

ЗАО «Сигнал-КОМ»

УТВЕРЖДЕН
ШКНР.00046-01 30 02-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«Крипто-КОМ 3.4»

ФОРМУЛЯР
для вариантов исполнения 42, 43

ШКНР.00046-01 30 02
Листов 21

СОДЕРЖАНИЕ

| | |
|--|----|
| 1. Общие указания..... | 3 |
| 2. Общие сведения об изделии..... | 4 |
| 3. Комплектность..... | 8 |
| 4. Основные технические данные и характеристики | 10 |
| 5. Требования к эксплуатации СКЗИ..... | 12 |
| 6. Свидетельство о приемке | 13 |
| 7. Свидетельство об упаковке | 14 |
| 8. Гарантии изготовителя (поставщика)..... | 15 |
| 9. Сведения о рекламациях..... | 16 |
| 10. Сведения о хранении..... | 18 |
| 11. Сведения о закреплении изделия при эксплуатации..... | 19 |
| 12. Сведения об изменениях..... | 20 |
| 13. Особые отметки..... | 21 |

1. ОБЩИЕ УКАЗАНИЯ

- 1.1. Перед эксплуатацией средства криптографической защиты информации (СКЗИ) «Крипто-КОМ 3.4» (далее – изделие) необходимо внимательно ознакомиться с формуляром и документами по эксплуатации СКЗИ, приведенными в разделе 3 «Комплектность».
- 1.2. Сотрудники допускаются к работе только после изучения документации (см. раздел 2 «Общие сведения об изделии»).
- 1.3. Формуляр входит в комплект поставки изделия.
- 1.4. Все записи в формуляре производятся отчетливо и аккуратно. Незаверенные исправления не допускаются.

2. ОБЩИЕ СВЕДЕНИЯ ОБ ИЗДЕЛИИ

- 2.1. Изделие: СКЗИ «Крипто-КОМ 3.4» ШКНР.00046-01.
- 2.2. Изготовитель: ЗАО «Сигнал-КОМ».
- 2.3. СКЗИ «Крипто-КОМ 3.4» предназначено для криптографической защиты открытой информации в информационных системах общего пользования (формирование/проверка электронной подписи) и обеспечения криптографической защиты конфиденциальной информации, не содержащей сведений, составляющих государственной тайны. Допускается использование СКЗИ «Крипто-КОМ 3.4» для криптографической защиты персональных данных.
- 2.4. СКЗИ «Крипто-КОМ 3.4» в вариантах исполнения 42, 43 поставляется для следующих операционных систем (при условии их поддержки производителем):
- Windows 7/8/8.1/10 (x86, x86_64);
 - Windows Server 2008/2008 R2/2012/2012 R2/2016 (x86, x86_64);
 - Linux Standard Base ISO/IEC 23360 (стандарты LSB 3.0,3.1,4.0,4.1,5.0):
 - Asianux 2, Server 3/4 (x86, x86_64)
 - ATOS LFS LC6 6 (x86)
 - Booyo 2 (x86, x86_64)
 - BOSS Linux 1/2/4 (x86, x86_64)
 - inWise 8 (x86)
 - Kylin 3 (x86, x86_64)
 - Linpus 9 (x86, x86_64)
 - Mandriva Linux 2006/2007/4/5 (x86, x86_64)
 - MontaVista Linux 5/6 (x86, x86_64)
 - NeoKylin 5/6 (x86, x86_64)
 - Open SUSE 10 (x86, x86_64)
 - Oracle Linux 4/5/6 (x86, x86_64)
 - Red Flag Linux 6 (x86)
 - Red Hat Enterprise Linux 4/5/6/7 (x86, x86_64)
 - SUSE Linux 9/10/11 (x86, x86_64)
 - Ubuntu 6/8/9 (x86, x86_64)
 - Xandros 1 (x86)
 - ALT Linux 7 (x86, x86_64);
 - Astra Linux Special Edition;
 - Cent OS 6/7 (x86, x86_64)
 - Debian 7/8 (x86, x86_64);
 - Fedora 23-25 (x86, x86_64)
 - Linux XP (x86, x86_64);
 - Mandriva Linux 2010.2 Powerpack;
 - ROSA Fresh R8/Enterprise Desktop X2/Enterprise Linux Server;
 - SUSE Linux 11/12;
 - Ubuntu 14-16 (x86, x86_64);
 - Альт Линукс СПТ 6.0;
 - РОСА КОБАЛЬТ/ХРОМ/НИКЕЛЬ 1.0 (x86, x86_64);
 - ТД ОС АИС ФССП России (GosLinux)
 - FreeBSD 9/10/11 (x86, x86_64);
 - Solaris 10/11 (x86, x86_64, SPARC).
- Примечание. В скобках указаны аппаратные платформы.
- 2.5. СКЗИ «Крипто-КОМ 3.4» в варианте исполнения 42 может использоваться в среде следующих виртуальных машин (гипервизоров):
- Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x86_64);
 - VMWare Workstation 11/12 (x86_64);
 - VMWare Player 7/12 (x86, x86_64);
 - VMWare vSphere ESXi 5.5/6.0 (x86_64);
 - Virtual Box 3.2/4.0/4.1/4.2/4.3/5.0/5.1 (x86, x86_64);
 - RHEV 3.4/3.5/3.6/4.0 (x86_64).

