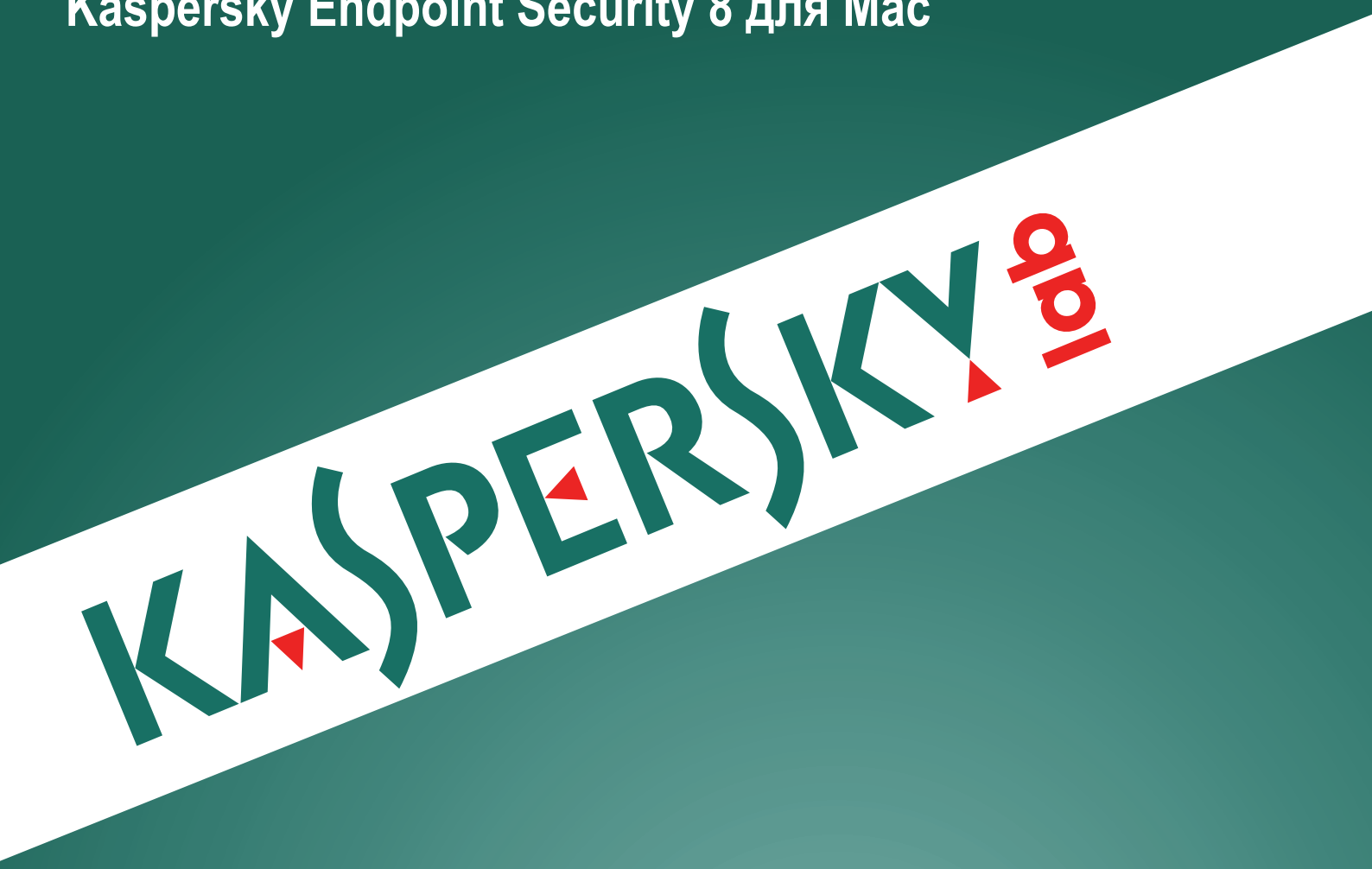
Kaspersky Endpoint Security 8 для Mac



Руководство администратора

ВЕРСИЯ ПРОГРАММЫ: 8.0

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 21.10.2010

http://www.kaspersky.ru
http://support.kaspersky.ru

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

Лицензионное соглашение ЗАО «Лаборатория Касперского» определяющее условия использования программного обеспечения (ПО) с конечным пользователем.

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программным обеспечением.

Нажатие Вами кнопки подтверждения согласия в окне с текстом Лицензионного соглашения при установке ПО или ввод соответствующего символа(-ов) означает Ваше безоговорочное согласие с условиями настоящего Лицензионного соглашения. Если Вы не согласны с условиями настоящего Лицензионного соглашения, Вы должны прервать установку ПО.

В случае наличия лицензионного договора или подобного документа, условия использования ПО, изложенные в таком договоре, являются превалирующими над условиями настоящего Лицензионного соглашения с конечным пользователем.

1. Определения

1.1. **ПО** - обозначает программное обеспечение, сопроводительные материалы, обновления, описанные в Руководстве Пользователя, Правообладателем которых является ЗАО «Лаборатория Касперского».

1.2. **Правообладатель** (обладатель исключительного права на ПО) - ЗАО «Лаборатория Касперского».

1.3. **Компьютер** - оборудование, для работы на котором предназначено ПО, на которое устанавливается ПО и/или на котором используется ПО.

1.4. **Пользователь (Вы)** - физическое лицо, которое устанавливает или использует ПО от своего лица или правомерно владеет копией ПО. Если ПО было загружено или приобретено от имени юридического лица, то под термином Пользователь (Вы) далее подразумевается юридическое лицо, для которого ПО было загружено или приобретено и которое поручило отдельному физическому лицу принять данное соглашение от своего лица.

1.5. **Партнеры** - организации, осуществляющие распространение ПО на основании договора с Правообладателем.

1.6. **Обновление(-я)** - все улучшения, исправления, расширения и/или модификации ПО.

1.7. **Руководство Пользователя** - сопроводительные печатные и иные материалы, Руководство Пользователя, Руководство Администратора, справочник, файл справки и аналогичные им печатные и электронные документы, Правообладателем которых является ЗАО «Лаборатория Касперского».

2. Предоставление лицензии

2.1. Вам предоставляется неисключительная лицензия на использование ПО для защиты компьютера от угроз, описанных в Руководстве Пользователя, при условии соблюдения Вами всех технических требований, описанных в Руководстве Пользователя, а также всех ограничений и условий использования ПО, указанных в настоящем Лицензионном соглашении.

В случае если Вы получили, загрузили и/или установили ПО, предназначенное для ознакомительных целей, Вы имеете право использовать ПО только в целях ознакомления и только в течение одного ознакомительного периода, если не прописано иначе, начиная с даты начальной установки ПО. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.

Если Вы используете ПО разных версий ПО или версии ПО для разных языков, если Вы получили ПО на нескольких носителях, если Вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее количество Ваших компьютеров, на которых установлены и/или используются все версии ПО, должно соответствовать количеству компьютеров, в полученных Вами лицензиях *в том случае*, если условия лицензий не утверждают иное; каждая приобретенная лицензия дает Вам право установить и использовать ПО на таком количестве компьютеров, которое указано в п.2.2 и п.2.3.

2.2. В случае приобретения ПО на материальном носителе Вы имеете право использовать ПО для защиты такого количества компьютеров, которое указано на упаковке.

2.3. В случае приобретения ПО через интернет Вы имеете право использовать ПО для защиты такого количества компьютеров, которое указано при приобретении ПО.

2.4. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

2.5. После активации ПО или выполнения процедуры установки файла ключа (за исключением ПО, предназначенного для ознакомительных целей) Вам предоставляется возможность в течение срока, указанного на упаковке (в случае приобретения ПО на материальном носителе) или указанного Вами при оформлении покупки (в случае приобретения ПО через интернет), получать от Правообладателя или его Партнеров:

- новые версии ПО по мере их выхода (через интернет);

- техническую поддержку (по телефону и/или через интернет).

3. Активация и сроки

3.1. Если Вы модифицируете свой компьютер или вносите изменения в программное обеспечение других правообладателей, установленное на компьютере, то может потребоваться повторная активация ПО или повторная процедура установки файла ключа. Правообладатель оставляет за собой право использовать средства для проверки наличия у Вас лицензионной копии ПО.

3.2. В случае приобретения ПО на материальном носителе срок использования ПО указывается на упаковке.

3.3. В случае приобретения ПО через интернет срок использования ПО указывается при приобретении ПО.

3.4. Вы имеете право использовать ПО, предназначенное для ознакомительных целей и распространяемое без выплаты вознаграждения, как указано в п.2.1, в течение 30 (тридцати) дней с момента активации ПО в соответствии с условиями настоящего Лицензионного соглашения.

3.5. Срок полезного использования ограничивается сроком использования ПО, указанным в п.3.2 и п.3.3; информацию о сроке использования ПО можно проверить с помощью средств, указанных в Руководстве Пользователя.

3.6. В случае приобретения ПО для защиты более чем одного компьютера срок использования ПО начинается с даты активации или установки файла ключа на первом компьютере.

3.7. В случае нарушения Вами какого-либо из условий данного Лицензионного соглашения Правообладатель вправе прервать действие данного Лицензионного соглашения в любое время без Вашего уведомления и без возмещения стоимости ПО или его части.

4. Техническая поддержка

4.1. Техническая поддержка, указанная в п. 2.5 настоящего Лицензионного соглашения, предоставляется при условии установки Пользователем последнего обновления ПО (за исключением ПО, предназначенного для ознакомительных целей).

Служба технической поддержки: http://support.kaspersky.com.

4.2. Данные Пользователя, указанные в Персональном кабинете/Личном кабинете, могут быть использованы специалистами Службы технической поддержки только при обработке его запроса в указанную Службу.

5. Ограничения

5.1. Вы не вправе декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на ПО, целиком или частично, за исключением случаев, предусмотренных законодательством.

5.2. Запрещается передавать право на использование ПО третьим лицам.

5.3. Запрещается передавать и предоставлять доступ к коду активации и/или файлу ключа третьим лицам в нарушение положений настоящего Лицензионного соглашения. Код активации и файл ключа являются конфиденциальной информацией.

5.4. Запрещается сдавать ПО в аренду, прокат или во временное пользование.

5.5. Запрещается использовать ПО с целью создания данных или кода, предназначенных для обнаружения, блокирования или лечения угроз, описанных в Руководстве Пользователя.

5.6. В случае нарушения Вами условий настоящего Лицензионного соглашения, Ваш файл ключа может быть заблокирован.

5.7. При использовании Вами ПО, предназначенного для ознакомительных целей, Вы не имеете права получать техническую поддержку, указанную в п.4 настоящего Лицензионного соглашения, а также передавать имеющийся у Вас экземпляр ПО третьим лицам.

5.8. За нарушение интеллектуальных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством.

6. Ограниченная гарантия и отказ от предоставления гарантий

6.1. Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в Руководстве Пользователя.

6.2. Вы соглашаетесь с тем, что никакое ПО не свободно от ошибок и Вам рекомендуется регулярно создавать резервные копии своих файлов.

6.3. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Руководстве Пользователя, а также в случае нарушения Пользователем условий настоящего Лицензионного соглашения.

6.4. Правообладатель не гарантирует Пользователю работоспособность ПО, если Пользователь не осуществляет обновления ПО, указанные в п.2.5 настоящего Лицензионного соглашения.

6.5. Правообладатель не гарантирует Пользователю защиту от угроз, описанных в Руководстве Пользователя, по окончании срока, указанного в п.3.2 и п.3.3 настоящего Лицензионного соглашения.

6.6. ЗА ИСКЛЮЧЕНИЕМ УСТАНАВЛИВАЕМОЙ В НАСТОЯЩЕМ ПУНКТЕ ОГРАНИЧЕННОЙ ГАРАНТИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ НА ЕГО ИСПОЛЬЗОВАНИЕ ИЛИ ПРОИЗВОДИТЕЛЬНОСТЬ. ЗА ИСКЛЮЧЕНИЕМ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ, СТЕПЕНЬ КОТОРЫХ НЕ МОЖЕТ БЫТЬ ИСКЛЮЧЕНА ИЛИ ОГРАНИЧЕНА В СООТВЕТСТВИИ С ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ (ВЫРАЖАЕМЫХ В ЯВНОЙ ИЛИ В ПОДРАЗУМЕВАЕМОЙ ФОРМЕ) НА ВСЕ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ НЕНАРУШЕНИЕ ПРАВ ТРЕТЬИХ ЛИЦ, КОММЕРЧЕСКОЕ КАЧЕСТВО, ИНТЕГРАЦИЮ ИЛИ ПРИГОДНОСТЬ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ВЫ СОГЛАШАЕТЕСЬ С ТЕМ, ЧТО ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, ЗА УСТАНОВКУ И ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ЗА РЕЗУЛЬТАТЫ, ПОЛУЧЕННЫЕ С ЕГО ПОМОЩЬЮ.

7. Ограничение ответственности

7.1. В МАКСИМАЛЬНОЙ СТЕПЕНИ, ДОПУСКАЕМОЙ ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И/ИЛИ ЕГО ПАРТНЕРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКИЕ-ЛИБО УБЫТКИ И/ИЛИ УЩЕРБ (В ТОМ ЧИСЛЕ УБЫТКИ В СВЯЗИ С НЕДОПОЛУЧЕННОЙ КОММЕРЧЕСКОЙ ПРИБЫЛЬЮ, ПРЕРЫВАНИЕМ ДЕЯТЕЛЬНОСТИ, УТРАТОЙ ИНФОРМАЦИИ ИЛИ ИНОЙ ИМУЩЕСТВЕННЫЙ УЩЕРБ), ВОЗНИКАЮЩИЕ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИЛИ НЕВОЗМОЖНОСТЬЮ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПРАВООБЛАДАТЕЛЬ И/ИЛИ ЕГО ПАРТНЕРЫ БЫЛИ УВЕДОМЛЕНЫ О ВОЗМОЖНОМ ВОЗНИКНОВЕНИИ ТАКИХ УБЫТКОВ И/ИЛИ УЩЕРБА. В ЛЮБОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ ПРАВООБЛАДАТЕЛЯ И/ИЛИ ЕГО ПАРТНЕРОВ ПО ЛЮБОМУ ИЗ ПОЛОЖЕНИЙ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ОГРАНИЧИВАЕТСЯ СУММОЙ, ФАКТИЧЕСКИ УПЛАЧЕННОЙ ВАМИ ЗА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. НАСТОЯЩИЕ ОГРАНИЧЕНИЯ НЕ МОГУТ БЫТЬ ИСКЛЮЧЕНЫ ИЛИ ОГРАНИЧЕНЫ В СООТВЕТСТВИИ С ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ.

8. Открытое (свободное) программное обеспечение

8.1. Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) Пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают Пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду («ПО с открытым исходным кодом»). Если такая лицензия предусматривает предоставление исходного кода Пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса на адрес source@kaspersky.com или сопровождается с продуктом. Если какая-либо лицензия на ПО с открытым исходным кодом требует, чтобы Правообладатель предоставлял права на использование, копирование или модификацию ПО с открытым исходным кодом, выходящие за рамки прав, предоставляемых настоящим Лицензионным соглашением, такие права имеют преимущественную силу над правами и ограничениями, оговоренными в настоящем Лицензионном соглашении.

9. Права на интеллектуальную собственность

9.1. Вы соглашаетесь с тем, что ПО, документация, как и все другие объекты авторского права, а также системы, идеи и методы работы, другая информация, которая содержится в ПО, товарные знаки - являются объектами интеллектуальной собственности Правообладателя или его Партнеров. Данное Лицензионное соглашение не дает Вам никаких прав на использование объектов интеллектуальной собственности, включая товарные знаки и знаки обслуживания Правообладателя или его Партнеров, за исключением переданных Вам прав Правообладателем или его Партнерами

9.2. Вы соглашаетесь с тем, что не будете модифицировать или изменять ПО никаким способом. Запрещается удалять или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.

10. Применимое законодательство

10.1. Настоящее Лицензионное соглашение регулируется в соответствии с законодательством Российской Федерации.

11. Контактная информация Правообладателя

Центральный офис:

ЗАО «Лаборатория Касперского», 1-й Волоколамский проезд 10 корпус 1

Москва, 123060

Российская Федерация

Тел.: +7 (495) 797-8700

Факс: +7 (495) 645-7939

Адрес электронной почты: info@kaspersky.com

Веб-сайт: www.kaspersky.com

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой Руководство по установке, настройке, использованию Kaspersky Endpoint Security 8 для Mac, а также удаленному управлению программой через Kaspersky Administration Kit. Документ предназначен как для широкой аудитории, так и для системных администраторов. Пользователи программы должны обладать навыками работы с компьютером Apple Macintosh: быть знакомыми с интерфейсом операционной системы Mac OS X, владеть основными приемами работы в ней, уметь пользоваться программами для работы с электронной почтой и интернетом.

Цель документа:

- помочь пользователю самостоятельно установить программу на компьютер, активировать ее и оптимально настроить программу с учетом задач пользователя;
- помочь администратору в решении задач, связанных с удаленным управлением программой через Kaspersky Administration Kit;
- обеспечить быстрый поиск информации, необходимой для решения вопросов, связанных с программой;
- рассказать о дополнительных источниках получения информации о программе, а также способах обращения в Службу технической поддержки «Лаборатории Касперского».

В ЭТОМ РАЗДЕЛЕ

В ЭТОМ ДОКУМЕНТЕ

В Руководство администратора Kaspersky Endpoint Security 8 включены следующие разделы:

Дополнительные источники информации

Этот раздел содержит информацию об источниках дополнительных сведений о программе, об интернет-ресурсах, на которых можно обсудить программу, поделиться идеями, задать вопросы и получить ответы.

Kaspersky Endpoint Security 8

Этот раздел содержит описание возможностей программы, а также краткую информацию о ее компонентах и основных функциях. Из раздела вы узнаете о назначении комплекта поставки и о комплексе услуг, доступных зарегистрированным пользователям программы. В разделе приведены аппаратные и программные требования, которым должен отвечать компьютер, чтобы на него можно было установить Kaspersky Endpoint Security.

Установка программы

Этот раздел содержит инструкции, которые помогут вам локально установить программу на компьютер. В этом же разделе описано, как удалить программу с компьютера.

Управление лицензиями

Этот раздел содержит информацию об основных понятиях, используемых в контексте лицензирования программы. В разделе вы узнаете, как активировать программу, где просмотреть информацию о текущей лицензии, а также как приобрести лицензию и продлить срок ее действия.

Интерфейс программы

Этот раздел содержит описание основных элементов графического интерфейса программы: значка и контекстного меню программы, главного окна, окна настройки и окон уведомлений.

Запуск и остановка программы

Этот раздел содержит информацию о том, как запустить программу и завершить работу с ней.

Состояние защиты компьютера

Этот раздел содержит информацию о том, как определить, защищен ли в данный момент компьютер или существуют угрозы его безопасности, а также о том, как устранить возникшие угрозы с помощью Ассистента безопасности.

Решение типовых задач

Этот раздел содержит описание задач, с которыми большинство пользователей сталкивается при работе с программой, и инструкции по выполнению этих задач.

Расширенная настройка программы

Этот раздел содержит подробную информацию о каждом компоненте программы с описанием алгоритма работы и настройки параметров компонента.

Работа с программой из командной строки

Этот раздел содержит описание работы с программой и ее компонентами с использованием командной строки.

Управление программой через Kaspersky Administration Kit

Этот раздел содержит подробное описание установки Kaspersky Endpoint Security на удаленный компьютер пользователя, а также установки ПО, необходимого для удаленного управления программой через Kaspersky Administration Kit. Из раздела вы узнаете о процедуре развертывания программы в сети предприятия и удаленном управлении программой через Kaspersky Administration Kit с использованием задач и групповых политик.

Обращение в Службу технической поддержки

Этот раздел содержит рекомендации по обращению за помощью в «Лабораторию Касперского».

Приложения

Этот раздел содержит справочную информацию, которая дополняет основной текст документа.

Глоссарий терминов

Этот раздел содержит список терминов, которые встречаются в документе, и их определения.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

В руководстве используются условные обозначения, описанные в таблице ниже.

Таблица 1. Условные обозначения

ПРИМЕР ТЕКСТА	ОПИСАНИЕ УСЛОВНОГО ОБОЗНАЧЕНИЯ
Обратите внимание, что...	Предупреждения выделяются красным цветом и заключаются в рамку. В предупреждениях содержится важная информация, например, связанная с критическими для безопасности компьютера действиями.
Рекомендуется использовать...	Примечания заключаются в рамку. В примечаниях содержится вспомогательная и справочная информация.
Пример: ...	Примеры приводятся в блоке на желтом фоне под заголовком «Пример».
Вирус – это...	Новые термины выделяются курсивом.
Command-A	Названия клавиш клавиатуры выделяются полужирным шрифтом. Названия клавиш, соединенные знаком «минус», означают комбинацию клавиш.
Включить	Названия элементов интерфейса, например, полей ввода, команд меню, кнопок, выделяются полужирным шрифтом.
➧ *Чтобы настроить расписание задачи, выполните следующие действия:*	Инструкции отмечаются значком в виде стрелки. Вводные фразы инструкций выделяются курсивом.
`kav update`	Текст в командной строке или текст сообщений, выводимых программой на экран, выделяются специальным шрифтом.
<IP-адрес вашего компьютера>	Переменные заключаются в угловые скобки. Вместо переменной в каждом случае подставляется соответствующее ей значение, угловые скобки при этом опускаются.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Вы можете обратиться к следующим источникам информации о программе:

- страница на веб-сайте «Лаборатории Касперского»;
- страница на веб-сайте Службы технической поддержки (База знаний);
- форум пользователей продуктов «Лаборатории Касперского»;
- электронная справочная система.

Страница на веб-сайте «Лаборатории Касперского»

На странице программы (http://www.kaspersky.com/ru/endpoint-security-mac) вы получите общую информацию об Kaspersky Endpoint Security 8, его возможностях и особенностях работы с ним. Вы можете приобрести Kaspersky Endpoint Security 8 или продлить срок его использования в нашем электронном магазине.

Страница на веб-сайте Службы технической поддержки (База знаний)

База знаний – раздел веб-сайта Службы технической поддержки (http://support.kaspersky.ru/kes8mac), содержащий рекомендации по работе с продуктами «Лаборатории Касперского». На этой странице вы найдете статьи, опубликованные специалистами Службы технической поддержки.

Эти статьи содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании Kaspersky Endpoint Security 8. Они сгруппированы по темам, например, «Устранение сбоев в работе», «Настройка Обновления» или «Настройка Файлового Антивируса». Статьи могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security 8, но и к другим продуктам «Лаборатории Касперского»; а также содержать новости Службы технической поддержки в целом.

Для перехода к Базе знаний откройте главное окно программы (на стр. 34), нажмите на кнопку  и в открывшемся окне нажмите на кнопку **Служба технической поддержки**.

Форум пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме (http://forum.kaspersky.com). Данный ресурс является разделом веб-сайта Службы технической поддержки и содержит вопросы, отзывы и пожелания пользователей Kaspersky Endpoint Security 8.

На форуме вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

Чтобы перейти к этому ресурсу, откройте главное окно программы (на стр. 34), нажмите на кнопку  и в открывшемся окне нажмите на кнопку **Форум**.

