АО «Лаборатория Касперского»

УТВЕРЖДЕН
643.46856491.00097-02 30 01-ЛУ

Программное изделие

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД 5.1 ЛЕГКИЙ АГЕНТ

Формуляр

643.46856491.00097-02 30 01

Листов 18

Литера

2020

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 для виртуальных сред 5.1 Легкий агент»

Версия: 5.1.44.295

Обозначение: 643.46856491.00097-02

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	Длина, байт	КС
Каталог D:			
1	ksvla-components_5.1.0.474_mlg.exe	369677296	02415c409efdf62ccce39a80e3b2028cd88ac6b18d02f8eb7353cb04899fa09e
2	KSVLA-MIB.txt	3415	f2fd2462e15838c9f7cb37f6dd78b492de1caede3dc6e797d1922d3ee7d36593
3	ksvla-svmbuild-5.1.44.295-kl.tar.bz2	374794145	3b37702b3fc86575c83ec3aece9b9982a88f94687101f9bdaa87f75e8f5d860d
4	license.txt	85371	e2f0ca29e468f7bb33796c40b0b46eef83d358d6d4263cbd8f114e24e1bb7f21
итого: файлов - 4		**744560227**	**297bc220a4055c2bc06f029840e541732dcaa4d115e3da7c87575f4000aa3c21**
Каталог D:\integrity_check\linux32bit			
5	integrity-check-tool	3679578	140e80b9e57a4f1e91af774485a23a57e1acef76ee81ad170672323f9eaf3244
итого: файлов - 1		**3679578**	**140e80b9e57a4f1e91af774485a23a57e1acef76ee81ad170672323f9eaf3244**
Каталог D:\integrity_check\linux64bit			
6	integrity-check-tool	3674502	12dbbbac84e9acecde027e0d4af84db22843f7e0f6e6407b21d141e10bdfe69c
итого: файлов - 1		**3674502**	**12dbbbac84e9acecde027e0d4af84db22843f7e0f6e6407b21d141e10bdfe69c**
Каталог D:\integrity_check\svm			
7	integrity-check-tool	3658014	977050ec2d053aa9e60355015e32b9c7a8266e114b8288390d9cd53f49972cb1
итого: файлов - 1		**3658014**	**977050ec2d053aa9e60355015e32b9c7a8266e114b8288390d9cd53f49972cb1**
Каталог D:\integrity_check\windows			
8	integrity_check_tool.exe	1319560	49dcebde515e9d7aedc00ee7499ac229a5660d7cbf4708a5779ba38dd09bdc67
итого: файлов - 1		**1319560**	**49dcebde515e9d7aedc00ee7499ac229a5660d7cbf4708a5779ba38dd09bdc67**
ВСЕГО: файлов - 8		**756891881**	**f1024207b9cd180a8401503798174d78e965df2af941b78cdaf35a2c0cd6182f**

Конец

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

4.1.2. управление работой САВЗ:
- а) возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;

4.1.3. управление параметрами САВЗ:
- а) возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;

4.1.4. управление установкой обновлений (актуализации) БД ПКВ САВЗ:
- 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 САВЗ:
- 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 методами.

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

4.1.8. контроль доступа к веб-ресурсам
- а) возможность контролировать доступ к веб-ресурсам.

4.1.9. контроль запуска программ
- а) возможность контролировать запуск программ.

4.1.10. контроль доступа программ к защищаемым ресурсам
- а) возможность контроля доступа программ к защищаемым ресурсам.

4.1.11. мониторинг файловых операций[1]
- а) мониторинг контроля выполнения файловых операций объектов, выбранных администратором безопасности.

4.1.12. контроль целостности компонентов ОО
- а) возможность верифицировать целостность компонентов.

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); ЗСВ.9 — Реализация и управление антивирусной защитой в виртуальной инфраструктуре.

[1] Данная функциональная возможность реализована для операционных систем семейства Windows Server.

