ООО "Крипто-Про"

УТВЕРЖДЕН
ЖТЯИ.00015-01 30 01-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ "КриптоПро CSP"

Версия 3.0

ФОРМУЛЯР

ЖТЯИ.00015-01 30 01

Листов 19

2005 г.

СОДЕРЖАНИЕ

1. Общие указания 3
2. Общие сведения об изделии 4
3. общие сведения и основные характеристики СКЗИ 6
4. Комплектность 8
5. Аппаратно-программные средства защиты от НСД 11
6. Свидетельство о приемке 12
7. Свидетельство об упаковке 13
8. Гарантии изготовителя (поставщика) 14
9. Сведения о рекламациях 15
10. Сведения о хранении 16
11. Сведения о закреплении изделия при эксплуатации 17
12. Сведения об изменениях 18
13. Особые отметки 19

1. ОБЩИЕ УКАЗАНИЯ

1.1 Формуляр на изделие - Средство криптографической защиты информации (СКЗИ) "КриптоПро CSP" версии 3.0 - 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 Перед эксплуатацией СКЗИ необходимо ознакомиться с формуляром и эксплуатационной документацией, приведенной в разделе 4 "Комплектность".

1.3 Порядок обеспечения информационной безопасности при использовании СКЗИ определяется руководителем эксплуатирующей организации на основе рекомендаций по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ.

1.4 Формуляр входит в комплект поставки СКЗИ "КриптоПро CSP" и должен постоянно храниться в органе (подразделении), ответственном за эксплуатацию СКЗИ.

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

2. ОБЩИЕ СВЕДЕНИЯ ОБ ИЗДЕЛИИ

2.1 Изделие - средство криптографической защиты информации "КриптоПро CSP" версии 3.0**,** ЖТЯИ.00015.

2.2 Изготовитель: ООО "КРИПТО-ПРО".

2.3 СКЗИ "КриптоПро CSP" версии 3.0 реализовано в 10 вариантах исполнения.

Вариант исполнения 1

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-01 99 01

Вариант исполнения 2

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-02 99 01

Вариант исполнения 3

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-03 99 01

Вариант исполнения 4

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-04 99 01

Вариант исполнения 5

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-05 99 01

Вариант исполнения 6

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-01 99 01
Средство защиты от несанкционированного доступа	

Вариант исполнения 7

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-02 99 01
Средство защиты от несанкционированного доступа	

Вариант исполнения 8

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-03 99 01
Средство защиты от несанкционированного доступа	

Вариант исполнения 9

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-04 99 01
Средство защиты от несанкционированного доступа	

Вариант исполнения 10

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-05 99 01
Средство защиты от несанкционированного доступа (только при использовании платформы IA32)	

Примечания:

Исполнение 1 - СКЗИ класса КС1, функционирующее под управлением ОС Windows 2000/XP/2003 (платформы IA32, IA64);

Исполнение 2 - СКЗИ класса КС1, функционирующее под управлением ОС Red Hat Linux 7 (платформа IA32);

Исполнение 3 - СКЗИ класса КС1, функционирующее под управлением ОС Red Hat Linux 9 (платформа IA32);

Исполнение 4 - СКЗИ класса КС1, функционирующее под управлением ОС FreeBSD 5 (платформа IA32);

Исполнение 5 - СКЗИ класса КС1, функционирующее под управлением ОС Solaris 9 Update 4 (платформы SPARC, IA32);

Исполнение 6 - СКЗИ класса КС2, функционирующее под управлением ОС Windows 2000/XP/2003 (платформа IA32);

Исполнение 7 - СКЗИ класса КС2, функционирующее под управлением ОС Red Hat Linux 7 (платформа IA32);

Исполнение 8 - СКЗИ класса КС2, функционирующее под управлением ОС Red Hat Linux 9 (платформа IA32);

Исполнение 9 - СКЗИ класса КС2, функционирующее под управлением ОС FreeBSD 5 (платформа IA32);

Исполнение 10 - СКЗИ класса КС2, функционирующее под управлением ОС Solaris 9 Update 4 (платформы SPARC, IA32).

3. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СКЗИ

3.1 СКЗИ "КриптоПро CSP" версии 3.0, ЖТЯИ.00015 предназначено для обеспечения защиты конфиденциальной информации.

3.2 СКЗИ "КриптоПро CSP" версии 3.0 в зависимости от варианта исполнения может функционировать под управлением одной из следующих операционных систем:

- Windows 2000/XP/2003 (платформы IA32, IA64);
- Red Hat Linux 7, 9 (платформа IA32);
- FreeBSD 5 (платформа IA32);
- Solaris 9 Update 4 (платформы SPARC, IA32).

Примечание. Порядок и сроки эксплуатации операционных систем, в среде которых функционирует СКЗИ "КриптоПро CSP" версии 3.0, 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 Алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями ГОСТ Р 34.10-94 "ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. СИСТЕМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ АСИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА" и 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 требованиями 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, 3.4 и 3.5.

