

АО «Лаборатория Касперского»

УТВЕРЖДЕН  
643.46856491.00084-03 30 01-ЛУ

Программное изделие  
KASPERSKY SECURITY 10.1 ДЛЯ WINDOWS SERVER  
Формуляр

643.46856491.00084-03 30 01

Листов 17

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

Литера

2018

## 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	9
8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ.....	11
9. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ .....	11
10. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА .....	12
11. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ.....	13
12. СВЕДЕНИЯ О ХРАНЕНИИ.....	13
13. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ .....	14
14. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ.....	14
15. ОБНОВЛЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ .....	15
16. ОСОБЫЕ ОТМЕТКИ.....	17

## 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 10.1 для Windows Server»

Версия: 10.1.0.622

Обозначение: 643.46856491.00084-03

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	Дата создания	Длина, байт	КС
<b>Каталог D:\</b>				
1	critical_fix_core_6(14306)_x64.msp	10.07.18 16-20	19161088	57c2c52c7acc779a5e376d3d832e98a1db795b6fdf4ab820c0dee7fc086c77db
2	critical_fix_core_6(14306)_x86.msp	10.07.18 16-20	19034112	eb1924972bc3a315cff758beed8968c9de08d3723f5765f44278ecab815e2349
3	ks4ws_10.1.0.622_ru.exe	07.03.18 21-57	297821728	d8756e2b0d179ce1a1f3ee451d5c880e89cd90cac025de1964f15e885b2e2147
<b>итого: файлов - 3</b>			<b>336016928</b>	<b>64ae8f905c18486e3033dbc673fb78668cbc18d7203803cde65755dfd21c75d5</b>
<b>ВСЕГО: файлов - 3</b>			<b>336016928</b>	<b>64ae8f905c18486e3033dbc673fb78668cbc18d7203803cde65755dfd21c75d5</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<sup>1</sup>:

- возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- возможность читать информацию из записей аудита;
- ограничение доступа к чтению записей аудита;
- упорядочение данных аудита;
- возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности САВЗ;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;
- поддержка определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами сервера;
- возможность выполнять проверки с целью обнаружения зараженных KB объектов;
- возможность выполнения проверок с целью обнаружения зараженных KB объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- возможность выполнять проверки с целью обнаружения зараженных KB объектов сигнатурными и эвристическими методами;
- возможность выполнять проверки с целью обнаружения зараженных KB объектов по команде и в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- возможность выполнять проверки с целью обнаружения зараженных KB объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность удаления (если технически возможно) файлов, в которых обнаружены KB, а также файлов, подозрительных на наличие KB, перемещение и изолирование объектов воздействия;

<sup>1</sup> 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: АВЗ.1 — Реализация антивирусной защиты; АВЗ.2 — Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

- возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных KB;
- возможность отображения сигнала тревоги на APM администратора, в том числе до подтверждения его получения или до завершения сеанса;
- возможность восстановления функциональных свойств зараженных объектов;
- возможность получения и установки обновлений БД ПКВ без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения;
- возможность мониторинга контроля выполнения файловых операций объектов;
- возможность проводить анализ журналов событий Windows;
- возможность выполнять проверки с целью обнаружения атаки эксплойтов в памяти процессов, в контейнерах Windows Server 2016;
- возможность при обнаружении признаков атаки эксплойтов на защищаемый процесс завершать процесс, сообщать о факте дискредитации уязвимости в процессе.

## 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 10.1 для Windows Server. Инсталляционный комплект	643.46856491.00084-03	1		На лазерном диске
2. Kaspersky Security 10.1 для Windows Server. Формуляр	643.46856491.00084-03 30 01	1		В печатном виде
3. Kaspersky Security 10.1 для Windows Server. Приложение 1 к формуляру	643.46856491.00084-03 30 02	1		В электронном виде
4. Kaspersky Security 10.1 для Windows Server. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00084-03 90 01	1		В электронном виде
5. Kaspersky Security 10.1 для Windows Server. Руководство пользователя	643.46856491.00084-03 90 02	1		В электронном виде
6. Kaspersky Security 10.1 для Windows Server. Руководство по эксплуатации для защиты сетевых хранилищ	643.46856491.00084-03 90 03	1		В электронном виде
7. Копия сертификата соответствия				
8. Упаковка		1		
<i>Примечание: поставка осуществляется с заверенной копией сертификатов соответствия на изделие при их наличии. В случае получения комплекта с веб-сайта производителя все материалы предоставляются в электронном виде (см. раздел 15 настоящего формуляра).</i>				

## 6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

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

6.1.1. Требования к серверу, на который устанавливается Kaspersky Security:

### Аппаратные требования к серверу

- x86-64-совместимые системы в однопроцессорной и многопроцессорной конфигурации;
- объем дискового пространства:
- для установки всех программных компонентов – 70 МБ;
- для загрузки и хранения антивирусных баз программы – 2 Гб (рекомендуется);
- для хранения объектов на карантине и в резервном хранилище – 400 МБ (рекомендуется);
- для хранения журналов – 1 Гб (рекомендуется).