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 для виртуальных сред 5.1 Легкий агент. Инсталляционный комплект	643.46856491.00097-02	1		На лазерном диске
2. Kaspersky Security для виртуальных сред 5.1 Легкий агент. Вспомогательный диск	б\о	1		На лазерном диске. Содержит компоненты среды функционирования для развертывания ОО.
3. Kaspersky Security для виртуальных сред 5.1 Легкий агент. Формуляр	643.46856491.00097-02 30 01	1		В печатном виде
4. Kaspersky Security для виртуальных сред 5.1 Легкий агент. Приложение 1 к формуляру	643.46856491.00097-02 30 02	1		На лазерном диске
5. Kaspersky Security для виртуальных сред 5.1 Легкий агент. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00097-02 90 01	1		На лазерном диске
6. Упаковка		1		
7. 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 для виртуальных сред 5.1 Легкий агент. Инсталляционный комплект	643.46856491.00097-02	1		В электронном виде
2. Kaspersky Security для виртуальных сред 5.1 Легкий агент. Вспомогательный диск	б\о	1		В электронном виде. Содержит компоненты среды функционирования для развертывания ОО.
3. Kaspersky Security для виртуальных сред 5.1 Легкий агент. Формуляр	643.46856491.00097-02 30 01	1		В электронном виде
4. Kaspersky Security для виртуальных сред 5.1 Легкий агент. Приложение 1 к формуляру	643.46856491.00097-02 30 02	1		В электронном виде
5. Kaspersky Security для виртуальных сред 5.1 Легкий агент. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00097-02 90 01	1		В электронном виде

Наименование изделия (составной части, документа)	Обозначение конструкторского документа	Кол-во	Порядковый учетный номер	Примечание
6. 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. Общие программные требования:

Для функционирования программного изделия в локальной сети организации должна быть установлена программа Kaspersky Security Center одной из следующих версий:

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

6.1.2. Программные требования к виртуальной инфраструктуре

Для работы программы Kaspersky Security в виртуальной инфраструктуре должен быть установлен один из следующих гипервизоров в зависимости от платформы виртуализации:

- Платформа Microsoft Hyper-V:
    - Гипервизор Microsoft Windows Server 2019 Hyper-V (в полном режиме или в режиме Server Core);
    - Гипервизор Microsoft Windows Server 2016 Hyper-V (в полном режиме или в режиме Server Core) со всеми доступными обновлениями;
    - Гипервизор Microsoft Windows Server 2012 R2 Hyper-V (в полном режиме или в режиме Server Core) со всеми доступными обновлениями;

Поддерживается установка и работа программы на гипервизорах Microsoft Windows Server (Hyper-V), входящих в состав кластера гипервизоров под управлением службы Windows Failover Clustering. На узлах кластера должна быть включена технология Cluster Shared Volumes.

- Платформа Citrix Hypervisor: гипервизор Citrix XenServer 7.1 LTSR.
- Платформа VMware vSphere:
    - Гипервизор VMware ESXi 6.7 с последними обновлениями;
    - Гипервизор VMware ESXi 6.5 с последними обновлениями;
    - Гипервизор VMware ESXi 6.0 с последними обновлениями.

Для развертывания и работы SVM (виртуальная машина защиты) на гипервизорах VMware ESXi в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой VMware vCenter Server 6.0, VMware vCenter Server 6.5 или VMware vCenter Server 6.7 со всеми доступными обновлениями. Поддерживается установка и работа программы в инфраструктуре под управлением как автономных серверов VMware vCenter Server, так и группы серверов VMware vCenter Server, работающих в режиме Linked mode.

При защите виртуальных машин в инфраструктуре VMware программа Kaspersky Security может использовать в своей работе VMware NSX Manager из пакета VMware NSX for vSphere 6.4.2. Если используется VMware NSX Manager, то Kaspersky Security может назначать теги безопасности (NSX Security Tags) защищенным виртуальным машинам.

