

АО «Лаборатория Касперского»

УТВЕРЖДЕН

643.46856491.00078-02 30 01-ЛУ

Программное изделие

Kaspersky Security 9.0 для Microsoft Exchange Servers

Формуляр

643.46856491.00078-02 30 01

Листов 14

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

2017

Литера

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ	3
2. ОБЩИЕ СВЕДЕНИЯ	3
3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	3
4. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ	4
5. КОМПЛЕКТНОСТЬ	5
6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ	5
7. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ ..	7
8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ	8
9. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ	8
10. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА	9
11. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ	10
12. СВЕДЕНИЯ О ХРАНЕНИИ	10
13. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ	11
14. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ	11
15. ОБНОВЛЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ	12
16. 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. Перед эксплуатацией необходимо ознакомиться с документацией к программному изделию, перечисленной в разделе «Комплектность».
- 1.3. Формуляр должен находиться в подразделении, ответственном за эксплуатацию программного изделия.
- 1.4. 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 Security 9.0 для Microsoft Exchange Servers*»

Версия: 9.4.189.0

Обозначение: 643.46856491.00078-02

Дата изготовления: _____

Наименование изготовителя: АО «Лаборатория Касперского»

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

Серийный номер: _____

Тип носителя: лазерный диск.

- 2.2. Сведения о применимых сертификатах соответствия и лицензиях:

Наименование и номер сертификата	Срок начала действия	Срок окончания действия	Знак соответствия

- 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 органов государственной власти Российской Федерации.
- 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., 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	Длина, байт	КС
Каталог E:\			
1	klcfiginst.msi	9723904	1ceff1710f527614ebe2af300e88318ace5d3e0174bf3e9ba1d9cb834963a9ff
2	release_notes_ru.txt	14032	6448b721e5a322a9d15284ec732be25681c3a9b91174aa0b90d37a8ccea11a31
3	setup_ru.exe	313583544	4d6ffb109f92052f506d2af2395a027a60aa306b621f7193e3820e43ff48ecc7
итого: файлов - 3		323321480	35c8bd40756351926add012e44f9d1a62f34a7d307d4e503d288bf4c588a5f09

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 безопасности¹:

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. Предотвращение утечек конфиденциальной информации:

¹ Функции безопасности 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: АВ3.1 — Реализация антивирусной защиты; АВ3.2 — Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

- а) контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы.

4.1.9. Анти-спам:

- а) 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).

4.1.10. Сигнализация:

- а) возможность отображения сигнала тревоги на АРМ администратора.

4.1.11. Идентификация и аутентификация:

- а) возможность аутентификации администратора безопасности при доступе к функциям управления САВЗ.

5. КОМПЛЕКТНОСТЬ

- 5.1. Сведения по комплектности приведены в таблице 2.

Таблица 2 – Сведения по комплектности программного изделия

Наименование изделия (составной части, документа)	Обозначение конструкторского документа	Кол-во	Порядковый учетный номер	Примечание
1. «Kaspersky Security 9.0 для Microsoft Exchange Servers». Инсталляционный комплект		1		На лазерном диске
2. «Kaspersky Security 9.0 для Microsoft Exchange Servers». Формуляр	643.46856491.00078-02 30 01	1		В печатном виде
3. «Kaspersky Security 9.0 для Microsoft Exchange Servers». Приложение 1 к формуляру	643.46856491.00078-02 30 02	1		В электронном виде
4. «Kaspersky Security 9.0 для Microsoft Exchange Servers». Подготовительные процедуры и руководство по эксплуатации	643.46856491.00078-02 90 01	1		В электронном виде
5. Упаковка		1		
<i>Примечание: поставка осуществляется с заверенной копией сертификатов соответствия на изделие при их наличии.</i>				

6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

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

5.1.1 Аппаратные требования

Аппаратные требования для установки Сервера безопасности соответствуют аппаратным требованиям защищаемого сервера Microsoft Exchange, за исключением объема оперативной памяти. Аппаратные требования для установки Сервера безопасности:

- процессор — в соответствии с аппаратными требованиями защищаемого сервера Microsoft Exchange;
- минимум 4 ГБ свободной оперативной памяти;
- 10 ГБ свободного дискового пространства, из них не менее 4 ГБ – для работы Модуля DLP. В зависимости от значений параметров программы и режима ее эксплуатации может потребоваться дополнительное дисковое пространство.

Совместно с Сервером безопасности устанавливается Консоль управления.

Консоль управления также может быть установлена отдельно от Сервера безопасности. Аппаратные требования для установки только Консоли управления:

- процессор Intel® Pentium® 400 МГц (рекомендуется 1000 МГц);
- 256 МБ свободной оперативной памяти;
- 500 МБ свободного дискового пространства для установки программы..

5.1.2 Программные требования

Для установки Сервера безопасности требуется одна из следующих операционных систем:

- Microsoft Windows Server 2016 Standard или Datacenter;
- Microsoft Windows Server 2012 R2 Standard или Datacenter (x64);
- Microsoft Windows Server 2012 Standard или Datacenter (x64);
- Microsoft Windows Small Business Server 2011 SP1 Standard (x64);
- Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise или Datacenter (x64).

