

АО «Лаборатория Касперского»

УТВЕРЖДЕН

643.46856491.00100-04 30 01-ЛУ

Программное изделие

KASPERSKY ENDPOINT SECURITY ДЛЯ WINDOWS

(ВЕРСИЯ 11.6.0.394)

Формуляр

643.46856491.00100-04 30 01

Листов 14

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

2021

Литера

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ	3
2. ОБЩИЕ СВЕДЕНИЯ.....	3
3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	4
4. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ	4
5. КОМПЛЕКТНОСТЬ	5
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. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА	10
12. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ.....	10
13. СВЕДЕНИЯ О ХРАНЕНИИ.....	11
14. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ	11
15. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ.....	12
16. ПОЛУЧЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭЛЕКТРОННОЙ ПОСТАВКЕ	13
17. ОБНОВЛЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ	13
18. ОСОБЫЕ ОТМЕТКИ.....	14

1. ОБЩИЕ УКАЗАНИЯ

- 1.1. Настоящий формуляр удостоверяет комплектность, гарантированное изготовителем качество программного изделия и содержит указания по его эксплуатации.
- 1.2. 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 Endpoint Security для Windows (версия 11.6.0.394)»

Версия: 11.6.0.394

Обозначение: 643.46856491.00100-04

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	Дата создания	Длина, байт	КС
Каталог D:\				
1	keswin_11.6.0.394_ru_aes56.exe	27.02.21 03-42	376331848	f9d152233f60af46d2bcbb99ae852b531cf976a315eec31158d8884c9a4f1a94
2	keswin_web_plugin_11.6.0.394.zip	27.02.21 03-42	93014895	76591ec9291383644d82a92d3d7f89cc64f3f38bf95e4e3669960253d33bcd80
итого: файлов - 2			469346743	8f884cea16732c229f3e12b493faa29f780a8528ecb08d27314e8a1f4974d714
ВСЕГО: файлов - 2			469346743	8f884cea16732c229f3e12b493faa29f780a8528ecb08d27314e8a1f4974d714
<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.

4. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- 4.1. В программном изделии реализованы следующие функции безопасности:
- 4.1.1. разграничение доступа к управлению САВЗ:
поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами серверов или пользователями ИС;
- 4.1.2. управление работой САВЗ:
возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;
- 4.1.3. управление параметрами САВЗ:
возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;
- 4.1.4. управление установкой обновлений (актуализации) БД ПКВ САВЗ:
получение и установку обновлений БД ПКВ: в автоматизированном режиме с сетевого ресурса; без применения средств автоматизации;
- 4.1.5. аудит безопасности САВЗ:
а) генерацию записи аудита для событий, подвергаемых аудиту;
б) чтение информации из записей аудита;
в) ассоциацию событий аудита с идентификаторами субъектов;
г) ограничение доступа к чтению записей аудита;
д) поиск, сортировку, упорядочение данных аудита;
- 4.1.6. выполнение проверок объектов воздействия:
а) выполнение проверок 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) выполнение проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
в) выполнение проверок 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 проверок с целью обнаружения зараженных КВ объектов сигнатурными и эвристическими методами;
- 4.1.7. обработка объектов воздействия:
а) удаление (если удаление технически возможно) кода КВ из оперативной памяти, удаления файлов, в

которых обнаружены КВ, а также файлов, подозрительных на наличие КВ, возможность перемещения и изолирования зараженных объектов, удаления кода КВ из файлов и системных областей носителей информации;

- б) блокирование доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных КВ;
- в) предоставление возможности блокирования сервера, на котором обнаружены зараженные файлы или блокирование АРМ, на котором обнаружены зараженные файлы;
- г) восстановление функциональных свойств зараженных объектов;

4.1.8. сигнализация САВЗ:
отображение сигнала тревоги об обнаружении КВ;

4.1.9. идентификация и аутентификация администратора безопасности:
возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью

4.1.10. ограничение программной среды:

- а) возможность контроля доступа к веб-ресурсам;
- б) возможность контроля за запуском ПО на защищаемом сервере или АРМ.

Примечание — Функции безопасности соответствуют следующим мерам защиты информации в информационных системах, согласно приказу №17 ФСТЭК России, и мерам 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).

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 Endpoint Security для Windows (версия 11.6.0.394). Инсталляционный комплект	643.46856491.00100-04	1		На лазерном диске
2. Kaspersky Endpoint Security для Windows (версия 11.6.0.394). Формуляр	643.46856491.00100-04 30 01	1		В печатном виде
3. Kaspersky Endpoint Security для Windows (версия 11.6.0.394). Формуляр. Приложение 1	643.46856491.00100-04 30 02	1		На лазерном диске
4. Kaspersky Endpoint Security для Windows (версия 11.6.0.394). Подготовительные процедуры и руководство по эксплуатации	643.46856491.00100-04 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		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 Endpoint Security для Windows (версия 11.6.0.394). Инсталляционный комплект	643.46856491.00100-04	1		В электронном виде

¹ Заверенная копия сертификата соответствия поставляется при его наличии. Согласно п.73 Положения о системе сертификации средств защиты информации, обновления программного изделия, направленные на устранение уязвимостей, доводятся до потребителей до проведения сертификационных испытаний.

