

АО «Лаборатория Касперского»

УТВЕРЖДЕН

643.46856491.00068-05 30 01-ЛУ

Программное изделие

KASPERSKY ENDPOINT SECURITY 10 ДЛЯ WINDOWS

Формуляр

643.46856491.00068-05 30 01

Листов 17

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.....	4
4. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ	4
5. КОМПЛЕКТНОСТЬ.....	6
6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ.....	6
7. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ	8
8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ	9
9. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ	9
10. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА.....	10
11. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ	11
12. СВЕДЕНИЯ О ХРАНЕНИИ	12
13. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ.....	13
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 незавершенные исправления не допускаются.

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Сведения о программном изделии:

Наименование: «Kaspersky Endpoint Security 10 для Windows»

Версия: 10.3.0.6294

Обозначение: 643.46856491.00068-05

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 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 дистрибутива программного изделия

№ пп	Имя файла	Дата создания	Длина, байт	КС
Каталог D:\				
1	kes10winsp2_ru_aes56.exe	13.03.17 11-46	274446872	6e557854463fbcc8e0767315b0f00d818023b6a324609dca785384dc87093e
итого: файлов — 1			274446872	6e557854463fbcc8e0767315b0f00d818023b6a324609dca785384dc87093e
ВСЕГО: файлов — 1			274446872	6e557854463fbcc8e0767315b0f00d818023b6a324609dca785384dc87093e
<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 Реализованные в программном изделии функции безопасности (АВЗ.1, АВЗ.2):

4.1.1 Аудит безопасности:

- а) возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
- б) возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- в) возможность читать информацию из записей аудита;
- г) ограничение доступа к чтению записей аудита;
- д) поиск, сортировка и упорядочение данных аудита;

4.1.2 Управление безопасностью:

¹ 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).

- а) возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности САВЗ;
- б) возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;
- в) поддержка определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и пользователями ИС.

4.1.3 Проверки объектов заражения:

- а) возможность выполнять проверки с целью обнаружения зараженных КВ объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
- б) возможность выполнения проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных.

4.1.4 Методы проверок объектов заражения:

- а) возможность выполнять проверки с целью обнаружения зараженных КВ объектов сигнатурными и эвристическими методами, методом запроса репутации;
- б) возможность выполнять проверки с целью обнаружения зараженных КВ объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- в) возможность выполнять проверки с целью обнаружения зараженных КВ объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой;

4.1.5 Обработка объектов, подвергшихся воздействию:

- а) возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены КВ, а также файлов, подозрительных на наличие КВ, возможность перемещения и изолирования зараженных объектов;

4.1.6 Блокирование:

- а) возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных КВ, АРМ или сервера, на которых обнаружены зараженные файлы;

4.1.7 Сигнализация:

- а) возможность отображения сигнала тревоги на АРМ пользователя или АРМ администратора безопасности, в том числе до подтверждения его получения или до завершения сеанса;

4.1.8 Восстановление объектов:

- а) возможность восстановления функциональных свойств зараженных объектов;

4.1.9 Обновление базы данных ПКВ:

- а) возможность получения и установки обновлений БД ПКВ без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса.

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 учётный номер	Примечание
1. «Kaspersky Endpoint Security 10 для Windows». Инсталляционный комплект		1		На лазерном диске
2. «Kaspersky Endpoint Security 10 для Windows». Формуляр	643.46856491.00068-05 30 01	1		Твердая копия
3. «Kaspersky Endpoint Security 10 для Windows». Приложение 1 к формуляру	643.46856491.00068-05 30 02	1		В электронном виде
4. «Kaspersky Endpoint Security 10 для Windows». Руководство администратора	643.46856491.00068-05 90 01	1		В электронном виде
5. Упаковка		1		

Примечание: поставка осуществляется с заверенной копией сертификатов соответствия на изделие при их наличии.

6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

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

6.1.1. Минимальные общие требования

- 2 ГБ свободного места на жестком диске;
- Microsoft® Internet Explorer® 7.0;
- Подключение к интернету для активации программного изделия, обновления БД ПКВ;
- Процессор Intel Pentium 1 ГГц (или совместимый аналог);
- Оперативная память:
 - для 32-разрядной операционной системы — 1 ГБ;
 - для 64-разрядной операционной системы — 2 ГБ.

6.1.2. Поддерживаемые операционные системы для рабочих станций

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1,
- Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1;
- Microsoft Windows 8 Professional / Enterprise x86 Edition,
- Microsoft Windows 8 Professional / Enterprise x64 Edition,
- Microsoft Windows 8.1 Enterprise x86 Edition,
- Microsoft Windows 8.1 Enterprise x64 Edition;
- Microsoft Windows 10 Pro / Enterprise x86 Edition (с ограничениями),
- Microsoft Windows 10 Pro / Enterprise x64 Edition (с ограничениями).

6.1.3. Поддерживаемые операционные системы для файловых серверов

- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1,
- Microsoft Windows Server 2008 Standard / Enterprise x86 Edition SP2,

- Microsoft Windows Server 2008 Standard / Enterprise x64 Edition SP2;
 - Microsoft Windows Small Business Server 2011 Essentials / Standard x64 Edition;
 - Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition,
 - Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition,
 - Microsoft Windows MultiPoint Server 2012 x64 Edition;
 - Microsoft Windows Server 2016 (с ограничениями).
- 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. При инсталляции программного изделия должен быть выбран тип установки «Стандартная установка».
- 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» (643.46856491.00082-02) в соответствии с руководством администратора 643.46856491.00082-02 90 02.
- В остальных случаях механизм облачной защиты KSN должен быть гарантировано отключен. Отключение данной функциональной возможности должно быть выполнено в соответствии со следующим порядком действий:
- 1) В главном окне приложения выбрать вкладку **Настройка**.
 - 2) Перейти по ветке **Дополнительные параметры — Параметры KSN**.
 - 3) Снять флаг с опции **Принимаю условия Положения и участвую в KSN**.
 - 4) Нажать на кнопку **Сохранить**. Взаимодействие с сервисом KSN прекращается.

8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное изделие «Kaspersky Endpoint Security 10 для Windows» 643.46856491.00068-05
(наименование программного изделия) (обозначение)

соответствует техническим условиям ТУ 643.46856491.00068-05
(стандарту) (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 Endpoint Security 10 для Windows (643.46856491.00068-05)
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.

Общая контрольная сумма ЛД:

6e557854463fbcc8e0767315b0f00d818023b6a324609dca785384dc87093e

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. Изготовитель гарантирует соответствие программного изделия требованиям ТУ 643.46856491.00068-05 при соблюдении потребителем условий транспортирования, правил хранения и эксплуатации.

Гарантийный срок хранения программного изделия на носителях информации — 1 год со дня изготовления программного изделия.

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.

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 643.46856491.00068-05 30 02 в электронном виде.