Электронная справочная система

В программу включены файлы полной и контекстной справки. В файле полной справки содержится информация о том, как управлять защитой компьютера: просматривать состояние защиты, проверять различные области компьютера на вирусы, выполнять обновление, работать с отчетами и хранилищами. Кроме того, в файле контекстной справки вы можете найти информацию о каждом окне программы: перечень и описание представленных в нем параметров и список решаемых задач.

Чтобы открыть полную справку, откройте главное окно программы (на стр. 34) и нажмите на кнопку  . Чтобы открыть контекстную справку, откройте окно или интересующую вас закладку окна и нажмите на кнопку  .

Если вы не нашли решения вашей проблемы в Базе знаний, на Форуме пользователей, в справке и документации, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 156).

KASPERSKY ENDPOINT SECURITY 8

Kaspersky Endpoint Security 8 для Mac (далее Kaspersky Endpoint Security) предназначен для защиты компьютеров, работающих под управлением операционной системы Mac OS X от воздействия вирусов и вредоносных программ. В программе реализованы следующие возможности:

Файловый Антивирус

Защита файловой системы компьютера в режиме реального времени: перехват и анализ обращений к файловой системе, лечение, удаление вредоносных и изоляция возможно зараженных объектов для дальнейшего анализа.

Поиск вирусов

Поиск и обезвреживание вредоносного кода по запросу пользователя: поиск и анализ вредоносных и возможно зараженных объектов в заданных областях проверки, лечение, удаление или изоляция объектов для дальнейшего анализа.

В состав Kaspersky Endpoint Security включены наиболее востребованные пользователями задачи поиска вирусов: полная проверка всех объектов компьютера и быстрая проверка критических областей.

Обновление

Обновление баз и модулей, входящих в состав Kaspersky Endpoint Security, с серверов обновлений «Лаборатории Касперского» и с Сервера администрирования Kaspersky Administration Kit, создание резервной копии всех обновляемых файлов на случай необходимости отката последнего произведенного обновления, копирование полученных обновлений в локальный источник для предоставления доступа к ним другим компьютерам сети (в целях экономии интернет-трафика).

Карантин

Помещение возможно зараженных объектов в хранилище карантина: хранение возможно зараженных объектов в папке карантина, их дальнейшая проверка с обновленными базами, восстановление объектов из хранилища по требованию пользователя.

Резервное хранилище

Создание копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта, представляющего информационную ценность.

Отчеты

Формирование подробного отчета о работе каждого компонента Kaspersky Endpoint Security.

Уведомления

Уведомление пользователя о возникновении определенных событий в работе Kaspersky Endpoint Security. Программа позволяет выбрать способ уведомления для каждого из типов событий: звуковое оповещение или всплывающее сообщение.

Вы можете изменять внешний вид Kaspersky Endpoint Security, используя собственные графические элементы и выбранную цветовую палитру.

При работе с Kaspersky Endpoint Security вы получаете полную информационную поддержку: программа выводит сообщения о состоянии защиты и предлагает вашему вниманию подробную справку. Ассистент безопасности (на

стр. 44), включенный в состав программы, позволяет получить полную картину текущего состояния защиты компьютера и перейти к немедленному устранению проблем.

В этом разделе

Комплект поставки

Kaspersky Endpoint Security вы можете приобрести у наших партнеров (коробочный вариант), а также в одном из интернет-магазинов (например, http://www.kaspersky.ru, раздел **Интернет-магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки программного продукта входят:

- Запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта и документация в формате PDF.
- Лицензионное соглашение.

Дополнительно в комплект поставки могут быть включены:

- Руководство пользователя в печатном виде (если данная позиция была включена в заказ) или Руководство по продуктам.
- Файл ключа программы, записанный на специальную дискету.
- Регистрационная карточка (с указанием серийного номера продукта).

Перед тем как распечатать конверт с компакт-диском, внимательно ознакомьтесь с лицензионным соглашением. Открывая запечатанный пакет с установочным компакт-диском, вы принимаете все условия лицензионного соглашения.

При покупке Kaspersky Endpoint Security в интернет-магазине вы копируете продукт с веб-сайта «Лаборатории Касперского», в дистрибутив которого помимо самого продукта включено также данное Руководство. Файл ключа или код активации будет вам отправлен по электронной почте по факту оплаты.

Аппаратные и программные требования к системе

Для нормального функционирования Kaspersky Endpoint Security компьютер пользователя должен удовлетворять следующим минимальным требованиям:

- компьютер Apple Macintosh на базе процессора Intel (процессор PowerPC не поддерживается);
- 1 ГБ оперативной памяти;
- 500 МБ свободного места на жестком диске;
- операционная система Mac OS X 10.5 или более поздняя или Mac OS X Server 10.6.

Для установки Агента администрирования, необходимого для удаленного управления Kaspersky Endpoint Security через Kaspersky Administration Kit, компьютер пользователя должен удовлетворять следующим минимальным требованиям:

- компьютер Apple Macintosh на базе процессора Intel (процессор PowerPC не поддерживается);
- 512 МБ оперативной памяти;
- 30 МБ свободного места на жестком диске;
- операционная система Mac OS X 10.5 или более поздняя или Mac OS X Server 10.6.

УСТАНОВКА ПРОГРАММЫ

Этот раздел содержит инструкции, которые помогут вам локально установить программу на компьютер. В этом же разделе описано, как удалить программу с компьютера.

В состав дистрибутива Kaspersky Endpoint Security входят программа установки и программа удаления.

Для удаленного управления Kaspersky Endpoint Security через Kaspersky Administration Kit требуется установка плагина управления Kaspersky Endpoint Security на рабочее место администратора и Агента администрирования на компьютер пользователя (см. раздел «Установка ПО, необходимого для удаленного управления Kaspersky Endpoint Security» на стр. 114). Также возможна удаленная установка Kaspersky Endpoint Security на компьютер пользователя (см. раздел «Удаленная установка Kaspersky Endpoint Security» на стр. 120).

В ЭТОМ РАЗДЕЛЕ

Подготовка к установке программы

Перед установкой Kaspersky Endpoint Security на компьютер выполните ряд подготовительных действий:

- Убедитесь, что ваш компьютер соответствует системным требованиям (см. раздел «Аппаратные и программные требования к системе» на стр. 18).
- Проверьте подключение компьютера к интернету. Доступ в интернет необходим для активации программы с помощью кода активации, а также для получения обновлений.
- Удалите с компьютера другие антивирусные программы, чтобы избежать возникновения системных конфликтов и снижения быстродействия операционной системы.

Процедура установки программы

Существуют следующие способы установки Kaspersky Endpoint Security на компьютер:

- Стандартная установка (см. раздел «Стандартная установка Kaspersky Endpoint Security» на стр. 21).

  Будет установлен набор компонентов программы по умолчанию.

- Выборочная установка (см. раздел «Выборочная установка Kaspersky Endpoint Security» на стр. 22).

  Позволяет выборочно устанавливать компоненты программы и рекомендуется опытным пользователям.

Стандартная установка Kaspersky Endpoint Security

Чтобы выполнить стандартную установку Kaspersky Endpoint Security на компьютер, выполните следующие действия:

1. Откройте содержимое дистрибутива Kaspersky Endpoint Security. Для этого вставьте установочный диск в дисковод.

   Если вы купили Kaspersky Endpoint Security в интернет-магазине, то на веб-сайте «Лаборатории Касперского» будет доступен для скачивания дистрибутив программы в формате ZIP. Распакуйте его и запустите dmg-файл, чтобы увидеть содержимое дистрибутива.

2. Запустите программу установки Kaspersky Endpoint Security. Для этого в окне с содержимым дистрибутива откройте установочный пакет **Kaspersky Endpoint Security**.

   Следуйте шагам программы установки, чтобы установить программу.

3. В окне **Введение** нажмите на кнопку **Продолжить**.

4. В окне **Информация** прочтите информацию об устанавливаемой программе.

   Убедитесь, что ваш компьютер соответствует указанным системным требованиям. Чтобы распечатать информацию, нажмите на кнопку **Напечатать**. Для сохранения информации в текстовом файле нажмите на кнопку **Сохранить**. Для продолжения установки нажмите на кнопку **Продолжить**.

5. В окне **Лицензия** ознакомьтесь с текстом лицензионного соглашения об использовании Kaspersky Endpoint Security, которое заключается между вами и ЗАО «Лаборатория Касперского». Текст соглашения доступен на нескольких языках. Чтобы распечатать текст соглашения, нажмите на кнопку **Напечатать**. Для сохранения соглашения в текстовом файле нажмите на кнопку **Сохранить**.

   Если вы согласны со всеми пунктами соглашения, нажмите на кнопку **Продолжить**. Откроется окно запроса подтверждения согласия с условиями лицензионного соглашения. Вы можете выполнить следующие действия:

   - Продолжить установку Kaspersky Endpoint Security. Для этого нажмите на кнопку **Подтверждаю**.
   - Вернуться к тексту соглашения. Для этого нажмите на кнопку **Прочитать лицензию**.
   - Прервать установку программы. Для этого нажмите на кнопку **Не подтверждаю**.

6. В окне **Тип установки** изучите информацию о диске, на который будет устанавливаться программа, и о необходимом для этого объеме свободного дискового пространства.

   Чтобы установить программу, используя предлагаемые стандартные параметры установки, нажмите на кнопку **Установить** и введите пароль администратора для подтверждения.

   Чтобы выбрать другой диск для установки программы, нажмите на кнопку **Изменить размещение установки** и выберите другой диск, после чего нажмите на кнопку **Продолжить**.

   Диск для установки программы должен быть загрузочным. На диске должна быть установлена операционная система версии не ниже указанной в системных требованиях (см. раздел «Аппаратные и программные требования к системе» на стр. 18).

   Дождитесь, пока программа установки Kaspersky Endpoint Security установит компоненты программы.

7. В окне **Сводка** прочтите информацию об окончании процесса установки и нажмите на кнопку **Закрыть** для завершения работы программы установки.

По завершении установки Kaspersky Endpoint Security запускается автоматически. Перезагрузка компьютера не требуется.

ВЫБОРОЧНАЯ УСТАНОВКА KASPERSKY ENDPOINT SECURITY

Чтобы выполнить выборочную установку Kaspersky Endpoint Security на компьютер, выполните следующие действия:

1. Откройте содержимое дистрибутива Kaspersky Endpoint Security. Для этого вставьте установочный диск в дисковод.

   Если вы купили Kaspersky Endpoint Security в интернет-магазине, то на веб-сайте «Лаборатории Касперского» будет доступен для скачивания дистрибутив программы в формате ZIP. Распакуйте его и запустите dmg-файл, чтобы увидеть содержимое дистрибутива.

2. Запустите программу установки Kaspersky Endpoint Security. Для этого в окне с содержимым дистрибутива откройте установочный пакет **Kaspersky Endpoint Security**.

   Следуйте шагам программы установки, чтобы установить программу.

3. В окне **Введение** нажмите на кнопку **Продолжить**.

4. В окне **Информация** прочтите информацию об устанавливаемой программе.

   Убедитесь, что ваш компьютер соответствует указанным системным требованиям. Чтобы распечатать информацию, нажмите на кнопку **Напечатать**. Для сохранения информации в текстовом файле нажмите на кнопку **Сохранить**. Для продолжения установки нажмите на кнопку **Продолжить**.

5. В окне **Лицензия** ознакомьтесь с текстом лицензионного соглашения об использовании Kaspersky Endpoint Security, которое заключается между вами и ЗАО «Лаборатория Касперского». Текст соглашения доступен на нескольких языках. Чтобы распечатать текст соглашения, нажмите на кнопку **Напечатать**. Для сохранения соглашения в текстовом файле нажмите на кнопку **Сохранить**.

   Если вы согласны со всеми пунктами соглашения, нажмите на кнопку **Продолжить**. Откроется окно запроса подтверждения согласия с условиями лицензионного соглашения. Вы можете выполнить следующие действия:

   - Продолжить установку Kaspersky Endpoint Security. Для этого нажмите на кнопку **Подтверждаю**.
   - Вернуться к тексту соглашения. Для этого нажмите на кнопку **Прочитать лицензию**.
   - Прервать установку программы. Для этого нажмите на кнопку **Не подтверждаю**.

6. В окне **Тип установки** изучите информацию о диске, на который будет устанавливаться программа, и о необходимом для этого объеме свободного дискового пространства.

   Чтобы выбрать другой диск для установки программы, нажмите на кнопку **Изменить размещение установки** и выберите другой диск, после чего нажмите на кнопку **Продолжить**.

   Диск для установки программы должен быть загрузочным. На диске должна быть установлена операционная система версии не ниже указанной в системных требованиях (см. раздел «Аппаратные и программные требования к системе» на стр. 18).

   Нажмите на кнопку **Настройка**, чтобы выбрать компоненты программы для выборочной установки.

7. В открывшемся окне укажите, какие компоненты программы будут установлены на компьютер. Снимите флажок рядом с названием тех компонентов, которые не нужно устанавливать.

   - **Поиск вирусов**. Обеспечивает проверку объектов в заданных пользователем областях.

     Этот компонент Kaspersky Endpoint Security устанавливается всегда.

   - **Файловый Антивирус**. Осуществляет проверку всех открываемых, запускаемых и сохраняемых объектов в режиме реального времени.

   - **Контекстное меню Finder**. Позволяет проверять на вирусы объекты, отображаемые в Finder. Запуск проверки осуществляется из контекстного меню объекта.

   - **Коннектор для Агента администрирования**. Необходим для удаленного управления программой через Kaspersky Administration Kit.

   После выбора компонентов нажмите на кнопку **Установить** и введите пароль администратора для подтверждения. Для возврата к стандартным параметрам установки (см. раздел «Стандартная установка Kaspersky Endpoint Security» на стр. 21) нажмите на кнопку **Стандартная установка**.

   Дождитесь, пока программа установки Kaspersky Endpoint Security установит выбранные компоненты программы.

8. В окне **Сводка** прочтите информацию об окончании процесса установки и нажмите на кнопку **Закрыть** для завершения работы программы установки.

   По завершении установки Kaspersky Endpoint Security запускается автоматически. Перезагрузка компьютера не требуется.

Подготовка к работе

После установки Kaspersky Endpoint Security мы рекомендуем вам выполнить следующие действия:

- Активировать Kaspersky Endpoint Security (см. раздел «Активация Kaspersky Endpoint Security» на стр. 28). Использование лицензионной версии позволит вам регулярно обновлять антивирусные базы и обеспечит доступ к сервисам Службы технической поддержки.

- Оценить текущее состояние защиты (см. раздел «Оценка состояния защиты компьютера» на стр. 44), чтобы убедиться, что Kaspersky Endpoint Security обеспечивает защиту компьютера на должном уровне.

- Обновить Kaspersky Endpoint Security (см. раздел «Как обновить базы и модули программы» на стр. 48). Необходимо поддерживать базы Kaspersky Endpoint Security в актуальном состоянии, чтобы программа всегда была готова обнаружить и обезвредить вредоносную программу.

- Выполнить полную проверку компьютера на вирусы (см. раздел «Как выполнить полную проверку компьютера на вирусы» на стр. 46).

В случае возникновения проблем или ошибок в работе программы, откройте окно отчетов о работе Kaspersky Endpoint Security (см. раздел «Отчеты» на стр. 99). Возможно причина сбоя будет описана в отчете. Если самостоятельно устранить проблему не удается, обратитесь в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 156).

Удаление программы

Удаляя Kaspersky Endpoint Security, вы подвергаете ваш компьютер серьезному риску заражения.

Рекомендуем перед началом удаления программы обработать все объекты, расположенные в хранилище карантина и в резервном хранилище. Все необработанные объекты хранилищ будут удалены без возможности восстановления.

Чтобы удалить Kaspersky Endpoint Security с компьютера, выполните следующие действия:

1. Откройте содержимое дистрибутива Kaspersky Endpoint Security. Для этого вставьте установочный диск в дисковод

   Если вы купили Kaspersky Endpoint Security в интернет-магазине, то на веб-сайте «Лаборатории Касперского» будет доступен для скачивания дистрибутив программы в формате ZIP. Распакуйте его и запустите dmg-файл, чтобы увидеть содержимое дистрибутива.

2. Запустите программу удаления Kaspersky Endpoint Security. Для этого в окне с содержимым дистрибутива выберите **Удаление Kaspersky Endpoint Security**.

   Следуйте ее шагам, чтобы удалить программу.

3. В окне **Введение** нажмите на кнопку **Продолжить**.

4. В окне **Информация** прочтите важную информацию. Для запуска процедуры удаления нажмите на кнопку **Удалить** и введите пароль администратора для подтверждения. Дождитесь, пока будет выполнено удаление программы.

5. В окне **Завершение** прочтите информацию об окончании процесса удаления и нажмите на кнопку **Готово** для завершения работы программы удаления.

   Перезагрузка компьютера после удаления Kaspersky Endpoint Security не требуется.

УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ

Этот раздел содержит информацию об основных понятиях, используемых в контексте лицензирования программы. В разделе вы узнаете, как активировать программу, где просмотреть информацию о текущей лицензии, а также как приобрести лицензию и продлить срок ее действия.

В ЭТОМ РАЗДЕЛЕ

О ЛИЦЕНЗИИ

Лицензия – это право на использование Kaspersky Endpoint Security и связанных с ним дополнительных услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами.

Каждая лицензия характеризуется сроком действия и типом.

Срок действия лицензии – период, в течение которого вам предоставляются дополнительные услуги:

- техническая поддержка;
- обновление баз и модулей программы.

Объем предоставляемых услуг зависит от типа лицензии.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия с ограниченным сроком действия, например, 30 дней, предназначенная для ознакомления с Kaspersky Endpoint Security.

  Пробная лицензия может быть использована только один раз.

  При наличии пробной лицензии вы можете обращаться в Службу технической поддержки только по вопросам активации программы или приобретения коммерческой лицензии. По завершении срока действия пробной лицензии Kaspersky Endpoint Security продолжает выполнять все свои функции, однако обновление антивирусных баз программы не производится. Для продолжения работы программы ее нужно активировать (см. раздел «Активация Kaspersky Endpoint Security» на стр. 28).

- *Коммерческая* – платная лицензия с ограниченным сроком действия (например, один год).

  Во время действия коммерческой лицензии доступны все функции программы и дополнительные услуги.

  По окончании срока действия коммерческой лицензии Kaspersky Endpoint Security продолжает выполнять все свои функции, однако обновление антивирусных баз не производится. Вы по-прежнему можете осуществлять антивирусную проверку компьютера и использовать компоненты защиты, но только на основе антивирусных баз, актуальных на дату окончания срока действия лицензии. Чтобы избежать заражения компьютера новыми вирусами, мы рекомендуем вам продлить лицензию на использование программы.

  После того как вы активировали программу с коммерческой лицензией, вы можете приобрести дополнительную лицензию для Kaspersky Endpoint Security и активировать ее. В этом случае по окончании срока действия активной лицензии дополнительная лицензия автоматически перейдет в статус активной, и программа продолжит работу без изменений. У Kaspersky Endpoint Security может быть только одна дополнительная лицензия.

ПРОСМОТР ИНФОРМАЦИИ О ЛИЦЕНЗИИ

➧ *Чтобы просмотреть информацию об используемой лицензии,*

откройте главное окно программы (на стр. 34) и нажмите на кнопку .

В открывшемся окне (см. рис. ниже) будет указан номер лицензии, ее тип (коммерческая или пробная), ограничение по количеству компьютеров, на которых можно использовать данную лицензию, дата и время окончания срока действия лицензии, а также остаток дней до этой даты.

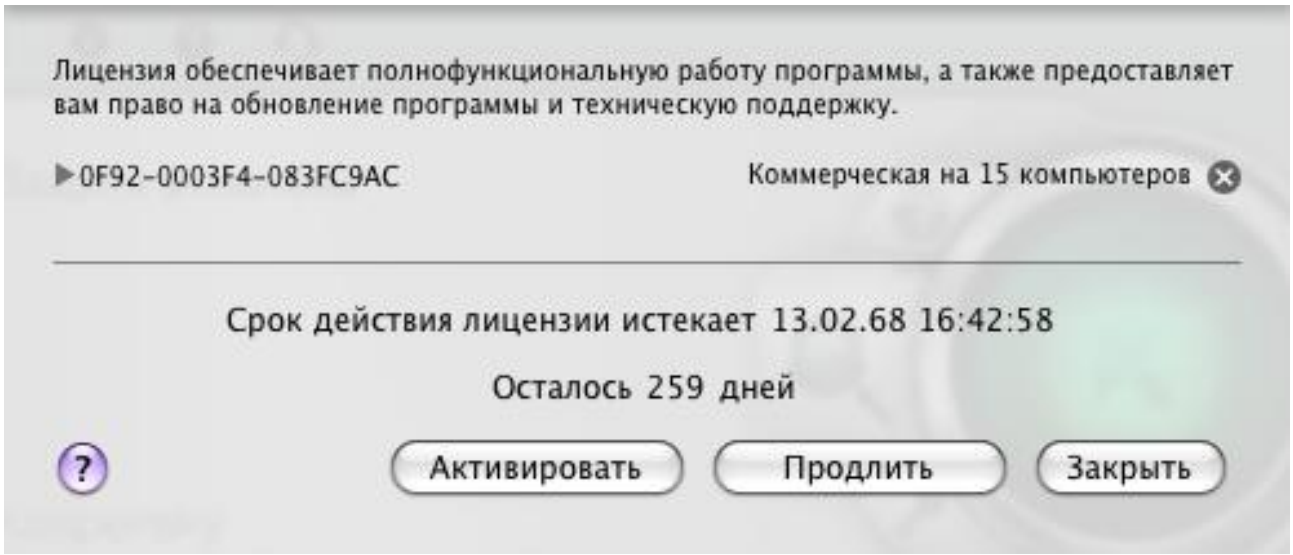


Рисунок 1. Управление лицензиями

Если лицензия отсутствует, то Kaspersky Endpoint Security сообщит вам об этом. Если программа не активирована, вы можете начать процедуру активации (см. раздел «Активация Kaspersky Endpoint Security» на стр. 28). Если активирована пробная версия программы, вы можете приобрести коммерческую лицензию (см. раздел «Приобретение лицензии» на стр. 27). Если срок действия коммерческой лицензии истекает, вы можете продлить срок ее действия (см. раздел «Продление лицензии» на стр. 27).

Приобретение лицензии

Чтобы приобрести новую лицензию, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку .
2. В открывшемся окне (см. рис. ниже) нажмите на кнопку **Приобрести**.

На открывшейся веб-странице вам будет предоставлена полная информация об условиях покупки лицензии через интернет-магазин «Лаборатории Касперского», либо у партнеров компании. По факту оплаты при покупке лицензии через интернет-магазин, вам будет отправлен код активации Kaspersky Endpoint Security (см. раздел «О коде активации» на стр. 28) на электронный адрес, указанный в форме заказа.