ШКНР.00046-01 30 02

В качестве гостевых виртуальных сред допускается использовать программно-аппаратные платформы, перечисленные в п. 2.4.

При использовании СКЗИ «Крипто-КОМ 3.4» в варианте исполнения 42 в среде виртуальных машин использование биологического датчика случайных чисел, основанного на взаимодействии оператора с компьютером, не допускается.

2.6. Порядок эксплуатации СКЗИ «Крипто-КОМ 3.4» должен проводиться в соответствии с разделом V «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

2.7. При встраивании СКЗИ «Крипто-КОМ 3.4» 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:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- при организации криптографической защиты информации 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 ФСБ России.

В рамках работ по оценке влияния необходимо проводить в том числе следующие исследования: проверку выполнения требований и рекомендаций, указанных в документации на СКЗИ; проверку неухудшения инженерно-криптографических свойств СКЗИ; проверку выполнения требований контроля целостности; анализ документации на прикладное программное обеспечение, используемое с СКЗИ; проверку соответствия пунктам 8, 9 «Требований к средствам электронной подписи»; проверку программного обеспечения BIOS ПЭВМ, на которой функционирует СКЗИ; и др.

2.8. СКЗИ «Крипто-КОМ 3.4» состоит из следующих модулей:

Таблица 1

| Код | Обозначение | Наименование |
|-----|---------------------|--|
| A1 | ШКНР.00046-01 94 01 | СКЗИ «Крипто-КОМ 3.4». Библиотека криптографических преобразований для вариантов исполнения 42, 43 (для разработчика). |
| A2 | ШКНР.00046-01 94 02 | СКЗИ «Крипто-КОМ 3.4». Библиотека криптографических преобразований для вариантов исполнения 42, 43 (для конечного пользователя). |
| A3 | ШКНР.00046-01 94 05 | СКЗИ «Крипто-КОМ 3.4». Программное обеспечение контроля целостности (утилита контроля целостности программного обеспечения). |

ШКНР.00046-01 30 02

| Код | Обозначение | Наименование |
|-----------------|---|---|
| A4 | ШКНР.00046-01 94 06 | СКЗИ «Крипто-КОМ 3.4». Утилита для удаления файлов. |
| A5 ¹ | RU.40308570.501410.001 11443195.4012-006 КБДЖ.468243-39 КБДЖ.468243.0667 | Программно-аппаратные комплексы защиты от несанкционированного доступа (НСД): - ПАК защиты от НСД «Соболь» (версии кода расширения BIOS 1.0.99, 1.0.180); - СЗИ НСД «Аккорд-АМДЗ» (версия 3.2); - АПМДЗ «Криптон-ЗАМОК/К» (изделие М-526А); - АПМДЗ «Криптон-ЗАМОК/У» (изделие М-526Б); - более поздние модификации перечисленных выше устройств или другие средства защиты от НСД, сертифицированные ФСБ России по «Требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ». |

¹ Средства защиты от НСД не входят в состав СКЗИ, но могут использоваться совместно с СКЗИ и поставляются по согласованию с Заказчиком.

