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 20

Серийный номер:

36361-10000-0XXXX-XXXXX-XXXXX

2010

9. СВЕДЕНИЯ О ХРАНЕНИИ

Дата установки на хранение	Дата снятия с хранения	Условия хранения	Должность, фамилия и подпись отв. лица
27.08.2012		Отдел №21 УФК	Главный специалист-эксперт Чебанова Н.В.

2. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

2.1 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.

2.2 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.

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

2.4 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".

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

1. 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. 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.

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
Главный специалист-эксперт	Чебанова Н.В.	от 25.02.2011 № 801		