### Рекомендуемая конфигурация:

- процессор: четырехпроцессорный 2,4 ГГц.
- объем оперативной памяти: 2 GB.
- дисковая подсистема: 4 Гб доступного пространства.

### Программные требования к серверу

Для установки и работы Kaspersky Security 10.1 для Windows Server требуется наличие на сервере Microsoft Windows Installer 3.1.

6.1.2. ОО может функционировать на одной из следующих 32-разрядных систем:

- Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1.

6.1.3. ОО может функционировать на одной из следующих 64-разрядных систем:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Windows Server 2008 R2 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Windows Hyper-V® Server 2008 R2 с пакетом обновлений SP1;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint™ Server 2011;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server;
- Windows Server 2012 Core Standard / Datacenter;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;Kaspersky Security 10.1 для Windows Server
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server;
- Windows Server 2016 Core Standard / Datacenter;
- Windows Storage Server 2016;
- Windows Hyper-V Server 2016.

**ОО функционирует на следующих типах терминальных серверов:**

- Microsoft Remote Desktop Services на базе Windows 2008 Server;
- Microsoft Remote Desktop Services на базе Windows 2008 R2 Server;
- Microsoft Remote Desktop Services на базе Windows 2012 Server;
- Microsoft Remote Desktop Services на базе Windows 2012 Server R2;
- Microsoft Remote Desktop Services на базе Windows Server 2016;
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15;
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

6.1.4. Требования к защищаемому сетевому хранилищу:

Изделие может использоваться для защиты следующих сетевых хранилищ:

- NetApp® с одной из следующих операционных систем:
  - Data ONTAP® 7.x и Data ONTAP 8.x в режиме 7-mode;
  - Data ONTAP 8.2.1 или выше в режиме cluster-mode.
- Dell EMC™ Celerra™ / VNX™ со следующим программным обеспечением:
  - операционная система EMC DART 6.0.36;
  - Антивирусный агент Celerra (CAVA) 4.5.2.3.
- Dell EMC Isilon™ с операционной системой OneFS™ 7.0.
- Hitachi NAS на одной из следующих платформ:
  - HNAS 4100;

- HNAS 4080;
  - HNAS 4060;
  - HNAS 4040;
  - HNAS 3090;
  - HNAS 3080.
- IBM® NAS серии IBM System Storage® N series.
  - Oracle® NAS Systems семейства Oracle ZFS Storage Appliance.
  - Dell™ NAS на платформе Dell Compellent™ FS8600.

6.1.5. Требования к компьютеру, на который устанавливается Консоль Kaspersky Security  
**Аппаратные требования к компьютеру**

- Рекомендуемый объем оперативной памяти – 128 МБ или более.
- Свободное дисковое пространство: 30 МБ.

**Программные требования к компьютеру**

Для установки и работы Консоли ОО требуется наличие на компьютере Microsoft Windows Installer 3.1. Консоль ОО может функционировать на одной из следующих 32-разрядных систем:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Microsoft Windows XP Professional с пакетом обновлений SP2;
- Microsoft Windows Vista®;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10.

ОО может функционировать на одной из следующих 64-разрядных систем:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint™ Server 2011;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server;
- Windows Storage Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server;
- Windows Storage Server 2016;
- Microsoft Windows XP Professional Edition с пакетом обновлений SP2;
- Microsoft Windows Vista;
- Microsoft Windows 7;
- Microsoft Windows 8;

- Microsoft Windows 8.1;
  - Microsoft Windows 10.
- 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 З). 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](http://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.

## **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 3.



**8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ**

Программное изделие «Kaspersky Security  
10.1 для Windows Server»  
(наименование программного изделия)

643.46856491.00084-03  
(обозначение)

соответствует техническим условиям  
(стандарту)

ТУ 643.46856491.00084-03  
(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**

**Kaspersky Security 10.1 для Windows Server (643.46856491.00084-03)**

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: 64ae8f905c18486e3033dbc673fb78668cbc18d7203803cde65755dfd21c75d5

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 643.46856491.00084-03 при соблюдении потребителем условий и правил эксплуатации, транспортирования и хранения, установленных в эксплуатационной документации.
- 10.2. Гарантийный срок эксплуатации программного изделия равен 1 году со дня приобретения.
- 10.3. 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.
- 10.4. 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, предпринимает необходимые действия для обновления программного изделия, описанные в разделе 15.
- 10.8. Гарантийное и послегарантийное обслуживание изделия осуществляется: АО «Лаборатория Касперского» (125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2).
- 10.9. Для изделий, поставляемых в МО РФ, 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
<b>Выпуск</b>	Регулярно в соответствии с установленной изготовителем процедурой, вплоть до окончания срока поддержки программного изделия	По необходимости (при выявлении уязвимостей)	По усмотрению изготовителя
<b>Публикация</b>	Непосредственно после выпуска	Непосредственно после выпуска	По прохождении инспекционного контроля
<b>Инспекционный контроль</b>	1 раз в год (полный пакет обновлений)	После выпуска — в срок, предусмотренный изготовителем	После выпуска — в срок, предусмотренный изготовителем
<b>Уведомление</b>	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
<b>Получение и применение</b>	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 643.46856491.00084-03 30 02 в электронном виде.