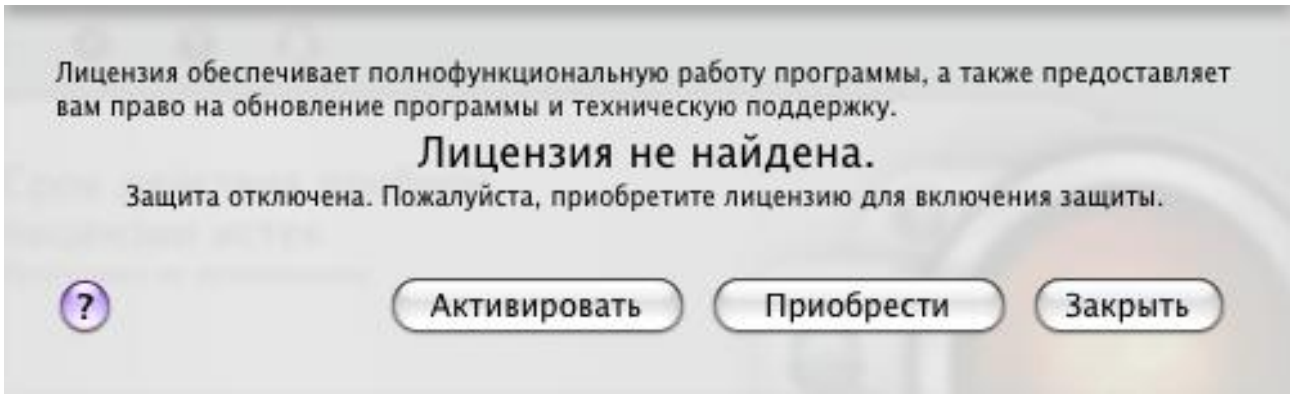


Рисунок 2. Приобретение лицензии

Продление лицензии

Необходимость продления лицензии на использование программы возникает по окончании срока действия имеющейся лицензии. В этом случае Kaspersky Endpoint Security продолжает выполнять все свои функции, однако обновление антивирусных баз не производится.

Чтобы продлить право пользования уже имеющейся лицензией, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку .
2. В открывшемся окне (см. рис. ниже) нажмите на кнопку **Продлить**.

На открывшейся веб-странице вам будет предоставлена полная информация об условиях продления срока действия лицензии через интернет-магазин «Лаборатории Касперского», либо у партнеров компании. По факту оплаты при продлении лицензии через интернет-магазин, вам будет отправлен код активации Kaspersky Endpoint Security (см. раздел «О коде активации» на стр. 28) на электронный адрес, указанный в форме заказа.

«Лаборатория Касперского» регулярно проводит акции, позволяющие продлить сроки действия лицензий на использование наших продуктов со скидкой. Следите за акциями на веб-сайте «Лаборатории Касперского» в разделе **Продукты → Акции и спецпредложения**.

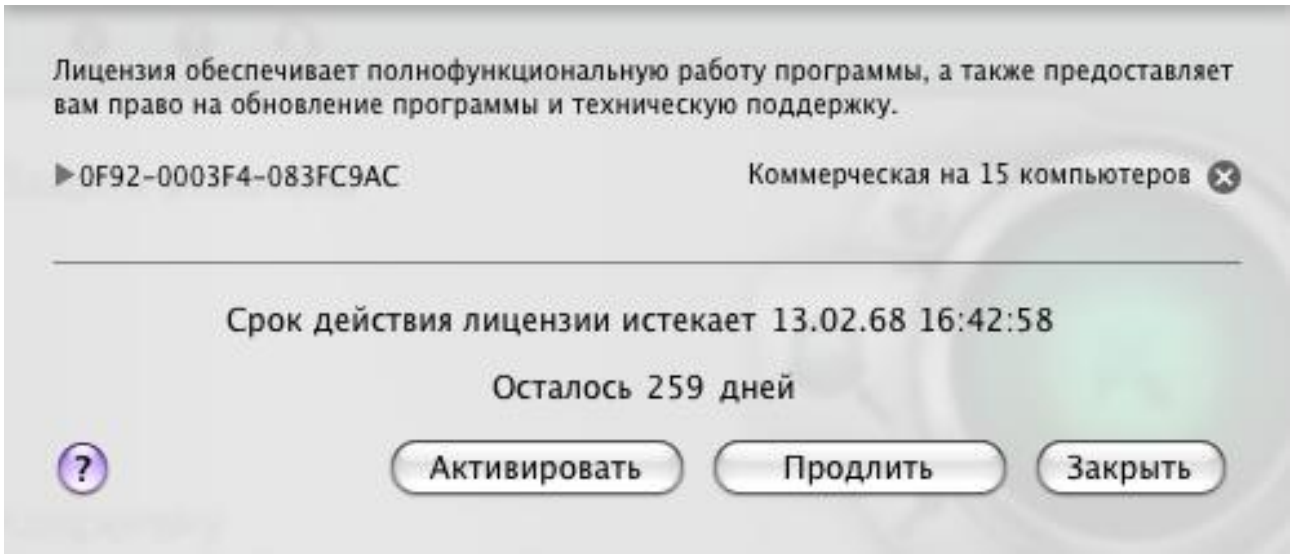


Рисунок 3. Управление лицензиями

О лицензионном соглашении

Лицензионное соглашение – это договор между физическим или юридическим лицом, правомерно владеющим экземпляром Kaspersky Endpoint Security, и ЗАО «Лаборатория Касперского». Соглашение входит в состав каждой программы «Лаборатории Касперского». В нем приводится детальная информация о правах и ограничениях на использование Kaspersky Endpoint Security.

О коде активации

Код активации – это код, который предоставляется вам при покупке коммерческой лицензии Kaspersky Endpoint Security. Этот код необходим для активации программы.

Код активации представляет собой последовательность латинских букв и цифр, разделенных дефисами на четыре блока по пять символов, например, AA111-AA111-AA111-AA111.

О файле ключа

Возможность использования Kaspersky Endpoint Security определяется наличием *файла ключа*. Файл ключа предоставляется вам на основании кода активации (см. раздел «О коде активации» на стр. 28), полученного при покупке программы, и дает право на ее использование со дня активации. Файл ключа содержит информацию о лицензии: тип, срок действия, количество компьютеров, на которые она распространяется.

Активация Kaspersky Endpoint Security

Перед активацией Kaspersky Endpoint Security убедитесь в том, что параметры системной даты компьютера соответствуют фактическим дате и времени.

Процедура активации заключается в установке файла ключа (см. раздел «О файле ключа» на стр. 28), на основании которого Kaspersky Endpoint Security будет проверять наличие прав на использование программы и определять срок ее использования.

Активация программы производится с помощью Ассистента активации. Следуйте его шагам, чтобы активировать программу.

На любом из шагов Ассистента активации вы можете нажать на кнопку **Отмена** и тем самым прервать активацию программы. Работа Ассистента активации будет завершена. Если программа не активирована, вам будут доступны все функции Kaspersky Endpoint Security, за исключением получения обновлений. Обновить программу возможно только один раз после ее установки.

В этом разделе

Активация пробной версии

Активация пробной версии предлагается Ассистентом активации только в том случае, если данная версия Kaspersky Endpoint Security ранее не устанавливалась на этот компьютер.

Выберите этот вариант активации, если вы хотите использовать пробную версию программы перед принятием решения о покупке коммерческой версии. Вам будет предоставлен бесплатный ключ со сроком действия, ограниченным пробной лицензией.

При активации пробной версии требуется подключение к интернету. Если на текущий момент соединение с интернетом отсутствует, вы можете провести активацию пробной версии позже.

Чтобы активировать пробную версию программы, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
2. В открывшемся окне нажмите на кнопку **Активировать**. Запустится Ассистент активации. Следуйте его шагам, чтобы активировать программу.
3. В окне **Способ активации** выберите способ активации программы **Активировать пробную версию**.
4. В окне **Получение файла ключа** дождитесь, пока Ассистент активации осуществит соединение с серверами «Лаборатории Касперского» и отправит данные для проверки. В случае успешной проверки, Ассистент получит и установит файл ключа со сроком действия, ограниченным пробной лицензией.

   Если период использования пробной лицензии для данной версии программы истек, на экран будет выведено соответствующее уведомление.
5. В окне **Информация о файле ключа** Ассистент активации информирует вас об успешном завершении процедуры активации. Кроме того, приводится информация об установленном ключе: номер ключа, его тип (пробный), а также дата окончания срока действия ключа. Нажмите на кнопку **Готово**, чтобы завершить работу Ассистента активации.

Активация программы с использованием кода активации

Используйте этот вариант активации, если вы приобрели коммерческую версию программы и вам был предоставлен код активации. На основании этого кода вы получите файл ключа, обеспечивающий доступ к функциональности Kaspersky Endpoint Security на срок действия лицензии.

При выборе активации с помощью кода активации требуется подключение к интернету. Если на текущий момент соединение с интернетом отсутствует, вы можете провести активацию позже.

Чтобы активировать программу с использованием кода активации, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
2. В открывшемся окне нажмите на кнопку **Активировать**. Запустится Ассистент активации. Следуйте его шагам, чтобы активировать программу.
3. В окне **Способ активации** выберите способ активации программы **Активировать, используя код активации**.
4. В окне **Ввод кода активации** введите код активации, полученный при покупке Kaspersky Endpoint Security.

   Код активации представляет собой последовательность цифр и букв, разделенных дефисами на четыре блока по пять символов, без пробелов, например, 11AA1-11AAA-1AA11-1A111. Обратите внимание, что код должен вводиться латинскими символами.
5. В окне **Получение файла ключа** дождитесь, пока Ассистент активации осуществит соединение с серверами «Лаборатории Касперского» и отправит код активации для проверки. В случае успешной проверки кода активации Ассистент получит файл ключа.

   Kaspersky Endpoint Security получает с сервера не физический файл с расширением key, а информацию, которая сохраняется в операционной системе. Чтобы получить реальный файл ключа, требуется пройти регистрацию пользователя на веб-сайте «Лаборатории Касперского» (http://www.kaspersky.ru/support).

   Если код активации не пройдет проверку, на экран будет выведено соответствующее уведомление. В этом случае обратитесь за информацией в компанию, где вы приобрели Kaspersky Endpoint Security.
6. В окне **Информация о файле ключа** Ассистент активации информирует вас об успешном завершении процедуры активации. Кроме того, в нем приводится информация об установленном ключе: номер ключа, его тип (коммерческий), а также дата окончания срока действия ключа. Нажмите на кнопку **Готово**, чтобы завершить работу Ассистента активации.

АКТИВАЦИЯ ПРОГРАММЫ С ИСПОЛЬЗОВАНИЕМ ФАЙЛА КЛЮЧА

Используйте этот вариант, чтобы активировать программу с помощью полученного ранее файла ключа.

При выборе активации с использованием файла ключа подключение к интернету не требуется. Рекомендуется использовать данный способ активации программы, если соединение компьютера с интернетом невозможно или временно недоступно.

Чтобы активировать программу с использованием полученного ранее файла ключа, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
2. В открывшемся окне нажмите на кнопку **Активировать**. Запустится Ассистент активации. Следуйте его шагам, чтобы активировать программу.
3. В окне **Способ активации** выберите способ активации программы **Использовать полученный ранее файл ключа**.

4. В окне **Выбор файла ключа** нажмите на кнопку **Выбрать** и в открывшемся стандартном окне выберите файл ключа с расширением key. В нижней части окна будет представлена информация об используемом ключе: номер ключа, его тип (коммерческий), а также дата окончания срока действия ключа.

5. В окне **Информация о файле ключа** Ассистент активации информирует вас об успешном завершении процедуры активации. Кроме того, приводится информация об установленном ключе: номер ключа, его тип, а также дата окончания срока действия ключа. Нажмите на кнопку **Готово**, чтобы завершить работу Ассистента активации.

ИНТЕРФЕЙС ПРОГРАММЫ

Этот раздел содержит описание основных элементов графического интерфейса программы: значка и контекстного меню программы, главного окна, окна настройки и окон уведомлений.

В ЭТОМ РАЗДЕЛЕ

ЗНАЧОК KASPERSKY ENDPOINT SECURITY

Сразу после установки Kaspersky Endpoint Security в строке меню появляется его значок. Значок служит индикатором работы программы. Если значок активный, это означает, что защита файловой системы компьютера от вредоносных программ в реальном времени включена. Неактивный значок свидетельствует о том, что защита выключена. Кроме того, контекстное меню значка обеспечивает доступ к основным командам Kaspersky Endpoint Security: выключение или возобновление защиты файловой системы компьютера, запуск задачи обновления и быстрой проверки компьютера на вирусы, переход к окну настройки программы и т.д.

По умолчанию значок располагается в строке меню. Вы можете изменить настройки программы так, чтобы значок Kaspersky Endpoint Security отображался в Dock или не отображался вообще.

- *Чтобы выбрать отображение значка программы в панели быстрого запуска Dock, выполните следующие действия:*

  1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Вид** (см. рис. ниже).
  2. В блоке **Отображение значка программы** выберите вариант **В Dock**.

- *Чтобы отключить отображение значка программы, выполните следующие действия:*

  1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Вид** (см. рис. ниже).
  2. В блоке **Отображение значка программы** выберите вариант **Нигде**.

Обратите внимание, что изменение данного параметра вступит в силу только после перезапуска Kaspersky Endpoint Security.

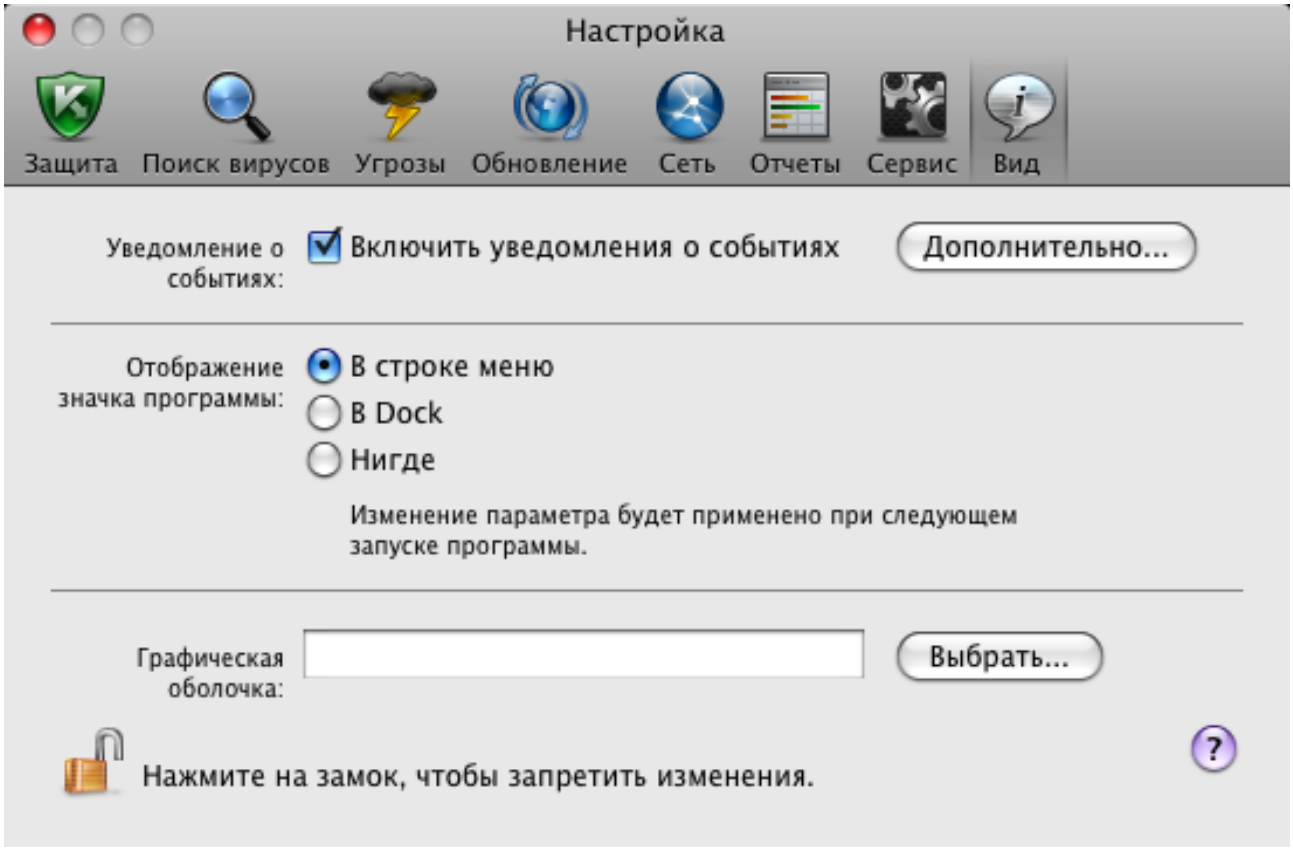


Рисунок 4. Окно настройки программы. Вид

Если вы выбрали отображение значка в строке меню, то при запуске программы или открытии главного окна значок в Dock появляться не будет. Также нельзя будет переключиться на программу, используя комбинацию клавиш **Command-Tab**.

Если отображение значка программы отключено, то программа будет выполняться в фоновом режиме. Чтобы открыть главное окно программы (на стр. 34), необходимо нажать на ярлык Kaspersky Endpoint Security в списке установленных на компьютере программ.

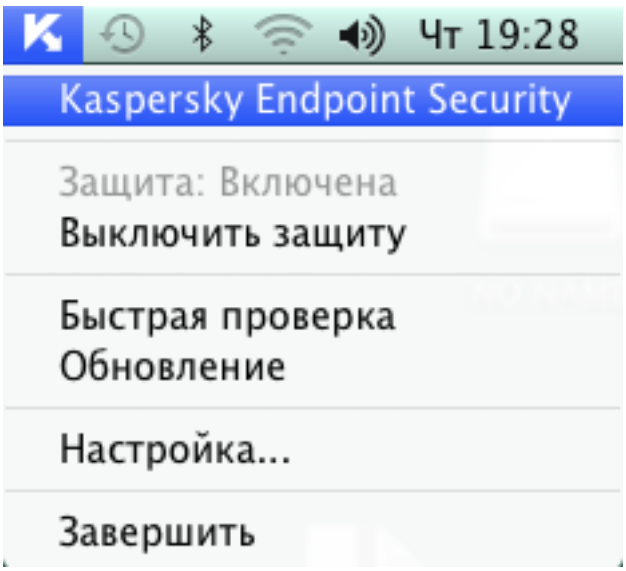


Рисунок 5. Контекстное меню значка Kaspersky Endpoint Security в строке меню

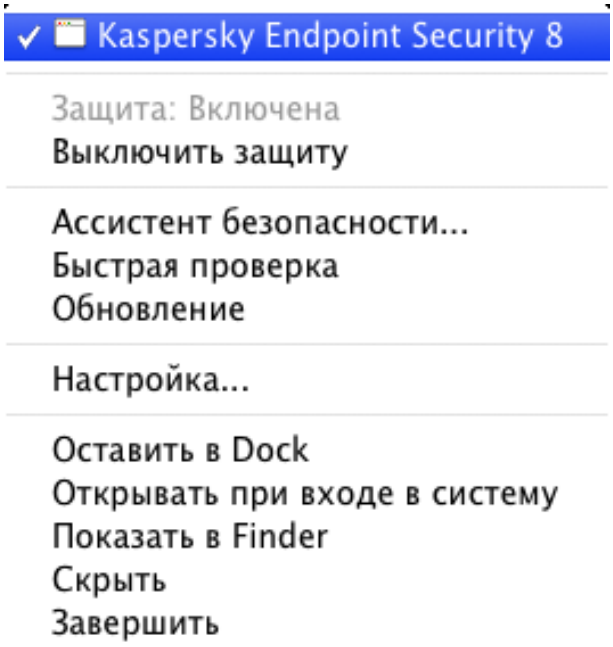


Рисунок 6. Контекстное меню значка Kaspersky Endpoint Security в Dock

Главное окно программы

- *Чтобы открыть главное окно программы,*

  нажмите на значок Kaspersky Endpoint Security в строке меню или в Dock (см. рис. выше) и в открывшемся контекстном меню выберите команду **Kaspersky Endpoint Security**.

Основная задача главного окна Kaspersky Endpoint Security (см. рис. ниже) – информировать пользователя о состоянии защиты компьютера и наличии в ней проблем, предоставлять информацию о работе компонентов программы (Файлового Антивируса, задач поиска вирусов и обновления), а также обеспечивать доступ к основным задачам и окну настройки программы.

Рисунок 7. Главное окно Kaspersky Endpoint Security 8

Существует три возможных состояния защиты (см. раздел «Оценка состояния защиты компьютера» на стр. 44), каждое из которых обозначено цветовым индикатором, аналогично сигналам дорожного светофора. О текущем состоянии защиты сигнализирует цвет индикатора главного окна. Зеленый цвет означает, что защита вашего компьютера осуществляется на должном уровне; желтый и красный цвета сигнализируют о наличии проблем в настройке параметров или работе Kaspersky Endpoint Security. Для получения подробной информации об этих проблемах и для их устранения воспользуйтесь Ассистентом безопасности (см. раздел «Ассистент безопасности» на стр. 44), который открывается при нажатии на цветовой индикатор.

В левой части главного окна, в дополнение к цветовому индикатору состояния защиты компьютера, приведена текстовая информация о состоянии защиты, а также перечислены угрозы безопасности, зафиксированные Ассистентом безопасности. Если в данный момент запущены задачи поиска вирусов или обновления, информация о процессе их выполнения (в процентах) также выносится в левую часть главного окна.

В нижней части окна приведена сводная статистика работы Файлового Антивируса, а также информация об используемых программой антивирусных базах.

Из главного окна вы можете выполнить обновление Kaspersky Endpoint Security, запустить задачи поиска вирусов в указанных областях, а также перейти к управлению лицензиями. Для этого воспользуйтесь следующими кнопками:

Запустить обновление Kaspersky Endpoint Security. По окончании обновления в окне отчетов (см. раздел «Отчеты» на стр. 99) будет предоставлена детальная информация о выполнении задачи.

Перейти к задачам поиска вирусов: **Быстрая проверка**, **Полная проверка** и **Поиск вирусов** в указанной пользователем области, а также ко всем пользовательским задачам поиска вирусов, если таковые были созданы. По завершении поиска вирусов в окне отчетов (см. раздел «Отчеты» на стр. 99) будет предоставлена детальная информация о выполнении задачи.

Перейти к окну, в котором представлена информация об используемой лицензии.

В верхней части главного окна расположена навигационная панель, которая содержит следующие кнопки:

Открыть окно отчетов (см. раздел «Отчеты» на стр. 99) Kaspersky Endpoint Security, а также получить доступ к карантину (см. раздел «Карантин» на стр. 94) и резервному хранилищу (см. раздел «Резервное хранилище» на стр. 97).

Открыть окно настройки программы (на стр. 35).

Открыть электронную справку Kaspersky Endpoint Security.

Открыть окно с информацией о способах получения технической поддержки (см. раздел «Обращение в Службу технической поддержки» на стр. 156).

Окно настройки программы

Окно настройки параметров Kaspersky Endpoint Security (см. рис. ниже) можно открыть следующими способами:

- нажав на кнопку  в главном окне программы (см. раздел «Главное окно программы» на стр. 34);

- выбрав пункт **Настройка** в контекстном меню, которое открывается при нажатии на значок Kaspersky Endpoint Security (на стр. 32) в Dock или в строке меню.

