ООО "КРИПТО-ПРО"

УТВЕРЖДЕН
ЖТЯИ.00050-02 30 01-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ "КриптоПро CSP"

Версия 3.6

ФОРМУЛЯР

ЖТЯИ.00050-02 30 01

Листов 18

2010

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие Средство криптографической защиты информации "КриптоПро CSP", СКЗИ ЖТЯИ.00050-02, 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 ЖТЯИ.00050-02 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 ЖТЯИ.00050-02 определяется руководителем эксплуатирующей организации на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ.

1.4. При эксплуатации СКЗИ ЖТЯИ.00050-02 должны использоваться только сертификаты открытых ключей, выпущенные доверенным органом сертификации. В качестве такого органа может выступать доверенный Удостоверяющий центр (УЦ), выпускающий сертификаты и поддерживающий списки отозванных сертификатов в соответствии с Регламентом УЦ, а также Служба корпоративной системы, обеспечивающая доверенные справочники сертификатов открытых ключей с поддержкой актуальности включаемых в справочники сертификатов.

1.5. При встраивании СКЗИ ЖТЯИ.00050-02 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:

1) если информация, обрабатываемая СКЗИ, подлежит защите в соответствии с законодательством Российской Федерации;

2) при организации защиты информации, обрабатываемой СКЗИ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;

3) при организации криптографической защиты 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.

Указанную оценку необходимо проводить по ТЗ, согласованному с 8 Центром ФСБ России.

1.6. Формуляр входит в комплект поставки СКЗИ ЖТЯИ.00050-02 и должен постоянно храниться в органе (подразделении), ответственном за эксплуатацию СКЗИ.

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

2. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ

При эксплуатации СКЗИ ЖТЯИ. 00050-02 должны выполняться следующие требования:

1. Средствами СКЗИ **НЕ ДОПУСКАЕТСЯ** обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

   ДОПУСКАЕТСЯ использование СКЗИ для криптографической защиты персональных данных.

2. Ключевая информация является **конфиденциальной**.

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

4. СКЗИ ЖТЯИ. 00050-02 должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

5. Размещение СКЗИ ЖТЯИ. 00050-02 в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

6. В случае, если в модели угроз, которым должно противостоять СКЗИ ЖТЯИ.00050-02 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).

7. Инсталляция СКЗИ ЖТЯИ.00050-02 на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

3. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1 СКЗИ ЖТЯИ.00050-02 предназначено для защиты открытой информации в информационных системах общего пользования (вычисление/проверка электронной цифровой подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах с выполнением функций:

- защищенное хранение пользовательских ключей в ключевом контейнере с использованием шифрования, имитозащиты и аутентификации доступа;
- шифрование, вычисление имитовставки, хэширование, формирование/проверка ЭЦП данных в областях памяти;
- формирование сессионных ключей и ключей обмена, их импорт/экспорт из/в ключевой контейнер;
- идентификация, аутентификация, шифрование и имитозащита TLS-соединений.

3.2 СКЗИ ЖТЯИ.00050-02 функционирует под управлением операционных систем:

- Windows 2000 (ia32);
- Windows XP/2003/Vista/2008/7/2008R2 (ia32, ia64, x64).
- Linux Standard Base ISO/IEC 23360 (ia32, x64), программно-аппаратные среды, удовлетворяющие стандарту LSB 4.x/3.x:
  - Linpus (ia32)
  - Mandriva (ia32, x64)
  - MontaVista Linux (ia32, x64)
  - Oracle Enterprise Linux (ia32, x64)
  - Open SUSE (ia32, x64)
  - Red Hat Enterprise Linux (ia32, x64)
  - Red Flag Linux (ia32)
  - SUSE Linux Enterprise (ia32, x64)
  - SUSE LINUX (ia32)
  - Ubuntu (ia32, x64)
  - Xandros (ia32)

  ALT Linux (ia32, x64);

  Debian (ia32, x64);

  Red Hat Enterprise Linux Version 3 Update 3 (ia32, x64);

  Trustverse Linux XP (ia32);
- FreeBSD 7/8 (ia32);
- Solaris 9/10 (sparc, ia32, x64);
- AIX 5/6 (Power PC). Только в исполнении 1.

