

АО «Лаборатория Касперского»

УТВЕРЖДЕН

643.46856491.00047-03 30 01-ЛУ

Программное изделие

KASPERSKY WEB TRAFFIC SECURITY 6.0

Формуляр

643.46856491.00047-03 30 01

Листов 16

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

2018

Литера

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

## 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 Web Traffic Security 6.0»

Версия: 6.0.0.1545

Обозначение: 643.46856491.00047-03

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., 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
1	kwts-control-6.0.0-1545.x86_64.rpm	78011545	58626bc59a11206fd28e936fbd3c1c6bd857b597c2968ea582d9f922036c8942
2	kwts-control-110n-ru_6.0.0.1545-1_all.deb	5390420	58c4aad3aa8cce489b87c6cc3c80051020af862159d79158d56e34e6d8b54e3
3	kwts-control_6.0.0-1545_amd64.deb	50936090	39e292d818249ee2f2a727433d1e981efdb7c0d77ccf283111390b1428675a63
4	kwts-control_ru-6.0.0.1545-1.noarch.rpm	7165633	aa71dc681f9e4c123bfc8c6a6817f5d4c8b37d4b811cc60c201ee3977c64aa70
5	kwts-worker-6.0.0-1545.x86_64.rpm	188199244	da56d37249afb64fddf110485e00ef5884b628cf33fd750a5748cc5ec92bfac
6	kwts-worker_6.0.0-1545_amd64.deb	116329198	4e43158be94a50fd5cb72d177ce72e925d3ba5fc7dbbda7848591da349c63b9e
<b>итого: файлов - 6</b>		<b>446032130</b>	<b>0720495007e6d8c913057839d2fa51973a293719a45c14a5d38563899fb0a980</b>

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) поддержка определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами серверов или пользователями ИС;

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 установку обновлений БД ПКВ без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса;

4.1.5. аудит безопасности САВЗ:

- а) генерация записей 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, сортировку, упорядочение данных аудита;

4.1.6. выполнение проверок объектов воздействия:

- а) выполнение проверок 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 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;  
 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;
  - г) восстановление функциональных свойств зараженных объектов;
- 4.1.8. сигнализация САВЗ:
- а) отображение сигнала тревоги об обнаружении КВ;
- 4.1.9. фильтрация сообщений протокола ICAP:
- а) выполнение фильтрации сообщений протокола ICAP;
- 4.1.10. идентификация и аутентификация:
- а) выполнение идентификации и аутентификации администраторов САВЗ.
- 4.2. Функциональные возможности продукта могут использоваться при реализации в информационных системах следующих мер защиты информации, согласно приказу №17 ФСТЭК России, и мер 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 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 Web Traffic Security 6.0. Инсталляционный комплект	643.46856491.00047-03	1		На лазерном диске
2. Kaspersky Web Traffic Security 6.0. Формуляр	643.46856491.00047-03 30 01	1		В печатном виде
3. Kaspersky Web Traffic Security 6.0. Приложение 1 к формуляру	643.46856491.00047-03 30 02	1		В электронном виде
4. Kaspersky Web Traffic Security 6.0. Подготовительные процедуры и руководство по эксплуатации	643.46856491.00047-03 90 01	1		В электронном виде
5. Упаковка		1		
<i>Примечание: поставка осуществляется с заверенной копией сертификатов соответствия на изделие при их наличии.</i>				

## 6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

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

Обрабатывающий сервер:

- процессор Intel Xeon E5606 (4 ядра) 1,86 ГГц или выше;
- 8 ГБ оперативной памяти;
- раздел подкачки объемом не менее 4 ГБ;
- 100 ГБ на жестком диске, из которых:
  - o 25 ГБ для хранения временных файлов;
  - o 25 ГБ для хранения файлов журналов.

Управляющий сервер:

- процессор Intel Xeon E5606 (4 ядра) 1,86 ГГц или выше;
- 8 ГБ оперативной памяти;
- раздел подкачки объемом не менее 4 ГБ;
- 100 ГБ на жестком диске.

