

АО «Лаборатория Касперского»

УТВЕРЖДЕН

643.46856491.00085-03 30 01-ЛУ

Программное изделие

KASPERSKY SECURE MAIL GATEWAY

Формуляр

643.46856491.00085-03 30 01

Листов 14

Инв. N подл.	Подп. и дата	Взам. инв. N	Инв. N дубл.	Подп. и дата

2019

Литера

## СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ .....	3
2. ОБЩИЕ СВЕДЕНИЯ.....	3
3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ .....	3
4. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ .....	4
5. КОМПЛЕКТНОСТЬ .....	6
6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ.....	6
7. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ	8
8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ.....	9
9. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ .....	9
10. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА .....	10
11. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ.....	10
12. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА .....	10
13. СВЕДЕНИЯ О ХРАНЕНИИ.....	11
14. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ .....	11
15. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ.....	12
16. ПОЛУЧЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭЛЕКТРОННОЙ ПОСТАВКЕ.....	13
17. ОБНОВЛЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ .....	13
18. ОСОБЫЕ ОТМЕТКИ.....	14

## 1. ОБЩИЕ УКАЗАНИЯ

- 1.1. Настоящий формуляр удостоверяет комплектность, гарантированное изготовителем качество программного изделия и содержит указания по его эксплуатации.
- 1.2. Программное изделие может поставляться в виде физического медиапака (физическая поставка) либо в электронном виде по сетям передачи данных (электронная поставка).
- 1.3. Перед эксплуатацией необходимо ознакомиться с документацией к программному изделию, перечисленной в разделе «Комплектность».
- 1.4. При электронной поставке программного изделия лицо, ответственное за эксплуатацию программного изделия, распечатывает твердую копию формуляра и производит необходимые записи в разделах.
- 1.5. Формуляр должен находиться в подразделении, ответственном за эксплуатацию программного изделия.
- 1.6. Все записи в формуляре производят только чернилами, отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления не допускаются.

## 2. ОБЩИЕ СВЕДЕНИЯ

- 2.1. Сведения о программном изделии:

Наименование: «Kaspersky Secure Mail Gateway»

Версия: 1.1.2.30

Обозначение: 643.46856491.00085-03

Дата изготовления (заполняется при физической поставке): \_\_\_\_\_

Наименование изготовителя: АО «Лаборатория Касперского»

Адрес: 125212, г. Москва, Ленинградское ш., 39А, стр. 2, тел. (495) 797-8700.

Серийный номер (заполняется при физической поставке): \_\_\_\_\_

Тип носителя (при физической поставке): лазерный диск.

- 2.2. Сведения о применимых сертификатах соответствия и лицензиях:

Наименование и номер сертификата	Срок начала действия	Срок окончания действия	Знак соответствия (заполняется при физической поставке)

- 2.3. Программное изделие является средством антивирусной защиты и предназначено для защиты от вредоносных компьютерных программ, в том числе в системах обработки данных и государственных информационных системах.
- 2.4. В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, введенными в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г., и Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, введенными в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г., программное изделие может использоваться в информационных системах 1 и 2 класса защищенности и для обеспечения защищенности персональных данных до 1 уровня включительно.

## 3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- 3.1. Контрольные суммы файлов инсталляционного комплекта программного изделия приведены в настоящем формуляре в таблице 1.
- 3.2. Контрольные суммы исполняемых файлов программного изделия после установки приведены в Приложении 1 к настоящему формуляру.

*Таблица 1 – Контрольные суммы файлов инсталляционного комплекта программного изделия*