ШКНР.00046-01 30 02

2.9. Комплект документации СКЗИ «Крипто-КОМ 3.4» включает следующие документы:

Таблица 2

| Код | Обозначение | Наименование |
|-----|---------------------|--|
| Д1 | ШКНР.00046-01 30 02 | СКЗИ «Крипто-КОМ 3.4». Формуляр для вариантов исполнения 42, 43. |
| Д2 | ШКНР.00046-01 31 02 | СКЗИ «Крипто-КОМ 3.4». Подсистема управления ключевой информацией для вариантов исполнения 42, 43. Общее описание. |
| Д3 | ШКНР.00046-01 33 02 | СКЗИ «Крипто-КОМ 3.4». Библиотека криптографических преобразований. Инструкция по встраиванию для вариантов исполнения 42, 43. |
| Д4 | ШКНР.00046-01 90 03 | СКЗИ «Крипто-КОМ 3.4». Правила пользования. |
| Д5 | ШКНР.00046-01 90 04 | СКЗИ «Крипто-КОМ 3.4». Параметры криптографических алгоритмов. |
| Д6 | ШКНР.00046-01 90 05 | СКЗИ «Крипто-КОМ 3.4». Программное обеспечение контроля целостности. Руководство пользователя. |
| Д7 | ШКНР.00046-01 90 06 | СКЗИ «Крипто-КОМ 3.4». Утилита для удаления файлов. Руководство пользователя. |
| КС | | Сертификат соответствия ФСБ России (копия) |

3. КОМПЛЕКТНОСТЬ

3.1. СКЗИ «Крипто-КОМ 3.4» поставляется в следующих вариантах исполнения:

Таблица 3

| Вариант исполнения | Операционные системы | Аппаратная платформа | Комплектация 1 (для разработчика) | Комплектация 2 (для конечного пользователя) | Уровень защиты |
|--------------------|---|----------------------|---|--|----------------|
| 42 | Windows | x86 | A1, A3, A4 Д1, Д2, Д3, Д4, Д5, Д6, Д7, КС | A2, A3, A4 Д1, Д2, Д4, Д6, Д7, КС | КС1 |
| 42 | Linux Standard Base ISO/IEC 23360, ALT Linux, Astra Linux, Cent OS, Debian, Fedora, Linux XP, Mandriva Linux, ROSA, SUSE, Ubuntu, Альт Линукс, POCA, GosLinux | « | « | « | « |
| 42 | Solaris | « | « | « | « |
| 42 | FreeBSD | « | « | « | « |
| 42 | Windows | x86-64 | « | « | « |
| 42 | Linux Standard Base ISO/IEC 23360, ALT Linux, Astra Linux, Cent OS, Debian, Fedora, Linux XP, Mandriva Linux, ROSA, SUSE, Ubuntu, Альт Линукс, POCA, GosLinux | « | « | « | « |
| 42 | Solaris | « | « | « | « |
| 42 | FreeBSD | « | « | « | « |
| 42 | Solaris | SPARC | « | « | « |
| 43 | Windows | x86 | A1, A3, A4, A5 Д1, Д2, Д3, Д4, Д5, Д6, Д7, КС | A2, A3, A4, A5 Д1, Д2, Д4, Д6, Д7, КС | КС2 |
| 43 | Linux Standard Base ISO/IEC 23360, ALT Linux, Astra Linux, Cent OS, Debian, Fedora, Linux XP, Mandriva Linux, ROSA, SUSE, Ubuntu, Альт Линукс, POCA, GosLinux | « | « | « | « |
| 43 | Solaris | « | « | « | « |
| 43 | FreeBSD | « | « | « | « |
| 43 | Windows | x86-64 | « | « | « |
| 43 | Linux Standard Base ISO/IEC 23360, ALT Linux, Astra Linux, Cent OS, Debian, Fedora, Linux XP, Mandriva Linux, ROSA, SUSE, Ubuntu, Альт Линукс, POCA, GosLinux | « | « | « | « |
| 43 | Solaris | « | « | « | « |
| 43 | FreeBSD | « | « | « | « |

