

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ  
«КРИПТОКОМ»

УТВЕРЖДЕН  
СЕИУ.00009-05 30 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ  
«MagPro КриптоПакет» версия 4.0

ФОРМУЛЯР

СЕИУ.00009-05 30  
Страниц 18

КОМПЛЕКТ **247ЖВ**– \_\_\_\_\_

[ Информация о количестве разрешённых установок ]

**СОДЕРЖАНИЕ**

1 ОБЩИЕ УКАЗАНИЯ .....	3
2 ОБЩИЕ СВЕДЕНИЯ ОБ ИЗДЕЛИИ .....	3
3 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ.....	4
4 КОМПЛЕКТНОСТЬ .....	6
5 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ.....	10
6 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ .....	11
7 ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА) .....	12
8 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ .....	13
9 СВЕДЕНИЯ О ХРАНЕНИИ .....	14
10. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ.....	16
11. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ .....	17
12. ОСОБЫЕ ОТМЕТКИ .....	18

## 1 ОБЩИЕ УКАЗАНИЯ

1.1 Перед установкой и применением средства криптографической защиты информации (СКЗИ) «MagПро КриптоПакет» версии 4.0 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 "MagПро КриптоПакет" версия 4.0» - СЕИУ.00009-05.

2.2 Изготовитель: ООО «Криптоком».

2.3 СКЗИ «MagПро КриптоПакет» версии 4.0 предназначено для защиты информационного обмена между абонентами сети конфиденциальной связи по протоколам TLS и CMS, а также организации виртуальных частных сетей (VPN). СКЗИ предназначено для использования как на серверах, так и на клиентских рабочих местах.

2.4 СКЗИ «MagПро КриптоПакет» версии 4.0 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 соответствием с ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 и ГОСТ 28147-89 (только для взаимодействия с

- ПО, не поддерживающим ГОСТ Р 34.12-2015) файлов и данных, содержащихся в областях оперативной памяти;
- имитозащита в соответствии с ГОСТ Р 34.13-2015, HMAC на основе ГОСТ Р 34.11-2012, а также ГОСТ 28147-89 (только для взаимодействия с ПО, не поддерживающим ГОСТ Р 34.13-2015) файлов и данных, содержащихся в областях оперативной памяти;
  - вычисления ключа парной связи по алгоритму VKO с использованием как эфемерных, так и долговременных 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 в соответствии с рекомендациями ТК26.

2.5 СКЗИ «МагПро КриптоПакет» версии 4.0 исполнения 3 – 8 являются функционально законченными СКЗИ, исполнения 1, 2 предназначены для построения функционально законченных СКЗИ.

### **3 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ**

3.1 СКЗИ должно функционировать на ПЭВМ на базе центральных процессоров Intel и совместимых с ними (архитектура x86 и x86\_64), процессоров семейства ARM (Advanced RISC Machine), а также на ПЭВМ Sun Microsystems.

3.2 Средство криптографической защиты информации «МагПро КриптоПакет» версия 4.0 функционирует в средах операционных систем:

Windows 8.1 / 10, Windows Server 2012 / 2016 / 2019;

Debian GNU/Linux 9(stretch) / 10(buster) / 11(bullseye);

Ubuntu 14.04, 16.04, 18.04, 20.04;

Linux Mint 19.x, 20.x, Linux Mint Debian Edition 4;

RedHat Enterprise Linux 7, 8;

CentOS 7, 8;

SUSE Linux 12, 15;

OpenSUSE 15.1, 15.2;

OS EMIAS 1.0;

Дистрибутивы Альт на базе платформ 8 и 9, включая Альт Сервер,

Альт Рабочая станция, Альт Рабочая станция К,

Альт Образование, Альт 8 СП, Simply Linux

MCBCсфера Сервер 7.3, MCBCсфера АРМ 7.3;

Гослинукс IC6;

РЕД ОС 7.2, 7.3;

Rosa Enterprise Desktop (RED) X4;

Rosa Enterprise Linux Server (RELS) 7.3;

Rosa Enterprise Linux Desktop (RELD) 7.3;

РОСА КОБАЛЬТ;

Astra Linux Special Edition Смоленск 1.6 aka исп.1, 1.7;

Astra Linux Special Edition Новороссийск;

Astra Linux Common Edition 2.12;

Numa Edge 1.0;

FreeBSD 12.x, 13.x;

macOS 10.15, 11;

Sun Solaris 10, 11;

OpenWRT 19.07, 21.02.