Для установки Сервера безопасности требуется следующее программное обеспечение:

- Один из следующих почтовых серверов:
 - Microsoft Exchange Server 2010 SP3, развернутый как минимум в одной из следующих ролей: Транспортный концентратор, Почтовый ящик или Пограничный транспорт;
 - Microsoft Exchange Server 2013 SP1, развернутый как минимум в одной из следующих ролей: Почтовый ящик, Пограничный транспорт или Сервер клиентского доступа (CAS);
 - Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
- Microsoft .NET Framework 4.5.
- Одна из следующих СУБД:
 - Microsoft SQL Server 2016 Express, Standard или Enterprise;
 - Microsoft SQL Server 2014 Express, Standard или Enterprise;
 - Microsoft SQL Server 2012 Express, Standard или Enterprise.

Для установки Консоли управления требуется одна из следующих операционных систем:

- Microsoft Windows Server 2016 Standard или Datacenter (x64);
- Microsoft Windows Server 2012 Standard или Datacenter (x64);
- Microsoft Windows Server 2012 R2 Standard или Datacenter (x64);
- Microsoft Windows Small Business Server 2011 SP1 Standard (x64);
- Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise или Datacenter (x64);
- Microsoft Windows 7 SP1 Professional, Enterprise или Ultimate (x86-64);
- Microsoft Windows 8 (x86-64);
- Microsoft Windows 8.1 (x86-64);
- Microsoft Windows 10 (x86-64).

Для установки Консоли управления требуется следующее программное обеспечение:

- Microsoft Management Console 3.0;
- Microsoft .NET Framework 4.5.

Для установки плагина управления Microsoft Exchange Servers для Kaspersky Security Center требуется:

- Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 (системные требования см. Руководство администратора Kaspersky Security Center 10 SP2, 643.46856491.00069-03).

- 6.2. Установка, предварительная настройка и эксплуатация программного изделия должны осуществляться в соответствии с эксплуатационной документацией, входящей в комплект поставки.
- 6.3. Для сохранения бинарной целостности запрещается устанавливать обновления сертифицированного программного изделия, не прошедшие инспекционный контроль (только для типа 3). Порядок получения обновлений, прошедших инспекционный контроль, изложен в разделе 15 настоящего формуляра.
- 6.4. Предприятие, осуществляющее эксплуатацию программного изделия, должно периодически (не реже одного раза в 6 месяцев) проверять отсутствие обнаруженных уязвимостей в изделии, используя сайт предприятия-изготовителя (<https://support.kaspersky.ru/vulnerability>), базу данных уязвимостей ФСТЭК России (www.bdu.fstec.ru) и иные общедоступные источники.
- 6.5. Перед началом эксплуатации программного изделия необходимо установить все доступные обновления используемых версий ПО среды функционирования.
- 6.6. 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» (643.46856491.00078-02) в соответствии с руководством

8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное изделие «Kaspersky Security
9.0 для Microsoft Exchange Servers»
(наименование программного изделия)

643.46856491.00078-02
(обозначение)

соответствует техническим условиям
(стандарту)

ТУ 643.46856491.00078-02
(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

PRODUCT **(643.46856491.00078-02)**

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: 35c8bd40756351926add012e44f9d1a62f34a7d307d4e503d288bf4c588a5f09

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.

10. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

- 10.1. Предприятие-изготовитель гарантирует соответствие программного изделия требованиям ТУ 643.46856491.00078-02 при соблюдении потребителем условий и правил эксплуатации, транспортирования и хранения, установленных в эксплуатационной документации.
- Гарантийный срок эксплуатации программного изделия равен 1 году со дня ввода в эксплуатацию.
- 10.2. В гарантийный период изготовитель безвозмездно устраняет все неисправности изделия, в том числе путем замены неисправного носителя программного изделия на исправный, при условии соблюдения потребителем правил и условий хранения, транспортировки и эксплуатации.
- 10.3. При замене по гарантии неисправного носителя программного изделия на исправно функционирующее, гарантийный срок исчисляется со дня поставки потребителю исправно функционирующего изделия.
- 10.4. Действие гарантийных обязательств на выполнение изделием своих функций прекращается, если потребителем внесены изменения в изделие без согласования с его изготовителем или изделие передано другому предприятию (потребителю).
- 10.5. Гарантийные обязательства изготовителя не распространяются на копии изделия, изготовленные по инициативе потребителя.
- 10.6. Изготовитель принимает на себя обязательства по поиску ошибок реализации и уязвимостей в изделии на протяжении гарантийного срока и срока действия сертификата соответствия РОСС RU.0001.01БИ00, а также обязательства по своевременному информированию потребителя о найденных ошибках и уязвимостях, методах безопасного использования изделия.
- 10.7. В случае обнаружения уязвимостей, изготовитель распространяет обновления безопасности потребителям. Для этого изготовитель:
- Доводит до потребителя информацию о наличии уязвимости и способах ее устранения путем рассылки по электронной почте, указанной при заказе изделия, и публикации на своем веб-сайте на странице <https://support.kaspersky.ru/vulnerability>;
 - Проводит, в установленном порядке, инспекционный контроль указанного обновления в системе сертификации;
 - Размещает информацию о способе получения обновления на своем веб-сайте на странице <https://support.kaspersky.ru/vulnerability>;
 - При внесении изменения ФСТЭК России в сертификат соответствия изготовитель доводит до потребителя копию измененного сертификата, а также изменения в эксплуатационную документацию.
 - Потребитель, при получении указанной информации, принимает решение о необходимости применения обновления программного изделия. Потребитель, в случае применения обновления, делает соответствующую отметку в настоящем формуляре с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.
- 10.8. Гарантийное и послегарантийное обслуживание изделия осуществляется: АО «Лаборатория Касперского» (125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2).
- 10.9. Порядок предъявления рекламаций по гарантийным обязательствам должен соответствовать ГОСТ РВ 15.703-2005.

15. ОБНОВЛЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ

15.1. Определены три типа обновлений программного изделия:

1 тип — обновление баз данных, необходимых для реализации функций безопасности (обновление БД ПКВ);

2 тип — обновление, направленное на устранение уязвимостей (критическое обновление);

3 тип — обновление, направленное на добавление и/или совершенствование реализации функций безопасности, на расширение числа поддерживаемых программных и аппаратных платформ (обновление версии программного изделия).

15.2. Этапы жизненного цикла обновлений программного изделия от выпуска до применения:

	1 тип	2 тип	3 тип
Выпуск	Регулярно в соответствии с установленной изготовителем процедурой, вплоть до окончания срока поддержки программного изделия	По необходимости (при выявлении уязвимостей)	По усмотрению изготовителя
Публикация	Непосредственно после выпуска	Непосредственно после выпуска	По прохождении инспекционного контроля
Инспекционный контроль	1 раз в год (полный пакет обновлений)	После выпуска — в срок, предусмотренный изготовителем	После выпуска — в срок, предусмотренный изготовителем
Уведомление	Реализовано в программном изделии	По электронной почте зарегистрированным пользователям*, на сайте изготовителя** — в срок не позднее 5 суток после публикации	По электронной почте зарегистрированным пользователям*, на сайте изготовителя** — в срок не позднее 5 суток после получения сертификата
Получение и применение	В соответствии с эксплуатационной документацией	Потребитель должен загрузить и применить обновление незамедлительно после получения уведомления	По усмотрению потребителя. Подробности см. в пп. 15.3 и 15.4

* Уведомления о выпуске обновлений 2 и 3 типов рассылаются по адресам электронной почты, указанным при заказе программного изделия, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: <http://support.kaspersky.ru/subscribe>).

** <http://support.kaspersky.ru/general/certificates>

15.3. Потребитель может получить обновление 3 типа следующими способами:

1. Приобрести новый комплект поставки программного изделия («медиа-пак»), содержащий обновление и эксплуатационную документацию в печатном виде, согласно комплекту поставки (см. п. 5.1), обратившись к дистрибьюторам АО «Лаборатория Касперского».
2. Загрузить обновление и комплект измененной эксплуатационной документации (включая эксплуатационный бюллетень) в электронном виде с веб-сайта АО «Лаборатория Касперского» (<https://certifiedbuilds.kaspersky.ru>).

Примечание: Применение обновления, полученного в электронном виде, допускается только при наличии у потребителя оригинального комплекта поставки программного изделия («медиа-пака») предыдущей версии в твердом виде.

15.4. При получении обновления 3 типа и комплекта измененной эксплуатационной документации в электронном виде потребитель должен осуществить следующие действия:

1. После загрузки файлов обновления и комплекта измененной эксплуатационной документации произвести проверку целостности загруженных файлов путем сверки контрольных сумм с указанными на веб-сайте АО «Лаборатория Касперского».
2. Записать установочный комплект, полученный в электронном виде, на физический носитель.
3. Промаркировать физический носитель в соответствии с разделом «Упаковка и маркировка» измененной версии формуляра. Соответствующий раздел в формуляре в части упаковки заполнить самостоятельно, указав ответственного за упаковку.

4. Внести изменения в эксплуатационную документацию, руководствуясь эксплуатационным бюллетенем. При необходимости заменить используемые эксплуатационные документы новыми редакциями.
5. При необходимости внести изменения в программное изделие в соответствии с инструкциями, изложенными в бюллетене.
6. Производить эксплуатацию обновленного программного изделия в соответствии с обновленной эксплуатационной документацией.
7. Замененные версии эксплуатационных документов, дистрибутива, копию сертификата соответствия (при необходимости) промаркировать как замененные и хранить вместе с актуальными версиями.

16. ОСОБЫЕ ОТМЕТКИ

16.1. Приложение 1 выполнено в виде отдельного документа 643.46856491.00078-02 30 02 в электронном виде.