Наименование изделия (составной части, документа)	Обозначение конструкторского документа	Кол-во	Порядковый учетный номер	Примечание
2. Kaspersky Endpoint Security для Windows (версия 11.6.0.394). Формуляр	643.46856491.00100-04 30 01	1		В электронном виде
3. Kaspersky Endpoint Security для Windows (версия 11.6.0.394). Формуляр. Приложение 1	643.46856491.00100-04 30 02	1		В электронном виде
4. Kaspersky Endpoint Security для Windows (версия 11.6.0.394). Подготовительные процедуры и руководство по эксплуатации	643.46856491.00100-04 90 01	1		В электронном виде
5. Копия выданного ФСТЭК России сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации ²		1		В электронном виде

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;
- Подключение к интернету для активации программного изделия, обновления БД ПКВ;
- Процессор 1 ГГц (с поддержкой инструкций SSE2);
- Оперативная память:
 - o для 32-разрядной операционной системы – 1 ГБ;
 - o для 64-разрядной операционной системы – 2 ГБ.

6.1.2. Поддерживаемые операционные системы для рабочих станций (32- и 64-разрядные версии):

- Microsoft Windows 7 SP1 Home / Professional / Ultimate / Enterprise;
- Microsoft Windows 8 Professional / Enterprise;
- Microsoft Windows 8.1 Professional / Enterprise;
- Microsoft Windows 10 Home / Pro / Education / Enterprise (TH1, TH2, RS1, RS2, RS3, RS4, RS5, 19H1, 19H2, 20H1, 20H2) (с ограничениями)³.

6.1.3. Поддерживаемые операционные системы для файловых серверов (64-разрядные версии):

- Windows Small Business Server 2011 Essentials / Standard⁴;
- Windows MultiPoint Server 2011;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter (с ограничениями);

² Копия сертификата соответствия поставляется при его наличии. Согласно п.73 Положения о системе сертификации средств защиты информации, обновления программного изделия, направленные на устранение уязвимостей, доводятся до потребителей до проведения сертификационных испытаний.

³ Особенности поддержки операционной системы Microsoft Windows 10 изложены в статье 13036 базы знаний Службы технической поддержки: <https://support.kaspersky.ru/13036>

⁴ Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2.

- Windows Server 2019 Essentials / Standard / Datacenter (с ограничениями)⁵.

6.1.4. Поддерживаемые виртуальные платформы:

- VMWare Workstation 16 Pro;
- VMware ESXi 7.0 Update 1a;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7;
- Citrix Provisioning 2009;
- Citrix Hypervisor 8.2 LTSR.

6.1.5. Программное изделие поддерживает работу со следующими версиями Kaspersky Security Center:

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 Patch A;
- Kaspersky Security Center 12 Patch B;
- Kaspersky Security Center 13.

6.2. Установка, предварительная настройка и эксплуатация программного изделия должны осуществляться в соответствии с эксплуатационной документацией, входящей в комплект поставки.

6.3. Использование операционных систем Microsoft Windows 7, Microsoft Windows 8 и Microsoft Windows Server 2008 R2 в качестве среды функционирования программного изделия допускается только для замены средств защиты информации, ранее установленных на аттестованных по требованиям безопасности информации объектах информатизации.

6.4. Активация программного изделия должна осуществляться только с использованием файла ключа.

6.5. 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.

6.6. 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.

6.7. Перед началом эксплуатации программного изделия необходимо установить все доступные обновления используемых версий ПО среды функционирования.

6.8. 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.

⁵ Особенности поддержки операционных систем Microsoft Windows Server 2016 и Microsoft Windows Server 2019 изложены в статье 13036 базы знаний Службы технической поддержки:
<https://support.kaspersky.ru/13036>

8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное изделие «Kaspersky Endpoint Security для
Windows (версия 11.6.0.394)»
(наименование программного изделия)

643.46856491.00100-04
(обозначение)

соответствует техническим условиям (стандарту)

ТУ 643.46856491.00100-04
(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 Endpoint Security для Windows

(версия 11.6.0.394)

(643.46856491.00100-04)

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: 8f884cea16732c229f3e12b493faa29f780a8528ecb08d27314e8a1f4974d714

Серийный номер: _____

Наименование пользователя: _____

№ сборки (PO): _____

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.

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). Сведения об обнаруженных уязвимостях программного изделия публикуются в банке данных угроз безопасности информации ФСТЭК России (<https://bdu.fstec.ru/vul>).

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 643.46856491.00100-04 30 02 в электронном виде.