде.

4. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ

4.1. СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) обеспечивает выполнение следующих функций:

- генерация случайных последовательностей с использованием программного датчика случайных чисел, основанного на использовании алгоритма ГОСТ Р 34.12-2015 (алгоритм блочного шифрования «Кузнечик») в режиме CTR-ACPKM согласно Рекомендациям по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»;
- создание ключей ЭП и ключей проверки ЭП в соответствии с ГОСТ Р 34.10 2012 (256 и 512 бит);
- хэширование данных в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 (256 и 512 бит);
- создание ЭП в соответствии с алгоритмом ГОСТ Р 34.10-2012 (256 и 512 бит);
- проверка ЭП в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10 2012 (256 и 512 бит);
- создание ключей шифрования для алгоритмов ГОСТ 28147-89, ГОСТ Р 34.12 2015 (алгоритмы блочного шифрования «Магма», «Кузнечик»);
- зашифрование и расшифрование данных в соответствии с ГОСТ 28147-89, ГОСТ Р 34.12-2015 (алгоритмы блочного шифрования «Магма», «Кузнечик»), ГОСТ Р 34.13-2015, а также Рекомендациями по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» и Р 1323565.1.026 2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование»;
- вычисление имитовставки в соответствии с ГОСТ 28147-89, ГОСТ Р 34.12 2015 (алгоритмы блочного шифрования «Магма», «Кузнечик»), ГОСТ Р 34.13-2015, а также Рекомендациями по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»;
- вычисление HMAC по алгоритмам HMAC_GOSTR3411, HMAC_GOSTR3411_2012_256 и HMAC_GOSTR3411_2012_512 в соответствии с RFC 4357 и Рекомендациями по стандартизации Р 50.1.113 2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- экспорт и импорт ключей в соответствии с RFC 4357, Рекомендациями по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» и Р 50.1.113 2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- согласование ключей по алгоритмам VKO_GOSTR3410_2012_256 и VKO_GOSTR3410_2012_512 в соответствии с Рекомендациями по стандартизации Р 50.1.113 2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- диверсификация ключей по алгоритмам KDF_GOSTR3411_2012_256 и KDF_TREE_GOSTR3411_2012_256 в соответствии с Рекомендациями по стандартизации Р 50.1.113 2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- псевдослучайные функции протоколов TLS и IPsec в соответствии с п.4.2 Рекомендаций по стандартизации Р 50.1.113 2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»; указанные псевдослучайные функции предназначены для использования в ППО, реализующем протоколы TLS и IPsec;
- выработка ключей экспорта KEG в соответствии с Рекомендациями по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»;

- выработка ключей защиты записей TLSTREE в соответствии с Рекомендациями по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».

4.2. Функции СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), перечисленные в п.4.1, реализованы с использованием следующих криптографических алгоритмов и механизмов:

- генерация случайных последовательностей с использованием программного датчика случайных чисел, основанного на использовании алгоритма ГОСТ Р 34.12-2015 (алгоритм блочного шифрования «Кузнечик») в режиме CTR-ACPKM согласно Рекомендациям по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»;
- создание ключей ЭП и ключей проверки ЭП в соответствии с ГОСТ Р 34.10-2012 (256 и 512 бит);
- хэширование данных в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 (256 и 512 бит);
- создание ЭП в соответствии с алгоритмом ГОСТ Р 34.10-2012 (256 и 512 бит);
- проверка ЭП в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (256 и 512 бит);
- создание ключей шифрования для алгоритмов ГОСТ 28147-89, ГОСТ Р 34.12-2015 (алгоритмы блочного шифрования «Магма», «Кузнечик»);
- зашифрование и расшифрование данных в соответствии с ГОСТ 28147-89, ГОСТ Р 34.12-2015 (алгоритмы блочного шифрования «Магма», «Кузнечик»), ГОСТ Р 34.13-2015, а также Рекомендациями по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» и Р 1323565.1.026-2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование»;
- вычисление имитовставки в соответствии с ГОСТ 28147-89, ГОСТ Р 34.12-2015 (алгоритмы блочного шифрования «Магма», «Кузнечик»), ГОСТ Р 34.13-2015, а также Рекомендациями по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»;
- вычисление HMAC по алгоритмам HMAC_GOSTR3411, HMAC_GOSTR3411_2012_256 и HMAC_GOSTR3411_2012_512 в соответствии с RFC 4357 и Рекомендациями по стандартизации Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- алгоритмы экспорта и импорта ключей в соответствии с RFC 4357, Рекомендациями по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» и Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- согласование ключей по алгоритмам VKO_GOSTR3410_2012_256 и VKO_GOSTR3410_2012_512 в соответствии с Рекомендациями по стандартизации Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- алгоритмы диверсификации KDF_GOSTR3411_2012_256 и KDF_TREE_GOSTR3411_2012_256 в соответствии с Рекомендациями по стандартизации Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- псевдослучайные функции протоколов TLS и IPsec в соответствии с п.4.2 Рекомендаций по стандартизации Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- алгоритм выработки ключей экспорта KEG в соответствии с Рекомендациями по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая

защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»;

- алгоритм выработки ключей защиты записей TLSTREE в соответствии с Рекомендациями по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».

4.3. Инициализирующие последовательности для ПДСЧ, входящего в состав СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), вырабатываются на местах эксплуатации:

- с использованием БДСЧ, входящего в состав СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2);
- с использованием ФДСЧ, входящих в состав сертифицированных МДЗ (АПМДЗ), используемых совместно с СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2);
- с использованием ФДСЧ, входящих в состав сертифицированных криптографических устройств соответствующего класса, используемых совместно с СКЗИ «Крипто КОМ 3.5» (варианты исполнения 1, 2) согласно пп. 4.6, 4.7.

4.4. Для хранения ключевой информации могут быть использованы следующие типы ключевых носителей:

Таблица 4

Тип ключевого носителя	Варианты исполнения
Накопители на гибком магнитном диске (НГМД)	1, 2
Разделы накопителей на жестком магнитном диске (НЖМД)	1, 2
Сменные носители с интерфейсом USB	1, 2
Электронные ключи с интерфейсом USB (eToken, JaCarta, Рутокен и др.)	1, 2
Криптографические устройства, перечисленные в пп.4.6, 4.7	1, 2
Карты флэш-памяти	1, 2
Реестр Windows	1, 2

Примечание. Хранение закрытых ключей в разделе жесткого диска и в реестре ОС Windows допускается только при условии распространения на ЭВМ (или съемный НЖМД ЭВМ) требований по обращению с ключевыми носителями.

4.5. СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) может обращаться через интерфейс PKCS#11 к криптографическим устройствам, реализующим функции генерации ключей, создания ЭП, проверки ЭП, хэширования, шифрования, ключевого обмена, генерации случайных последовательностей и др. Данные устройства могут также использоваться для хранения закрытых ключей в неэкспортируемом виде, исключающем возможность их считывания во внешнюю память или копирование на другой носитель. СКЗИ «Крипто-КОМ 3.5» может использовать механизмы (генерация ключей, создание ЭП, проверка ЭП, хэширование, шифрование, ключевой обмен, генерация случайных последовательностей и др.), реализованные в криптографических устройствах, совместно с программной реализацией криптографических алгоритмов СКЗИ «Крипто-КОМ 3.5» (хэширование, шифрование и др.).

4.6. Перечень криптографических устройств с интерфейсом PKCS #11, поддерживаемых СКЗИ «Крипто-КОМ 3.5» (вариант исполнения 1), включает[1]:

- СКЗИ «SmartToken-PRO»;
- СКЗИ «Рутокен ЭЦП 2.0 2100» (сертификат соответствия № СФ/124-4248 от 10.04.2022);
- СКЗИ «Рутокен ЭЦП 2.0 3000» (сертификат соответствия № СФ/124-4077 от 17.06.2021);

[1] Криптографические устройства должны иметь действующий сертификат соответствия (заключение о соответствии) ФСБ России.

