ООО «КРИПТО-ПРО»

УТВЕРЖДЕН
ЖТЯИ.00088-01 30 01-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

«КриптоПро CSP»

Версия 4.0 2-Base

ФОРМУЛЯР

ЖТЯИ.00088-01 30 01

2016 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1 Формуляр на изделие «Средство криптографической защиты информации «КриптоПро CSP» v 4.0» ЖТЯИ.00088-01 (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 руководителем эксплуатирующей организации на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации.

1.4 При эксплуатации СКЗИ должны использоваться сертификаты ключей электронной подписи (сертификаты открытых ключей), выпущенные Удостоверяющим центром, сертифицированным ФСБ России по классу защиты не ниже класса защиты используемого СКЗИ.

1.5 При встраивании СКЗИ в прикладные системы необходимо по Техническому заданию, согласованному с 8 Центром 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 защиты конфиденциальной информации, обрабатываемой СКЗИ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- при организации криптографической защиты конфиденциальной информации, обрабатываемой СКЗИ, 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;
- 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 в прикладные системы с целью оценки обоснованности и достаточности мер, принятых для защиты информации, обрабатываемой СКЗИ.

Проведение оценки влияния приложений, перечисленных в п.2 Правил пользования ЖТЯИ.00088-01 95 01, не требуется.

В случае использования вызовов, не входящих в перечень Приложения 2 документа ЖТЯИ.00088-01 95 01. Правила пользования, необходимо производить разработку отдельного СКЗИ на базе «КриптоПро CSP» версия 4.0 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 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.

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

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

2. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ

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

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 При эксплуатации СКЗИ необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).

2.10 Установка СКЗИ на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации (п. 2 ЖТЯИ.00088-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть).

3. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1 СКЗИ предназначено для защиты открытой информации в информационных системах общего пользования (вычисление/проверка электронной подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах с выполнением следующих функций:

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

2) шифрование, вычисление имитовставки, хэширование, создание/проверка электронной подписи данных в областях памяти;

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

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

5) аутентификация в домене Windows с использованием «КриптоПро Winlogon».

3.2 СКЗИ функционирует в следующих программно-аппаратных средах:

Windows

Включает программно-аппаратные среды:

- Windows 7/8/8.1/Server 2003/2008 (x86, x64);
- Windows Server 2008 R2/2012/2012 R2 (x64).

LSB Linux

Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x:

- CentOS 4/5/6/7 (x86, x64, POWER, ARM);
- ТД ОС АИС ФССП России (GosLinux) (x86, x64);
- Red OS (x86, x64);
- Fedora 19/20 (x86, x64, ARM);
- Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM);
- Oracle Linux 4/5/6/7 (x86, x64);
- OpenSUSE 13.2, Leap 42 (x86, x64, ARM);
- SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM);
- Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM);
- Синтез-ОС.РС (x86, x64, POWER, ARM);
- Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10 (x86, x64, POWER, ARM);
- Linux Mint 13/14/15/16/17 (x86, x64);
- Debian 7/8 (x86, x64, POWER, ARM);
- Astra Linux Special Edition (x86-64).

Unix

Включает программно-аппаратные среды:

- ALT Linux 7 (x86, x64, ARM);
- ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64);
- РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);
- FreeBSD 9, pfSense 2.x (x86, x64);
- AIX 5/6/7 (POWER);

Solaris

Включает программно-аппаратные среды:

- Solaris 10 (sparc, x86, x64);
- Solaris 11 (sparc, x64).

Примечания:

1. При эксплуатации СКЗИ необходимо учитывать, что порядок и сроки эксплуатации операционных систем, в среде которых функционирует СКЗИ, определяются производителями операционных систем. Использование операционных систем, поддержка которых остановлена

производителем, не допускается.

2. Для следующих ОС необходима серверная лицензия:
   Microsoft Windows Server 2003;
   Microsoft Windows Server 2008;
   Microsoft Windows Server 2008 R2;
   Microsoft Windows Server 2012;
   Microsoft Windows Server 2012 R2;
   Все ОС с архитектурой, отличной от x86/x64 (POWER, Sparc);
   Red Hat Enterprise Linux Server;
   Ubuntu Server;
   Solaris;
   FreeBSD;
   AIX.

3.3 Алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализован в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

3.4 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».

3.5 Алгоритмы выработки значения хэш-функции реализованы в соответствии с ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается.

3.6 Сетевая аутентификация реализована на базе протокола TLS v.1.0 с использованием алгоритмов п.п. 3.3-3.5 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)»;

3.7 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.

3.8 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.

Носитель/ОС	**Windows IA32**	**Windows x64**	**Linux**	**FreeBSD**	**Solaris**	**AIX**
ГМД 3,5'', USB диски	+	+	+	+	+	-
Смарткарты GEMALTO (GemSim1, GemSim2, Optelio, OptelioCL, OptelioCL2, Native)	+	+	+	+	+	-
eToken, Jacarta	+	+	+	-	-	-
USB-токены Рутокен ЭЦП (Flash, Bluetooth), Рутокен Lite	+	+	+	+	-	-
Смарткарты Рутокен Lite SC, Рутокен ЭЦП SC	+	+	+	+	-	-
Рутокен S	+	+	+	-	-	-
Novacard	+	+	+	+	+	-
Смарткарты РИК (ОСКАР 1, ОСКАР 2, Магистра, TRUST, TRUSTS, TRUSTD)	+	+	+	+	+	-

Смарткарта УЭК	+	+	+	+	+	-
Смарткарта MS_KEY K	+	+	-	-	-	-
ESMART Token	+	+	+	-	-	-
Смарткарты Athena IDProtect, MorphoKST, Cha cardOS, Cha JCOP	+	+	-	-	-	-
Смарткарты Алиот INPASPOT Series, SCOne Series	+	+	+	-	-	-
Раздел HDD ПЭВМ (в Windows - реестр)	+	+	+	+	+	+
Идентификаторы Touch-Memory DS1995, DS1996	+	-	-	-	-	-

Примечания:

1. Хранение закрытых ключей на HDD ПЭВМ и USB дисках (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) допускается только при условии распространения на HDD, USB диск или на ПЭВМ с HDD требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00088–01 91 01. Руководство администратора безопасности общая часть).

