ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«КРИПТОКОМ»

УТВЕРЖДЕН
СЕИУ.00009-04 30 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «МагПро КриптоПакет» версия 3.0

ФОРМУЛЯР

СЕИУ.00009-04 30
Страниц 16

КОМПЛЕКТ 247ЖБ – _____

2017

СОДЕРЖАНИЕ

1 ОБЩИЕ УКАЗАНИЯ

1.1 Перед установкой и применением средства криптографической защиты информации (СКЗИ) «МагПро КриптоПакет» версии 3.0 необходимо внимательно ознакомиться с формуляром, документами по эксплуатации СКЗИ и правилами пользования.

Установка СКЗИ производится только в соответствии с указаниями, приведенными в документации на СКЗИ, с дистрибутивного носителя. Сведения об установке программных и аппаратно-программных средств СКЗИ заносятся в паспорта (формуляры) соответствующих рабочих мест с установленными средствами СКЗИ.

1.2 СКЗИ подлежит поэкземплярному учету.

1.3 Эксплуатация СКЗИ разрешается только на территории Российской Федерации.

1.4 К эксплуатации и сопровождению СКЗИ допускаются специалисты, изучившие эксплуатационные документы данного СКЗИ.

В случае нарушений при обеспечении безопасности информации виновные лица должны привлекаться к ответственности в соответствии с требованиями эксплуатирующей организации.

1.5 Формуляр входит в комплект поставки СКЗИ.

1.6 Формуляр должен находиться в подразделении организации, ответственном за эксплуатацию СКЗИ.

1.7 В формуляр заносятся сведения о состоянии СКЗИ в течение всего периода его эксплуатации.

1.8 Записи в формуляре необходимо производить чернилами или пастой черного, фиолетового или синего цвета. Записи должны быть заверены подписью ответственного лица. Подчистки в записях не допускаются.

2 ОБЩИЕ СВЕДЕНИЯ ОБ ИЗДЕЛИИ

2.1 Изделие «Средство криптографической защиты информации "МагПро КриптоПакет" версия 3.0» - СЕИУ.00009-04.

2.2 Изготовитель: ООО «Криптоком».

2.3 СКЗИ «МагПро КриптоПакет» версии 3.0 предназначено для защиты информационного обмена между абонентами сети конфиденциальной связи по протоколам TLS и S/MIME, а также организации виртуальных частных сетей (VPN). СКЗИ предназначено для использования как на серверах, так и на рабочих станциях. СКЗИ не предназначено для защиты речевой информации.

2.4 СКЗИ «МагПро КриптоПакет» версии 3.0 реализует следующие функции:

- создание и проверка электронной подписи в соответствии с ГОСТ Р 34.10 для файлов и данных, содержащихся в областях оперативной памяти;
- зашифрование и расшифрование в соответствии с ГОСТ 28147-89 файлов и данных, содержащихся в областях оперативной памяти;

- имитозащита в соответствии с ГОСТ 28147-89 и HMAC на основе ГОСТ Р 34.11-2012 файлов и данных, содержащихся в областях оперативной памяти;
- вычисления ключа парной связи по алгоритму VKO с использованием как долговременных, так и эфемерных пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10;
- вычисления значения хэш-функции в соответствии с ГОСТ Р 34.11 для файлов и данных, содержащихся в областях оперативной памяти;
- выработки случайного числа заданной длины;
- создания закрытых ключей и ключей электронной подписи;
- вычисления открытых ключей и ключей проверки подписи в соответствии с ГОСТ Р 34.10;
- формирования производного сеансового ключа;
- импорт криптографических ключей в СКЗИ и их экспорт из СКЗИ;
- реализации протокола TLS с использованием российских криптоалгоритмов.

2.5 СКЗИ «МагПро КриптоПакет» версии 3.0 исполнения 3 – 8 являются функционально законченными СКЗИ, исполнения 1, 2 предназначены для построения функционально законченных СКЗИ.

3 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1 Средство криптографической защиты информации «МагПро КриптоПакет" версия 3.0 функционирует на ПЭВМ на базе центральных процессоров Intel и совместимых с ними (архитектура x86 и x86_64), процессоров ARMv5,6,7,8 и на ПЭВМ Sun Microsystems (архитектура Ultra SPARC).

3.2 Средство криптографической защиты информации «МагПро КриптоПакет» версия 3.0 функционирует в средах операционных систем Windows 7 SP1/8.1/10; Windows Server 2008R2 SP1/2012/2012R2/2016; Debian GNU/Linux 7(wheezy) / 8(jessie) / stretch; Ubuntu 14.04, 16.04; Linux Mint 17.x, 18.x, Linux Mint Debian Edition 2; Red Hat Enterprise Linux 6, 7; CentOS 6, 7; SUSE Linux 11, 12; OpenSUSE 42.2, 42.3; OS EMIAS 1.0; Альт Линукс 6, 7, 8; МСВСфера Сервер 6.3, МСВСфера АРМ 6.3; Атликс 3.1; Rosa Enterprise Desktop (RED) X2, X3; Rosa Enterprise Linux Server (RELS) 6, 7; РОСА КОБАЛЬТ 1.0; Astra Linux Special Edition РУСБ.10015-07; Гослинукс IC4; FreeBSD 10.x, 11.x; Oracle Solaris 10, 11; MacOS 10.12. Срок использования СКЗИ на конкретной операционной системе не должен превышать срок поддержки этой операционной системы производителем.

