АО «Лаборатория Касперского»

УТВЕРЖДЕН
643.46856491.01-2021-ЛУ

Программное изделие

KASPERSKY SECURITY 9.0 ДЛЯ MICROSOFT EXCHANGE SERVERS

Формуляр

643.46856491.00078-05 30 01

Листов 15

Литера

2021

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

СОДЕРЖАНИЕ

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 Security 9.0 для Microsoft Exchange Servers»

Версия: 9.6.96.0

Обозначение: 643.46856491.00078-05

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 применимом сертификате соответствия:

Наименование и номер сертификата	Срок начала действия	Срок окончания действия	Идентификатор
Сертификат соответствия № _____, выдан ФСТЭК России			РОСС RU.01._____._____

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
Каталог E:		
1	Kaspersky Security_9.6.96.0_ru-RU.exe	287681d0d1d678bb830d241e9858622f02bc0006313f58cd419af595029f0f23
2	klcfginst.msi	d8f52a43b3a3e497397a04ccb097b2d5e6faa5b411970a7dda46ed65be3d6143
итого: файлов - 2		**f083ab9362759c2cba7720d228cfd0fae446a5b220a852b09bdc18f0bca26e60**

Контрольные суммы рассчитаны с использованием средства фиксации и контроля исходного состояния программного комплекса «ФИКС» версии 2.0.2 (сертификат ФСТЭК России № 1548, техническая поддержка до 15.01.2025 г., лицензия № ЦС 50 – 7400 Л629640, знак соответствия № Л629640) по алгоритму «ГОСТ-34.11-94, программно».

4. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

4.1. 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;

4.2. Управление работой программного изделия:

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

4.3. Управление параметрами программного изделия:

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

4.4. 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;

4.5. 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;

4.6. 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;

4.7. Обработка объектов воздействия:

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

4.8. Сигнализация:

а) возможность отображение сигнала тревоги об обнаружении КВ.

4.9. Анти-спам:

а) управление входящими информационными потоками для выявления и удаления 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 Security 9.0 для Microsoft Exchange Servers. Инсталляционный комплект	643.46856491.00078-05	1		На лазерном диске
2. Kaspersky Security 9.0 для Microsoft Exchange Servers. Формуляр	643.46856491.00078-05 30 01	1		В печатном виде
3. Kaspersky Security 9.0 для Microsoft Exchange Servers. Формуляр. Приложение 1	643.46856491.00078-05 30 02	1		На лазерном диске
4. Kaspersky Security 9.0 для Microsoft Exchange Servers. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00078-05 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 Security 9.0 для Microsoft Exchange Servers. Инсталляционный комплект	643.46856491.00078-05	1		В электронном виде
2. Kaspersky Security 9.0 для Microsoft Exchange Servers. Формуляр	643.46856491.00078-05 30 01	1		В электронном виде
3. Kaspersky Security 9.0 для Microsoft Exchange Servers. Формуляр. Приложение 1	643.46856491.00078-05 30 02	1		В электронном виде
4. Kaspersky Security 9.0 для Microsoft Exchange Servers. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00078-05 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 требования.

Аппаратные требования для установки Сервера безопасности соответствуют аппаратным требованиям защищаемого сервера Microsoft Exchange, за исключением объема оперативной памяти. Совместно с Сервером безопасности устанавливается Консоль управления.
Аппаратные требования для установки Сервера безопасности:

- процессор – в соответствии с аппаратными требованиями защищаемого сервера Microsoft Exchange;
- минимум 2 ГБ свободной оперативной памяти.
- 6 ГБ свободного дискового пространства.

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

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

6.1.2 Программные требования.

Для установки Сервера безопасности требуется одна из следующих операционных систем:

- Microsoft Windows Server 2019 Standard или Datacenter (Desktop Experience);
- Microsoft Windows Server 2019 Core;
- Microsoft Windows Server 2016 Standard или Datacenter;
- Microsoft Windows Server® 2012 R2 Standard или Datacenter.