- СКЗИ «Рутокен ЭЦП 2.0 3000 micro» (сертификат соответствия № СФ/124-4078 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 3000 Type-C» (сертификат соответствия № СФ/124-4079 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 Flash» (сертификат соответствия № СФ/121-4075 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 micro» (сертификат соответствия № СФ/124-3991 от 11.12.2020);
- СКЗИ «Рутокен ЭЦП 2.0» (сертификат соответствия № СФ/124-3990 от 02.12.2020);
- СКЗИ «Рутокен ЭЦП 2.0 Исполнение А» (сертификат соответствия № СФ/121-4072 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 Touch» (сертификат соответствия № СФ/124-3993 от 11.12.2020);
- СКЗИ «Рутокен ЭЦП 3.0» (варианты исполнения 1, 2) (сертификат соответствия № СФ/124-4307 от 11.08.2022);
- СКЗИ «Рутокен ЭЦП 3.0» (вариант исполнения 5) (сертификат соответствия № СФ/124-4398 от 01.12.2022);
- СКЗИ «MS_KEY K» – «АНГАРА» (вариант исполнения 8.1.1) (сертификат соответствия № СФ/124-4311 от 12.08.2022);
- СКЗИ «ESMART Token ГОСТ на базе отечественной микросхемы MIK51SC72DV6» (варианты исполнения 1, 2, 3) (сертификат соответствия № СФ/124-4048 от 01.04.2021).

4.7. Перечень криптографических устройств с интерфейсом PKCS #11, поддерживаемых СКЗИ «Крипто-КОМ 3.5» (вариант исполнения 2), включает[1]:

- СКЗИ «Рутокен ЭЦП 2.0 2100» (сертификат соответствия № СФ/124-4248 от 10.04.2022);
- СКЗИ «Рутокен ЭЦП 2.0 3000» (сертификат соответствия № СФ/124-4077 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 3000 micro» (сертификат соответствия № СФ/124-4078 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 3000 Type-C» (сертификат соответствия № СФ/124-4079 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 Flash» (сертификат соответствия № СФ/121-4075 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 micro» (сертификат соответствия № СФ/124-3991 от 11.12.2020);
- СКЗИ «Рутокен ЭЦП 2.0» (сертификат соответствия № СФ/124-3990 от 02.12.2020);
- СКЗИ «Рутокен ЭЦП 2.0 Исполнение А» (сертификат соответствия № СФ/121-4072 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 Touch» (сертификат соответствия № СФ/124-3993 от 11.12.2020);
- СКЗИ «Рутокен ЭЦП 3.0» (варианты исполнения 1, 2) (сертификат соответствия № СФ/124-4307 от 11.08.2022);
- СКЗИ «Рутокен ЭЦП 3.0» (вариант исполнения 5) (сертификат соответствия № СФ/124-4398 от 01.12.2022);
- СКЗИ «MS_KEY K» – «АНГАРА» (вариант исполнения 8.1.1) (сертификат соответствия № СФ/124-4311 от 12.08.2022).;
- СКЗИ «ESMART Token ГОСТ на базе отечественной микросхемы MIK51SC72DV6» (варианты исполнения 2, 3) (сертификат соответствия № СФ/124-4048 от 01.04.2021).

4.8. Все остальные носители должны использоваться только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене.

4.9. Контроль целостности программного обеспечения СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) обеспечивается с помощью утилиты контроля целостности из состава СКЗИ или с помощью программно-аппаратных модулей доверенной загрузки, перечисленных в п. 2.9 (Таблица 1). Должен обеспечиваться контроль целостности следующих программных модулей из состава СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2):

- ШКНР.00064-01 94 02 Библиотека криптографических преобразований (для конечного пользователя);
- ШКНР.00064-01 94 05 Программное обеспечение контроля целостности;

[1] Криптографические устройства должны иметь действующий сертификат соответствия (заключение о соответствии) ФСБ России.