3.3 Средство криптографической защиты информации «МагПро КриптоПакет» версия 4.0 поддерживает использование в качестве датчиков случайных чисел и ключевых носителей аппаратных устройств «Аккорд», «Соболь» и «Вьюга», а также сертифицированных устройств с интерфейсом PKCS#11 («Рутокен ЭЦП», «JaCarta» и др.) в тех операционных системах, для которых производителями этих устройств поставляются драйверы.

3.4 Для обеспечения защиты от несанкционированного доступа СКЗИ «МагПро КриптоПакет» версия 4.0 исполнение 2, 4, 6, 8 должны эксплуатироваться совместно либо с аппаратно-программными модулями доверенной загрузки, либо с 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 Р 34.12/13-2015 и ГОСТ 28147-89, алгоритмы имитозащиты соответствуют ГОСТ Р 34.12/13-2015, ГОСТ 28147-89 и НМАС 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 4.0 удовлетворяет «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), «Специальным требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу КС, 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.

## 4 КОМПЛЕКТНОСТЬ

### 4.1 Общий состав изделия:

Код	Обозначение	Наименование
<b>Программные модули</b>		
A1	СЕИУ.00009-05 12	Библиотека реализации алгоритмов ГОСТ libcryptocom
A2	СЕИУ.00009-05 12 01	Библиотека libcrypto
A3	СЕИУ.00009-05 12 02	Библиотека libssl
A4	СЕИУ.00009-05 12 03	Утилита openssl
A5	СЕИУ.00009-05 12 05	Средство контроля целостности СКЗИ и СФК integrity
A7	СЕИУ.00009-05 12 07	Средство защиты доступа к сетевым ресурсам «КриптоТуннель»
A9	СЕИУ.00009-05 12 09	Виртуальная частная сеть «OpenVPN-ГОСТ»
A10	СЕИУ.00009-05 12 10	Программа генерации файла инициализации программного ДСЧ mkseed
A11	СЕИУ.00009-05 12 11	Программа генерации файла инициализации программного ДСЧ gmkseed
A12	СЕИУ.00009-05 12 12	Утилита curl
<b>Аппаратно-программные модули доверенной загрузки (модули доверенной загрузки)</b>		
M0*	зависит от выбранного модуля	Аппаратно-программный модуль доверенной загрузки (модуль доверенной загрузки), имеющий действующий сертификат ФСБ России *

Код	Обозначение	Наименование
<b>Документация</b>		
Д0	СЕИУ.00009-05 31	Описание применения.
Д2	СЕИУ.00009-05 33 01	Библиотека libcrypto. Руководство программиста
Д3	СЕИУ.00009-05 33 02	Библиотека libssl. Руководство программиста
Д4	СЕИУ.00009-05 34 03	Утилита openssl. Руководство по использованию
Д5	СЕИУ.00009-05 34 05	Средство контроля целостности СКЗИ и СФК integrity. Руководство по использованию
Д7	СЕИУ.00009-05 34 07	Средство защиты доступа к сетевым ресурсам «КриптоТуннель». Руководство по использованию
Д9	СЕИУ.00009-05 32 09	Виртуальная частная сеть «OpenVPN-ГОСТ». Руководство по использованию
Д10	СЕИУ.00009-05 34 10	Программа генерации файла инициализации программного ДСЧ mkseed. Руководство по использованию
Д11	СЕИУ.00009-05 34 11	Программа генерации файла инициализации программного ДСЧ gmseed. Руководство по использованию
Д12	СЕИУ.00009-05 34 12	Утилита curl. Руководство по использованию
П1	СЕИУ.00009-05 94	Правила пользования

\* АПМДЗ (МДЗ) в комплект поставки не входит и приобретается отдельно.