ШКНР.00046-01 30 02

| Вариант исполнения | Операционные системы | Аппаратная платформа | Комплектация 1 (для разработчика) | Комплектация 2 (для конечного пользователя) | Уровень защиты |
|--------------------|----------------------|----------------------|--|---|----------------|
| 43 | Solaris | SPARC | A1, A3, A4, Д1, Д2, Д3, Д4, Д5, Д6, Д7, КС | A2, A3, A4, Д1, Д2, Д4, Д6, Д7, КС | « |

Примечания.

1. Расшифровка кодов A1, A2, A3, A4, A5, Д1, Д2, Д3, Д4, Д5, Д6, Д7, КС приведена в таблицах 1, 2.
2. В комплектации 2 (для конечного пользователя) СКЗИ «Крипто-КОМ 3.4» поставляется в составе приложений, библиотек более высокого уровня и т.п.
3. Документация поставляется в электронном виде в формате PDF (Adobe Acrobat). Формуляр и копия сертификата поставляются в печатном виде.
- 3.2. Подтверждение соответствия сред функционирования, в составе которых используется СКЗИ «Крипто-КОМ 3.4» в исполнениях 42, 43 требованиям к средствам ЭП, установленным частями 2 и 3 статьи 12 Федерального закона № 63-ФЗ «Об электронной подписи», должно проводиться в случае их использования для создания и проверки квалифицированных ЭП, создания ключей квалифицированных ЭП и ключей их проверки.

Указанное подтверждение соответствия необходимо проводить по ТЗ, согласованному с ФСБ России.

В случае использования СКЗИ «Крипто-КОМ 3.4» в исполнениях 42, 43 для создания и проверки простой или неквалифицированной ЭП, а также для создания ключей простой или неквалифицированной ЭП, указанная проверка не требуется, но рекомендуется.
- 3.3. При использовании СКЗИ «Крипто-КОМ 3.4» в исполнениях 42, 43 в системах автоматической обработки электронных документов для автоматического создания и (или) автоматической проверки электронных подписей, требования к средствам ЭП, установленные частями 2 и 3 статьи 12 Федерального закона № 63-ФЗ «Об электронной подписи», не применяются.

4. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ

- 4.1. Алгоритмы зашифрования/расшифрования информации и вычисления имитовставки выполнены в соответствии с требованиями ГОСТ 28147-89.
- 4.2. Алгоритм создания электронной подписи (ЭП) выполнен в соответствии с требованиями ГОСТ Р 34.10-2012.
- 4.3. Алгоритмы проверки электронной подписи (ЭП) выполнены в соответствии с требованиями ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001.
- 4.4. Алгоритмы вычисления хэш-функции выполнены в соответствии с требованиями ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94.
- 4.5. Ключевая система СКЗИ «Крипто-КОМ 3.4» 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.
- 4.6. В качестве источника случайных чисел могут использоваться следующие типы ДСЧ¹:
 - физический ДСЧ в составе ПАК защиты от НСД «Соболь», RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180), ЗАО НИП «Информзащита»;
 - физический ДСЧ в составе СЗИ НСД «Аккорд-АМДЗ» версия 3.2, 11443195.4012-006, ОКБ САПР;
 - физический ДСЧ в составе АПМДЗ «Криптон-ЗАМОК/К» (изделие М-526А), КБДЖ.468243-39, ООО «АНКАД»;
 - физический ДСЧ в составе АПМДЗ «Криптон-ЗАМОК/У» (изделие М-526Б), КБДЖ.468243.0667, ООО «АНКАД»;
 - биологический ДСЧ;
 - инициализирующая последовательность для программного ДСЧ.

Примечания.

