

УТВЕРЖДЕН

ЖТЯИ.00102-12 30 01-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

**«КриптоПро CSP»**

Версия 5.0 R2 KC2

Исполнение 2-КриптоАРМ

Формуляр

ЖТЯИ.00102-12 30 01

## Содержание

1 ОБЩИЕ УКАЗАНИЯ . . . . .	3
2 ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ . . . . .	4
3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ . . . . .	5
4 КОМПЛЕКТНОСТЬ . . . . .	7
5 АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ЗАЩИТЫ ОТ НСД . . . . .	8
6 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ . . . . .	9
7 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ . . . . .	10
8 ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА) . . . . .	11
9 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ . . . . .	12
10 СВЕДЕНИЯ О ХРАНЕНИИ . . . . .	13
11 СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ . . . . .	14
12 СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ . . . . .	15
13 ОСОБЫЕ ОТМЕТКИ . . . . .	16

## 1 ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие «Средство криптографической защиты информации «КriptoПро CSP» версия 5.0 R2 KC2 исполнение 2-КriptoАРМ» ЖТЯИ.00102-12 (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 использовании программного интерфейса СКЗИ «КriptoПро CSP» версия 5.0 R2 KC2 исполнение 2-КriptoАРМ необходимо проводить разработку отдельного СКЗИ на базе «КriptoПро CSP» версия 5.0 R2 KC2 исполнение 2-КriptoАРМ (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)).

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»).

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 «КriptoПро CSP» версия 5.0 R2 KC2 исполнение 2-КriptoАРМ 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. СКЗИ должно использоваться с аппаратно-программным модулем доверенной загрузки (АПМДЗ), сертифицированным ФСБ России.

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

2.9. При эксплуатации СКЗИ необходимо руководствоваться Положением ПКЗ-2005.

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.00102-12 95 01. Правила пользования»).

### 3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1. Исполнение 2-КриптоАРМ СКЗИ КриптоПро CSP версии 5.0 R2 KC2 предназначено для выполнения следующих функций:

- 1) предоставление графического интерфейса для:
  - формирования и проверки ЭП (в формате CMS) файлов;
  - шифрования и расшифрования данных (в формате CMS) в файлах;
  - создания и управления ключевой информацией;
- 2) установка защищённого соединения по протоколу TLS.

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 R2 KC2 Исполнение 2-Base (ЖТЯИ.00102-02).

3.3. СКЗИ функционирует в следующих программно-аппаратных средах:

#### Windows

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

Windows Server 2016/2019 (x64)

#### LSB Linux

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

CentOS 7/8 (x64)

ОСь (OS-RT) (x64)

РЕД ОС 7.1/7.2 (x64)

Ubuntu 19.10/20.04 (x64)

Astra Linux Special Edition, Common Edition (x64)

#### Unix

Альт Рабочая Станция 8/9, Альт Сервер 8/9, Альт 8 СП, Альт Образование 8/9 (x64)

ROSA Enterprise Desktop (RED X4) (x64)

ROSA Enterprise Linux Desktop, Enterprise Linux Server (x64)

РОСА КОБАЛЬТ (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».

При использовании функций шифрования и имитозащиты рекомендуется применять алгоритмы ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) и ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018).

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 1.0, 1.1, 1.2 с использованием алгоритмов п.п. 3.4.–3.6. 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)».

3.8. Формирование ключей ЭП (закрытых ключей) производится на типы носителей, поддерживаемых СКЗИ «КриптоПро CSP» версии 5.0 R2 KC2 Исполнение 2-Base (табл. 3.1 Формуляра ЖТЯИ.00102-02 30 01) на операционных системах, приведенных в п. 3.3.

## 4 КОМПЛЕКТНОСТЬ

Таблица 4.1. Комплектация «КриптоПро CSP» версия 5.0 R2 KC2 исполнение 2-КриптоАРМ

Наименование		Обозначение
1	КриптоПро CSP. КриптоАРМ. ПО «КриптоАРМ ГОСТ».	ЖТЯИ.00102-12 99 01, см. Примечание, п. 1
2	Аппаратно-программный модуль доверенной загрузки (АПМДЗ).	см. Примечание, п. 2
3	КриптоПро CSP. КриптоАРМ. Модуль поддержки КриптоПро OSCP.	ЖТЯИ.00102-12 99 02, см. Примечание, п. 3
4	КриптоПро CSP. КриптоАРМ. Модуль поддержки КриптоПро TSP.	ЖТЯИ.00102-12 99 03, см. Примечание, п. 3
5	КриптоПро CSP. КриптоАРМ. Модуль поддержки формата усовершенствованной ЭП (CAvES)	ЖТЯИ.00102-12 99 04, см. Примечание, п. 3
6	КриптоПро CSP. КриптоАРМ. Формуляр.	ЖТЯИ.00102-12 30 01
7	КриптоПро CSP. КриптоАРМ. Руководство администратора. Windows.	ЖТЯИ.00102-12 91 01
8	КриптоПро CSP. КриптоАРМ. Руководство администратора. Linux.	ЖТЯИ.00102-12 91 02
9	КриптоПро CSP. КриптоАРМ. Руководство пользователя	ЖТЯИ.00102-12 92 01
10	КриптоПро CSP. КриптоАРМ. Правила пользования	ЖТЯИ.00102-12 95 01
11	КриптоПро CSP. КриптоАРМ. Руководство программиста	ЖТЯИ.00102-12 96 01
12	СКЗИ КриптоПро CSP версии 5.0 R2 KC2 исполнение 2-Base	ЖТЯИ.00102-02, см. Примечание, п. 4
13	Сертификат СКЗИ (копия).	

### Примечание.

1. Для использования необходимо приобретать лицензию на право использования ПО «КриптоАРМ ГОСТ», поставляется отдельно по согласованию с Заказчиком.
2. Необходимо использовать АПМДЗ, сертифицированный ФСБ России, поставляется отдельно по согласованию с пользователем.
3. Для использования необходимо приобретать лицензию на право использования ПО «КриптоПро OSCP Client»/«КриптоПро TSP Client» из состава ПАК «Службы УЦ» версии 2.0, поставляется отдельно по согласованию с Заказчиком.
4. Для использования необходимо приобретать лицензию на право использования СКЗИ «КриптоПро CSP» версии 5.0, поставляется отдельно по согласованию с Заказчиком. Использование СКЗИ «КриптоПро CSP» версии 5.0 в конкретной программно-аппаратной среде ограничивается лицензией.
5. Комплект документации предназначен для администраторов безопасности, разработчиков прикладного программного обеспечения и пользователей СКЗИ.
6. 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.



## 5 АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ЗАЩИТЫ ОТ НСД

Изделие «КriptoПро CSP» версия 5.0 R2 KC2 исполнение 2-КriptoАРМ (ЖТЯИ.00102-12) 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 KC2 исполнение 2-КристоАРМ (ЖТЯИ.00102-12)

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 KC2 исполнение 2-КристоАРМ (ЖТЯИ.00102-12)

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