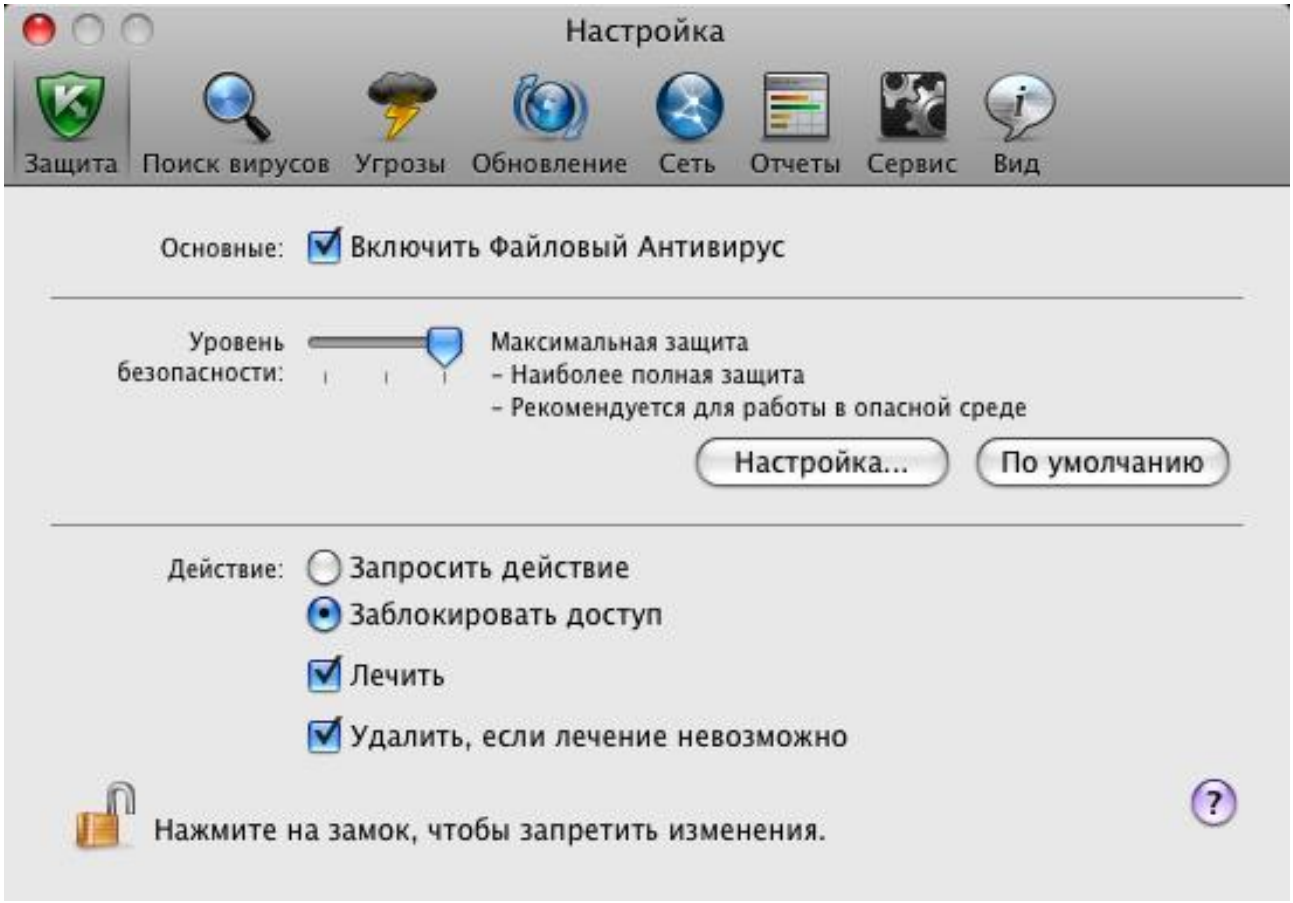


Рисунок 8. Окно настройки программы. Защита

Закладки, расположенные в верхней части окна, обеспечивают быстрый доступ к следующим функциям программы:

- настройке Файлового Антивируса;
- настройке задач поиска вирусов;
- настройке обновления программы;
- выбору контролируемых вредоносных программ и формированию доверенной зоны;
- сервисным параметрам Kaspersky Endpoint Security.

Для детальной настройки некоторых параметров вам будет предложено открыть окна настройки второго и третьего уровней.

Чтобы запретить изменение параметров работы Kaspersky Endpoint Security пользователям, не имеющим прав администратора, нажмите на кнопку , расположенную в нижней части окна. Для снятия ограничений на изменение параметров потребуется ввести учетные данные администратора компьютера.

Кнопка обеспечивает доступ к справочной системе Kaspersky Endpoint Security с описанием параметров текущего окна программы.

Окна уведомлений и всплывающие сообщения

В процессе работы Kaspersky Endpoint Security возникают различные события. Они могут иметь информационный характер или нести важную информацию. Например, событие может уведомлять об успешно выполненном обновлении, а может сообщать об ошибке в работе Файлового Антивируса или в ходе выполнения задачи поиска вирусов, которую необходимо срочно устранить. Программа проинформирует вас о возникновении событий с помощью *окон уведомлений* и *всплывающих сообщений*.

В этом разделе

Об уведомлениях

В процессе работы Kaspersky Endpoint Security уведомляет о возникновении событий следующих типов:

- **Критические события** – события критической важности, уведомления о которых настоятельно рекомендуется получать, поскольку они указывают на проблемы в работе Kaspersky Endpoint Security или на уязвимости в защите вашего компьютера: например, *базы программы устарели* или *истек срок действия ключа*.

- **Отказ функционирования** – события, приводящие к неработоспособности Kaspersky Endpoint Security: например, *базы программы повреждены*.

- **Важные события** – события, на которые обязательно нужно обратить внимание, поскольку они отображают важные ситуации в работе Kaspersky Endpoint Security: например, *защита отключена* или *компьютер давно не проверялся на вирусы*.

- **Информационные события** – события справочного характера, например, *все опасные объекты вылечены*.

Чтобы быть в курсе событий, происходящих во время работы Kaspersky Endpoint Security, воспользуйтесь сервисом уведомлений.

Способы получения уведомлений

Уведомления могут быть реализованы любым из следующих способов или обоими одновременно:

- всплывающие экранные сообщения;

- звуковое оповещение.

Kaspersky Endpoint Security поддерживает технологию Growl для вывода уведомлений. Если система Growl подключена, экранные сообщения выводятся с ее использованием.

НАСТРОЙКА ПОЛУЧЕНИЯ УВЕДОМЛЕНИЙ

Чтобы получать уведомления о событиях, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Вид** (см. рис. ниже).

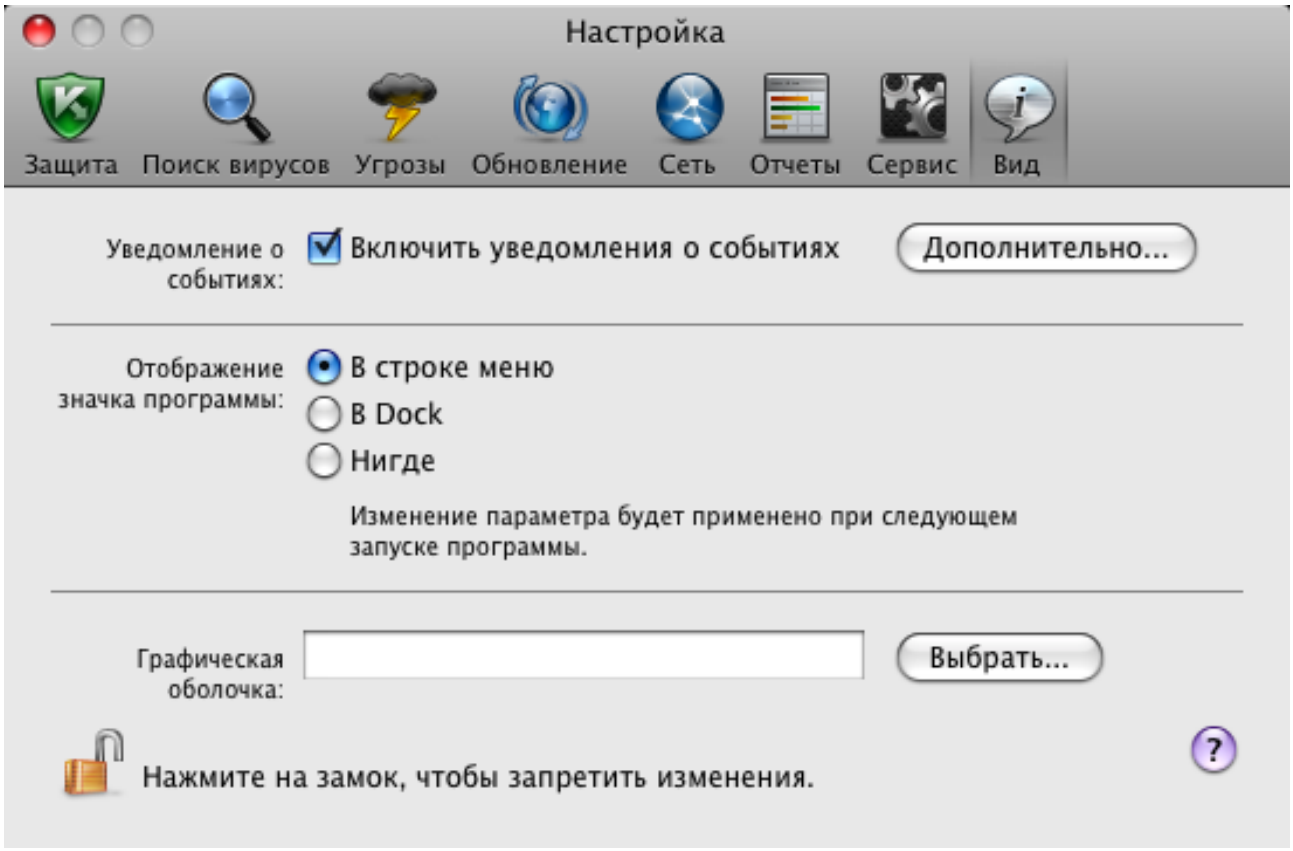


Рисунок 9. Окно настройки программы. Вид

2. Установите флажок **Включить уведомления о событиях** в блоке **Уведомление о событиях** и перейдите к детальной настройке. Для этого нажмите на кнопку **Дополнительно**.

В открывшемся окне (см. рис. ниже) вы можете настроить следующие способы получения уведомлений о перечисленных выше событиях:

- *Всплывающее экранное сообщение*, содержащее информацию о возникшем событии.

  Чтобы использовать данный тип уведомления, в графе **Экран** установите флажок напротив события, о котором вы хотите быть уведомлены.

- *Звуковое оповещение*.

  Если вы хотите, чтобы данное уведомление сопровождалось звуковым сигналом, в графе **Звук** установите флажок напротив события.

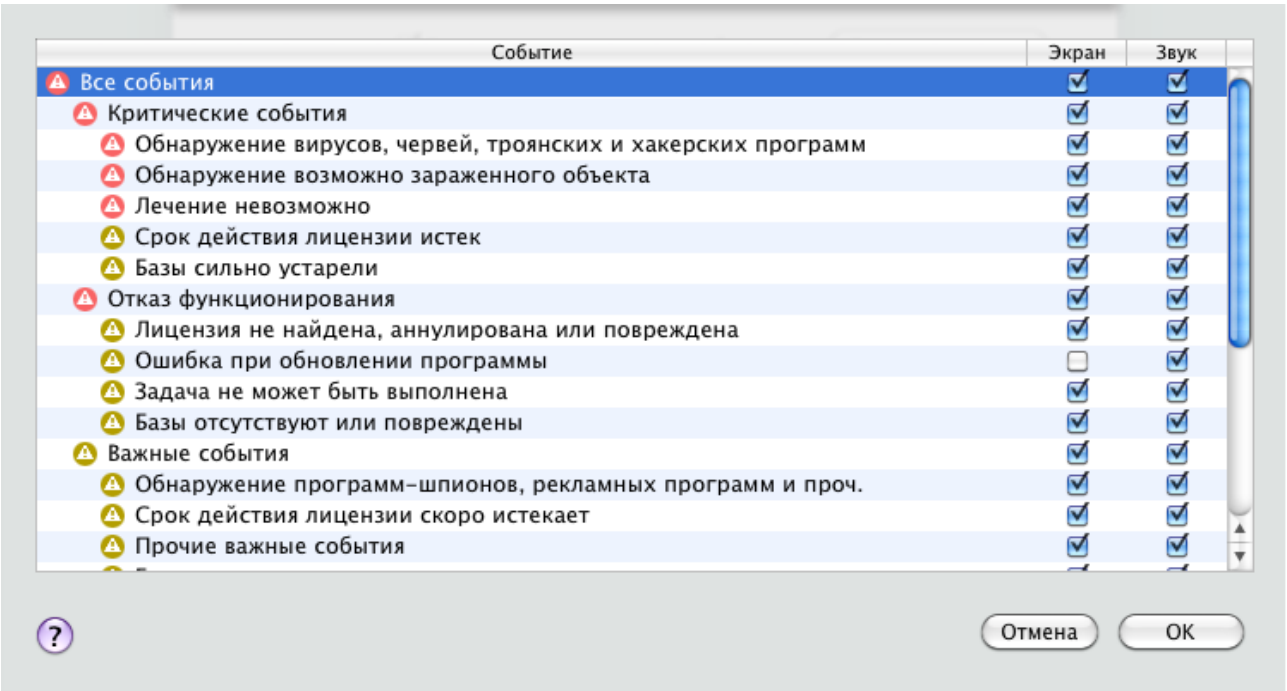


Рисунок 10. Настройка получения уведомлений

О всплывающих сообщениях

Всплывающие сообщения Kaspersky Endpoint Security выводит на экран, чтобы проинформировать о событиях, не требующих от вас обязательного выбора действия. Всплывающие сообщения появляются под значком программы в строке меню и автоматически исчезают с экрана вскоре после появления.

Настройка интерфейса Kaspersky Endpoint Security

Вы можете изменять внешний вид Kaspersky Endpoint Security, создавая и используя различные графические элементы и выбранную цветовую палитру. Все используемые в интерфейсе программы цвета, шрифты, пиктограммы, тексты могут быть изменены.

➡ *Чтобы подключить графическую оболочку, выполните следующие действия:*

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Вид** (см. рис. ниже).

2. В блоке **Графическая оболочка** нажмите на кнопку **Выбрать** и в открывшемся стандартном окне выберите папку, в которой расположены файлы графической оболочки.

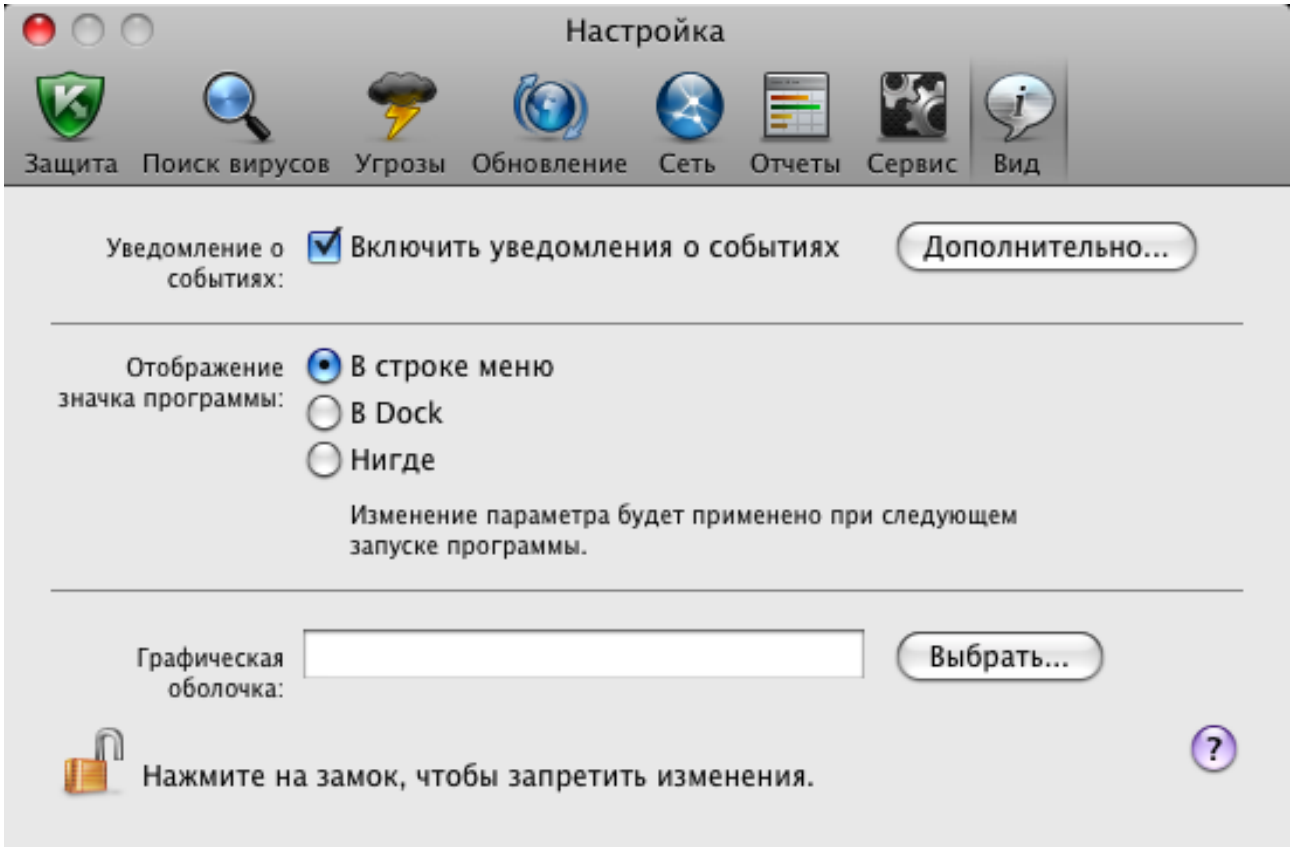


Рисунок 11. Окно настройки программы. Вид

ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ

Этот раздел содержит информацию о том, как запустить программу и завершить работу с ней.

Сразу же после установки программа запускается автоматически и значок Kaspersky Endpoint Security (на стр. 32) появляется в строке меню.

В ЭТОМ РАЗДЕЛЕ

Завершение работы Kaspersky Endpoint Security

Если по какой-либо причине вам требуется полностью завершить работу Kaspersky Endpoint Security, нажмите на значок Kaspersky Endpoint Security (на стр. 32) в строке меню или в Dock и в открывшемся меню выберите команду **Завершить**. Работа программы будет остановлена и процесс будет удален из оперативной памяти компьютера.

После завершения работы с Kaspersky Endpoint Security компьютер продолжит работать в незащищенном режиме и может быть подвергнут риску заражения.

Настройка автозапуска Kaspersky Endpoint Security

По умолчанию Kaspersky Endpoint Security запускается автоматически при включении компьютера или после перезагрузки операционной системы.

- *Чтобы выключить режим автозапуска, выполните следующие действия:*

1. Откройте окно настройки программы (на стр. 35), выберите закладку **Сервис** (см. рис. ниже).

2. В блоке **Автозагрузка** снимите флажок **Запускать программу при включении компьютера**.

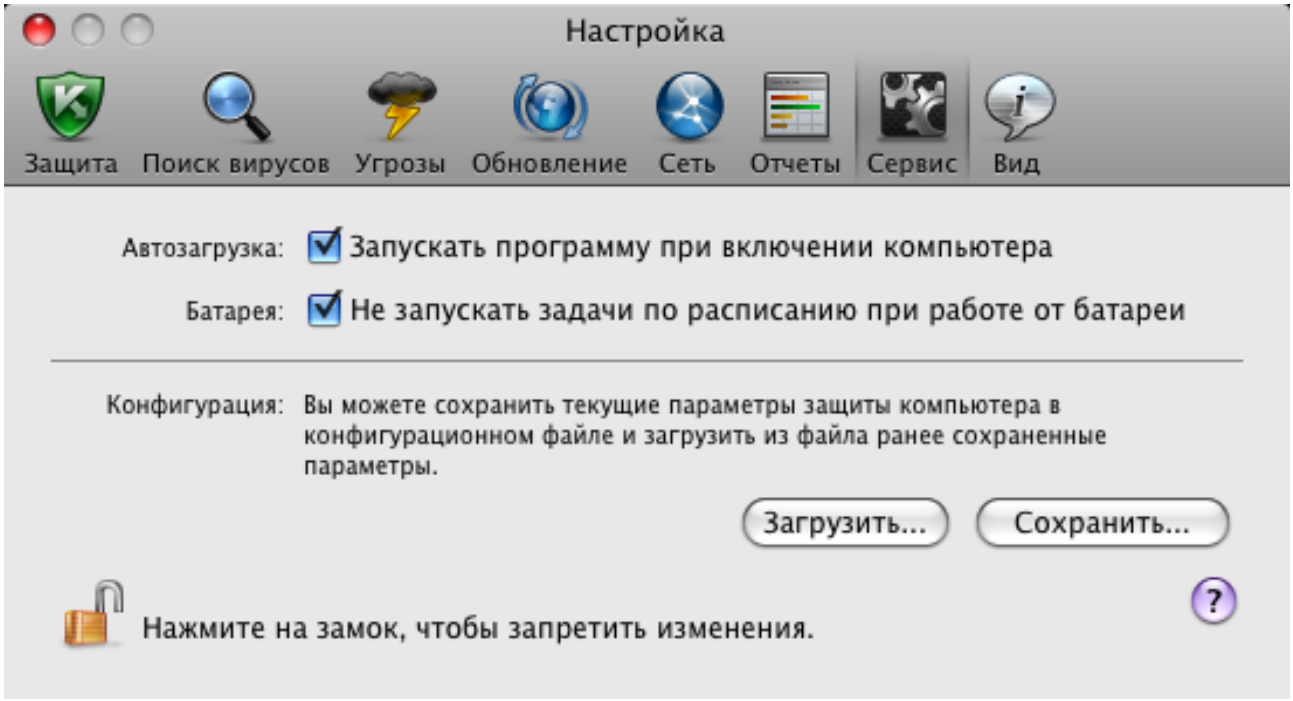


Рисунок 12. Окно настройки программы. Сервис

Выключение режима автозапуска Kaspersky Endpoint Security приведет к тому, что при следующем включении компьютера или после перезагрузки операционной системы компьютер будет работать в незащищенном режиме и может быть подвергнут риску заражения.

Настройка режима экономичного энергопотребления

По умолчанию Kaspersky Endpoint Security работает в режиме экономичного энергопотребления. В таком режиме задачи поиска вирусов, для которых установлено расписание их запуска, не будут запущены, если компьютер работает от батареи.

Чтобы отключить режим экономичного энергопотребления, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35), выберите закладку **Сервис** (см. рис. ниже).

2. В блоке **Батарея** снимите флажок **Не запускать задачи по расписанию при работе от батареи**.