Для установки Сервера безопасности требуется следующее программное обеспечение:

- Один из следующих почтовых серверов:
  - Microsoft Exchange Server 2019, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт;
  - Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: 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 .NET Framework 4.5.
- Одна из следующих систем управления базами данных (СУБД):
  - Microsoft SQL Server 2019 Express, Standard или Enterprise;
  - Microsoft SQL Server 2017 Express, Standard или Enterprise;
  - 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 2019 Standard или Datacenter (Desktop Experience);
- Microsoft Windows Server 2019 Core;
- Microsoft Windows Server 2016 Standard или Datacenter;
- Microsoft Windows Server 2012 R2 Standard или Datacenter;
- Microsoft Windows 10;
- Microsoft Windows 8.1;
- Microsoft Windows 8.

Для установки Консоли управления требуется следующее программное обеспечение:

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

Для установки любого из перечисленных компонентов программы требуется пакет обновлений Microsoft Windows KB2999226.
Для установки плагина управления требуется одна из следующих версий Kaspersky Security Center:

- Kaspersky Security Center 11;
- Kaspersky Security Center 10 Service Pack 3.

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.

6.4. Предприятие, осуществляющее эксплуатацию программного изделия, должно периодически (не реже одного раза в 6 месяцев) проверять наличие 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» (643.46856491.00082-02) в соответствии с руководством администратора 643.46856491.00082-02 90 02. В остальных случаях механизм облачной защиты KSN должен быть гарантировано отключен.

6.7. Согласно приказам № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России, изделие может использоваться в государственных информационных системах 1 и 2 класса защищенности и для обеспечения защищенности персональных данных до 1 уровня включительно.

7. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

7.1. Периодический контроль основных характеристик при эксплуатации и хранении программного изделия состоит в проверке сохранности исполняемого кода, записанного на носителях информации.

7.2. Проверка сохранности программного изделия осуществляется путем подсчета контрольных сумм файлов программного изделия после установки и сравнения их с контрольными суммами, указанными в таблице КС исполняемых модулей, приведенными в Приложении 1 к настоящему формуляру.

7.3. Контроль основных характеристик программного изделия проводится при первичном закреплении за ответственным лицом.

7.4. Результаты периодического контроля основных характеристик программного изделия фиксируются в таблице 4.

Таблица 4 – Периодический контроль основных характеристик при эксплуатации и хранении

Проверяемая характеристика		**Дата проведения измерения**					
		20__ г.		**20__ г.**		**20__ г.**	
Наименование измерения	**Величина**	**Фактическая величина**	**Замерил (должность, подпись)**	**Фактическая величина**	**Замерил (должность, подпись)**	**Фактическая величина**	**Замерил (должность, подпись)**

8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное изделие «Kaspersky Security 9.0 для Microsoft Exchange Servers» — 643.46856491.00078-05

(наименование программного изделия) — (обозначение)

соответствует техническим условиям (стандарту) — ТУ 643.46856491.00078-05

(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 Security 9.0 для Microsoft Exchange Servers _____ ***(643.46856491.00078-05)***

наименование — обозначение

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

наименование или код предприятия (организации)

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

Маркировано идентификатором № РОСС RU.01._____._____, где:

- первая группа знаков указывает на систему сертификации ФСТЭК России РОСС RU.01.
- вторая группа знаков указывает на номер сертификата соответствия средства защиты информации.
- третья группа знаков указывает на уникальный порядковый номер идентификатора сертифицированного средства защиты информации.

Контрольная сумма: `f083ab9362759c2cba7720d228cfd0fae446a5b220a852b09bdc18f0bca26e60`

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 программное изделие дополнительно маркируется с применением электронной подписи. Описание процедуры проверки электронной подписи приведено в разделе 16 настоящего формуляра.

10. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

10.1. В период гарантийного обслуживания предприятие-разработчик оказывает техническую поддержку в объеме, указанном в разделе 11 настоящего формуляра.