- Платформа KVM (Kernel-based Virtual Machine): гипервизор KVM на базе одной из следующих операционных систем:
    - Ubuntu Server 18.04 LTS;
    - Ubuntu Server 16.04 LTS;
    - Red Hat Enterprise Linux Server 7.6;

- CentOS 7.6.

Для развертывания SVM на гипервизорах KVM под управлением операционной системы CentOS требуется удалить или закомментировать строку Defaults requiretty в конфигурационном файле /etc/sudoers операционной системы гипервизора.

- Платформа Proxmox VE: гипервизор Proxmox VE 5.4.

Уточнение: Поддерживается только Proxmox VE на базе KVM. Не поддерживается работа программы на гипервизоре Proxmox VE с использованием LXC (Linux Containers).

- Платформа Скала-Р: гипервизор Р-Виртуализация 7.0.6.

Для развертывания и работы SVM (виртуальная машина защиты) на гипервизорах Р-Виртуализация в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой Скала-Р Управление 1.30.

- Платформа HUAWEI FusionSphere: гипервизор HUAWEI FusionCompute CNA 6.3.1.

Для развертывания и работы SVM (виртуальная машина защиты) на гипервизорах HUAWEI FusionCompute CNA в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой HUAWEI FusionCompute VRM 6.3.1.

Для развертывания SVM на гипервизорах Microsoft Windows Server (Hyper-V) и VMware ESXi вы можете использовать сервер управления виртуальной инфраструктурой Microsoft System Center Virtual Machine Manager (далее "Microsoft SCVMM") одной из следующих версий:

- Microsoft SCVMM 2019 с последними обновлениями;
- Microsoft SCVMM 2016 с последними обновлениями;
- Microsoft SCVMM 2012 R2 с последними обновлениями.

6.1.3. Требования к ресурсам SVM с установленным компонентом Сервер защиты Kaspersky Security:

Для функционирования Kaspersky Security для SVM требуется выделить следующее минимальное количество системных ресурсов:

- двухъядерный виртуальный процессор;
- 2 ГБ выделенной оперативной памяти;
- 30 ГБ выделенного свободного места на диске;
- виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

6.1.4. Требования к виртуальной машине с установленным компонентом Легкий агент для Windows

Перед установкой Легкого агента для Windows на виртуальной машине под управлением гипервизора Citrix Hypervisor (Citrix XenServer) должна быть установлена программа XenTools.

Перед установкой Легкого агента для Windows на виртуальной машине под управлением гипервизора VMware ESXi должен быть установлен пакет VMware Tools.

Перед установкой Легкого агента для Windows на виртуальной машине под управлением гипервизора HUAWEI FusionCompute CNA должен быть установлен пакет HUAWEI Tools.

На виртуальной машине под управлением гипервизора Microsoft Windows Server (Hyper-V) должен быть установлен пакет служб интеграции (Integration Services).

Для установки и функционирования Легкого агента для Windows на виртуальной машине должна быть установлена одна из следующих гостевых операционных систем:

- Windows 10 Desktop Pro / Enterprise / LTSC / RS4 / RS5 / 19H1 (32 / 64-разрядная);
- Windows 8.1 Update 1 Professional / Enterprise (32 / 64-разрядная);
- Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-разрядная)[2];
- Windows Server 2019 Standard / Datacenter (в полном режиме) (64-разрядная);
- Windows Server 2016 Standard / Datacenter (в полном режиме) (64-разрядная);

[2] Использование Изделия с данной операционной системой в качестве среды функционирования допускается только для замены средств защиты информации, ранее установленных на аттестованных по требованиям безопасности информации объектах информатизации.

- Windows Server 2012 R2 Standard / Datacenter / Essentials (в полном режиме) (64-разрядная);
- Windows Server 2012 Standard / Datacenter / Essentials (в полном режиме) (64-разрядная);
- Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (в полном режиме) (64-разрядная)[3].