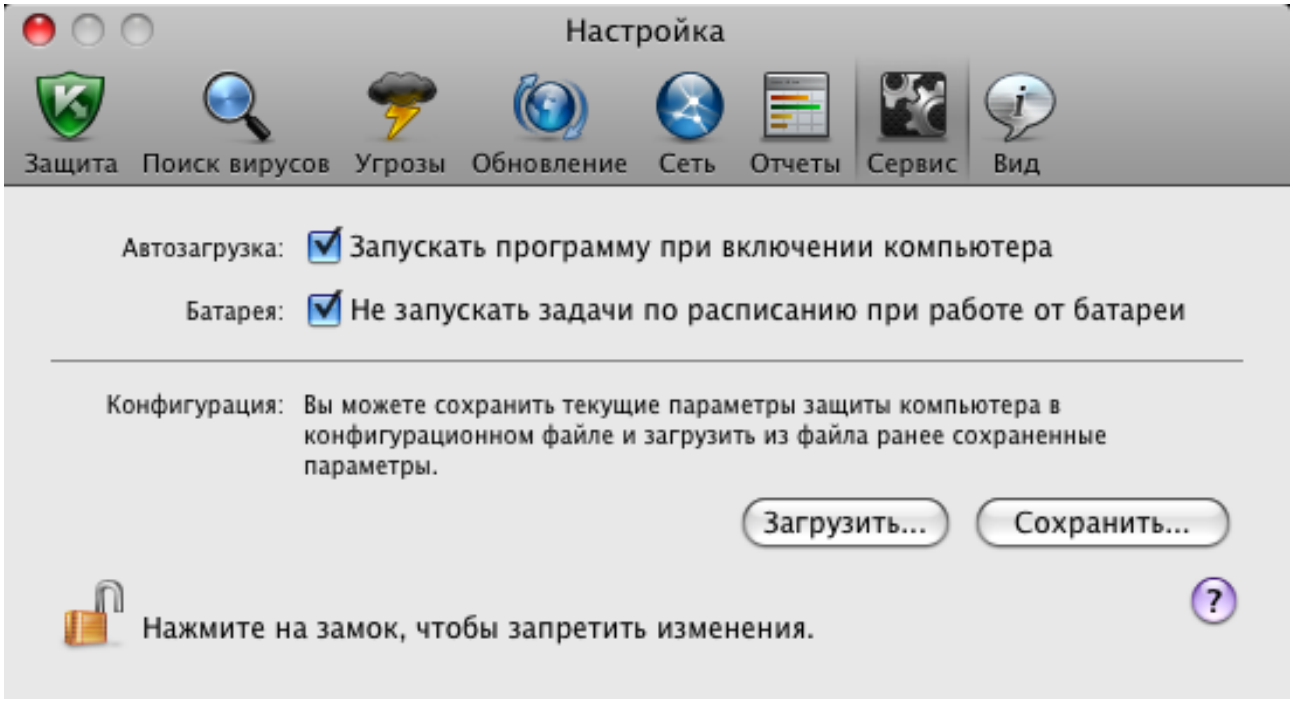


Рисунок 13. Окно настройки программы. Сервис

СОСТОЯНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

Состояние защиты вашего компьютера отражает наличие или отсутствие в данный момент угроз, влияющих на общий уровень безопасности системы. К угрозам в этом случае относятся не только обнаруженные вредоносные программы, но и использование устаревших антивирусных баз, отключение Файлового Антивируса, использование минимальных параметров работы Kaspersky Endpoint Security.

Ассистент безопасности поможет последовательно просмотреть имеющиеся угрозы и перейти к их устранению.

В ЭТОМ РАЗДЕЛЕ

Оценка состояния защиты компьютера

Состояние защиты компьютера отображается в главном окне программы (см. раздел «Главное окно программы» на стр. 34) в виде цветового индикатора, аналогичного сигналам дорожного светофора. В зависимости от ситуации цвет индикатора будет изменяться. При наличии угроз в системе безопасности цветовой индикатор будет дополняться информационным текстом.

Цветовой индикатор может принимать одно из следующих значений:

- **Зеленый**. Защита вашего компьютера обеспечивается на должном уровне.

  Это означает, что вы своевременно обновили антивирусные базы, Файловый Антивирус включен, Kaspersky Endpoint Security работает с параметрами, рекомендуемыми специалистами «Лаборатории Касперского», а в результате выполнения задач поиска вирусов не было обнаружено вредоносных объектов, либо обнаруженные вредоносные объекты были обезврежены.

- **Желтый**. Уровень защиты вашего компьютера снижен по сравнению с предыдущим состоянием.

  Это свидетельствует о наличии некоторых проблем в работе или настройке Kaspersky Endpoint Security. Например, есть незначительные отклонения от рекомендуемого режима работы, базы Kaspersky Endpoint Security не обновлялись в течение нескольких дней.

- **Красный**. Ваш компьютер подвергается угрозе заражения.

  Это состояние сигнализирует о наличии проблем, которые могут привести к заражению компьютера и потере данных. Например, произошел сбой в работе Файлового Антивируса, Kaspersky Endpoint Security очень давно не обновлялся, были обнаружены вредоносные объекты, которые необходимо срочно обезвредить, или программа не активирована.

При наличии проблем в системе защиты рекомендуется немедленно устранить их. Для этого нажмите на цветовой индикатор главного окна, чтобы запустить Ассистент безопасности (на стр. 44).

Ассистент безопасности

Ассистент безопасности – это сервис, который позволяет проанализировать имеющиеся угрозы и перейти к их непосредственному устранению (см. рис. ниже).

Чтобы запустить Ассистент безопасности,

нажмите на цветовой индикатор главного окна программы (см. раздел «Главное окно программы» на стр. 34).

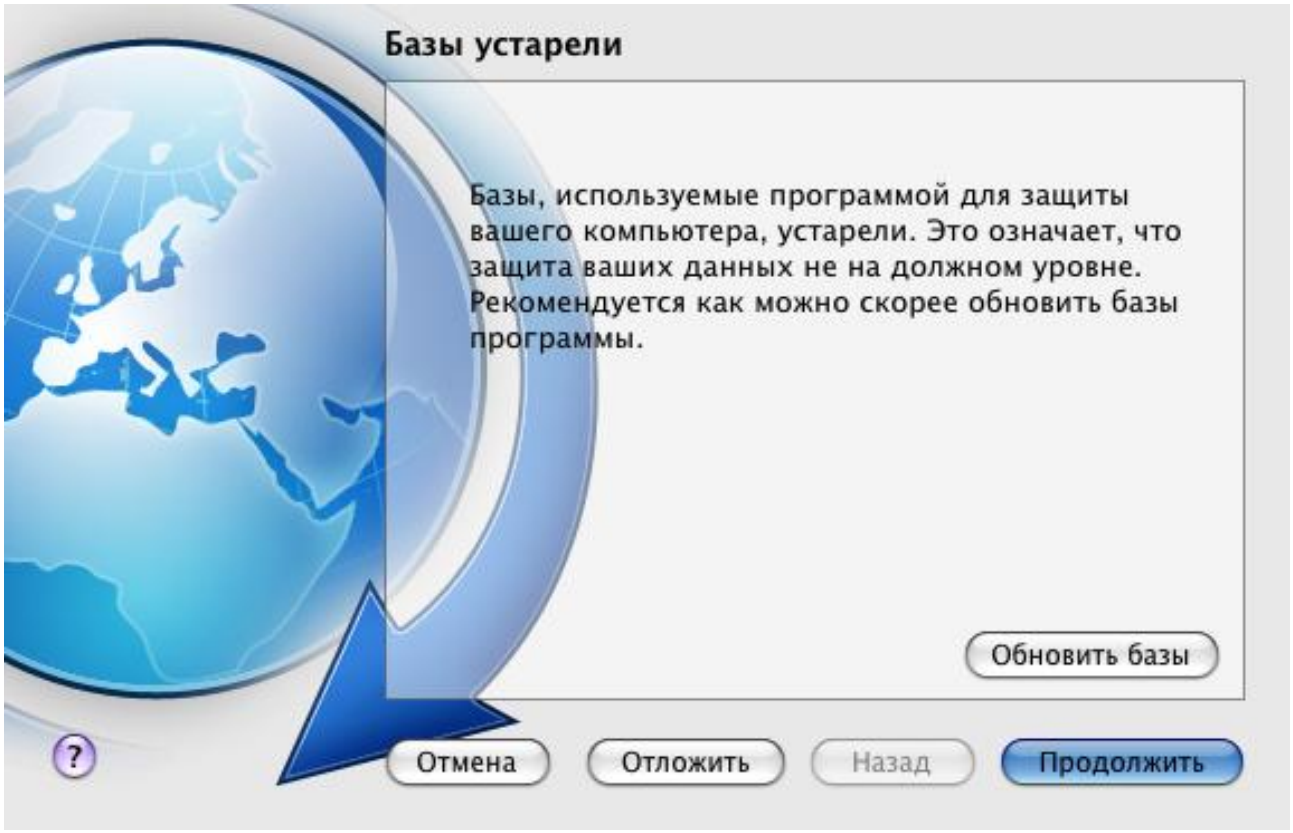


Рисунок 14. Интерфейс Ассистента безопасности

Чтобы ознакомиться со списком существующих угроз, воспользуйтесь кнопками **Продолжить** и **Назад**. Для каждой угрозы дается подробное описание, и предлагаются следующие варианты действий:

- **Устранить угрозу немедленно**.

  Для устранения угрозы нажмите на кнопку с названием рекомендуемого действия. Например, если на компьютере обнаружены зараженные объекты, то рекомендуемым действием будет **Лечить зараженные объекты**. Если используемые программой антивирусные базы устарели, то рекомендуемое действие – **Обновить базы**. Подробную информацию об угрозе можно получить в окне отчетов (см. раздел «Отчеты» на стр. 99).

- **Отложить устранение угрозы**.

  Если по какой-либо причине вы не хотите устранить угрозу немедленно, отложите данное действие, чтобы вернуться к устранению угрозы позже. Для этого воспользуйтесь кнопкой **Отложить**. Обратите внимание, что данная возможность не предусмотрена для таких серьезных угроз, как, например, наличие необработанных вредоносных объектов, сбой в работе Файлового Антивируса, повреждение файлов баз Kaspersky Endpoint Security.

Если вы завершили работу Ассистента безопасности без устранения серьезных угроз, цвет индикатора в главном окне программы будет и далее сигнализировать о наличии проблем. Если вы отложили устранение некоторых угроз, то при повторном открытии Ассистента безопасности отложенные угрозы не будут присутствовать в списке активных угроз. Тем не менее, вы можете вернуться к просмотру и устранению отложенных угроз, нажав на кнопку **Просмотреть отложенные угрозы** в заключительном окне Ассистента безопасности.

РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

Этот раздел содержит описание задач, с которыми большинство пользователей сталкивается при работе с программой, и инструкции по выполнению этих задач.

В ЭТОМ РАЗДЕЛЕ

КАК ВЫПОЛНИТЬ ПОЛНУЮ ПРОВЕРКУ КОМПЬЮТЕРА НА ВИРУСЫ

В Kaspersky Endpoint Security входит созданная по умолчанию задача полной проверки компьютера. Выполняя эту задачу, программа проверит на вирусы все жесткие диски.

Чтобы запустить задачу полной проверки компьютера, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
2. В открывшемся меню выберите задачу  **Полная проверка**.

С результатами выполнения задачи можно ознакомиться в окне отчетов (см. раздел «Статистика поиска вирусов» на стр. 82).

КАК ВЫПОЛНИТЬ БЫСТРУЮ ПРОВЕРКУ КОМПЬЮТЕРА

В Kaspersky Endpoint Security входит созданная по умолчанию задача быстрой проверки компьютера. Выполняя эту задачу, программа проверит на вирусы критические области компьютера: папки, содержащие файлы операционной системы и системные библиотеки, поражение которых вредоносными программами может привести к повреждению операционной системы вашего компьютера.

Чтобы запустить задачу быстрой проверки компьютера, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
2. В открывшемся меню, выберите задачу  **Быстрая проверка**.

С результатами выполнения задачи можно ознакомиться в окне отчетов (см. раздел «Статистика поиска вирусов» на стр. 82).

КАК ПРОВЕРИТЬ НА ВИРУСЫ ФАЙЛ, ПАПКУ ИЛИ ДИСК

Если вам требуется проверить на вирусы отдельный объект (один из жестких дисков, отдельную папку или файл, или сменное устройство), воспользуйтесь встроенной задачей **Поиск вирусов**.

Чтобы проверить на вирусы отдельный объект, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
2. В открывшемся меню выберите задачу  **Поиск вирусов**. Откроется окно выбора объектов проверки.
3. Сформируйте список объектов проверки (см. раздел «Формирование списка объектов проверки» на стр. 73) и нажмите на кнопку **Запустить**, чтобы запустить задачу поиска вирусов.

С результатами выполнения задачи можно ознакомиться в окне отчетов (см. раздел «Статистика поиска вирусов» на стр. 82).

Проверку на вирусы любого объекта на вашем компьютере можно запустить из программы Finder, если был установлен компонент **Контекстное меню Finder** (см. раздел «**Выборочная установка Kaspersky Endpoint Security**» на стр. 22). Для этого откройте контекстное меню объекта и выберите команду **Проверить на вирусы**[1].

КАК НАСТРОИТЬ ПРОВЕРКУ КОМПЬЮТЕРА ПО РАСПИСАНИЮ

Залогом безопасности данных на вашем компьютере является своевременная проверка на вирусы. Вы можете сформировать расписание запуска задач поиска вирусов **Быстрая проверка** и **Полная проверка**. В соответствии с заданным режимом программа будет автоматически запускать задачу и выполнять проверку всего компьютера или наиболее критических областей файловой системы.

[1] В операционных системах Mac OS X версии ниже 10.6 запуск может отличаться.

- *Чтобы настроить расписание запуска задач **Быстрая проверка** и **Полная проверка**, выполните следующие действия:*

  1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Поиск вирусов.**
  2. В списке слева выберите имя задачи, а в блоке **Режим запуска** включите запуск задачи по расписанию. Чтобы отредактировать расписание запуска задачи, нажмите на кнопку **Изменить**.
  3. В открывшемся окне установите частоту, с которой должна запускаться задача поиска вирусов.

С результатами выполнения задач можно ознакомиться в окне отчетов (см. раздел «Статистика поиска вирусов» на стр. 82).

КАК ПРИОБРЕСТИ ИЛИ ПРОДЛИТЬ ЛИЦЕНЗИЮ

Если вы установили Kaspersky Endpoint Security, не имея лицензии, можно приобрести лицензию уже после установки программы. Когда срок действия имеющейся лицензии подходит к концу, вы можете его продлить. При покупке лицензии и продлении срока ее действия вы получаете код активации, с помощью которого нужно активировать программу (см. раздел «Активация Kaspersky Endpoint Security» на стр. 28).

- *Чтобы приобрести лицензию, выполните следующие действия:*

  1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
  2. В открывшемся окне нажмите на кнопку **Приобрести**.

     Откроется веб-страница интернет-магазина, где вы можете приобрести лицензию.

- *Чтобы продлить срок действия лицензии, выполните следующие действия:*

  1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
  2. В открывшемся окне нажмите на кнопку **Продлить**.

     Откроется веб-страница интернет-магазина, где вы можете продлить срок действия лицензии.

КАК ОБНОВИТЬ БАЗЫ И МОДУЛИ ПРОГРАММЫ

«Лаборатория Касперского» обновляет антивирусные базы и модули Kaspersky Endpoint Security, используя специальные серверы обновлений и Сервер администрирования Kaspersky Administration Kit. *Серверы обновлений «Лаборатории Касперского»* – интернет-сайты «Лаборатории Касперского», на которые регулярно выкладываются обновления Kaspersky Endpoint Security.

Для успешной загрузки обновлений с серверов требуется подключение компьютера к интернету.

По умолчанию Kaspersky Endpoint Security периодически проверяет наличие пакета обновлений на серверах «Лаборатории Касперского». Обнаружив свежие обновления, Kaspersky Endpoint Security скачивает их в фоновом режиме и устанавливает на компьютер.

- *Чтобы вручную запустить обновление Kaspersky Endpoint Security,*

  откройте главное окно программы (на стр. 34) и нажмите на кнопку  .

С результатами выполнения задачи обновления можно ознакомиться в окне отчетов (см. раздел «Статистика обновления» на стр. 92).

Как перенести параметры программы в Kaspersky Endpoint Security, установленный на другом компьютере

Kaspersky Endpoint Security предоставляет возможность экспорта и импорта своих параметров. Это полезно, например, в том случае, когда программа установлена у вас и на домашнем компьютере, и в офисе. Дома вы можете настроить программу на удобный для вас режим работы, сохранить эти параметры на диск и импортировать их на свой рабочий компьютер. Параметры хранятся в специальном конфигурационном файле.

- *Чтобы сохранить в файл текущие параметры работы Kaspersky Endpoint Security, выполните следующие действия:*

  1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Сервис**.
  2. В блоке **Конфигурация** нажмите на кнопку **Сохранить**. Откроется окно **Сохранить**.
  3. В поле **Сохранить как** введите имя файла и выберите папку, в которую он будет сохранен.

- *Чтобы импортировать параметры работы Kaspersky Endpoint Security из конфигурационного файла, выполните следующие действия:*

  1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Сервис**.
  2. В блоке **Конфигурация** нажмите на кнопку **Загрузить** и в открывшемся стандартном окне выберите файл, содержащий параметры Kaspersky Endpoint Security.

Что делать, если программа заблокировала доступ к файлу

Kaspersky Endpoint Security блокирует доступ к файлу или программе, если Файловый Антивирус (на стр. 57) подозревает, что запрашиваемый объект заражен или возможно заражен вредоносной программой, и выбрано действие **Заблокировать доступ**.

- *Чтобы обработать опасные объекты, перечисленные на закладке **Обнаружено** окна отчетов, выполните следующие действия:*

  1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  . Откроется окно отчетов Kaspersky Endpoint Security.
  2. В левой части окна отчетов выберите **Обнаружено**. В правой части окна будет представлен список обнаруженных опасных объектов с указанием их статуса.
  3. Нажмите на кнопку **Лечить все**. При обработке каждого объекта на экране появится уведомление, предлагающее вам принять решение о дальнейших действиях над объектом. Если в окне уведомления вы установите флажок **Применить во всех подобных случаях**, то выбранное действие будет применено ко всем объектам с таким же статусом.

- *Чтобы обработать возможно зараженные объекты, помещенные в хранилище карантина, выполните следующие действия:*

  1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  . Откроется окно отчетов Kaspersky Endpoint Security.
  2. В левой части окна отчетов выберите **Карантин**. В правой части окна будет представлено содержимое хранилища.

3. Нажмите на кнопку **Проверить все**, чтобы проверить и лечить все возможно зараженные объекты карантина с использованием текущей версии баз Kaspersky Endpoint Security.

   Изменение статуса объектов, помещенных в хранилище карантина, происходит только после их проверки с использованием антивирусных баз, выпущенных не ранее, чем через три дня после помещения файла на карантин.

4. Нажмите на кнопку **Восстановить**, чтобы восстановить файлы в папку, заданную пользователем, или в папку, из которой они были перенесены в хранилище карантина (по умолчанию).

   Рекомендуем вам восстанавливать только объекты со статусами *ложное срабатывание*, *OK*, *вылечен*, поскольку восстановление объектов с другими статусами может привести к заражению вашего компьютера.

5. Нажмите на кнопку **Удалить** или **Очистить все**, чтобы удалить выбранный объект из хранилища карантина или полностью очистить хранилище карантина.

Если вы уверены в безопасности объектов, доступ к которым блокируется Файловым Антивирусом, включите их в доверенную зону, создав правило исключения (см. раздел «Формирование доверенной зоны» на стр. 54).

Что делать, если вы подозреваете, что объект заражен вирусом

Если вы подозреваете, что объект может быть заражен, прежде всего проверьте его на вирусы (см. раздел «Как проверить на вирусы файл, папку или диск» на стр. 47).

Если в результате проверки Kaspersky Endpoint Security сообщит, что объект не заражен, но вы подозреваете обратное, поместите объект на *карантин*. Объекты, помещенные в хранилище карантина, хранятся в запакованном виде и не представляют угрозы для вашего компьютера. Возможно, после обновления баз Kaspersky Endpoint Security сможет однозначно определить угрозу и обезвредить ее.

Чтобы поместить объект в хранилище карантина, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  . Откроется окно отчетов Kaspersky Endpoint Security.

2. В левой части окна отчетов выберите **Карантин**. В правой части окна будет представлено содержимое хранилища.

3. Нажмите на кнопку **Добавить** и в открывшемся стандартном окне выберите нужный файл. Он будет добавлен в список со статусом *добавлен пользователем*.

Kaspersky Endpoint Security может изменить статус файла, помещенного на карантин вручную, после проверки его с использованием обновленных баз не ранее, чем через три дня с момента его первой проверки после помещения в хранилище карантина. Если файлу будет присвоен статус *ложное срабатывание*, файл будет автоматически восстановлен. Если файл будет признан зараженным, он будет удален из карантина с помещением копии файла в резервное хранилище.

Как восстановить удаленный или вылеченный программой объект

Не рекомендуется без крайней необходимости восстанавливать удаленные и вылеченные объекты, поскольку они могут представлять угрозу для вашего компьютера.

Иногда в процессе лечения зараженных объектов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступной, можно попытаться восстановить исходный объект из его резервной копии.

Чтобы восстановить удаленный или измененный при лечении объект, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  . Откроется окно отчетов Kaspersky Endpoint Security.

2. В левой части окна отчетов выберите **Резервное хранилище**. В правой части окна будет представлено содержимое хранилища в виде списка резервных копий объектов.

3. Выберите резервную копию необходимого объекта в списке и нажмите на кнопку **Восстановить**. Подтвердите действие в открывшемся окне. Объект будет восстановлен в исходное местоположение с тем же именем, которое было у него до лечения или удаления. Если в исходном местоположении уже находится объект с таким именем (данная ситуация возможна при восстановлении объекта, копия которого уже была создана перед лечением), на экран будет выведено соответствующее предупреждение. Вы можете изменить местоположение восстанавливаемого объекта или переименовать его.

   Рекомендуем вам сразу после восстановления проверить объект на вирусы. Возможно с обновленными антивирусными базами его удастся вылечить без потери целостности.

Как просмотреть отчет о работе программы

Информация о событиях, возникших в работе Файлового Антивируса (см. раздел «Файловый Антивирус» на стр. 57), при выполнении задач поиска вирусов (см. раздел «Поиск вирусов» на стр. 69) или обновления (см. раздел «Обновление программы» на стр. 84) отображается в окне отчетов (см. раздел «Отчеты» на стр. 99).

Чтобы открыть окно отчетов,

откройте главное окно программы (на стр. 34) и нажмите на кнопку  .

Что делать при появлении уведомлений программы

Уведомления программы (см. раздел «Окна уведомлений и всплывающие сообщения» на стр. 37) в виде всплывающих экранных сообщений информируют о событиях, происходящих в процессе работы программы и требующих вашего внимания.

При появлении на экране уведомления следует выбрать один из предложенных вариантов действия. Оптимальный вариант – тот, который рекомендован экспертами «Лаборатории Касперского» по умолчанию.

РАСШИРЕННАЯ НАСТРОЙКА ПРОГРАММЫ

Этот раздел содержит подробную информацию о каждом компоненте программы с описанием алгоритма работы и настройки параметров компонента.

В ЭТОМ РАЗДЕЛЕ

ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ

Область защиты компьютера формируется с помощью настройки следующих параметров:

- перечня вредоносного ПО, защита от которого обеспечивается программой;
- объектов доверенной зоны, которые будут исключены из защиты.

В ЭТОМ РАЗДЕЛЕ

ВЫБОР КОНТРОЛИРУЕМЫХ ВРЕДОНОСНЫХ ПРОГРАММ

Kaspersky Endpoint Security предлагает защиту от разных видов вредоносного программного обеспечения. Вне зависимости от установленных параметров программа защищает компьютер от наиболее опасных видов вредоносных программ – вирусов, троянских программ и хакерских утилит. Эти программы могут нанести значительный вред вашему компьютеру. Для обеспечения большей безопасности компьютера можно расширить список обнаруживаемых угроз, включив контроль разного рода нежелательных программ.

