**ООО "КРИПТО-ПРО"**

---

**УТВЕРЖДЕН**
**ЖТЯИ.00074-01 30 01-ЛУ**

# СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

# "КриптоПро IPsec"

Версия 1.0

ФОРМУЛЯР

ЖТЯИ.00074-01 30 01

2012

**СОДЕРЖАНИЕ**

# 1. ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр на изделие Средство криптографической защиты информации "КриптоПро IPsec", СКЗИ ЖТЯИ.00074-01, 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.00074-01 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. СКЗИ «КриптоПро IPSec» версии 1.0 функционирует на базе СКЗИ «КриптоПро CSP» версии 3.6.1 (ЖТЯИ.00050-03).

1.4. Порядок обеспечения информационной безопасности при использовании СКЗИ ЖТЯИ.00074-01 определяется руководителем эксплуатирующей организации на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ ЖТЯИ.00074-01 и ЖТЯИ.00050-03.

1.5. При эксплуатации СКЗИ ЖТЯИ.00074-01 должны использоваться сертификаты открытых ключей, выпущенные Удостоверяющим центром, сертифицированным по классу защиты не ниже класса защиты используемого СКЗИ.

1.6. При встраивании СКЗИ ЖТЯИ.00074-01 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:

- для исполнения 3 (класс защиты КС3) – во всех случаях;

- для исполнений 1 (класс защиты КС1) и 2 (класс защиты КС2) - 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.

1.7. Формуляр входит в комплект поставки СКЗИ ЖТЯИ.00074-01 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.00074-01 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. Внешняя гамма, используемая для инициализации состояния программного ДСЧ, является **конфиденциальной**.
5. Размещение СКЗИ ЖТЯИ.00074-01 в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.
6. При эксплуатации СКЗИ ЖТЯИ.00074-01 необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).
7. Инсталляция СКЗИ ЖТЯИ.00074-01 на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.
8. СКЗИ должно использоваться со средствами антивирусной защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

# 3. ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ

3.1. СКЗИ ЖТЯИ.00074-01 предназначено для защиты открытой информации в информационных системах общего пользования 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;

- генерация ключей, используемых в протоколах КриптоПро IKE, ESP;

- использование ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE и ISAKMP;

- использование комбинированного алгоритма шифрования IPsec (ESP) на основе ГОСТ 28147-89;

- обеспечение целостности IPsec (ESP) на основе ГОСТ Р 34.11-94;

- защита IP-соединений с использованием протоколов IPsec;

- аутентификация сетевых соединений с использованием ключей ЭП (сертификатов открытых ключей) либо PSK.

СКЗИ ЖТЯИ.00074-01 выпускается в трех исполнениях:

- Исполнение 1 (уровень защиты КС1);
- Исполнение 2 (уровень защиты КС2);
- Исполнение 3 (уровень защиты КС3).

3.2. СКЗИ ЖТЯИ.00074-01 функционирует в программно-аппаратных средах:

Windows XP/2003/Vista/2008/7/2008R2 (ia32, x64).

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

3.3. СКЗИ ЖТЯИ.00074-01 предназначено для эксплуатации совместно с СКЗИ КриптоПро CSP v. 3.6.1 (ЖТЯИ.00050-03).

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

3.5. 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".

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

3.7. Сетевая аутентификация реализована на базе протокола IPsec с использованием алгоритмов п.п. 3.4 -3.6.

3.8. Режимы аутентификации, шифрования и обеспечения целостности реализованы в соответствии с методическими рекомендациями, разработанными техническим комитетом по стандартизации "Криптографическая защита информации":

- Комбинированный алгоритм шифрования вложений IPsec (ESP) на основе ГОСТ 28147-89;

- Алгоритмы обеспечения целостности IPsec (ESP) на основе ГОСТ Р 34.11-94;

- Использование ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE и ISAKMP.

# 4. КОМПЛЕКТНОСТЬ

**Комплектация исполнения 1**

| Наименование | Обозначение |
|---|---|
| СКЗИ КриптоПро IPsec v.1.0. | ЖТЯИ.00074-01 99 01 |
| СКЗИ КриптоПро IPsec. Руководство администратора безопасности. | ЖТЯИ.00074-01 90 02 |
| СКЗИ КриптоПро IPsec v.1.0. Формуляр. | ЖТЯИ.00074-01 30 01 |
| СКЗИ КриптоПро CSP v.3.6.1. Формуляр. Исполнение 1. | ЖТЯИ.00050-03 30 01 |
| Сертификат СКЗИ (копия). | |

**Комплектация исполнения 2**

| Наименование | Обозначение |
|---|---|
| СКЗИ КриптоПро IPsec v.1.0. | ЖТЯИ.00074-01 99 01 |
| СКЗИ КриптоПро Ipsec. Руководство администратора безопасности. | ЖТЯИ.00074-01 90 02 |
| СКЗИ КриптоПро IPsec v.1.0. Формуляр. | ЖТЯИ.00074-01 30 01 |
| СКЗИ КриптоПро CSP v.3.6.1. Формуляр. Исполнение 2. | ЖТЯИ.00050-03 30 01 |
| Сертификат СКЗИ (копия). | |

**Комплектация исполнения 3**

| Наименование | Обозначение |
|---|---|
| СКЗИ КриптоПро IPsec v.1.0. | ЖТЯИ.00074-01 99 01 |
| СКЗИ КриптоПро IPsec. Руководство администратора безопасности. | ЖТЯИ.00074-01 90 02 |
| СКЗИ КриптоПро IPsec v.1.0. Формуляр. | ЖТЯИ.00074-01 30 01 |
| Secure Pack Rus версия 3.0. Формуляр. | ЕАРМ.5090005.032-01 30 01 |
| СКЗИ КриптоПро CSP v.3.6.1. Формуляр. Исполнение 4. | ЖТЯИ.00050-03 30 01 |
| Сертификат СКЗИ (копия). | |

**Примечания:**

1. Комплект документации предназначен администраторов, использующих СКЗИ.
2. Программное обеспечение и эксплуатационная документация поставляются 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.
3. Использование варианта исполнения СКЗИ в конкретной программно-аппаратной среде ограничивается лицензией.

# 5. АППАРАТНО-ПРОГРАММНОЕ СРЕДСТВО ЗАЩИТЫ ОТ НСД

Изделие "КриптоПро IPsec", ЖТЯИ. 00074-01, вариант исполнений 2, 3 комплектуется 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 IPSec" версии 1.0, ЖТЯИ. 00074-01,

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 IPSec" версии 1.0, ЖТЯИ. 00074-01,

серийный № дистрибутива _____

упаковано в

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

Дата упаковки: "___"_____ 20___ г.

М. П.

Упаковку произвел _____

# 8. ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)

Пользователь приобретает изделие и несет ответственность за его использование в соответствии с рекомендациями, изложенными в эксплуатационной документации.

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

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.

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".

Данные о поставке (продаже) изделия:

_____

_____

(наименование организации-поставщика (продавца) изделия)

Дата поставки: "___" _____ _____г.

М.П.

_____

(подпись)

# 9. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

127018 г. Москва, а/я КРИПТО-ПРО.

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

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.

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

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