3.7 Ключевая система СКЗИ "КриптоПро CSP" версии 3.0, ЖТЯИ.00015 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 следующие типы носителей:

Носители/ОС	Windows IA32	Windows IA64	Linux	Solaris	FreeBSD
ГМД 3,5'', USB диски	+	+	+	+	+
Электронные USB ключи e-Token R2	+	-	-	-	-
Смарт-карты РИК	+	+	+	+	+
Смарт-карты Оскар	+	+	+	+	+
Смарт-карты MPCOS/EMV	+	+	-	-	-
HDD ПЭВМ (реестр Windows)	+	+	+	+	+
Таблетки Touch-Memory DS1995, DS1996	+	-	-	-	-

3.9 Формирование закрытых ключей производится с использованием следующих типов считывателей:

Считыватели/ОС	Windows IA32	Windows IA64	Linux	Solaris	Free BSD
Дисковод/USB дисковод	+	+	+	+	+
PS/SC совместимый считыватель смарт-карт	+	+	+	+	+
«Аккорд-АМДЗ»	+	-	-	-	-
Электронный замок «Соболь»	+	-	-	-	-
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 IA64	Linux	Solaris	Free BSD
Биологический ДСЧ	+	+	+	+	+
«Аккорд-АМДЗ»	+	-	+	-	-
Электронный замок «Соболь»	+	-	+	-	-

Примечание. Допускается хранение закрытых ключей на HDD ПЭВМ для вариантов исполнения СКЗИ класса КС2 при условии распространения на ПЭВМ требований по обращению с ключевыми носителями.

4. КОМПЛЕКТНОСТЬ

СКЗИ "КриптоПро CSP" версии 3.0 ЖТЯИ.00015 поставляется в следующих комплектациях:

Комплектация варианта исполнения 1

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-01 99 01
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows 2000/XP/2003.	ЖТЯИ.00015-01 90 02-01
КриптоПро CSP. Инструкция по использованию КриптоПро CSP и TLS.	ЖТЯИ.00015-01 90 02-05
КриптоПро CSP. Руководство программиста.	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 1 (копия).	

Комплектация варианта исполнения 2

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-02 99 01
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Red Hat Linux 7, 9	ЖТЯИ.00015-01 90 02-02
КриптоПро CSP. Руководство программиста	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 2 (копия)	

Комплектация варианта исполнения 3

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-03 99 01
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Red Hat Linux 7, 9	ЖТЯИ.00015-01 90 02-02
КриптоПро CSP. Руководство программиста	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 3 (копия)	

Комплектация варианта исполнения 4

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-04 99 01
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности.	ЖТЯИ.00015-01 90 02

Наименование	Обозначение
Общая часть.	
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD 5	ЖТЯИ.00015-01 90 02-03
КриптоПро CSP. Руководство программиста	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 4 (копия)	

Комплектация варианта исполнения 5

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-05 99 01
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris 9 Update 4	ЖТЯИ.00015-01 90 02-04
КриптоПро CSP. Руководство программиста	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 5 (копия)	

Комплектация варианта исполнения 6

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-01 99 01
Средство защиты от несанкционированного доступа	См. Примечания, п. 2
КриптоПро CSP. Описание реализации	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows 2000/XP/2003	ЖТЯИ.00015-01 90 02-01
КриптоПро CSP. Инструкция по использованию КриптоПро CSP и TLS	ЖТЯИ.00015-01 90 02-05
КриптоПро CSP. Руководство программиста	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 6 (копия)	

Комплектация варианта исполнения 7

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-02 99 01
Средство защиты от несанкционированного доступа	См. Примечания, п. 2
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Red Hat Linux 7, 9	ЖТЯИ.00015-01 90 02-02
КриптоПро CSP. Руководство программиста	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 7 (копия)	

Комплектация варианта исполнения 8

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-03 99 01
Средство защиты от несанкционированного доступа	См. Примечания, п. 2
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Red Hat Linux 7, 9	ЖТЯИ.00015-01 90 02-02
КриптоПро CSP. Руководство программиста	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 8 (копия)	

Комплектация варианта исполнения 9

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-04 99 01
Средство защиты от несанкционированного доступа	См. Примечания, п. 2
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD 5	ЖТЯИ.00015-01 90 02-03
КриптоПро CSP. Руководство программиста.	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 9 (копия)	

Комплектация варианта исполнения 10

Наименование	Обозначение
КриптоПро CSP. Базовые модули.	ЖТЯИ.00015-05 99 01
Средство защиты от несанкционированного доступа	См. Примечания, п.п. 2, 3
КриптоПро CSP. Описание реализации.	ЖТЯИ.00015-01 90 01
КриптоПро CSP. Руководство администратора безопасности. Общая часть.	ЖТЯИ.00015-01 90 02
КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris 9 Update 4	ЖТЯИ.00015-01 90 02-04
КриптоПро CSP. Руководство программиста	ЖТЯИ.00015-01 90 03
Сертификат СКЗИ, исполнение 10 (копия)	

Примечания:

1. Комплект документации предназначен администраторам безопасности и разработчикам прикладного программного обеспечения, использующего СКЗИ.

2. В качестве средства защиты от несанкционированного доступа может использоваться сертифицированный программно-аппаратный комплекс защиты от НСД (электронный замок) с физическим датчиком случайных чисел; поставка - по согласованию с пользователем.

3. Только при использовании платформы IA32.

4. Программное обеспечение и документация (в формате PDF - Adobe Acrobat Reader) поставляется в электронном виде на CD-ROM, копия сертификата СКЗИ и формуляр – в печатном виде.

5. АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ НСД

Изделие "КриптоПро CSP", ЖТЯИ.00015, 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.00015,

комплектация варианта исполнения _____

серийный № дистрибутива _____

носители:

☐ CD-ROM _____ шт.

соответствует эталону, хранящемуся в ООО "Крипто-Про", и признано годным для эксплуатации.

Дата выпуска: "_____"_____ 200__ г.

М.П. Главный инженер ООО "Крипто-Про" _____

7. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие "КриптоПро CSP", ЖТЯИ.00015,

комплектация варианта исполнения _____

серийный № дистрибутива _____

упаковано в

☐ бумажный конверт

☐ коробку

☐ пластиковый конверт

☐ _____

Дата упаковки: "___"_____ 200___ 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.

8.5 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 6 "Свидетельство о приемке".

9. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

127018 г. Москва, ул. Образцова 38, ООО "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