

УТВЕРЖДЕН

ЖТЯИ.00101-13 30 01-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

«КриптоПро CSP»

Версия 5.0 R3 KC1

(исполнение 1-КриптоАРМ ГОСТ 3)

Формуляр

ЖТЯИ.00101-13 30 01

С учетом извещения об изменениях ЖТЯИ.00101-13.1-2024

Содержание

1 ОБЩИЕ УКАЗАНИЯ	3
2 ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ	4
3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ	5
4 КОМПЛЕКТНОСТЬ	8
5 МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ	10
6 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ	11
7 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ	12
8 ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)	13
9 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ	14
10 СВЕДЕНИЯ О ХРАНЕНИИ	15
11 СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ	16
12 СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ	17
13 ОСОБЫЕ ОТМЕТКИ	18

1 ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие «Средство криптографической защиты информации «КриптоПро CSP» версия 5.0 R3 KC1 (исполнение 1-КриптоАРМ ГОСТ 3)» ЖТЯИ.00101-13 (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 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.00101-13 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 KC1 (исполнение 1-КриптоАРМ ГОСТ 3) 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 мобильных 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.00101-13 95 01. Правила пользования»).

3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1. СКЗИ «КриптоПро CSP» версия 5.0 R3 KC1 (исполнение 1-КриптоАРМ ГОСТ 3) предназначено для выполнения следующих функций:

- предоставление графического интерфейса:
 - формирования и проверки ЭП файлов;
 - зашифрования и расшифрования данных в файлах;
 - создания и управления ключевой информацией;
 - почтового клиента (формирования и проверки подписи, зашифрования и расшифрования почтовых сообщений);
- установка защищённого соединения по протоколу TLS;
- защита IMAP/POP3 соединений с сервером входящей почты и SMTP соединений с сервером исходящей почты с использованием протокола TLS;
- предоставление программного интерфейса для работы с криптографическими сообщениями формата CMS, S/MIME и объектами инфраструктуры PKI.

3.2. В качестве средства криптографической защиты информации, реализующего функции формирования ключевой информации, хэширования, создания/проверки ЭП, шифрования/расшифрования данных и установки TLS-соединения, используется СКЗИ «КриптоПро CSP» версии 5.0 R3 KC1 (исполнение 1-Base) (ЖТЯИ.00101-03).

3.3. СКЗИ функционирует в следующих программно-аппаратных средах:

Windows

Windows 7*/10 (x86, x64)

Windows 11 (x64)

Windows Server 2019 (x64)

**Версия Embedded/Embedded POSReady*

LSB Linux

Дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360

CentOS 8 (x64)

РЕД ОС 7.3 (x64)

Ubuntu 20.04/22.04 (x64)

Astra Linux Special Edition (x64)

Unix

Альт Рабочая Станция 9 (x64)

Альт Сервер 10, Альт Рабочая Станция 10, Альт Образование 10 (x64)

Альт СП релиз 10 (x64)

РОСА «КОБАЛТ» 7.9 Рабочая станция (x64)

AlterOS 7.5 (x64)

Mac OS X 12/13/14 (x64)

Аврора

ОС «Аврора» 4.0 (ARMv7)

iOS

Apple iOS (включая iPadOS) 15/16/17 (ARM64)

Android

Android 10/11/12/13/14 (ARM64)

Виртуальные среды

Oracle VirtualBox 7.0.6 (x64)

**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 и Linux Server.

3.4. 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».

3.5. 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.

3.6. 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».

3.7. Сетевая аутентификация на базе протокола TLS с использованием алгоритмов п.п. 3.4.–3.6. 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)»;

3.8. Формирование защищенных сообщений в формате CMS с использованием алгоритмов п.п. 3.4.–3.6. 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. Формирование ключей ЭП (закрытых ключей) производится на типы носителей, поддерживаемых СКЗИ «КriptoПро CSP» версии 5.0 R3 KC1 (исполнение 1-Base) (табл. 3.1 Формуляра ЖТЯИ.00101-03 30 01) на операционных системах, приведенных в п. 3.3.

4 КОМПЛЕКТНОСТЬ

Таблица 4.1. Комплектация «КриптоПро CSP» версия 5.0 R3 KC1 (исполнение 1-КриптоАРМ ГОСТ 3)

Наименование		Обозначение
Программно-аппаратные модулиⁱ		
1	КриптоАРМ ГОСТ 3. ПО «КриптоАРМ ГОСТ 3»	См. Примечание, п. 1
2	КриптоПро CSP версии 5.0 R3 KC1 (исполнение 1-Base)	См. Примечание, п. 2
Эксплуатационная документацияⁱⁱ		
1	КриптоПро CSP. КриптоАРМ ГОСТ 3. Формуляр	ЖТЯИ.00101-13 30 01
2	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство администратора. Windows	ЖТЯИ.00101-13 91 01
3	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство администратора. Linux	ЖТЯИ.00101-13 91 02
4	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство администратора. MacOS	ЖТЯИ.00101-13 91 03
5	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство пользователя	ЖТЯИ.00101-13 92 01
6	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство пользователя. iOS	ЖТЯИ.00101-13 92 02
7	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство пользователя. Android	ЖТЯИ.00101-13 92 03
8	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство пользователя. Аврора	ЖТЯИ.00101-13 92 04
9	КриптоПро CSP. КриптоАРМ ГОСТ 3. Правила пользования	ЖТЯИ.00101-13 95 01
10	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство программиста. SDK	ЖТЯИ.00101-13 96 01
11	КриптоПро CSP. КриптоАРМ ГОСТ 3. Руководство программиста. API	ЖТЯИ.00101-13 96 02
12	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) или посредством загрузки через информационно-телекоммуникационные сети (в том числе Интернет), формуляр и заверенная копия сертификата — всегда в печатном виде. Программное обеспечение СКЗИ «КриптоПро CSP» версии 5.0 R3 KC1 (исполнение 1-Base) и документация на указанное СКЗИ поставляются отдельно от остальных компонентов комплектации.

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

**Примечание.**

1. Для использования необходимо приобретать "Лицензию на право использования ПО «КриптоАРМ ГОСТ» версии 3 на одном рабочем месте/на сервере или "Лицензию на право использования ПО «КриптоАРМ ГОСТ» версии 3 Защищенная почта на одном рабочем месте или "Лицензию на обновление до «КриптоАРМ ГОСТ» версии 3 Защищенная почта на одном рабочем месте или "Лицензию на обновление до «КриптоАРМ ГОСТ» версии 3 на одном сервере". Указанные лицензии не входят в комплект поставки и поставляются отдельно по согласованию с Заказчиком.

2. 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.

5 МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ

Изделие «КриптоПро CSP» версия 5.0 R3 KC1 (исполнение 1-КриптоАРМ ГОСТ 3) (ЖТЯИ.00101-13) 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 «КристоПро CSP» версия 5.0 R3 KC1 (исполнение 1-КристоАРМ ГОСТ 3) (ЖТЯИ.00101-13)

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-КриптоАРМ ГОСТ 3) (ЖТЯИ.00101-13)

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