10.2. Гарантийное и послегарантийное обслуживание программного изделия осуществляется: АО «Лаборатория Касперского» (125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2).

11. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

11.1. Изготовитель принимает на себя обязательства по технической поддержке программного изделия в объеме, указанном на странице https://support.kaspersky.ru/support/rules веб-сайта изготовителя.

11.2. В период оказания технической поддержки изготовитель гарантирует осуществление программным изделием функциональных возможностей, изложенных в настоящем формуляре, при соблюдении пользователем требований по эксплуатации, изложенных в эксплуатационной документации.

11.3. Срок оказания технической поддержки для программного изделия указан на странице https://support.kaspersky.ru/support/lifecycle веб-сайта изготовителя. Изготовитель не позднее чем за 1 год до окончания производства и (или) технической поддержки программного изделия информирует об этом потребителей и ФСТЭК России.

11.4. Программное изделие, используемое после прекращения технической поддержки, не является сертифицированным.

11.5. Изготовитель принимает на себя обязательства по поиску ошибок реализации и уязвимостей в программном изделии на протяжении срока действия технической поддержки, а также обязательства по своевременному информированию потребителя о найденных ошибках и уязвимостях путем рассылки электронной почты, а также публикации на странице https://support.kaspersky.ru/support.

12. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

12.1. Рекламации предъявляются в адрес АО «Лаборатория Касперского» (125212, г. Москва, Ленинградское шоссе, 39А, стр. 2) в письменном виде с указанием даты обнаружения неисправности, содержания и условий возникновения неисправности.

12.2. Рекламации подписываются руководителем подразделения, принимающего и эксплуатирующего программное изделие.

12.3. Сведения о рекламациях заносятся в таблицу 5.

Таблица 5 – Сведения о рекламациях

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

13. СВЕДЕНИЯ О ХРАНЕНИИ

13.1. При физической поставке программное изделие должно допускать пересылку заказчику (потребителю) в тарной упаковке на любое расстояние.

13.2. При электронной поставке программное изделие распространяется по сетям связи. Процедура получения программного изделия описана в разделе 16 настоящего формуляра.

13.3. Носители информации в упаковке должны храниться в отапливаемом помещении с температурой воздуха от 10 до 40°С) и максимальной относительной влажностью не более 80% при 25°С без конденсации влаги внутри помещения, при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей.

13.4. Условия хранения должны исключать резкие изменения температуры (не более 10°С/час) и влажности окружающего воздуха (не более 10%/час).

13.5. Сведения о хранении носителей информации с программным изделием заносятся в таблицу 6.

Таблица 6 – Сведения о хранении

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

14. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

14.1. Сведения о закреплении программного изделия при эксплуатации заносятся в таблицу 7.

14.2. При первичном закреплении необходимо провести контроль комплектности программного изделия (см. раздел 5).

Таблица 7 – Сведения о закреплении программного изделия при эксплуатации

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

15. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

15.1. Сведения об изменениях заносятся в таблицу 8.

Таблица 8 – Сведения об изменениях

Основание (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись ответственного лица за проведения изменения	Подпись лица, ответственного за эксплуатацию программного изделия

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). При необходимости записать инсталляционный комплект на физический носитель и промаркировать его идентификатором, указанным в п.2.2.

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).

17.3. Порядок получения обновлений программного изделия.

Получение обновлений версии программного изделия или обновлений, направленных на устранение уязвимостей, осуществляется путем загрузки соответствующего дистрибутива с комплектом измененной эксплуатационной документации с веб-сайта АО «Лаборатория Касперского» (https://support.kaspersky.ru/common/certificates). Подлинность и целостность обновлений обеспечивается применением электронной подписи.

17.4. Порядок применения обновлений программного изделия.

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). При необходимости записать инсталляционный комплект на физический носитель и промаркировать его идентификатором, указанным в п.2.2.

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 643.46856491.00078-05 30 02 в электронном виде.