При установке Управляющего и Обрабатывающего сервера на одном физическом сервере:

- 2 процессора Intel Xeon E5606 (8 ядер) 1,86 ГГц или выше;
- 16 ГБ оперативной памяти;
- раздел подкачки объемом не менее 4 ГБ;
- 200 ГБ на жестком диске, из которых:
  - o 25 ГБ для хранения временных файлов;
  - o 25 ГБ для хранения файлов журналов.

Программные требования к серверам для установки Kaspersky Web Traffic Security 6.0:

- Red Hat Enterprise Linux версии 7.5 x64;
- Ubuntu 18.04.1 LTS;
- Debian 9.5;
- SUSE Linux Enterprise Server 12 SP3;
- CentOS версии 7.5 x64;
- Операционная система «Альт Линукс СПТ 7.0»;
- Astra Linux Special Edition 1.6. Только при отключенном механизме мандатного разграничения доступа и отключенном механизме создания замкнутой программной среды.

Дополнительные требования

- Nginx версий 1.10.3, 1.12.2, 1.14.0, 1.14.2;
- HAProxy для балансировки нагрузки версии 1.5;
- Squid версии 3.5.20, если вы устанавливаете сервис Squid на Обрабатывающий сервер;
- Active Directory на сервере Windows Server 2008 R2 или Windows Server 2012 R2;

- в операционной системе должна быть установлена локализация en\_US.UTF-8.

- 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 16 настоящего формуляра.
- 6.4. 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](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) в соответствии с руководством администратора 643.46856491.00082 90 02.  
В остальных случаях механизм облачной защиты KSN должен быть гарантировано отключен.



## 8. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программное изделие «Kaspersky Web  
Traffic Security 6.0»  
(наименование программного изделия)

643.46856491.00047-03  
(обозначение)

соответствует техническим условиям  
(стандарту)

ТУ 643.46856491.00047-03  
(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 Web Traffic Security 6.0

(643.46856491.00047-03)

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: **0720495007e6d8c913057839d2fa51973a293719a45c14a5d38563899fb0a980**

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.*



## 12. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

- 12.1. Изготовитель принимает на себя обязательства по технической поддержке программного изделия в объеме, указанном на странице <https://support.kaspersky.ru/support/rules> веб-сайта изготовителя.
- 12.2. В период оказания технической поддержки изготовитель гарантирует осуществление программным изделием функциональных возможностей, изложенных в формуляре, при соблюдении пользователем требований по эксплуатации, изложенных в эксплуатационной документации.
- 12.3. Срок оказания технической поддержки для программного изделия указан на странице <https://support.kaspersky.ru/support/lifecycle> веб-сайта изготовителя. Потребитель обязан самостоятельно контролировать статус поддержки программного изделия.
- 12.4. Использование программного изделия после прекращения технической поддержки не допускается.
- 12.5. 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 рассылок с почтового ящика Certification\_news@kaspersky.com.
- 12.6. 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, сертификационные испытания обновления безопасности в системе сертификации;
  - Размещает обновление безопасности, измененную эксплуатационную документацию, обновленный сертификат соответствия (в случае переоформления) на странице <https://certifiedbuilds.kaspersky.ru/>;
  - Потребитель, при получении указанной информации, предпринимает необходимые действия для обновления программного изделия, описанные в разделе 16.





## 16. ОБНОВЛЕНИЕ ПРОГРАММНОГО ИЗДЕЛИЯ

16.1. 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).

16.2. 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. 16.3 и 16.4

\* 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: <https://certifiedbuilds.kaspersky.ru>).

\*\* <https://support.kaspersky.ru/general/certificates>

16.3. 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.*

16.4. 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.

## **17. ОСОБЫЕ ОТМЕТКИ**

17.1. Приложение 1 выполнено в виде отдельного документа 643.46856491.00047-03 30 02 в электронном виде.