УТВЕРЖДЕН
ЖТЯИ.00091-02 30 01-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «КриптоПро JCP»

Версия 2.0 R2

ФОРМУЛЯР
ЖТЯИ.00091-02 30 01

2018

Оглавление

1. ОБЩИЕ УКАЗАНИЯ

1.1.Формуляр на изделие - Средство криптографической защиты информации (СКЗИ) «КриптоПро JCP» версия 2.0 R2 - является документом, удостоверяющим гарантированные предприятием-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 «КриптоПро JCP» версия 2.0 R2 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-2005)».

1.3.Порядок обеспечения информационной безопасности при использовании СКЗИ «КриптоПро JCP» версия 2.0 R2 определяется руководителем эксплуатирующей организации на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ.

1.4.Для эксплуатации СКЗИ необходимо выполнить требования по размещению СКЗИ:

1. В случае планирования размещения СКЗИ в помещениях, в которых присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, АС иностранного производства, на которых функционирует СКЗИ, должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации;

2. В случае планирования размещения СКЗИ в помещениях, в которых отсутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и не установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, решение о проведении проверок АС иностранного производства, на которых функционирует СКЗИ, принимается организацией, обеспечивающей эксплуатацию данных СКЗИ.

1.5.Использование СКЗИ для защиты речевой информации запрещено без проведения соответствующих дополнительных исследований.

1.6.Порядок обеспечения информационной безопасности при использовании СКЗИ определяется руководителем эксплуатирующей организации на основе организационно-технических мер защиты, изложенных в эксплуатационной документации на СКЗИ.

1.7.При эксплуатации СКЗИ «КриптоПро JCP» версия 2.0 R2 должны использоваться сертификаты открытых ключей, выпущенные Удостоверяющим центром, сертифицированным по классу защиты не ниже класса защиты используемого СКЗИ.

1.8.При встраивании СКЗИ «КриптоПро JCP» версия 2.0 R2 в прикладные системы необходимо по Техническому заданию, согласованному с ФСБ России, проводить оценку влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований в 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 (далее - государственные органы);

- при организации криптографической защиты информации конфиденциального характера 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 (далее - организации, выполняющие государственные заказы);

- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;

- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;

- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации. В остальных случаях рекомендуется проводить установленным порядком проверку корректности встраивания СКЗИ «КриптоПро JCP» версия 2.0 R2 в прикладные системы с целью оценки обоснованности и достаточности мер, принятых для защиты информации, обрабатываемой СКЗИ.

Также в вышеперечисленных случаях для ограничения возможности влияния аппаратных компонентов СВТ на функционирование СКЗИ необходимо проведение исследований на соответствие ПО BIOS СВТ, на которых установлено СКЗИ, «Временным требованиям проведения исследований ПО BIOS».

Проведение оценки влияния приложений, входящих в состав операционных систем, не требуется.

В остальных случаях рекомендуется проводить установленным порядком проверку корректности встраивания СКЗИ в прикладные системы с целью оценки обоснованности и достаточности мер, принятых для защиты информации, обрабатываемой СКЗИ.

В случае использования вызовов, не входящих в перечень п. 10 документа ЖТЯИ.00091-02 92 01. Правила пользования, необходимо производить разработку отдельного СКЗИ на базе «КриптоПро JCP» версия 2.0 R2 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)).

1.9.СКЗИ соответствует «Требованиям к средствам электронной подписи» (Приложение 1 к Приказу ФСБ РФ 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.

1.10.Формуляр входит в комплект поставки СКЗИ «КриптоПро JCP» версия 2.0 R2 и должен постоянно храниться в органе (подразделении), ответственном за эксплуатацию СКЗИ.

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

2.ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ

При эксплуатации СКЗИ «КриптоПро JCP» версия 2.0 R2 должны выполняться следующие требования:

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

2. Допускается использование СКЗИ для криптографической защиты персональных данных.

3. Ключевая информация является **конфиденциальной**.

4. Срок действия ключа проверки ЭП– не более 15 лет после окончания срока действия соответствующего ключа ЭП.

5. Внешняя гамма, используемая для инициализации состояния программного ДСЧ, является **конфиденциальной**.

6. СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах. В случае их отсутствия рекомендуется по возможности использовать существующие антивирусные средства защиты.

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

8. При эксплуатации СКЗИ «КриптоПро JCP» версия 2.0 R2 необходимо руководствоваться ПКЗ-2005.

9. При эксплуатации СКЗИ «КриптоПро JCP» версия 2.0 R2 необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).

10. Установка СКЗИ на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации (п. 5 ЖТЯИ.91-02 90 01. КриптоПро JCP. Руководство администратора безопасности).

3.ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СКЗИ

3.1.СКЗИ «КриптоПро JCP версия 2.0 R2 предназначено для защиты открытой информации в информационных системах общего пользования (вычисление/проверка электронной подписи) обеспечения защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах с выполнением функций:

1) формирование сессионных ключей, ключей обмена и ключей создания/проверки ЭП, их импорт/экспорт из/в ключевой контейнер;

2) защищенное хранение пользовательских ключей в ключевом контейнере с использованием шифрования, имитозащиты и аутентификации доступа;

3) хэширование, формирование/проверка электронной подписи данных в областях памяти;

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

5) шифрование/расшифрование данных, вычисление имитовставки в областях памяти.