Контроль целостности системы работает только на виртуальных машинах с файловой системой NTFS или FAT32.

Во избежание задержек процесса установки программы на операционных системах Windows 7 и Windows Server 2008 R2 убедитесь, что операционная система Windows автоматически обновляет списки доверенных и недоверенных (отозванных) сертификатов поставщиков программного обеспечения через интернет посредством Windows Update. Для систем, не имеющих доступа к Windows Update, или систем, на которых автоматическое обновление списков доверенных и недоверенных сертификатов отключено, требуется обеспечить актуальность этих списков вручную согласно рекомендациям Microsoft, описанным на сайте технической поддержки Microsoft:

- https://support.microsoft.com/en-us/kb/2677070;
- https://support.microsoft.com/en-us/kb/2813430.

Легкий агент для Windows может защищать виртуальные машины в составе инфраструктуры, в которой используются следующие решения для виртуализации:

- Citrix Virtual Apps and Desktops 7 1903;
- Citrix XenApp and XenDesktop 7.15 LTSR с последними установленными обновлениями;
- Citrix Provisioning 7 1903;
- Citrix Provisioning Services 7.15 с последними установленными обновлениями;
- VMware Horizon 7.8.

Если вы используете решения для виртуализации Citrix Virtual Apps and Desktops (Citrix XenApp and XenDesktop), Citrix Provisioning (Citrix Provisioning Services) и VMware Horizon, вам нужно настроить на золотом образе рекомендованные исключения, указанные на странице программы в Базе знаний (https://support.kaspersky.ru/14052).

Легкий агент для Windows может защищать виртуальные машины, на которых установлен Endpoint Sensor программы Kaspersky Anti Targeted Attack Platform 3.6.

6.1.5. Требования к виртуальной машине с установленным компонентом Легкий агент для Linux

Для установки и функционирования Легкого агента для Linux виртуальная машина должна удовлетворять следующим минимальным аппаратным требованиям:

- виртуальный процессор с частотой 1,5 ГГц;
- объем свободного места на диске – 2 ГБ;
- объем оперативной памяти – 2 ГБ;
- виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Программные требования для установки и функционирования Легкого агента для Linux:

- интерпретатор языка Perl версии 5.0 (http://www.perl.org);
- утилита which;
- установленный пакет dmidecode;
- для выполнения процедуры удаленной установки Легкого агента для Linux требуется установленный пакет sudo.

Уточнение: если операционная система не поддерживает технологию fanotify, для обработки операций над объектами файловой системы потребуется компиляция модуля ядра операционной системы Linux. Для этого на виртуальной машине должен находиться исходный код ядра

[3] Использование Изделия с данной операционной системой в качестве среды функционирования допускается только для замены средств защиты информации, ранее установленных на аттестованных по требованиям безопасности информации объектах информатизации.

операционной системы и установленные пакеты для компиляции (gcc, binutils, glibc, glibc-devel, make, ld).

Перед установкой Легкого агента для Linux на виртуальной машине под управлением гипервизора Citrix Hypervisor (Citrix XenServer) должна быть установлена программа XenTools.

Перед установкой Легкого агента для Linux на виртуальной машине под управлением гипервизора VMware ESXi должен быть установлен пакет VMware Tools.

Перед установкой Легкого агента для Linux на виртуальной машине под управлением гипервизора HUAWEI FusionCompute CNA должен быть установлен пакет HUAWEI Tools.

На виртуальной машине под управлением гипервизора Microsoft Windows Server (Hyper-V) должен быть установлен пакет служб интеграции (Integration Services).