4.2 Исполнения изделия:

**Исполнение № 1**

A1	A2	A3		A5		A10	A11		Д0	
	Д2	Д3		Д5		Д10	Д11		П1	

**Исполнение № 2**

A1	A2	A3		A5		A10	A11		Д0	M0*
	Д2	Д3		Д5		Д10	Д11		П1	

\* АПМДЗ (МДЗ) в комплект поставки не входит и приобретается отдельно.

**Исполнение № 3**

A1	A2	A3	A4	A5		A10	A11	A12	Д0	
			Д4	Д5		Д10	Д11	Д12	П1	

**Исполнение № 4**

A1	A2	A3	A4	A5		A10	A11	A12	Д0	M0*
			Д4	Д5		Д10	Д11	Д12	П1	

\* АПМДЗ (МДЗ) в комплект поставки не входит и приобретается отдельно.

**Исполнение № 5**

A1	A2	A3	A4	A5	A7	A10	A11	A12	Д0	
			Д4	Д5	Д7	Д10	Д11	Д12	П1	

**Исполнение № 6**

A1	A2	A3	A4	A5	A7	A10	A11	A12	Д0	M0*
			Д4	Д5	Д7	Д10	Д11	Д12	П1	

\* АПМДЗ (МДЗ) в комплект поставки не входит и приобретается отдельно.

**Исполнение № 7**

A1	A2	A3	A4	A5	A9	A10	A11	A12	Д0	
			Д4	Д5	Д9	Д10	Д11	Д12	П1	

**Исполнение № 8**

A1	A2	A3	A4	A5	A9	A10	A11	A12	Д0	M0*
			Д4	Д5	Д9	Д10	Д11	Д12	П1	

\* АПМДЗ (МДЗ) в комплект поставки не входит и приобретается отдельно.

4.3 Содержание поставляемых электронных носителей:

<b>Файлы дистрибутива:</b>	
Имя файла	Контрольная сумма файла
<b>Программные модули:</b>	
/opt/openvpn-gost/sbin/openvpn	
/opt/stunnel-gost/bin/stunnel	
/opt/cryptopack4/bin/openssl	
/opt/cryptopack4/bin/curl	
/opt/cryptopack4/bin/mkseed	
/opt/cryptopack4/bin/gmkseed	
/opt/cryptopack4/lib/libcrypto.so.1.1	
/opt/cryptopack4/lib/libssl.so.1.1	
/opt/cryptopack4/lib/libcurl.so.4.7.0	
/opt/cryptopack4/lib/libidn2.so.0	
/opt/cryptopack4/lib/libunistring.so.2	
/opt/cryptopack4/lib/engines-1.1/libcryptocom.so	
/opt/cryptopack4/lib/engines-1.1/generic/libcryptocom.so	

<b>Документация:</b>		
Имя файла	Тип файла	Описание
rules	pdf	Правила пользования
opisanie_primeneniya	pdf	Описание применения
openvpn	pdf	OpenVPN-ГОСТ
tunnel	pdf	КриптоТуннель
openssl	pdf	Утилита openssl
curl	pdf	Утилита curl
mkseed	pdf	Программа клавиатурной инициализации ДСЧ
gmkseed	pdf	Программа графической инициализации ДСЧ
integrity	pdf	Средство контроля целостности

## 5 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие «Средство криптографической защиты информации “МагПро КryptoПакет” версия 4.0»

учетный индекс **H-24B**

учетный номер дистрибутива **247ЖВ** – \_\_\_\_\_

исполнение \_\_\_\_\_

вид носителя: \_\_\_\_\_ 1 шт.

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

[ Информация о количестве разрешённых установок ]

Дата выпуска: \_\_\_\_\_

М.П.

\_\_\_\_\_ / \_\_\_\_\_

## 6 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Изделие «Средство криптографической защиты информации “МагПро КriptoПакет” версия 4.0»

учетный индекс **H-24B**

учетный номер дистрибутива **247ЖВ** — \_\_\_\_\_

исполнение \_\_\_\_\_

вид носителя: \_\_\_\_\_ 1 шт.

упаковано в

\* бумажный конверт \_\_\_\_\_

\* коробку \_\_\_\_\_

Носители снабжены этикетками, идентифицирующими принадлежность к изделию.

[ Информация о количестве разрешённых установок ]

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.









**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**