Вредоносные и нежелательные программы, защиту от которых обеспечивает Kaspersky Endpoint Security, сгруппированы следующим образом:

- **Вирусы, черви, троянские и хакерские программы**. Эта группа объединяет наиболее распространенные и опасные категории вредоносных программ. Защита от них обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов «Лаборатории Касперского» Kaspersky Endpoint Security всегда контролирует вредоносные программы данной группы.

- **Шпионское и рекламное ПО**. Данная группа объединяет нежелательное программное обеспечение, которое может причинить неудобство пользователю или даже нанести ему ущерб.

- **Программы скрытого дозвона**. В эту группу включены программы, которые устанавливают телефонные соединения через модем в скрытом режиме (в том числе программы дозвона до порнографических телефонных служб).

- **Другие программы**. Эта группа включает программы, которые не являются вредоносными или опасными, однако при некотором стечении обстоятельств могут быть использованы для нанесения вреда вашему компьютеру.

Чтобы выбрать группы вредоносного программного обеспечения, от которых Kaspersky Endpoint Security будет защищать ваш компьютер, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Угрозы** (см. рис. ниже).

2. В блоке **Категории вредоносного ПО** установите флажок рядом с теми группами вредоносных программ, защиту от которых должен обеспечивать Kaspersky Endpoint Security.

Kaspersky Endpoint Security всегда обеспечивает защиту вашего компьютера от вирусов, червей, троянских и хакерских программ. Поэтому снять флажок рядом с этой группой невозможно.

В зависимости от выбранных групп Kaspersky Endpoint Security будет полностью или частично использовать антивирусные базы во время работы Файлового Антивируса (см. раздел «Файловый Антивирус» на стр. 57) и при поиске вирусов (см. раздел «Поиск вирусов» на стр. 69).

Если выбраны все группы вредоносного ПО, Kaspersky Endpoint Security обеспечивает максимально полную антивирусную защиту компьютера. Если выбрана защита только от вирусов, червей, троянских и хакерских программ, то Kaspersky Endpoint Security не контролирует нежелательные и другие вредоносные программы, которые могут быть установлены на вашем компьютере и своими действиями нанести моральный или материальный ущерб.

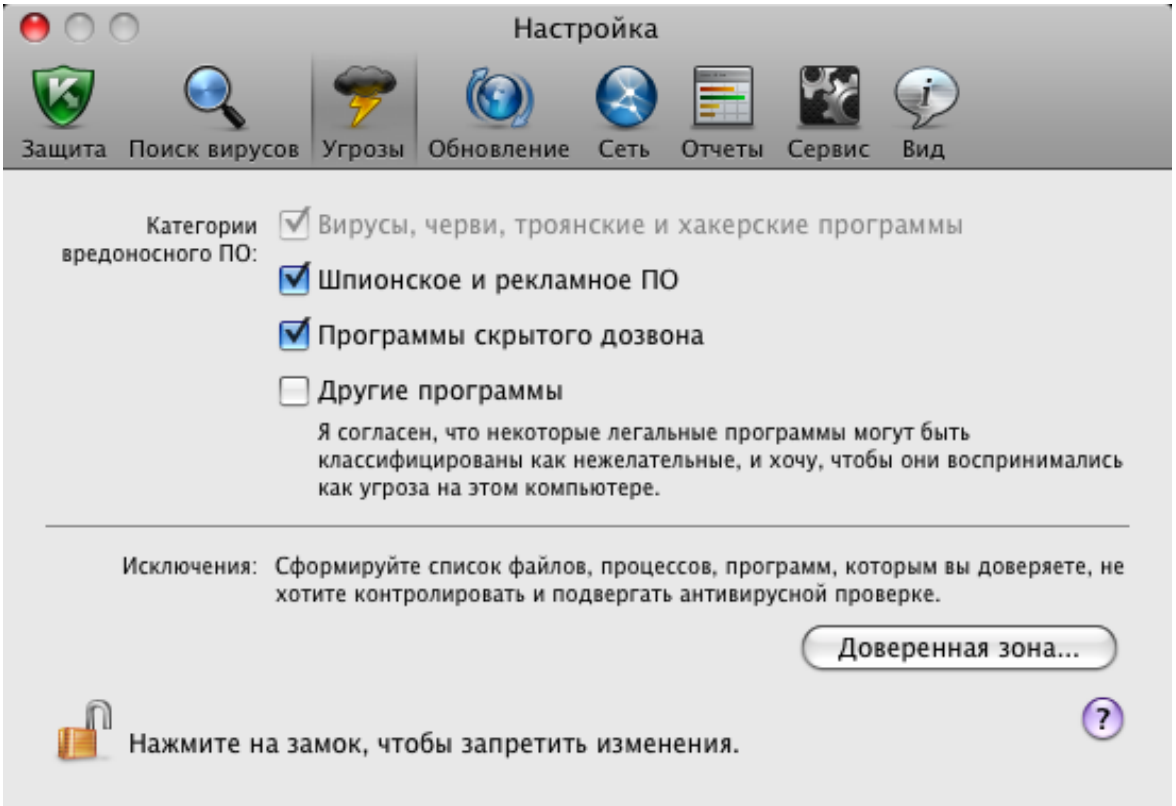


Рисунок 15. Окно настройки программы. Угрозы

Специалисты «Лаборатории Касперского» не рекомендуют отключать контроль за шпионским, рекламным программным обеспечением и программами скрытого дозвона. Если Kaspersky Endpoint Security относит программу, которая, по вашему мнению, не является опасной, к категории нежелательных программ, рекомендуется настроить для нее правило исключения (см. раздел «Формирование доверенной зоны» на стр. 54).

Формирование доверенной зоны

Доверенная зона – это сформированный пользователем перечень объектов, которые Kaspersky Endpoint Security не контролирует в процессе своей работы.

Доверенную зону формирует пользователь, принимая во внимание особенности объектов, с которыми он работает, а также специфику программ, установленных на компьютере. Создание такого списка исключений может потребоваться, например, в случае, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или программе, а вы уверены, что они не нанесут вреда компьютеру.

Правило исключения – это совокупность условий, при которых объект не будет проверяться Kaspersky Endpoint Security. Исключать из проверки можно файл определенного формата (см. раздел «Список объектов, проверяемых по расширению» на стр. 158), файлы по маске (см. раздел «Разрешенные маски исключений файлов» на стр. 160), некоторую область (например, папку или программу), процессы программ или объекты по типу угрозы согласно классификации Вирусной энциклопедии (http://www.securelist.com).

Объект исключения не подлежит проверке, если проверяется диск или папка, в которой он расположен. Однако при выборе проверки именно этого объекта правило исключения применено не будет.

Тип угрозы – это статус, который присвоен объекту Kaspersky Endpoint Security при проверке. Статус присваивается на основании классификации вредоносных и нежелательных программ, представленных в Вирусной энциклопедии «Лаборатории Касперского».

Нежелательное программное обеспечение не имеет вредоносных функций, но может быть использовано в качестве вспомогательного компонента вредоносной программы, поскольку может содержать бреши и ошибки. В эту категорию попадают, например, программы удаленного администрирования, IRC-клиенты, FTP-серверы, всевозможные утилиты для остановки процессов или сокрытия их работы, клавиатурные шпионы, программы вскрытия паролей, автоматического дозвона на платные сайты. Данное программное обеспечение не классифицируется как вирусы (not-a-virus). Его можно разделить на типы, например, Adware, Joke, Riskware и т.п. (подробную информацию о нежелательных программах, обнаруживаемых Kaspersky Endpoint Security, смотрите в Вирусной энциклопедии (http://www.securelist.com)). В результате проверки такие программы могут быть заблокированы. Поскольку некоторые из них широко применяются пользователями, предусмотрена возможность исключения их из проверки.

Чтобы создать новое правило исключения или просмотреть и изменить уже созданные правила исключения, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Угрозы** (см. рис. ниже).

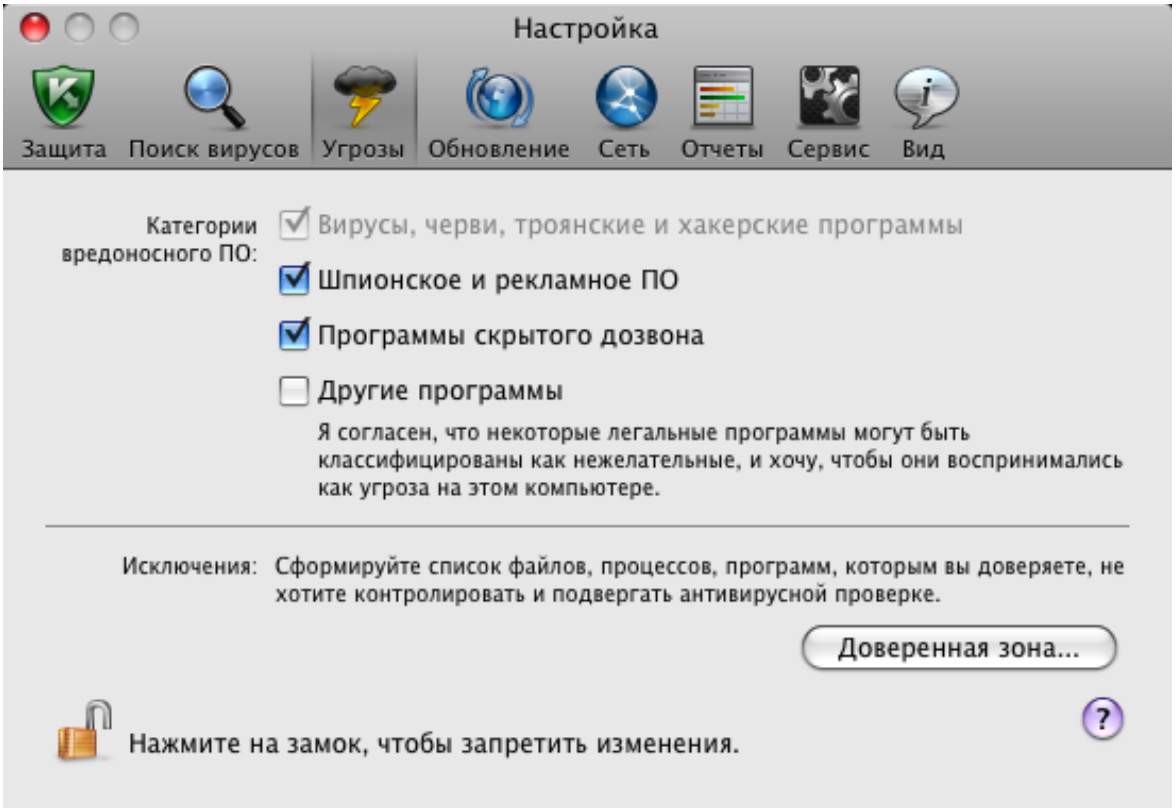


Рисунок 16. Окно настройки программы. Угрозы

2. В блоке **Исключения** нажмите на кнопку **Доверенная зона** (см. рис. выше). Откроется окно (см. рис. ниже) со списком объектов, которые Kaspersky Endpoint Security не будет контролировать в процессе своей работы.

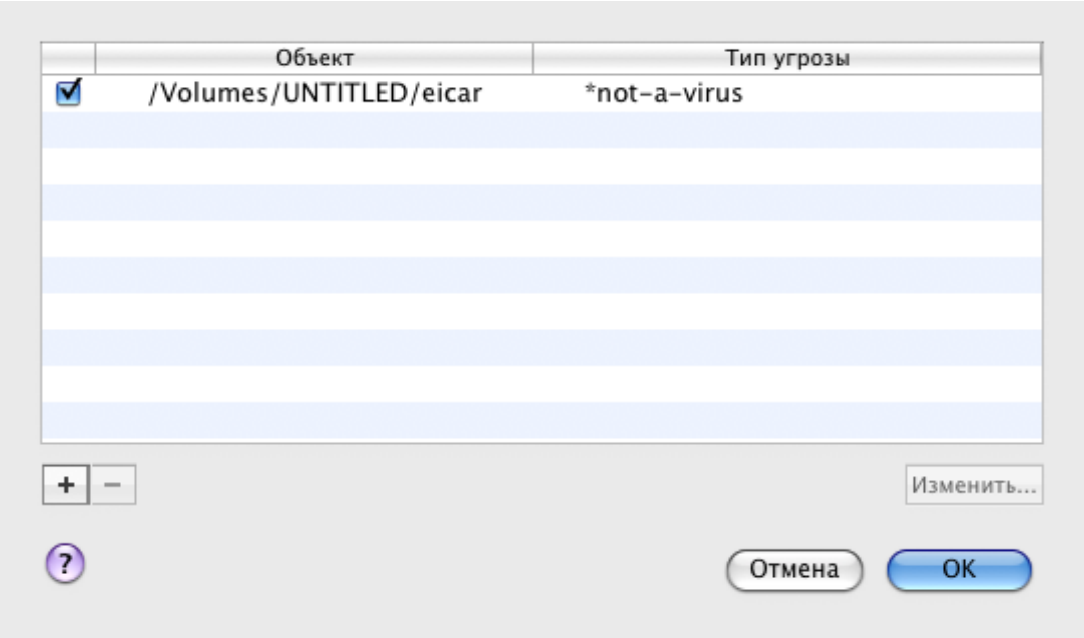


Рисунок 17. Список объектов исключения

Вы можете выполнить следующие действия:

- Создать новое правило исключения.

  Нажмите на кнопку  и в открывшемся окне **Правило исключения** (см. рис. ниже) задайте его условия.

- Изменить уже созданное правило исключения.

  Выберите правило исключения в списке и нажмите на кнопку **Изменить**. В открывшемся окне **Правило исключения** (см. рис. ниже) внесите изменения в его условия.

- Временно отказаться от использования правила исключения.

  Выберите правило исключения в списке и снимите флажок рядом с ним. Правило исключения перестанет применяться до тех пор, пока флажок не будет вновь установлен.

- Удалить правило исключения.

  Выберите правило исключения в списке и нажмите на кнопку  .

Создание правила исключения

В открывшемся окне **Правило исключения** задайте условия правила исключения в соответствии со следующими параметрами:

- **Объект / Все объекты**. Укажите файл, папку или маску файла (см. раздел «Разрешенные маски исключений файлов» на стр. 160) в качестве объекта исключения. Вы можете ввести имя / маску имени объекта в поле вручную или нажать на кнопку **Выбрать** и выбрать объект в открывшемся стандартном окне.

  Выбор значения **Все объекты** подразумевает исключение из проверки всех объектов компьютера, которым присвоен тип угрозы, заданный в поле ниже.

- **Типы угроз / Все угрозы**. Параметр позволяет исключать из проверки объекты, исходя из типа угрозы, присвоенного согласно классификации Вирусной энциклопедии. Для ввода названия угрозы используйте значения раскрывающегося списка: **начинаются с**, **заканчиваются на**, **содержат**, **целое слово** и в поле справа укажите соответствующую часть названия. Например, если выбрано значение **начинаются с not-a-virus**, из проверки будут исключены легальные, но нежелательные программы. Также допускается указывать имя угрозы по маске (см. раздел «Разрешенные маски исключений по классификации Вирусной энциклопедии» на стр. 161).

  При выборе значения **Все угрозы** из проверки будут исключены объекты, указанные в поле **Объект** выше, вне зависимости от присвоенного им типа угрозы.

  При одновременном выборе объекта исключения и типа угрозы, правило будет срабатывать следующим образом:

  - Если в качестве объекта указан некоторый файл, а в качестве типа угрозы – определенный статус, то указанный файл будет исключением только в том случае, если в процессе проверки ему будет присвоен статус заданной угрозы.

  - Если в качестве объекта указана некоторая область или папка, а в качестве типа угрозы – определенный статус, то из проверки исключаются объекты заданного статуса, обнаруживаемые только в указанной области / папке.

- **Компонент / Все компоненты**. Выберите компоненты Kaspersky Endpoint Security, в работе которых должно быть использовано создаваемое правило: **Файловый Антивирус** или **Поиск вирусов**.

Выбор варианта **Все компоненты** означает, что правило будет использоваться всеми задачами поиска вирусов, а также Файловым Антивирусом.

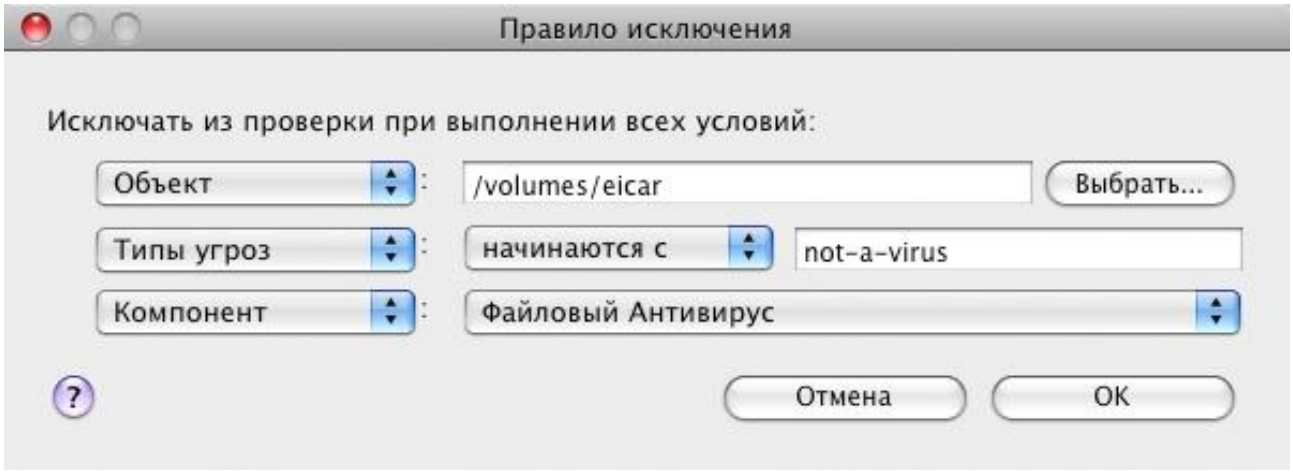


Рисунок 18. Создание правила исключения

Файловый Антивирус

Файловая система компьютера может содержать вирусы и прочие вредоносные программы, которые, проникнув однажды со съемного диска или из интернета, способны храниться годами и никак не проявлять себя.

Файловый Антивирус – компонент, контролирующий файловую систему компьютера в режиме реального времени. По умолчанию он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, запускаемые и сохраняемые файлы на компьютере и присоединенных дисках.

Файловый Антивирус работает с файлами согласно следующему алгоритму:

1. Перехватывает обращение пользователя или программы к каждому файлу.

2. Проверяет наличие информации о перехваченном файле в базе iSwift (см. раздел «Настройка дополнительных параметров» на стр. 64). На основании полученной информации принимается решение о необходимости проверки файла.

3. Анализирует файл на присутствие вирусов. Распознавание вредоносных объектов происходит с использованием антивирусных баз Kaspersky Endpoint Security. Базы содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания.

В зависимости от результатов анализа возможны следующие варианты поведения Kaspersky Endpoint Security:

- Если в файле не было обнаружено вредоносного кода, он сразу же становится доступным для работы.

- Если в файле был обнаружен вредоносный код, Файловый Антивирус блокирует файл и пытается его лечить. После успешного лечения файл становится доступным для работы; если лечение произвести не удалось, файл удаляется. Копия файла помещается в резервное хранилище (на стр. 97).

- Если в файле обнаружен код, похожий на вредоносный, файл помещается в специальное хранилище – карантин (на стр. 94). Позже можно попытаться вылечить его, используя обновленные антивирусные базы.

По умолчанию Kaspersky Endpoint Security запускается при старте операционной системы и защищает ваш компьютер в течение всего сеанса работы. Свидетельством работы Файлового Антивируса служит значок Kaspersky Endpoint Security (на стр. 32). Активный значок означает, что защита вашего компьютера включена, неактивный – что защита выключена.

В этом разделе

Выключение защиты файлов

Специалисты «Лаборатории Касперского» настоятельно рекомендуют не отключать защиту, обеспечиваемую Файловым Антивирусом в режиме реального времени, поскольку это может привести к заражению вашего компьютера и потере данных.

Обратите внимание, что в данном случае защита рассматривается именно в контексте работы Файлового Антивируса (см. раздел «Файловый Антивирус» на стр. 57). Отключение или приостановка его работы не оказывает влияния на выполнение задач поиска вирусов (см. раздел «Поиск вирусов» на стр. 69) и обновления (см. раздел «Обновление программы» на стр. 84).

Выключить Файловый Антивирус можно несколькими способами. Однако прежде чем делать это, рекомендуем определить причину, по которой вы хотите выключить защиту файлов.

Вероятно, возникшую проблему можно решить другим способом: изменить уровень безопасности (см. раздел «Выбор уровня безопасности» на стр. 61) или отключить защиту только определенных файлов, создав правило исключения (см. раздел «Формирование доверенной зоны» на стр. 54). Так, например, если вы работаете с некоторой базой данных, которая, на ваш взгляд, не может содержать вирусов, просто добавьте папку с ее файлами в доверенную зону. Возможно, вам может потребоваться приостановить на время работу Файлового Антивируса в случае, если Kaspersky Endpoint Security конфликтует с другими программами, установленными на вашем компьютере

➧ *Чтобы выключить Файловый Антивирус, воспользуйтесь любым из следующих способов:*

- Нажмите на значок Kaspersky Endpoint Security (на стр. 32) и в открывшемся контекстном меню выберите команду **Выключить защиту** (см. рис. ниже).

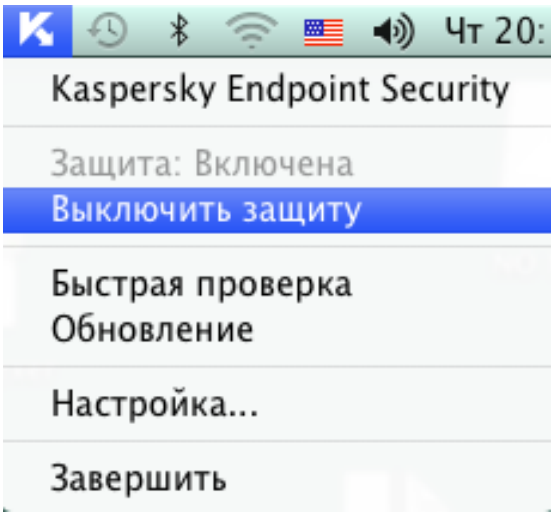


Рисунок 19. Выключение Файлового Антивируса

- Откройте окно настройки программы (на стр. 35), выберите закладку **Защита** и снимите флажок **Включить Файловый Антивирус** (см. рис. ниже).