1. Источники аппаратно-генерируемых случайных чисел могут использоваться только при наличии действующего сертификата ФСБ России.
2. При функционировании СКЗИ «Крипто-КОМ 3.4» на аппаратной платформе SPARC в качестве источника случайных чисел не может использоваться биологический ДСЧ.

¹ Перечень источников случайных чисел может изменяться и расширяться

ШКНР.00046-01 30 02

- 4.7. Для хранения ключевой информации могут быть использованы следующие типы ключевых носителей:

Таблица 4

| Тип ключевого носителя | Варианты исполнения |
|---|---------------------|
| Накопители на гибком магнитном диске (НГМД) | 42, 43 |
| Разделы накопителей на жестком магнитном диске (НЖМД) | 42, 43 |
| Сменные носители с интерфейсом USB | 42, 43 |
| Электронные ключи с интерфейсом USB (eToken, Rutoken и др.) | 42, 43 |
| Криптографические устройства, перечисленные в Таблица 5 | 42, 43 |
| Карты флэш-памяти | 42, 43 |
| Реестр Windows | 42, 43 |

Примечание. Хранение закрытых ключей в разделе жесткого диска и в реестре ОС Windows допускается только при условии распространения на ЭВМ (или съемный НЖМД ЭВМ) требований по обращению с ключевыми носителями.

- 4.8. СКЗИ «Крипто-КОМ 3.4» может обращаться через интерфейс PKCS#11 к криптографическим устройствам, реализующим функции генерации ключей, создания ЭП, проверки ЭП, хэширования, шифрования, ключевого обмена, генерации случайных последовательностей и др. Данные устройства могут также использоваться для хранения закрытых ключей в неэкспортируемом виде, исключая возможность их считывания во внешнюю память или копирование на другой носитель. СКЗИ «Крипто-КОМ 3.4» может использовать механизмы (генерация ключей, создание ЭП, проверка ЭП, хэширование, шифрование, ключевой обмен, генерация случайных последовательностей и др.), реализованные в криптографических устройствах, совместно с программной реализацией криптографических алгоритмов СКЗИ «Крипто-КОМ 3.4» (хэширование, шифрование и др.). Перечень криптографических устройств, поддерживаемых СКЗИ «Крипто-КОМ 3.4», включает:

Таблица 5

| Тип криптографического устройства | Предприятие-изготовитель |
|-----------------------------------|-------------------------------|
| РУТОКЕН ЭЦП | ЗАО «Актив-софт», ООО «АНКАД» |
| eToken ГОСТ/JaCarta ГОСТ | ЗАО «Аладдин Р.Д.» |
| ESMART Token ГОСТ | ОАО «НИИМЭ и Завод Микрон» |

Примечание. СКЗИ, реализованные с использованием устройств, перечисленных в Таблице 6, должны быть сертифицированы по требованиям ФСБ России к СКЗИ по классу КС1, КС2 или КС3.

Все остальные носители должны использоваться только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене.

- 4.9. Контроль целостности программного обеспечения СКЗИ «Крипто-КОМ 3.4» обеспечивается с помощью утилиты контроля целостности из состава СКЗИ или с помощью программно-аппаратных средств защиты от НСД.

5. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ СКЗИ

- 5.1. Средствами СКЗИ не допускается обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

Допускается использование СКЗИ для криптографической защиты персональных данных.

- 5.2. Ключевая информация является конфиденциальной.
- 5.3. СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.
- 5.4. Размещение СКЗИ в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.
- 5.5. В случае, если в модели угроз, которым должно противостоять СКЗИ 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). При подключении ПЭВМ с установленным СКЗИ к каналам связи, выходящим за пределы контролируемой территории, защита канала связи должна обеспечиваться применением оптических развязывающих устройств.
- 5.6. Установка СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

ШКНР.00046-01 30 02

6. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие СКЗИ «Крипто-КОМ 3.4» ШКНР.00046-01 соответствует эталону, хранящемуся в ЗАО «Сигнал-КОМ» и признано годным для эксплуатации.

Дата выпуска: " _____ " _____ 20____ г.