№ пп	Имя файла	КС
<b>Каталог F:\</b>		
1	klcfginst.msi	1edc909de849460d7667e62bdee1d75f7739da4674f9056dc027ac71f56f98cf
2	klms-1.1.2-30.i386.rpm	e7e91a68504bbf180d342dcd39d3a73541f0f1bf6a23ce098304cc6549410bfe
3	klms-appliance-1.1.2-30.i386.rpm	22f0b77d677c2e5bf559a3b5c516fad314b647697af3222a76f203357e855985
4	klms_de-1.1.2-30.noarch.rpm	0a1df9d637ba5ac2c453d5a7dd7aeb985d6fcedb72285c63b608e1399fb4ca80
5	klms_fr-1.1.2-30.noarch.rpm	ac0712d936ad2ec44e832bad8f3eee33b3526b8f133a569c5ab652982344c16a
6	klms_ru-1.1.2-30.noarch.rpm	b8c6a402d642fa2ea7d4b56c03267ae06dc00f07a5704268f4e0101b4dff5bdf
7	klms_zh-CN-1.1.2-30.noarch.rpm	9e733a5e8116ae5fb940067247fd357c2ddb51c5a3a834d01c406c2d87c416d9
8	klms_zh-TW-1.1.2-30.noarch.rpm	d8de4175e08e19458f409d426239bf7a38a9c8f5f7066bbdd19a3939f13ea546
9	klmsui-1.1.2-30.appliance.x86_64.rpm	2adb3d9001d462ac25d1fd9656da15b75143fb61b1572632f27dcfd42cea2371
10	klmagent-10.1.1-48.i386.rpm	897d1e75a6da5c983e66d9676b21e7f2c844ab53e306b4512dfcfd013cfab6ca
11	ram-0.4.4-6.noarch.rpm	eead6f2fdced8b931d6345d31c6753f3c4a7dc5d7a97aea98224ef5b20f3a0d
<b>итого: файлов - 11</b>		<b>ceb456412505bdb93dad927771ede42d1bd7204711d163da7f6e9afe74186a8</b>
<i>Конец</i>		

Контрольные суммы рассчитаны с использованием средства фиксации исходного состояния программного комплекса «ФИКС» версии 2.0.2 (сертификат ФСТЭК России № 1548, действителен до 15.01.2020 г., лицензия № ЦС 50 – 7400 Л629640, знак соответствия № Л629640) по алгоритму «ГОСТ-34.11-94, программно».

#### **4. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ**

4.1. В программном изделии реализованы следующие функции безопасности:

4.1.1. Разграничение доступа к управлению программным изделием:

- а) поддержка определенных ролей для программного изделия и их ассоциации с конкретными администраторами безопасности, администраторами серверов и пользователями ИС;

4.1.2. Управление работой программного изделия:

- а) возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности программного изделия;

4.1.3. Управление параметрами программного изделия:

- а) возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности программного изделия;

4.1.4. Управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ):

- а) получение и установка обновлений БД ПКВ без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса; автоматически через сетевые подключения;

4.1.5. Аудит безопасности:

- а) генерация записи аудита для событий, подвергаемых аудиту;
- б) чтение информации из записей аудита;
- в) ассоциация событий аудита с идентификаторами субъектов;
- г) ограничение доступа к чтению записей аудита;
- д) поиск, сортировка, упорядочение данных аудита;

4.1.6. Выполнение проверок объектов воздействия:

- а) выполнение проверки с целью обнаружения зараженных КВ объектов;
- б) выполнение проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- в) выполнение проверки с целью обнаружения зараженных КВ объектов по команде; в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- г) выполнение проверки с целью обнаружения зараженных КВ объектов сигнатурными и эвристическими методами;

4.1.7. Обработка объектов воздействия:

- а) удаление (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из зараженных объектов.

- 4.1.8. Выполнение проверок сообщений электронной почты:  
выполнение проверок сообщений электронной почты на предмет наличия незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

*Примечание — Функциональные возможности соответствуют следующим мерам защиты информации в информационных системах, согласно приказу №17 ФСТЭК России, и меры по обеспечению безопасности персональных данных, согласно приказу №21 ФСТЭК России: АВЗ.1 — Реализация антивирусной защиты; АВЗ.2 — Обновление базы данных признаков вредоносных компьютерных программ (вирусов); ОЦЛ.4 - Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).*

## 5. КОМПЛЕКТНОСТЬ

5.1. Сведения по комплектности при физической поставке представлены в таблице 2.

Таблица 2 – Сведения по комплектности программного изделия при физической поставке

Наименование изделия (составной части, документа)	Обозначение конструкторского документа	Кол-во	Порядковый учетный номер	Примечание
1. Kaspersky Secure Mail Gateway. Инсталляционный комплект	643.46856491.00085-03	1		На лазерном диске
2. Kaspersky Secure Mail Gateway. Формуляр	643.46856491.00085-03 30 01	1		В печатном виде
3. Kaspersky Secure Mail Gateway. Приложение 1 к формуляру	643.46856491.00085-03 30 02	1		На лазерном диске
4. Kaspersky Secure Mail Gateway. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00085-03 90 01	1		На лазерном диске
5. Упаковка		1		
6. Заверенная копия выданного ФСТЭК России сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации		1		В печатном виде

5.2. Сведения по комплектности при электронной поставке представлены в таблице 3.