3.2.Исполнения 1 и 2 СКЗИ «КриптоПро JCP» версия 2.0 R2, функционирует под управлением следующих Java-машин:

- Java-машина производства Oracle «Java(TM) 7 Runtime Environment, Standard Edition» версии 1.7 и «Java(TM) 8 Runtime Environment, Standard Edition» версии 1.8 на 32-битной и 64-битной платформе.
- Java-машина производства Oracle «Java(TM) 10 Runtime Environment, Standard Edition» версии 10 и «Java(TM) 11 Runtime Environment, Standard Edition» версии 11 на 64-битной платформе.
- Java-машины J9VM производства IBM «Java(TM) 7 Runtime Environment, Standard Edition» версии 1.7 и «Java(TM) 8 Runtime Environment, Standard Edition» версии 1.8 на 32-битной и 64-битной платформе.

3.3.Порядок и сроки эксплуатации виртуальных машин, в среде которых функционирует СКЗИ «КриптоПро JCP» версия 2.0 R2, определяются производителями виртуальных машин.

3.4.СКЗИ предназначено для использования на следующих программно-аппаратных платформах:

Windows

Windows Vista/7/8/8.1/10 (x86, x64) (только совместно с Java-машиной производства Oracle);
Windows Server 2003/2008/2008 R2/2012/2012 R2/2016 (x64) (только совместно с Java-машиной производства Oracle);

LSB Linux

3.5.ОС Linux, удовлетворяющие стандарту Linux Standart Base ISO/IEC 23360 (x86, x64) версии LSB 4.x:

CentOS 4/5/6/7 (x86, x64);
ТД ОС АИС ФССП России (GosLinux) (x86, x64);
Red OS (x86, x64);
Fedora 23/24/25/26/27 (x86, x64);
Mandriva Enterprise Server 5, Business Server 1 (x86, x64);
Oracle Linux 5/6/7 (x86, x64);
OpenSUSE 12.2/12.3/13.1/13.2 (x86, x64);
SUSE Linux Enterprise 10/11/12 (x86, x64, POWER);
Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER);
Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10/15.04/15.10/16.04/16.04.1/16.

10/17.04/17.10/18.04 (x86, x64, POWER);
Linux Mint 13/14/15/16/17/18 (x86, x64);
Debian 7/8/9 (x86, x64, POWER);

Unix

ALT Linux 6/7 (x86, x64);
ALT Linux 6/7 (ARM) (только совместно с Java-машиной производства Oracle);
Ubuntu Phone (ARM) (только совместно с Java-машиной производства Oracle);
ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64);
РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);
Astra Linux (x86, x64);
FreeBSD 8/9/10/11/pfSense 2.x (x86, x64);
AIX 5/6/7 (POWER) (только совместно с Java-машиной производства IBM);
Mac OS X 10.7/10.8/10.9/10.10/10.11/10.12 (x64);
Solaris 10 (sparc, x86, x64) (только совместно с Java-машиной производства Oracle);
Solaris 11 (sparc, x64) (только совместно с Java-машиной производства Oracle).

3.6.Алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализован в соответствии с ГОСТ 2814789 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

3.7.Алгоритмы формирования и проверки электронной подписи реализованы в соответствии с ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2019 года не допускается.

3.8.Алгоритмы выработки значения хэш-функции реализованы в соответствии с ГОСТ Р 34.112012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

3.9.Сетевая аутентификация реализована на базе протокола TLS v.1.0 с использованием алгоритмов п.п. 3.4-3.6 в соответствии с документом «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS). Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)»;

3.10.Ключевая система СКЗИ «КриптоПро JCP» версия 2.0 R2, 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.

3.11.Хранение закрытых ключей производится на следующих типах носителей:

Носители/ОС	**Windows**	**Linux**	**FreeBSD**	**Solaris**	**AIX**	**Mac OS X**
ГМД 3,5’’, USB диски	+	+	+	+	-	+
eToken, JaCarta	+	+	-	-	-	-
Смарткарты Оскар с использованием считывателей, совместимых с OpenCard Framework	+	+	-	-	-	+
Rutoken	+	+	-	-	-	+
Раздел HDD ПЭВМ	+	+	+	+	+	+

1. Хранение закрытых ключей на HDD ПЭВМ и USB дисках допускается только при условии распространения на HDD, USB диск или на ПЭВМ с HDD требований по обращению с ключевыми носителями (п.10.7 ЖТЯИ.00091-01 90 01. Руководство администратора безопасности).

2. Все вышеперечисленные носители используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене.

3. Использование носителей других типов - только по согласованию с ФСБ России.

3.12.Формирование случайной последовательности производится с использованием ПДСЧ с инициализацией от БиоДСЧ.

3.13.СКЗИ «КриптоПро JCP» версия 2.0 R2 поставляется в двух исполнениях уровня защиты КС1, отличающихся предоставляемыми услугами по защите информации.