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.

4. Использование в качестве пассивного хранилища ключевой информации Рутокен ЭЦП Bluetooth возможно только при наличии сертификата соответствия ФСБ России на указанное устройство; для иных носителей использовать для передачи данных бесконтактный интерфейс запрещено.

3.9 Формирование закрытых ключей производится с использованием следующих типов считывателей, указанных в Таблице 3.2.

Таблица 3.2 – Способы формирования закрытых ключей.

Считыватели/ОС	**Windows IA32**	**Windows x64**	**Linux**	**FreeBSD**	**Solaris**	**AIX**
Дисковод/USB дисковод	+	+	+	+	+	-
PS/SC совместимый считыватель смарт-карт	+	+	+	-	+	-
Физический ДСЧ в составе ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180)	+	+	+	+	-	-
Физический ДСЧ в составе АПМДЗ-У М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ	+	+	+	-	-	-
Устройство чтения таблеток Touch-Memory Dallas: DS9097E, DS9097U, DS1410E	+	-	-	-	-	-
Раздел, реестр HDD ПЭВМ	+	+	+	+	+	+

3.10 Формирование случайной последовательности производится с использованием ДСЧ, указанных в Таблице 3.3.

Таблица 3.3 – Возможные варианты использования различных ДСЧ для выработки случайной последовательности.

ДСЧ/ОС	**Windows IA32**	**Windows x64**	**Linux**	**FreeBSD**	**Solaris**	**AIX**
Физический ДСЧ в составе ПАК защиты от НСД «Соболь» RU.40308570.501410.001 ПС (версии кода расширения BIOS 1.0.99, 1.0.180)	+	+	+	+	-	-
Физический ДСЧ в составе АПМДЗ-У М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ	+	+	+	-	-	-
Внешняя гамма	+	+	+	+	+	+

Примечание: Использование других сертифицированных типов ДСЧ - только по согласованию с ФСБ России.

4. КОМПЛЕКТНОСТЬ

Таблица 4.1 - Комплектация исполнения 2-Base

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00088-01 99 01
Средство защиты от несанкционированного доступа	См. Примечание п. 1
КриптоПро CSP v. 4.0. Формуляр.	ЖТЯИ.00088-01 30 01
КриптоПро CSP. Описание реализации.	ЖТЯИ.00088-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00088-01 91 01
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows .	ЖТЯИ.00088-01 91 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux.	ЖТЯИ.00088-01 91 03
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD.	ЖТЯИ.00088-01 91 04
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris.	ЖТЯИ.00088-01 91 05
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX.	ЖТЯИ.00088-01 91 06
КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС Windows.	ЖТЯИ.00088-01 92 01
КриптоПро CSP. Приложение командной строки для подписи и шифрования файлов	ЖТЯИ.00088-01 93 01
КриптоПро CSP. Руководство программиста.	ЖТЯИ.00088-01 94 01
КриптоПро CSP. Правила пользования.	ЖТЯИ.00088-01 95 01
КриптоПро CSP. Руководство программиста.	ЖТЯИ.00088-01 96 01
Сертификат СКЗИ (копия).	

Примечания:

1. Для защиты от несанкционированного доступа могут использоваться следующие средства:
   - ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180);
   - Аппаратно-программный модуль доверенной загрузки универсальный М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ;

   Поставка - по согласованию с пользователем.

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

3. Программное обеспечение и документация в электронном виде в формате PDF (Adobe Acrobat Reader) на CD-ROM для всех исполнений СКЗИ поставляется единым дистрибутивом, формуляр и копия сертификата, заверенная ООО «КРИПТО-ПРО», - в печатном виде.

4. Использование варианта исполнения СКЗИ в конкретной программно-аппаратной среде ограничивается лицензией.

5. АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ЗАЩИТЫ ОТ НСД

Изделие «КриптоПро CSP» v 4.0» ЖТЯИ.00088-01, вариант исполнения 2-Base укомплектовано аппаратно-программным средством защиты информации от несанкционированного доступа.

Наименование средства, ТУ	Серийный номер, дата выпуска

Главный инженер

ООО «КРИПТО-ПРО»

_____

М.П.

/_____/

«___»_____ 20__г.

6. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие «КриптоПро CSP» v 4.0» ЖТЯИ.00088-01,

серийный № дистрибутива _____

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» _____ /_____/

7. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие «КриптоПро CSP» v 4.0» ЖТЯИ.00088-01,

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 разделе 6 «Свидетельство о приемке».

8.5 Данные о поставке (продаже) изделия:

_____

_____

(наименование организации-поставщика (продавца) изделия)

Дата поставки: "___" _____ 20__г.

М.П.

_____

(подпись)

9. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

127018 г. Москва, а/я КРИПТО-ПРО.

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 таблице 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 ответственного 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