Примечание. Порядок и сроки эксплуатации операционных систем, в среде которых функционирует СКЗИ, определяются производителями операционных систем.

3.3 Алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализован в соответствии с ГОСТ 28147-89 "СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ".

3.4 Алгоритм формирования и проверки ЭЦП реализован в соответствии с ГОСТ Р 34.10-2001. "ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ".

3.5 Алгоритм выработки значения хэш-функции реализован в соответствии с ГОСТ Р 34.11-94 "ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ФУНКЦИЯ ХЭШИРОВАНИЯ".

3.6 Сетевая аутентификация реализована на базе протокола TLS v.1.0 (RFC 2246) с использованием алгоритмов п.п. 3.3 -3.5.

3.7 Ключевая система СКЗИ ЖТЯИ.00050-02 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 Формирование закрытых ключей производится на типы носителей:

Носители/ОС	**Windows IA32**	**Windows x64**	**Windows IA64**	**Linux**	**FreeBSD**	**Solaris**	**AIX**
ГМД 3,5'', USB диски	+	+	+	+	+	+	-
eToken	+	+	-	+	-	-	-
Смарткарты РИК	+	-	-	+	-	-	-
Смарткарты Оскар, Магистра	+	+	-	+	-	-	-
Rutoken	+	+	-	+	-	-	-
Раздел HDD ПЭВМ (в Windows -реестр)	+	+	+	+	+	+	+
Идентификаторы Touch-Memory DS1995, DS1996	+	-	-	-	-	-	-

Примечания 1. Допускается хранение закрытых ключей на HDD ПЭВМ (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) для исполнения 2 СКЗИ класса КС2 при условии распространения на HDD или на ПЭВМ с HDD требований по обращению с ключевыми носителями.

2. Использование носителей других типов - только по согласованию с ООО «КРИПТО-ПРО».

3.9 Формирование закрытых ключей производится с использованием следующих типов считывателей:

Считыватели/ОС	**Windows IA32**	**Windows x64**	**Windows IA64**	**Linux**	**FreeBSD**	**Solaris**	**AIX**
Дисковод/USB дисковод	+	+	+	+	+	+	-
PS/SC совместимый считыватель смарт-карт	+	+	+	+	-	+	-
ПАК защиты от НСД "Соболь" УВАЛ.00300-58-01ТУ или RU.40308570.501410.001 ПС	+	-	-	-	-	-	-
ПАК защиты от НСД "Аккорд-АМДЗ" 4012-006-11443195-2005 ТУ.	+	-	-	-	-	-	-
Устройство чтения таблеток Touch-Memory Dallas: DS9097E, DS9097U, DS1410E	+	-	-	-	-	-	-
HDD ПЭВМ (реестр Windows)	+	+	+	+	+	+	+

3.10 Формирование случайной последовательности производится с использованием следующих типов ДСЧ:

ДСЧ/ОС	**Windows IA32**	**Windows x64**	**Windows IA64**	**Linux**	**FreeBSD**	**Solaris**	**AIX**
Биологический ДСЧ	+	+	+	+	+	+	+
Физический ДСЧ в составе ПАК защиты от НСД "Соболь" УВАЛ.00300-58-01 ТУ или RU.40308570.501410.001 ПС	+	-	-	+	-	-	-
Физический ДСЧ в составе ПАК защиты от НСД "Аккорд-АМДЗ", 4012-006-11443195-2005 ТУ.	+	-	-	-	-	-	-
Внешняя гамма	+	+	+	+	+	+	+

Примечание: Использование других сертифицированных типов ДСЧ - только по согласованию с ООО «КРИПТО-ПРО».