4.КОМПЛЕКТНОСТЬ

СКЗИ «КриптоПро JCP» версия 2.0 R2, поставляется в следующих комплектациях:

Комплектация исполнения 1

Наименование	Обозначение
КриптоПро JCP. Базовые модули.	ЖТЯИ.00091-02 99 01
КриптоПро JCP. Формуляр.	ЖТЯИ.00091-02 30 01
КриптоПро JCP. Руководство программиста.	ЖТЯИ.00091-02 33 01
КриптоПро JCP. Руководство администратора безопасности.	ЖТЯИ.00091-02 90 01
КриптоПро JCP. Инструкция по использованию.	ЖТЯИ.00091-02 91 01
КриптоПро JCP. Правила пользования.	ЖТЯИ.00091-02 92 01
КриптоПро JCP. Использование класса-загрузчика новой лицензии	ЖТЯИ.00091-02 93 01
КриптоПро JCP. Описание реализации	ЖТЯИ.00091-02 94 01
Сертификат СКЗИ (копия)	

Комплектация исполнения 2

Наименование	Обозначение
КриптоПро JCP. Базовые модули.	ЖТЯИ.00091-02 99 01
КриптоПро JCP. Модули шифрования.	ЖТЯИ.00091-02 99 02
КриптоПро JCP. Формуляр.	ЖТЯИ.00091-02 30 01
КриптоПро JCP. Руководство программиста	ЖТЯИ.00091-02 33 01
КриптоПро JCP. Руководство программиста. Модули шифрования	ЖТЯИ.00091-02 33 02
КриптоПро JCP. Руководство программиста (JTLS).	ЖТЯИ.00091-02 33 03
КриптоПро JCP. Руководство администратора безопасности.	ЖТЯИ.00091-02 90 01
КриптоПро JCP. Инструкция по использованию.	ЖТЯИ.00091-02 91 01
КриптоПро JCP. Инструкция по использованию (JTLS).	ЖТЯИ.00091-02 91 02
КриптоПро JCP. Правила пользования.	ЖТЯИ.00091-02 92 01
КриптоПро JCP. Использование класса-загрузчика новой лицензии	ЖТЯИ.00091-02 93 01
КриптоПро JCP. Описание реализации	ЖТЯИ.00091-02 94 01
Сертификат СКЗИ (копия)	

Примечания:

1. Исполнение 1 (уровень защиты КС1) функционирует в программно-аппаратных платформах 3.3 и выполняет функции 1-3 п. 3.1.
2. Исполнение 2 (уровень защиты КС1) функционирует в программно- аппаратных платформах 3.3 и выполняет функции 1-5 п. 3.1.
3. Комплект документации предназначен администраторам безопасности и разработчикам прикладного программного обеспечения, использующего СКЗИ.
4. Программное обеспечение и документация (в формате PDF - Adobe Acrobat Reader и HTML) поставляется в электронном виде на CD-ROM, формуляр и копия сертификата СКЗИ – в печатном виде.

5.СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие «КриптоПро JCP» версия 2.0 R2, ЖТЯИ.00091-02

комплектация варианта исполнения _____

Учётный № СКЗИ _____

носители:

☐ CD-ROM _____ шт.

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

Дата выпуска: "_____"_____ 20__ г.

М.П. Главный инженер ООО "КРИПТО-ПРО" _____

6.СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие «КриптоПро JCP» версия 2.0 R2, ЖТЯИ.00091-02

комплектация варианта исполнения _____

Учётный № СКЗИ _____

упаковано в

- ⁋ бумажный конверт
- ⁋ коробку
- ⁋ пластиковый конверт
- ⁋ _____

Дата упаковки: «___»_____ 20___ г.

М. П.

Упаковку произвел _____

7.ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)

7.1.Пользователь приобретает изделие и несет ответственность за его использование в соответствии с эксплуатационной документацией.

7.2.Предприятие-изготовитель гарантирует работоспособность изделия в соответствии с заявленными характеристиками.

7.3.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.

7.4.Гарантийный срок изделия — 12 месяцев с момента поставки при условии соблюдения пользователем требований эксплуатационной документации на изделие.

7.5.Данные о поставке (продаже) изделия:

_____

_____

(наименование организации-поставщика (продавца) изделия)

Дата поставки: «_____» _____ _____г.

М.П.

_____

(подпись)

Примечание. При отсутствии данных о дате поставки изделия гарантийный срок отсчитывается от даты его выпуска, указанной в разделе 5 «Свидетельство о приемке».

8.СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

127018 г. Москва, ул. Сущевский вал 18, ООО «КРИПТО-ПРО».

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

8.3.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.

8.4.Предприятие-изготовитель принимает рекламацию, если не установлена вина получателя в возникновении дефекта в изделии.

8.5.Сведения о рекламациях фиксируются в таблице 1.

Таблица 1 – Сведения о рекламациях.

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

9.СВЕДЕНИЯ О ХРАНЕНИИ

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

10.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

11.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

12.ОСОБЫЕ ОТМЕТКИ