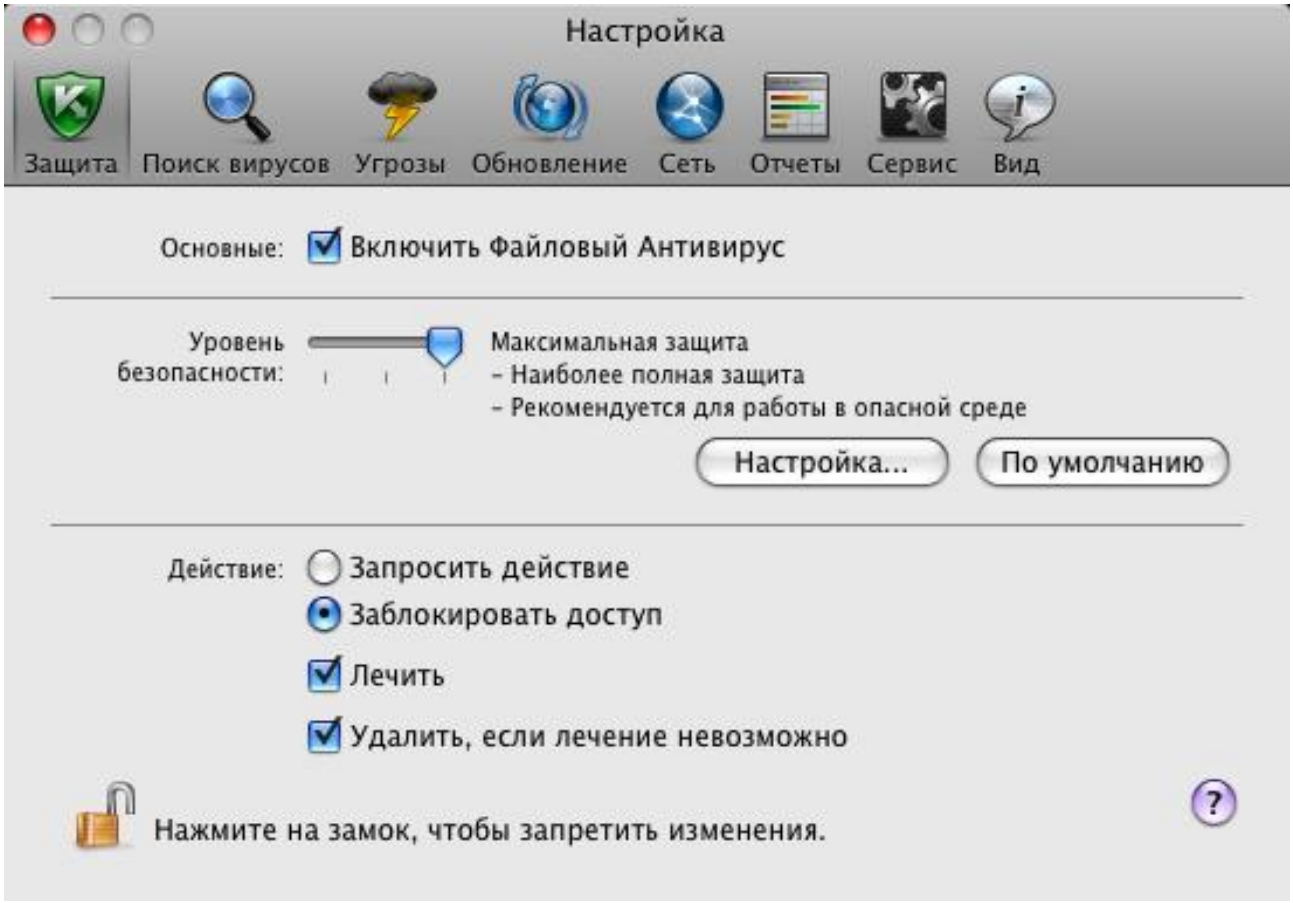


Рисунок 20. Окно настройки программы. Защита

Если вы отключили Файловый Антивирус, то после перезапуска Kaspersky Endpoint Security он не будет включен автоматически. Необходимо восстановить защиту файловой системы компьютера вручную (см. раздел «Возобновление защиты вашего компьютера» на стр. 59).

ВОЗОБНОВЛЕНИЕ ЗАЩИТЫ ВАШЕГО КОМПЬЮТЕРА

Если Файловый Антивирус был отключен, то возобновить защиту файловой системы компьютера можно только вручную по требованию пользователя. Автоматического включения Файлового Антивируса после перезагрузки операционной системы или Kaspersky Endpoint Security не происходит.

Чтобы включить Файловый Антивирус, воспользуйтесь одним из следующих способов:

- Нажмите на значок Kaspersky Endpoint Security (на стр. 32) и в открывшемся контекстном меню выберите команду **Включить защиту** (см. рис. ниже).

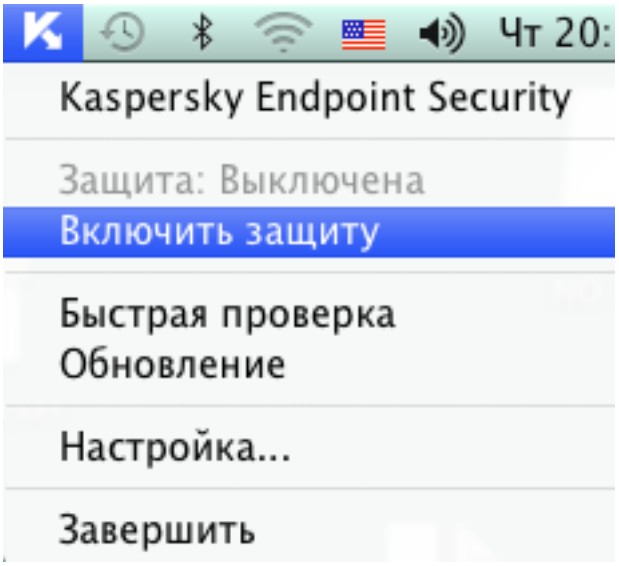


Рисунок 21. Включение Файлового Антивируса

- Откройте окно настройки программы (на стр. 35), выберите закладку **Защита** и установите флажок **Включить Файловый Антивирус** (см. рис. ниже).

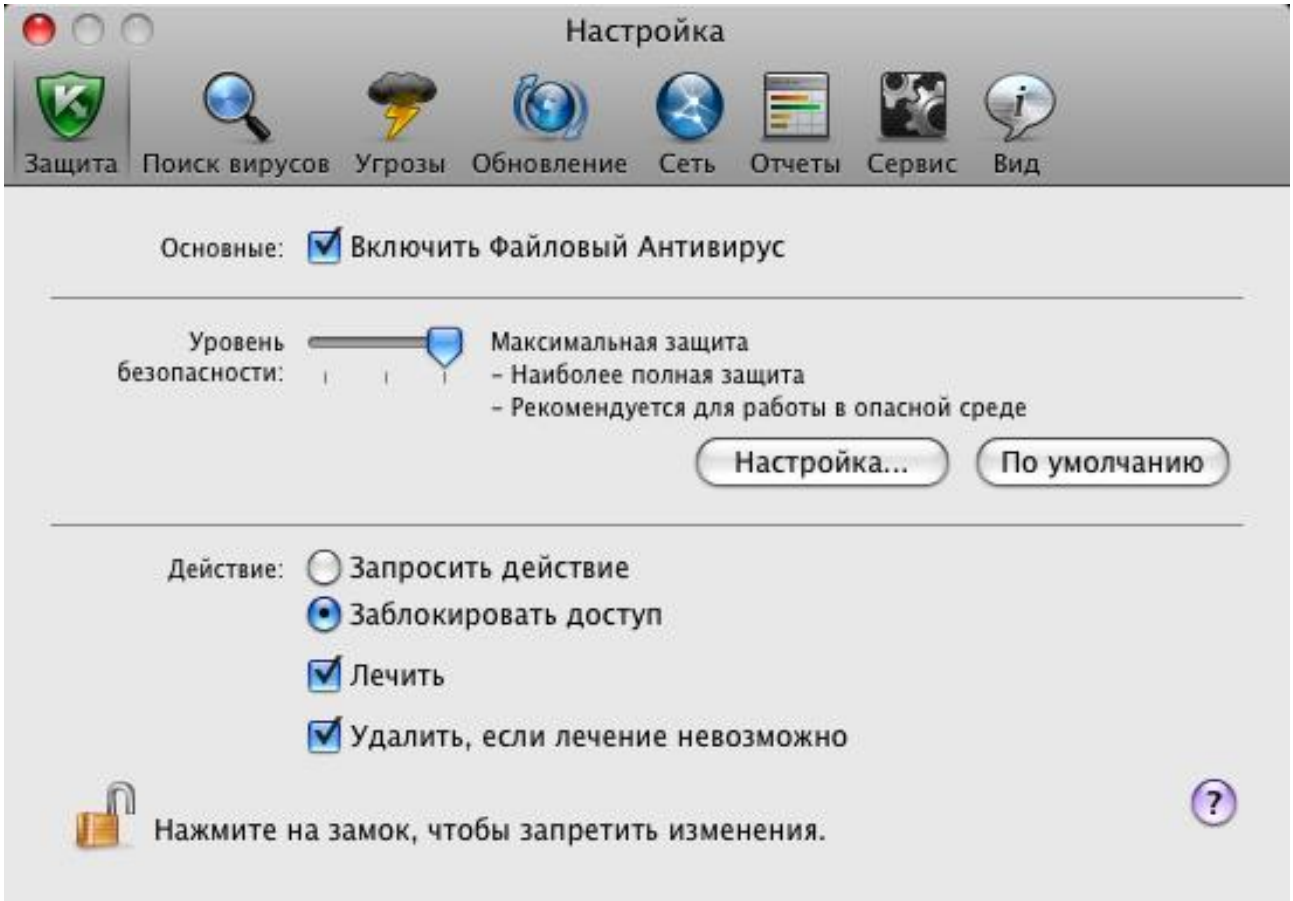


Рисунок 22. Окно настройки программы. Защита

- Воспользуйтесь Ассистентом безопасности (см. раздел «Ассистент безопасности» на стр. 44). Приостановка или полное отключение защиты значительно повышает риск заражения компьютера, поэтому такая угроза немедленно фиксируется Ассистентом безопасности.

НАСТРОЙКА ФАЙЛОВОГО АНТИВИРУСА

Работа Файлового Антивируса контролируется с помощью следующих настроек:

- **Уровень безопасности**.

  Уровень безопасности – это набор параметров, определяющих соотношение между тщательностью и скоростью проверки объектов на вирусы. Существует три предустановленных уровня безопасности (см. раздел «Выбор уровня безопасности» на стр. 61) с параметрами, разработанными специалистами «Лаборатории Касперского».

- **Действие над обнаруженным объектом**.

  Действие (см. раздел «Выбор действия над объектами» на стр. 66) определяет поведение Kaspersky Endpoint Security при обнаружении зараженного или возможно зараженного объекта.

ВЫБОР УРОВНЯ БЕЗОПАСНОСТИ

Файловый Антивирус обеспечивает защиту файловой системы компьютера на одном из следующих уровней:

- **Максимальная защита** – уровень, на котором осуществляется максимально полный контроль всех открываемых, сохраняемых и запускаемых файлов.

- **Рекомендуемый** – уровень, параметры которого рекомендованы экспертами «Лаборатории Касперского».

- **Максимальная скорость** – уровень, параметры которого позволяют вам комфортно работать с программами, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на данном уровне сокращен.

По умолчанию Файловый Антивирус работает на **Рекомендуемом** уровне безопасности. Вы можете повысить или понизить уровень защиты файловой системы, выбрав уровень **Максимальная защита** или **Максимальная скорость** соответственно, или изменив настройки текущего уровня.

Чтобы изменить уровень безопасности, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Защита** (см. рис. ниже).

2. В блоке **Уровень безопасности** переместите ползунок по шкале. Регулируя уровень безопасности, вы определяете соотношение между скоростью выполнения проверки и количеством проверяемых файлов: чем меньше файлов подвергается анализу на вирусы, тем выше скорость проверки.

Если ни один из перечисленных уровней безопасности не соответствует вашим требованиям, выполните дополнительную настройку параметров защиты. Для этого рекомендуется выбрать наиболее близкий к вашим пожеланиям уровень безопасности в качестве базового и изменить его параметры. В этом случае название уровня безопасности изменится на **Пользовательский**.

Чтобы изменить параметры текущего уровня безопасности, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Защита** (см. рис. ниже).

2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

3. В открывшемся окне отредактируйте параметры защиты файлов:

   - на закладке **Общие** (см. раздел «Определение типов проверяемых файлов» на стр. 62) определите типы проверяемых файлов;
   - на закладке **Область защиты** (см. раздел «Формирование области защиты» на стр. 63) укажите диски или папки, которые должны контролироваться Файловым Антивирусом;
   - на закладке **Дополнительно** (см. раздел «Настройка дополнительных параметров» на стр. 64) настройте режим работы компонента.

4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

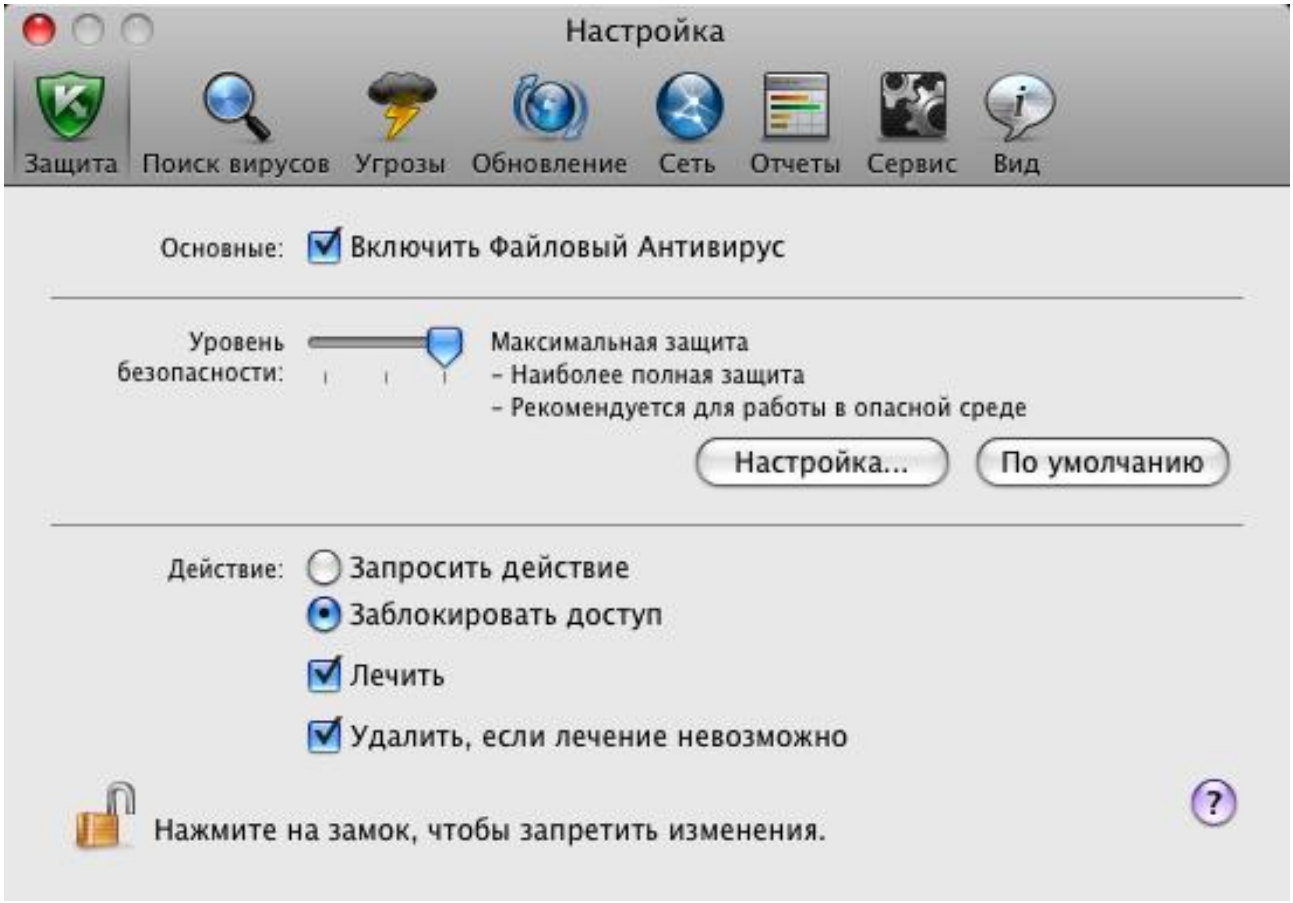


Рисунок 23. Окно настройки программы. Защита

Определение типов проверяемых файлов

Указывая тип проверяемых файлов, вы определяете, файлы какого формата и размера будут проверяться Файловым Антивирусом на вирусы при открытии, исполнении и сохранении. Также вы можете настроить производительность проверки.

Чтобы указать тип проверяемых Файловым Антивирусом объектов и настроить производительность проверки, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Защита**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

3. В открывшемся окне выберите закладку **Общие** (см. рис. ниже) и настройте следующие параметры:

   - В блоке **Типы файлов** укажите, объекты какого формата будут проверяться Kaspersky Endpoint Security на вирусы при открытии, исполнении и сохранении.
   - В блоке **Оптимизация** настройте производительность проверки.
   - В блоке **Составные файлы** выберите, какие составные файлы необходимо анализировать на присутствие вирусов и установите ограничение на проверку больших объектов.

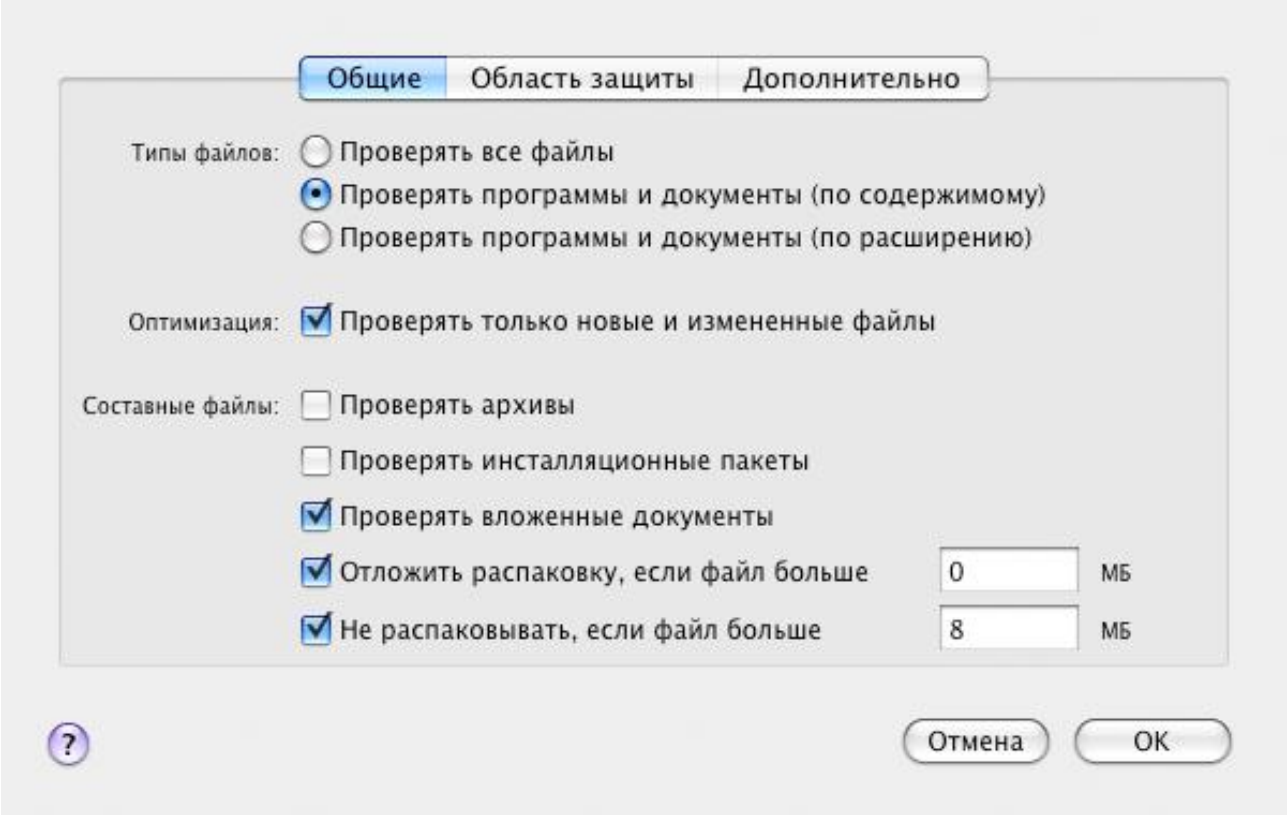


Рисунок 24. Файловый Антивирус. Настройка параметров проверки

ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ

По умолчанию Файловый Антивирус проверяет все файлы в момент обращения к ним, независимо от того, на каком носителе они расположены (жесткий диск, CD / DVD-ROM или флеш-карта).

➧ *Чтобы сформировать список объектов, входящих в область защиты, выполните следующие действия:*

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Защита**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
3. В открывшемся окне выберите закладку **Область защиты** (см. рис. ниже). На закладке представлен список объектов, которые будут проверяться Файловым Антивирусом. По умолчанию включена защита всех объектов, расположенных на жестких, сменных и сетевых дисках, подключенных к компьютеру.

Вы можете выполнить следующие действия:

- Добавить объект для проверки.

  Нажмите на кнопку [+] и в открывшемся стандартном окне выберите папку или файл.

- Изменить объект списка (доступно только для объектов, добавленных пользователем).

  Выберите объект и нажмите на кнопку **Изменить**. В открывшемся стандартном окне внесите необходимые изменения.

- Временно отключить проверку объекта списка.

  Выберите объект и снимите флажок рядом с ним. Файловый Антивирус не будет контролировать этот объект до тех пор, пока флажок не будет вновь установлен.

- Удалить объект (доступно только для объектов, добавленных пользователем).

  Выберите объект и нажмите на кнопку  .