4. КОМПЛЕКТНОСТЬ

Исполнения СКЗИ ЖТЯИ.00050-02 поставляются в комплектациях:

Комплектация исполнения 1

Наименование	**Обозначение**
КриптоПро CSP. Базовые модули.	ЖТЯИ.00050-02 99 01
КриптоПро CSP. Описание реализации.	ЖТЯИ.00050-02 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00050-02 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows .	ЖТЯИ.00050-02 90 02-01
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux.	ЖТЯИ.00050-02 90 02-02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD.	ЖТЯИ.00050-02 90 02-03
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris.	ЖТЯИ.00050-02 90 02-04
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX.	ЖТЯИ.00050-02 90 02-05
КриптоПро CSP. Инструкция по использованию.	ЖТЯИ.00050-02 90 03
КриптоПро CSP. Руководство программиста.	ЖТЯИ.00050-02 90 05
Сертификат СКЗИ (копия).	

Комплектация исполнения 2

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00050-02 99 01
Средство защиты от несанкционированного доступа	См. Примечания, п. 2
КриптоПро CSP. Описание реализации.	ЖТЯИ.00050-02 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00050-02 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows .	ЖТЯИ.00050-02 90 02-01
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux.	ЖТЯИ.00050-02 90 02-02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD.	ЖТЯИ.00050-02 90 02-03
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris.	ЖТЯИ.00050-02 90 02-04
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX.	ЖТЯИ.00050-02 90 02-05
КриптоПро CSP. Инструкция по использованию.	ЖТЯИ.00050-02 90 03
КриптоПро CSP. АРМ выработки внешней гаммы.	ЖТЯИ.00050-02 90 04
КриптоПро CSP. Руководство программиста.	ЖТЯИ.00050-02 90 05
Сертификат СКЗИ (копия).	

Примечания.

1. Исполнение 1 (уровень защиты КС1), исполнение 2 (уровень защиты КС2) функционируют в программно-аппаратных средах, указанных в п. 3.2.
2. В качестве средства защиты от несанкционированного доступа используется Программно-аппаратный комплекс с физическим датчиком случайных чисел "Соболь" УВАЛ.00300-58-01 ТУ или RU.40308570.501410.001 ПС .
   В программно-аппаратных средах с ОС Windows может использоваться также Программно-аппаратное средство "Аккорд-АМДЗ" 4012-006-11443195-2005 ТУ.
   Поставка - по согласованию с пользователем.

Наименование	Обозначение

Использование других сертифицированных программно-аппаратных комплексов защиты от несанкционированного доступа - только по согласованию с ООО «КРИПТО-ПРО».

3. Комплект документации предназначен администраторам безопасности и разработчикам прикладного программного обеспечения, использующего СКЗИ.
4. Программное обеспечение и документация для всех исполнений СКЗИ поставляется единым дистрибутивом в электронном виде в формате PDF (Adobe Acrobat Reader) на CD-ROM, формуляр и копия сертификата, заверенная ООО "КРИПТО-ПРО", - в печатном виде.
5. Использование варианта исполнения СКЗИ в конкретной программно-аппаратной среде ограничивается лицензией.

5. АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ЗАЩИТЫ ОТ НСД

Изделие "КриптоПро CSP", ЖТЯИ. 00050-02, вариант исполнения __ укомплектовано аппаратно-программным средством защиты информации от несанкционированного доступа.

Наименование средства, ТУ	Серийный номер, дата выпуска

М.П. Главный инженер ООО "КРИПТО-ПРО"

6. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие "КриптоПро CSP", ЖТЯИ. 00050-02,

серийный № дистрибутива _____

носители:

☐ CD-ROM _____ шт.

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

Дата выпуска: "_____"_____ _____ г.

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

7. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие "КриптоПро CSP", ЖТЯИ. 00050-02,

серийный № дистрибутива _____

упаковано в

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

Дата упаковки: "___"_____ _____ 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 5 "Свидетельство о приемке".

8.5 Данные о поставке (продаже) изделия:

_____

_____

(наименование организации-поставщика (продавца) изделия)

Дата поставки: "___" _____ _____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 1.

Таблица 1

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