3.3 Средство криптографической защиты информации «МагПро КриптоПакет» версия 3.0 поддерживает использование аппаратных устройств «Аккорд», «Соболь», «АПМДЗ-И/М2» и «Вьюга» в качестве датчиков случайных чисел и ключевых носителей в тех операционных системах, для которых производителями этих устройств поставляются драйвера.

3.4 Для обеспечения защиты от несанкционированного доступа СКЗИ «МагПро КриптоПакет" версия 3.0 исполнение 1, 3, 5, 7 рекомендуется эксплуатировать совместно с аппаратно-программными модулями доверенной загрузки, имеющими действующий сертификат ФСБ России, а СКЗИ «МагПро КриптоПакет" версия 3.0

исполнение 2, 4, 6, 8 должны эксплуатироваться совместно с аппаратно-программными модулями доверенной загрузки, имеющими действующий сертификат ФСБ России.

3.5 Совместно с СКЗИ должны использоваться сертифицированные ФСБ России или ФСТЭК России средства антивирусной защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

3.6 Алгоритмы шифрования и расшифровывания соответствуют ГОСТ 28147-89, алгоритмы имитозащиты соответствуют ГОСТ 28147-89 и HMAC на основе ГОСТ Р 34.11-2012, алгоритмы вычисления хэш-функции соответствуют ГОСТ Р 34.11-94/2012, алгоритмы создания и проверки ЭП соответствуют ГОСТ Р 34.10-2001/2012.

3.7 Допустимый срок действия ключей шифрования и ключей ЭП – не более 1 года 3 месяцев, ключей проверки ЭП – не более 15 лет после окончания срока действия соответствующих ключей ЭП.

3.8 Средство криптографической защиты информации «МагПро КриптоПакет" версия 3.0 соответствует «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню КС1 (для исполнений 1, 3, 5, 7) и КС2 (для исполнений 2, 4, 6, 8), а также «Требованиям к средствам электронной подписи» по уровню КС1 (для исполнении 1, 3, 5) и КС2 (для исполнений 2, 4, 6) при выработке и проверке подписи в автоматическом режиме.

В то же время исполнение 1 и 2 могут быть использованы только для построения на их основе функционально законченных СКЗИ.

4 КОМПЛЕКТНОСТЬ

4.1 Общий состав изделия:

Код	Обозначение	Наименование
Программные модули		
А1	СЕИУ.00009-04 12	Библиотека реализации алгоритмов ГОСТ libcryptocom
А2	СЕИУ.00009-04 12 01	Библиотека libcrypto
А3	СЕИУ.00009-04 12 02	Библиотека libssl
А4	СЕИУ.00009-04 12 03	Утилита openssl
А5	СЕИУ.00001-04 12 05	Средство контроля целостности СКЗИ и СФК Integrity
А6	СЕИУ.00001-04 12 06	Программа генерации ключей mkkey
А7	СЕИУ.00001-04 12 07	Средство защиты доступа к сетевым ресурсам «КриптоТуннель»
А9	СЕИУ.00001-04 12 09	Виртуальная частная сеть «OpenVPN-ГОСТ»
А10	СЕИУ.00001-04 12 10	Программа генерации файла инициализации программного ДСЧ mkseed
Аппаратно-программные модули		
М0*	зависит от выбранного модуля	Аппаратно-программный модуль доверенной загрузки, имеющий действующий сертификат ФСБ России *
Документация		
Д0	СЕИУ.00009-04 31	Описание применения.
Д2	СЕИУ.00009-04 33 01	Библиотека libcrypto. Руководство программиста
Д3	СЕИУ.00009-04 33 02	Библиотека libssl. Руководство программиста
Д4	СЕИУ.00009-04 34 03	Утилита openssl. Руководство по использованию
Д5	СЕИУ.00001-04 34 05	Средство контроля целостности СКЗИ и СФК Integrity. Руководство по использованию
Д6	СЕИУ.00001-04 34 06	Программа генерации ключей mkkey. Руководство по использованию
Д7	СЕИУ.00001-04 34 07	Средство защиты доступа к сетевым ресурсам «КриптоТуннель». Руководство по использованию
Д9	СЕИУ.00001-04 32 09	Виртуальная частная сеть «OpenVPN-ГОСТ». Руководство по использованию
Д10	СЕИУ.00001-04 34 10	Программа генерации файла инициализации программного ДСЧ mkseed. Руководство по использованию
П1	СЕИУ.00009-04 94	Правила пользования

* АПМДЗ в комплект поставки не входит и приобретается отдельно.