- ШКНР.00064-01 94 06 Утилита удаления файлов;
- ШКНР.00064-01 94 07 Программное обеспечение регламентного контроля ДСЧ.

5. ТРЕБОВАНИЯ К ЭКСКПЛУАТАЦИИ СКЗИ

5.1. Средствами СКЗИ не допускается обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

Допускается использование СКЗИ для криптографической защиты персональных данных.

5.2. Ключевая информация является конфиденциальной.

5.3. СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

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

5.5. В случае, если в модели угроз, которым должно противостоять СКЗИ в информационной системе заказчика, признана опасной утечка по техническим каналам, ПЭВМ, на которых устанавливается СКЗИ, 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). Каналы связи ПЭВМ с установленным СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), выходящие за пределы контролируемой зоны, должны быть защищены одним из следующих способов:

- применением волоконно-оптических линий связи;
- применением радиоканалов GSM, GPRS, 3G/4G, Wi-Fi, а также других современных каналов мобильной или беспроводной связи;
- применением сертифицированных СКЗИ для передачи информации по каналам связи.

5.6. Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

6. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие СКЗИ «Крипто-КОМ 3.5» ШКНР.00064-01 соответствует эталону, хранящемуся в АО «СИГНАЛ-КОМ» и признано годным для эксплуатации.

Дата выпуска: "_____"_____ 20____ г.

М.П. _____

(должность)

_____

(подпись)

7. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие СКЗИ «Крипто-КОМ 3.5» ШКНР.00064-01

Вариант исполнения № _____ Комплектация № _____

Операционная система_____

Аппаратная платформа_____

Регистрационный № дистрибутива _____

Вид носителя:

- ☐ DVD-ROM _____ шт.
- ☐ CD-ROM _____ шт.
- ☐

Упаковано в

- ☐ бумажный конверт
- ☐ коробку
- ☐
- ☐ _____

Носители ПО снабжены этикетками, идентифицирующими их принадлежность к изделию.

Дата упаковки: "_____"_____ 20_____ г.

М. П.

Упаковку произвел _____

(подпись)

8. ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)

8.1. Пользователь приобретает изделие СКЗИ «Крипто-КОМ 3.5» и несет ответственность за его использование в соответствии с рекомендациями, изложенными в эксплуатационной документации.

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

8.3. В случае выявления в изделии дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения, 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.

8.4. Гарантийный срок изделия — 12 (двенадцать) месяцев. Гарантийный срок на программно-аппаратный комплекс защиты от НСД определяется их изготовителями.

8.5. Начальной датой исчисления гарантийного срока изделия является дата поставки изделия (см. 8.7).

8.6. Действие гарантийных обязательств прекращается при истечении гарантийного срока.

8.7. Данные о поставке (продаже) изделия:

АО «СИГНАЛ-КОМ»

наименование организации-поставщика (продавца) изделия

Дата поставки: "_____" _____ 20____г.

М.П.

_____

(подпись)

Примечание. При отсутствии данных, приведенных в п. 8.7, датой поставки изделия считается дата выпуска, указанная в разд. 6 «Свидетельство о приемке».

9. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

Россия, г. Москва, 115193, Москва, а/я 6.

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

9.2. Рекламации, связанные с эксплуатацией программно-аппаратного комплекса защиты от НСД и УКЗД, должны направляться их изготовителям.

9.3. При несоответствии поставляемого изделия, его тары, упаковки, консервации, маркировки и комплектности требованиям сопроводительной документации, пользователь обязан направить рекламацию предприятию-изготовителю в течение 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 представлены в Таблица 5

Таблица 5

Должность, фамилия и подпись отв. Лица	
Меры, принятые по рекламации	
Содержание рекламации	
Дата	

10. СВЕДЕНИЯ О ХРАНЕНИИ

Таблица 6

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

11. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

Таблица 7

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

Таблица 8

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

13. ОСОБЫЕ ОТМЕТКИ