Для установки и функционирования Легкого агента для Linux на виртуальной машине должна быть установлена одна из следующих гостевых операционных систем для серверов:

- Debian GNU / Linux 9.11 (64-разрядная);
- Debian GNU / Linux 8.11 (64-разрядная);
- Debian GNU / Linux 8.11 i386 (32-разрядная);
- Ubuntu Server 18.04 LTS (64-разрядная);
- Ubuntu Server 16.04 LTS (64-разрядная);
- CentOS 7.7 (64-разрядная);
- CentOS 6.10 (64-разрядная);
- Red Hat Enterprise Linux Server 8 (64-разрядная);
- Red Hat Enterprise Linux Server 7.7 (64-разрядная);
- Red Hat Enterprise Linux Server 6.10 (64-разрядная);
- SUSE Linux Enterprise Server 15 (64-разрядная);
- ALT Linux 8 (64-разрядная);
- ALT Linux 7.0.6 (64-разрядная);
- Oracle Linux 7.6 (64-разрядная);
- Astra Linux SE 1.6 (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды);
- Astra Linux SE 1.5 (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды).

6.1.6. Программные и аппаратные требования для компонента Сервер интеграции

Для установки и функционирования Сервера интеграции и Консоли Сервера интеграции на компьютере должна быть установлена одна из следующих операционных систем:

- Windows Server 2019 Standard / Datacenter / Essentials (64-разрядная);
- Windows Server 2016 Standard / Datacenter (64-разрядная);
- Windows Server 2012 R2 Standard / Datacenter / Essentials (64-разрядная);
- Windows Server 2012 Standard / Datacenter / Essentials (64-разрядная);
- Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (64-разрядная)[4].

На компьютере, на котором вы планируете установить Консоль Сервера интеграции, операционная система должна быть установлена в полном режиме (Full mode).

Для работы Сервера интеграции, Консоли Сервера интеграции и плагинов управления Kaspersky Security требуется платформа Microsoft .NET Framework 4.6. Если платформа не установлена, при наличии доступа в интернет мастер установки компонентов Kaspersky Security предложит ее

[4] Использование Изделия с данной операционной системой в качестве среды функционирования допускается только для замены средств защиты информации, ранее установленных на аттестованных по требованиям безопасности информации объектах информатизации.

установить в ходе установки Сервера интеграции, Консоли Сервера интеграции и плагинов управления Kaspersky Security.

Для установки и функционирования Сервера интеграции и Консоли Сервера интеграции компьютер должен удовлетворять следующим минимальным аппаратным требованиям:

- четырехъядерный виртуальный процессор с частотой 2 ГГц;
- объем свободного места на диске:
    - для Консоли Сервера интеграции – 4 ГБ;
    - для Сервера интеграции – 4 ГБ;
- объем оперативной памяти:
    - для Консоли Сервера интеграции – 4 ГБ;
    - для Сервера интеграции – 4 ГБ.

В зависимости от размера виртуальной инфраструктуры может изменяться необходимый объем оперативной памяти и объем свободного места на диске. Для увеличения производительности работы Сервера интеграции рекомендуется 10 ГБ свободного места на диске.

Для работы командлетов PowerShell требуется Windows PowerShell 4.0. Командлет используется для замены самоподписанного SSL-сертификата Сервера интеграции. Замену рекомендуется выполнить после установки Сервера интеграции. Для работы программы Kaspersky Security и защиты виртуальной инфраструктуры Windows PowerShell не требуется.

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 версии сертифицированного программного изделия, не прошедшие сертификационные испытания. 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) 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.

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 для виртуальных сред 5.1 Легкий агент» — 643.46856491.00097-02

(наименование программного изделия) — (обозначение)

соответствует техническим условиям (стандарту) ТУ 643.46856491.00097-02

(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

9.1. Раздел заполняется при физической поставке изделия.

Kaspersky Security для виртуальных сред 5.1 Легкий агент ***(643.46856491.00097-02)***

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 разделе 2 настоящего формуляра в соответствующее место.

Контрольная сумма: `f1024207b9cd180a8401503798174d78e965df2af941b78cdaf35a2c0cd6182f`

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.

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). 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).

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). 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 643.46856491.00097-02 30 02 в электронном виде.