4.2 Исполнения изделия:

Исполнение № 1

А1	А2	А3		А5				Д0	
	Д2	Д3		Д5				П1	

Исполнение № 2

А1	А2	А3		А5				Д0	М0*
	Д2	Д3		Д5				П1	

* АПМД3 в комплект поставки не входит и приобретается отдельно.

Исполнение № 3

А1	А2	А3	А4	А5	А6		А10	Д0	
			Д4	Д5	Д6		Д10	П1	

Исполнение № 4

А1	А2	А3	А4	А5	А6		А10	Д0	М0*
			Д4	Д5	Д6		Д10	П1	

* АПМД3 в комплект поставки не входит и приобретается отдельно.

Исполнение № 5

А1	А2	А3	А4	А5	А6	А7	А10	Д0	
			Д4	Д5	Д6	Д7	Д10	П1	

Исполнение № 6

А1	А2	А3	А4	А5	А6	А7	А10	Д0	М0*
			Д4	Д5	Д6	Д7	Д10	П1	

* АПМД3 в комплект поставки не входит и приобретается отдельно.

Исполнение № 7

А1	А2	А3	А4	А5	А6	А9	А10	Д0	
			Д4	Д5	Д6	Д9	Д10	П1	

Исполнение № 8

А1	А2	А3	А4	А5	А6	А9	А10	Д0	М0*
			Д4	Д5	Д6	Д9	Д10	П1	

* АПМД3 в комплект поставки не входит и приобретается отдельно.

4.3 Содержание поставляемых электронных носителей:

Файлы дистрибутива:		
Имя файла	**Объем файла (байт)**	**Контрольная сумма файла**

Программные модули:		
Имя файла	**Объем файла (байт)**	**Контрольная сумма файла**

Документация:		
Имя файла	**Тип файла**	
opisanie_primeneniya	pdf	
libcrypto	pdf	
libssl	pdf	
openssl	pdf	
mkkey	pdf	
mkseed	pdf	
openvpn	pdf	
tunnel	pdf	
integrity	pdf	
rules	pdf	

5 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие «Средство криптографической защиты информации “МагПро КриптоПакет” версия 3.0»

учетный индекс Н-24Б

учетный номер дистрибутива 247ЖБ – _____

исполнение _____

вид носителя: _____

соответствует эталону, хранящемуся в ООО "Криптоком", и признано годным к эксплуатации.

Дата выпуска: _____

М.П.

_____ /_____ /

6 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие «Средство криптографической защиты информации “МагПро КриптоПакет” версия 3.0»

учетный индекс Н-24Б

учетный номер дистрибутива 247ЖБ – _____

исполнение _____

вид носителя: _____

упаковано в

* бумажный конверт ___
* коробку ___.

Носители снабжены этикетками, идентифицирующими принадлежность к изделию.

Дата упаковки: _____

М.П. Упаковку произвел _____ /_____ /
(подпись)

7 ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)

7.1 Предприятие - изготовитель гарантирует работоспособность изделия в соответствии с объявленными характеристиками при соблюдении пользователем требований эксплуатационных документов на изделие.

7.2 Гарантийный срок изделия - 12 (двенадцать) месяцев.

7.3 Начальной датой исчисления гарантийного срока изделия является дата продажи изделия.

7.4 Действие гарантийных обязательств прекращается при истечении гарантийного срока, либо при нарушении пользователем в течение гарантийного срока правил транспортировки, хранения и эксплуатации изделия, которые привели к появлению дефектов в изделии.

7.5 В случае выявления в течение гарантийного срока в изделии дефектов, не связанных с нарушением пользователем правил эксплуатации, транспортирования и хранения, изделие подлежит рекламации и предприятие - изготовитель обязуется при получении рекламации устранить дефекты своими силами и средствами вплоть до поставки нового изделия.

7.6 Дефекты, возникшие в изделии при хранении и транспортировке изделия по вине изготовителя (поставщика), предприятие - изготовитель также обязуется устранить своими силами и средствами вплоть до поставки другого изделия.

8 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

117218, г. Москва, а/я 28, ООО "Криптоком".

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

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

8.4 При несоответствии поставляемого изделия, его тары, упаковки, маркировки и комплектности сопроводительным документам, пользователь имеет право направить рекламацию в письменном виде предприятию - изготовителю в течение 60 (шестидесяти) дней со дня поставки изделия.

8.5 Сведения о предъявленных рекламациях должны заноситься в таблицу.

Дата	Содержание рекламации	Меры, принятые по рекламации	Должность, фамилия и подпись ответственного лица

9 СВЕДЕНИЯ О ХРАНЕНИИ

Дата установки на хранение	Дата снятия с хранения	Условия хранения	Должность, фамилия и подпись ответственного лица

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

11. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

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

12. ОСОБЫЕ ОТМЕТКИ