Таблица 3 – Сведения по комплектности программного изделия при электронной поставке

Наименование изделия (составной части, документа)	Обозначение конструкторского документа	Кол-во	Порядковый учетный номер	Примечание
1. Kaspersky Secure Mail Gateway. Инсталляционный комплект	643.46856491.00085-03	1		В электронном виде
2. Kaspersky Secure Mail Gateway. Формуляр	643.46856491.00085-03 30 01	1		В электронном виде
3. Kaspersky Secure Mail Gateway. Приложение 1 к формуляру	643.46856491.00085-03 30 02	1		В электронном виде
4. Kaspersky Secure Mail Gateway. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00085-03 90 01	1		В электронном виде
5. Копия выданного ФСТЭК России сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации		1		В электронном виде

## 6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

6.1. Программное изделие должно функционировать на компьютерах, имеющих следующие конфигурации вычислительной среды.

6.1.1. Аппаратные и программные требования для создания виртуальной машины из бинарных компонентов:

- Перед началом работы нужно создать виртуальную машину с установленными файлами программы.
- На виртуальной машине должна быть установлена операционная система CentOS 6.9.
- Объем дискового пространства в каталогах / и /root (как правило, это раздел /dev/sda2) – не менее 250 ГБ;

6.1.2. Программные требования для развертывания образа виртуальной машины Kaspersky Secure Mail Gateway:

- Образ виртуальной машины Kaspersky Secure Mail Gateway может быть развернут на следующих гипервизорах:
  - o VMware ESXi 6.5 Update 3;

- VMware ESXi 6.7 Update 3;
- Microsoft Hyper-V Server 2012 R2.

6.1.3. Аппаратные требования для развертывания образа виртуальной машины Kaspersky Secure Mail Gateway:

- Ресурсы, выделенные для развертывания образа виртуальной машины Kaspersky Secure Mail Gateway, должны удовлетворять следующим требованиям:
  - сетевой адаптер E1000;
  - объем дискового пространства – не менее 100 ГБ;
  - не менее 4 ГБ оперативной памяти;
  - 1 четырехъядерный процессор.

6.1.4. Программные требования для работы с Kaspersky Secure Mail Gateway через веб-интерфейс:

- Для работы веб-интерфейса на компьютере должен быть установлен один из следующих браузеров:
  - Mozilla™ Firefox™ версии 70;
  - Internet Explorer® версии 11;
  - Google Chrome™ версии 78.

6.2. Установка, предварительная настройка и эксплуатация программного изделия должны осуществляться в соответствии с эксплуатационной документацией, входящей в комплект поставки.

6.3. Активация программного изделия должна осуществляться только с использованием файла ключа.

6.4. Для сохранения бинарной целостности запрещается устанавливать обновления сертифицированного программного изделия, не прошедшие сертификационные испытания (только для типа 3). Порядок получения обновлений, прошедших сертификационные испытания, изложен в разделе 17 настоящего формуляра.

6.5. Предприятие, осуществляющее эксплуатацию программного изделия, должно периодически (не реже одного раза в 6 месяцев) проверять отсутствие обнаруженных уязвимостей в программном изделии, используя сайт предприятия-изготовителя (<https://support.kaspersky.ru/vulnerability>), базу данных уязвимостей ФСТЭК России ([www.bdu.fstec.ru](http://www.bdu.fstec.ru)) и иные общедоступные источники.

6.6. Перед началом эксплуатации программного изделия необходимо установить все доступные обновления используемых версий ПО среды функционирования.

6.7. Применение механизма облачной защиты KSN при использовании программного изделия для защиты информации ограниченного доступа (информация, содержащая сведения, составляющие государственную тайну, конфиденциальная информация) допускается только при условии совместного использования с сертифицированным программным комплексом «Kaspersky Security Center совместно с Kaspersky Private Security Network» (643.46856491.00082).

В остальных случаях механизм облачной защиты KSN должен быть гарантировано отключен.





## 8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное изделие «Kaspersky Secure Mail Gateway»

(наименование программного изделия)

643.46856491.00085-03

(обозначение)

соответствует техническим условиям (стандарту)

ТУ 643.46856491.00085-03

(номер технических условий или стандарта)

и признано годным для эксплуатации.

Дата выпуска \_\_\_\_\_

М.П.

Подпись лиц, ответственных за приемку

## 9. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

9.1. Раздел заполняется при физической поставке изделия.

**Kaspersky Secure Mail Gateway** **(643.46856491.00085-03)**

наименование

обозначение

упакован (о) **АО «Лаборатория Касперского»**

наименование или код предприятия (организации)

согласно требованиям, предусмотренным инструкцией **ЯМДИ.460649.003**.