М.П.

(должность)

(подпись)

ШКНР.00046-01 30 02

7. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие СКЗИ «Крипто-КОМ 3.4» ШКНР.00046-01

Вариант исполнения № _____ Комплектация № _____

Операционная система _____

Аппаратная платформа _____

Регистрационный № дистрибутива _____

Вид носителя:

☐ DVD-ROM _____ шт.☐ CD-ROM _____ шт.☐ дискеты 3.5" (ГМД) _____ шт.☐

Упаковано в

☐ бумажный конверт☐ коробку☐☐ _____

Носители ПО снабжены этикетками, идентифицирующими их принадлежность к изделию.

Дата упаковки: " _____ " _____ 20 ____ г.

М. П.

Упаковку произвел _____

(подпись)

8. ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)

- 8.1. Пользователь приобретает изделие СКЗИ «Крипто-КОМ 3.4» и несет ответственность за его использование в соответствии с рекомендациями, изложенными в эксплуатационной документации.
- 8.2. Предприятие-изготовитель гарантирует работоспособность изделия в соответствии с объявленными характеристиками при соблюдении пользователем требований эксплуатационной документации на изделие.
- 8.3. В случае выявления в изделии дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения, изделие подлежит рекламации, и 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 во всех остальных экземплярах изделия.
- 8.4. Гарантийный срок изделия — 12 (двенадцать) месяцев. Гарантийный срок на программно-аппаратный комплекс защиты от НСД определяется их изготовителями.
- 8.5. Начальной датой исчисления гарантийного срока изделия является дата поставки изделия (см. 8.7).
- 8.6. Действие гарантийных обязательств прекращается при истечении гарантийного срока.
- 8.7. Данные о поставке (продаже) изделия:

ЗАО «Сигнал-КОМ»

наименование организации-поставщика (продавца) изделия

Дата поставки: " _____ " _____ 20____ г.

М.П.

(подпись)

Примечание. При отсутствии данных, приведенных в п. 8.7, датой поставки изделия считается дата выпуска, указанная в разд. 6 «Свидетельство о приемке».

9. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

- 9.1. Рекламации, связанные с эксплуатацией изделия, должны направляться предприятию-изготовителю в письменном виде по адресу:
Россия, г. Москва, 115193, Москва, а/я 6.
Срок рассмотрения рекламации — 1 (один) месяц со дня получения.
- 9.2. Рекламации, связанные с эксплуатацией программно-аппаратного комплекса защиты от НСД и УКЗД, должны направляться их изготовителям.
- 9.3. При несоответствии поставляемого изделия, его тары, упаковки, консервации, маркировки и комплектности требованиям сопроводительной документации, пользователь обязан направить рекламацию предприятию-изготовителю в течение 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 представлены в Таблица 6

Таблица 6

| Дата | Содержание рекламации | Меры, принятые по рекламации | Должность, фамилия и подпись отв. Лица |
|------|-----------------------|------------------------------|---|
| | | | |

10. СВЕДЕНИЯ О ХРАНЕНИИ**Таблица 7**

| Должность, фамилия и подпись отв. Лица | | | | | | | | |
|---|--|--|--|--|--|--|--|--|
| Условия хранения | | | | | | | | |
| Дата снятия с хранения | | | | | | | | |
| Дата установки на хранение | | | | | | | | |

11. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ**Таблица 8**

| Должность ответственного лица | Фамилия ответственного лица | Номер и дата приказа о назна- чении | Номер и дата приказа об освобождении | Подпись ответственного лица |
|-------------------------------------|-----------------------------------|---|--|-----------------------------------|
| | | | | |

12. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

Таблица 9

| № п/п | Дата проведения изменения | Дата утверждения изменения (вх № сопр. документа и дата) | Содержание изменения | Должность, фамилия и подпись лица, ответственного за изменения | Подпись лица, ответственного за эксплуатацию изделия |
|-------|---------------------------|--|----------------------|--|--|
| | | | | | |

ШКНР.00046-01 30 02

13. ОСОБЫЕ ОТМЕТКИ