Маркировано знаком соответствия № \_\_\_\_\_ системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00). Наклеивается в пункте 2 настоящего формуляра в соответствующее место.

Контрольная сумма: cebf456412505bdb93dad927771ede42d1bd7204711d163da7f6e9afe74186a8

Серийный номер: \_\_\_\_\_

Наименование пользователя: \_\_\_\_\_

№ сборки (РО): \_\_\_\_\_

Дата упаковки \_\_\_\_\_

Упаковку произвел \_\_\_\_\_ (подпись)

Изделие после упаковки принял \_\_\_\_\_ (подпись)

М.П.

*Примечание. Форму заполняют на предприятии, производившем упаковку.*

9.2. При электронной поставке маркирование программного изделия осуществляется с применением электронной подписи. Описание процедуры проверки электронной подписи приведено в разделе 16 настоящего формуляра.







## 16. ПОЛУЧЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭЛЕКТРОННОЙ ПОСТАВКЕ

### 16.1. Порядок получения программного изделия:

Получение программного изделия осуществляется путем загрузки дистрибутива с веб-сайта АО «Лаборатория Касперского» (<https://support.kaspersky.ru/common/certificates>). Подлинность и целостность программного изделия обеспечивается применением электронной подписи.

### 16.2. Порядок эксплуатации программного изделия:

1). После загрузки дистрибутива программного изделия с комплектом эксплуатационной документации необходимо произвести проверку его подлинности и целостности путем проверки электронной подписи. Порядок проверки подлинности электронной подписи изложен в статье <https://support.kaspersky.ru/15257>.

2). Записать установочный комплект на физический носитель (лазерный диск).

3). Производить эксплуатацию обновленного программного изделия в соответствии с эксплуатационной документацией.

## 17. ОБНОВЛЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ

### 17.1. Типы обновлений программного изделия.

Рассматриваются следующие типы обновлений программного изделия:

- обновление баз данных, необходимых для реализации функций безопасности (обновление БД ПКВ);
- обновление, направленное на устранение уязвимостей;
- обновление, направленное на добавление и/или совершенствование реализации функций безопасности, на расширение числа поддерживаемых программных и аппаратных платформ (обновление версии программного изделия).

### 17.2. Уведомления об обновлениях программного изделия.

Уведомления об обновлении БД ПКВ реализованы на программном уровне.

Уведомления об обнаруженных уязвимостях, обновлениях, направленных на устранение уязвимостей, и обновлениях версии программного изделия доводятся до потребителей путем отправки сообщений на адреса электронной почты, указанные при заказе программного изделия или подписке на рассылку «Новости о сертифицированных продуктах» ([https://support.kaspersky.ru/email\\_subscriptions/form](https://support.kaspersky.ru/email_subscriptions/form)).

### 17.3. Порядок получения обновления программного изделия.

Обновление, направленное на устранение уязвимостей, можно получить на веб-сайте АО «Лаборатория Касперского» (<https://support.kaspersky.ru/common/certificates>). Подлинность и целостность обновлений обеспечивается применением электронной подписи.

Обновление версии программного изделия можно получить следующими способами.

Открыть статью о соответствующем продукте на веб-сайте АО «Лаборатория Касперского» (<https://support.kaspersky.ru/common/certificates>) и скачать дистрибутив обновления программного изделия с комплектом измененной эксплуатационной документации.

### 17.4. Порядок применения обновлений.

1). После загрузки файлов обновления программного изделия и комплекта измененной эксплуатационной документации произвести проверку подлинности и целостности загруженных файлов путем проверки электронной подписи. Порядок проверки подлинности электронной подписи изложен в статье <https://support.kaspersky.ru/15257>.

2). Записать инсталляционный комплект на физический носитель (лазерный диск).

3). Внести изменения в эксплуатационную документацию, руководствуясь инструкциями в бюллетене. При необходимости заменить используемые эксплуатационные документы новыми редакциями.

4). При необходимости внести изменения в настройки программного изделия, руководствуясь инструкциями в бюллетене.

5). Производить эксплуатацию обновленного программного изделия в соответствии с обновленной эксплуатационной документацией.

6). При необходимости промаркировать замененные версии эксплуатационных документов, дистрибутива, копии сертификата соответствия как замененные и хранить вместе с актуальными версиями.

## **18. ОСОБЫЕ ОТМЕТКИ**

18.1. Приложение 1 выполнено в виде отдельного документа 643.46856491.00085-03 30 02 в электронном виде.