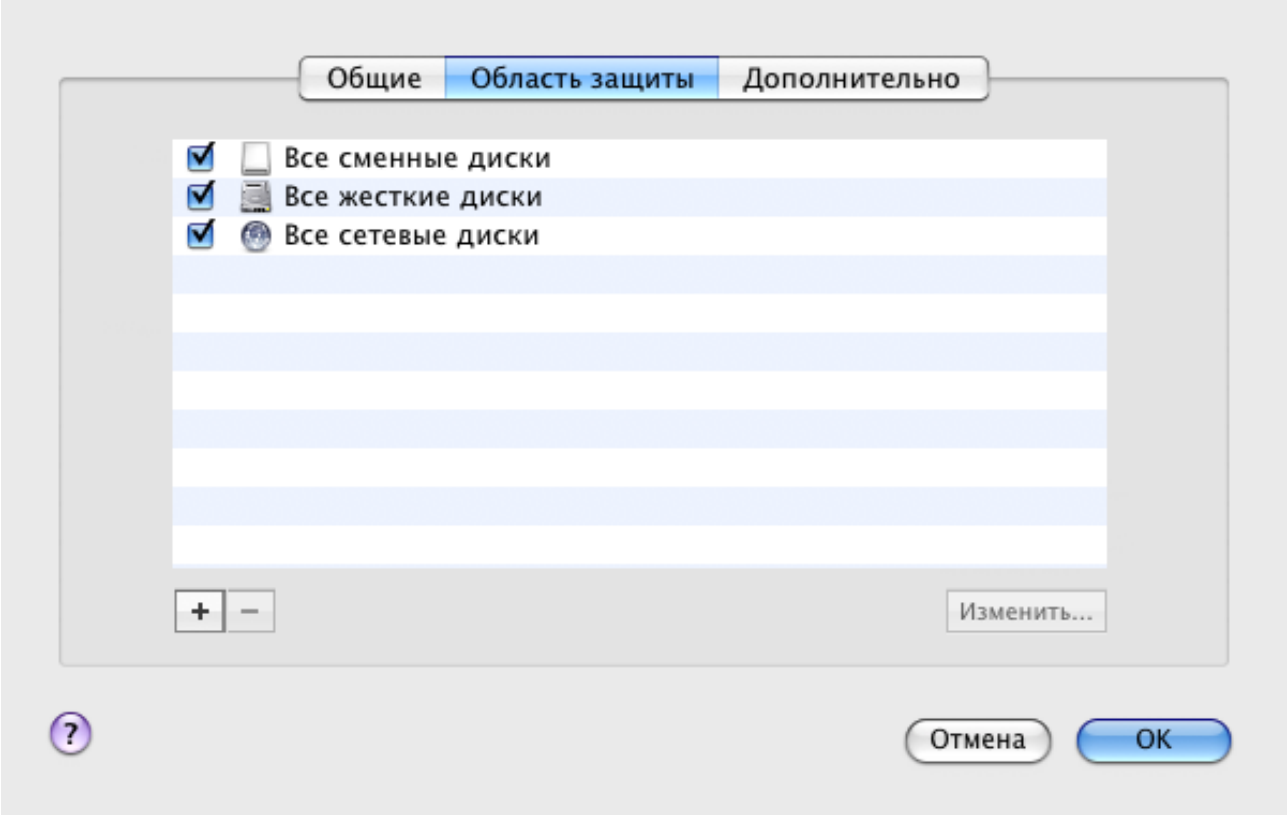


Рисунок 25. Файловый Антивирус. Формирование защищаемой области

Ограничить круг защищаемых объектов можно следующими способами:

- указать только те папки, диски или файлы, которые нужно защищать;
- сформировать список объектов, которые защищать не нужно (см. раздел «Формирование доверенной зоны» на стр. 54);
- объединить первый и второй способы, то есть сформировать область защиты, и исключить из нее ряд объектов.

Настройка дополнительных параметров

В качестве дополнительных параметров работы Файлового Антивируса вы можете настроить режим проверки объектов файловой системы, включить технологию iSwift, повышающую производительность обработки объектов, а также настроить расписание работы компонента.

Чтобы настроить дополнительные параметры Файлового Антивируса, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Защита**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
3. В открывшемся окне выберите закладку **Дополнительно** (см. рис. ниже) и настройте следующие параметры:
   - В блоке **Режим проверки** выберите режим срабатывания Файлового Антивируса.
   - В блоке **Производительность** выберите технологию проверки.
   - В блоке **Приостановка задачи** включите приостановку работы Файлового Антивируса по расписанию и настройте параметры расписания.
   - В блоке **Эвристический анализатор** настройте использование Файловым Антивирусом эвристического анализатора.

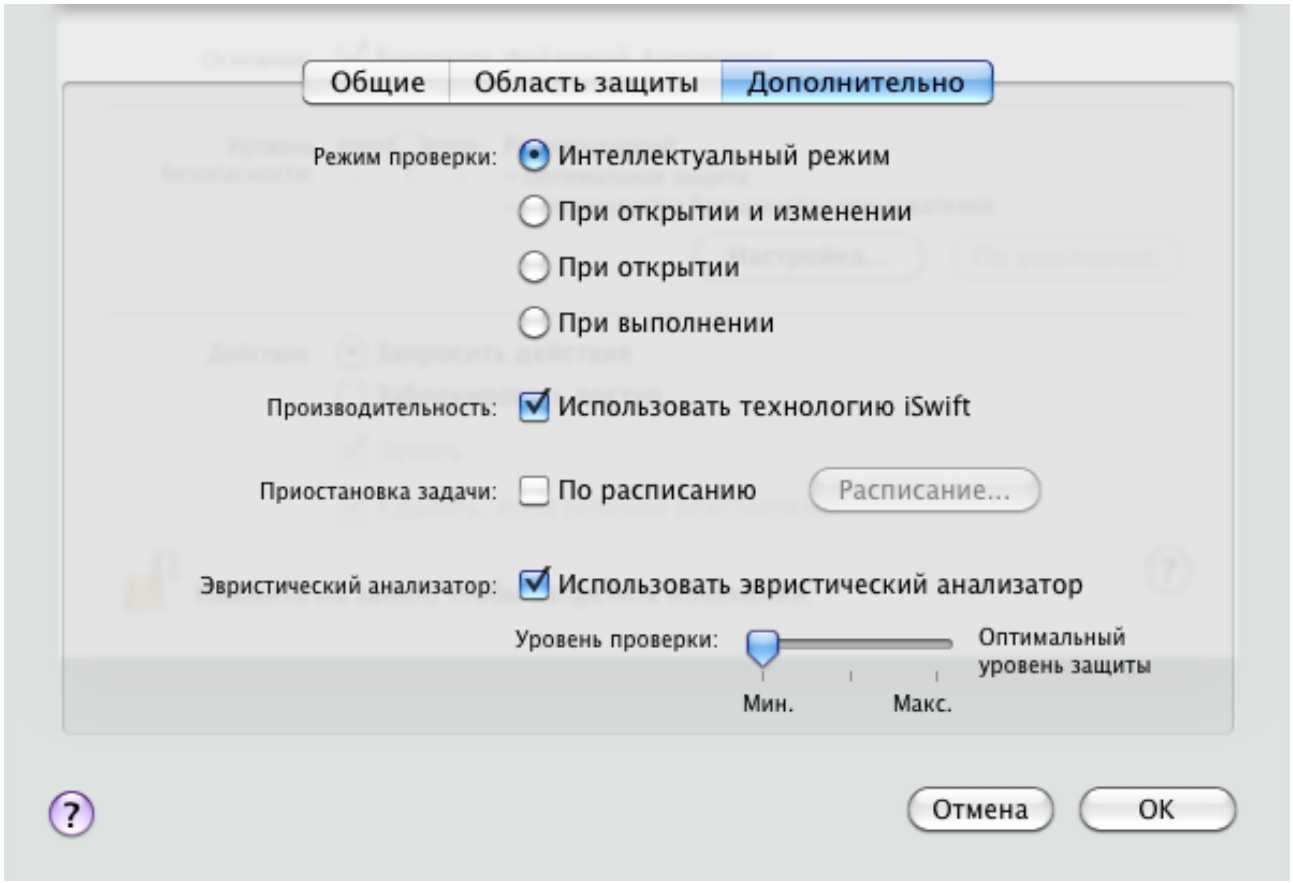


Рисунок 26. Файловый Антивирус. Настройка дополнительных параметров

ВЫБОР ДЕЙСТВИЯ НАД ОБЪЕКТАМИ

Если в результате проверки файла на вирусы выясняется, что он заражен или возможно заражен, дальнейшее поведение Файлового Антивируса зависит от статуса объекта и выбранного действия.

По результатам проверки объект может быть идентифицирован следующим образом:

- как вредоносный, например, *вирус* или *троянская программа*;
- как *возможно зараженный*, когда в результате проверки однозначно невозможно определить, заражен объект или нет. Это означает, что в файле обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

По умолчанию все вредоносные объекты подвергаются лечению, а все возможно зараженные помещаются в хранилище карантина (см. раздел «Карантин» на стр. 94).

Чтобы выбрать действие, которое должен выполнить Файловый Антивирус при обнаружении зараженного или возможно зараженного объекта, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Защита** (см. рис. ниже).
2. В блоке **Действие** выберите действие Файлового Антивируса.

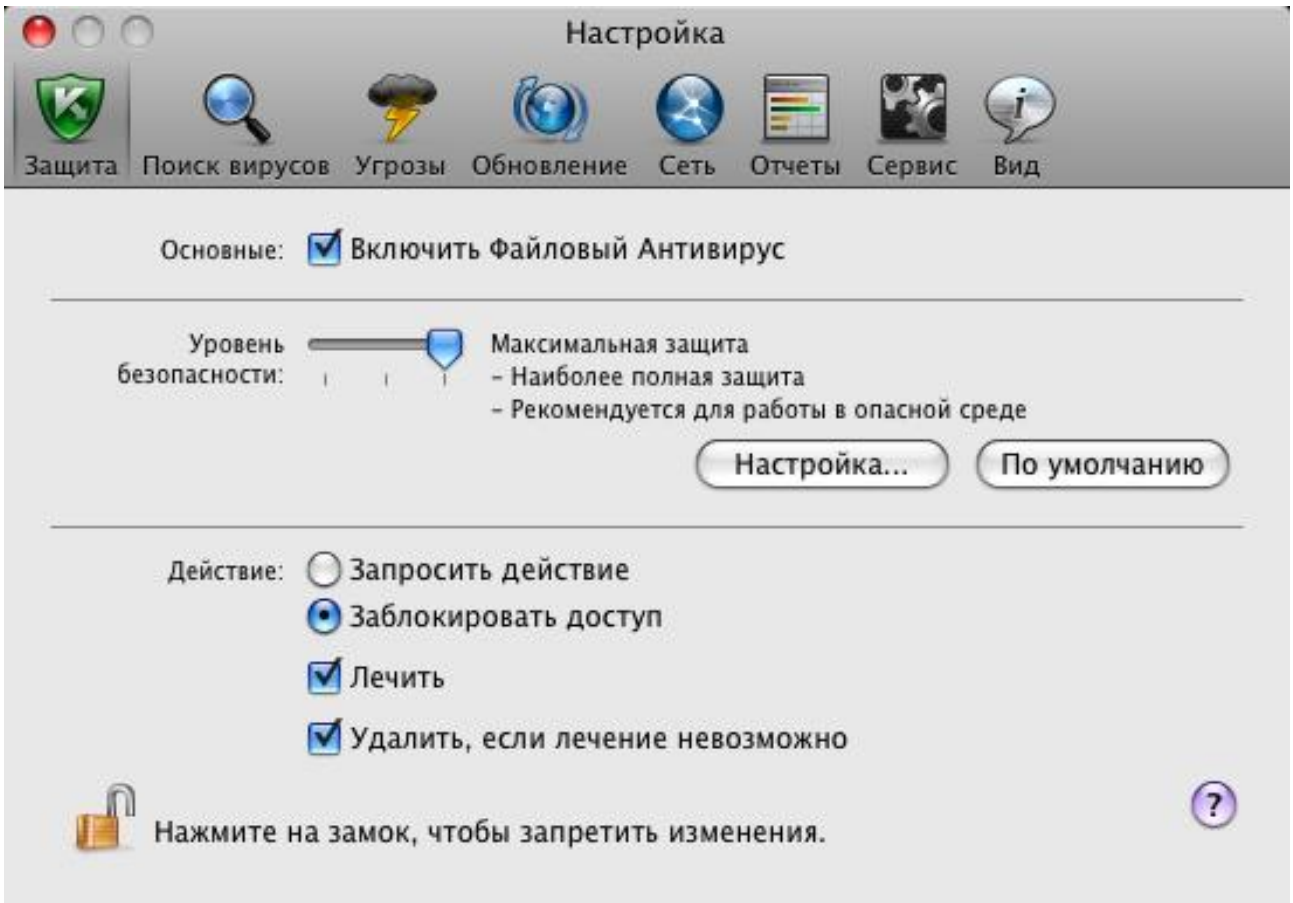


Рисунок 27. Окно настройки программы. Защита

Перед лечением или удалением объекта Kaspersky Endpoint Security создает его резервную копию и помещает ее в резервное хранилище (на стр. 97) на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

ВОССТАНОВЛЕНИЕ ПАРАМЕТРОВ ЗАЩИТЫ ФАЙЛОВ ПО УМОЛЧАНИЮ

В любой момент вы можете вернуться к параметрам настройки Файлового Антивируса по умолчанию. Они считаются оптимальными для обеспечения безопасности вашего компьютера от вредоносных программ, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы восстановить параметры Файлового Антивируса по умолчанию, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Защита** (см. рис. ниже).

2. В блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

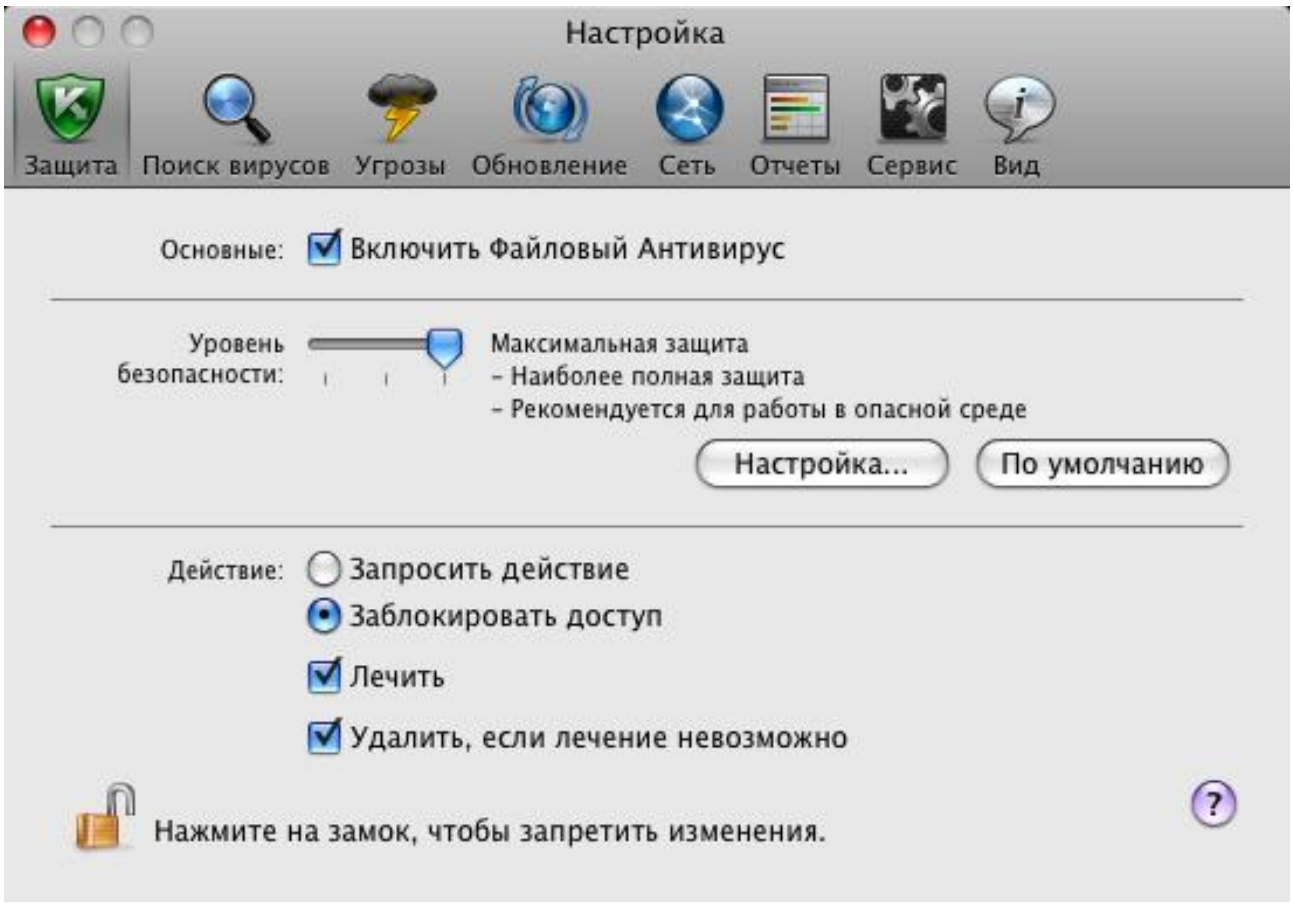


Рисунок 28. Окно настройки программы. Защита

СТАТИСТИКА ЗАЩИТЫ ФАЙЛОВ

Сводная статистика текущей работы Файлового Антивируса (количество объектов, проверенных с момента последнего запуска компонента, количество обнаруженных и вылеченных опасных объектов, имя файла, который проверялся последним) представлена в нижней части главного окна программы (см. раздел «Главное окно программы» на стр. 34).

Также Kaspersky Endpoint Security предоставляет подробный отчет о работе Файлового Антивируса.

Чтобы просмотреть отчет, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
2. В разделе **Выполняемые задачи** открывшегося окна отчетов выберите **Файловый Антивирус**.

Если Файловый Антивирус в данный момент отключен, просмотреть детальный отчет о результатах его прошлого запуска можно в разделе **Завершенные задачи**.

Если Файловый Антивирус завершил работу с ошибкой, просмотрите отчет и попробуйте перезапустить компонент. Если самостоятельно разобраться в проблеме не удается, обратитесь в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 156).

Подробная информация о работе Файлового Антивируса представлена в окне отчетов справа на следующих закладках:

- На закладке **Обнаружено** перечислены все опасные объекты, обнаруженные в процессе защиты файловой системы компьютера. Для каждого объекта указано имя и путь к папке, в которой он хранится, а также статус, присвоенный этому объекту Файловым Антивирусом. Если удалось точно установить, какой вредоносной программой поражен объект, ему присваивается статус *вирус*, *троянская программа* и т.д. Если тип вредоносного воздействия точно установить не удалось, объекту присваивается статус *возможно зараженный*. Рядом со статусом также указывается действие, выполненное над объектом (*обнаружен*, *вылечен*).
- На закладке **События** приводится полный список событий, зафиксированных в работе Файлового Антивируса с указанием времени наступления события, его имени, статуса и причины возникновения. Событиям могут быть присвоены следующие статусы:
  - информационное событие (например: *объект не обработан: пропущен по типу*);
  - внимание (например: *обнаружен вирус*);
  - примечание (например: *архив защищен паролем*).
- На закладке **Статистика** приводится информация об общем количестве проверенных объектов, а в отдельных графах отражено, сколько объектов из общего числа проверенных являются архивами, сколько опасных объектов, сколько вылеченных, сколько помещенных на карантин и т.д.
- На закладке **Параметры** перечислены основные параметры, в соответствии с которыми работает Файловый Антивирус. Чтобы быстро перейти к настройке компонента, нажмите на кнопку **Изменить параметры**.

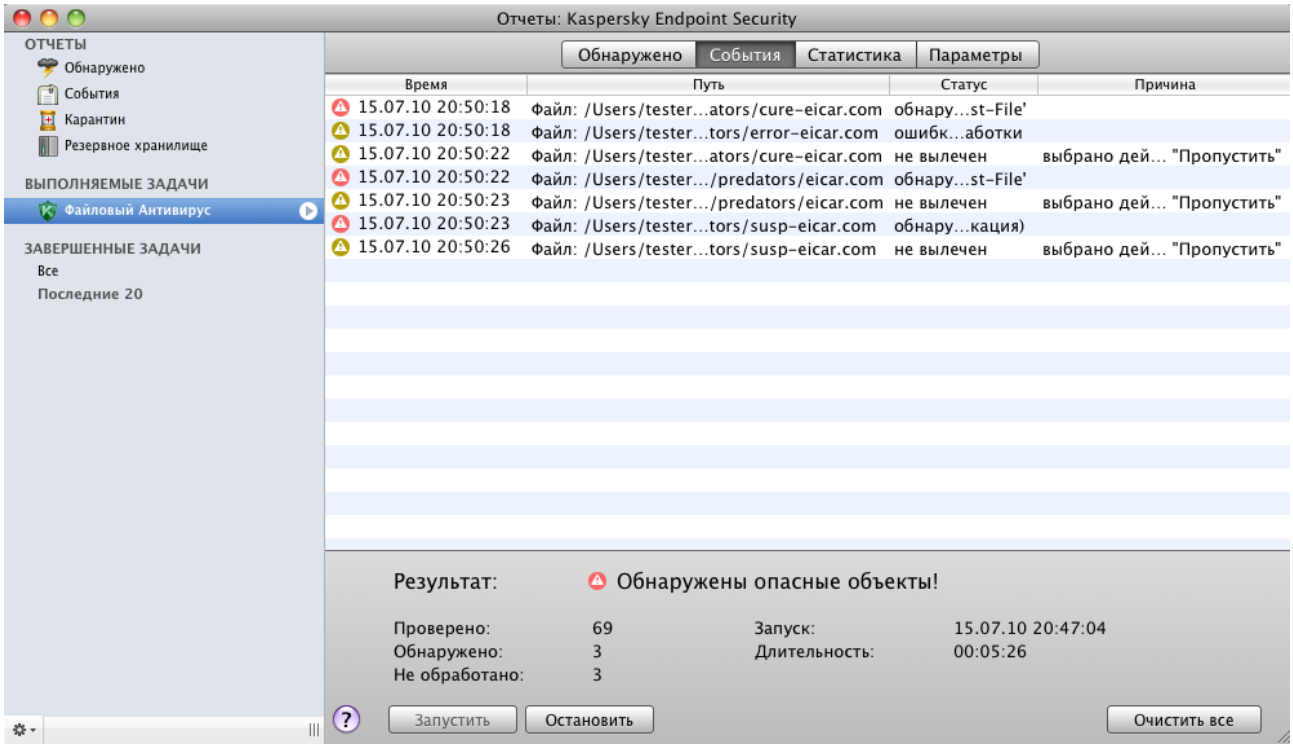


Рисунок 29. Окно отчетов. Файловый Антивирус

Поиск вирусов

Помимо защиты файловой системы компьютера Файловым Антивирусом (см. раздел «Файловый Антивирус» на стр. 57) в режиме реального времени, крайне важно периодически проводить проверку компьютера на вирусы. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены Файловым Антивирусом, например, из-за установленного низкого уровня безопасности или по другим причинам.

Kaspersky Endpoint Security предлагает следующие встроенные задачи поиска вирусов:

- **Поиск вирусов**

  Проверка на вирусы отдельного объекта (файла, папки, диска, сменного устройства).

- **Полная проверка**

  Поиск вирусов на вашем компьютере с тщательной проверкой всех жестких дисков.

- **Быстрая проверка**

  Проверка на присутствие вирусов только критических областей компьютера: папок, содержащих файлы операционной системы и системных библиотек.

По умолчанию эти задачи выполняются с рекомендуемыми параметрами. Вы можете изменять эти параметры (см. раздел «Настройка задач поиска вирусов» на стр. 75), а также устанавливать режим запуска задач поиска вирусов (см. раздел «Настройка запуска задач поиска вирусов по расписанию» на стр. 79).

В ЭТОМ РАЗДЕЛЕ

УПРАВЛЕНИЕ ЗАДАЧАМИ ПОИСКА ВИРУСОВ

Запуск задач поиска вирусов может осуществляться вручную (см. раздел «Запуск / остановка задач поиска вирусов» на стр. 70) или автоматически согласно расписанию (см. раздел «Настройка запуска задач поиска вирусов по расписанию» на стр. 79). Кроме того, в Kaspersky Endpoint Security предусмотрена возможность создания пользовательских задач (см. раздел «Создание задач поиска вирусов» на стр. 71).

ЗАПУСК / ОСТАНОВКА ЗАДАЧ ПОИСКА ВИРУСОВ

Чтобы запустить задачу поиска вирусов вручную, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку .
2. В открывшемся окне (см. рис. ниже) выберите нужную задачу: **Полная проверка**, **Быстрая проверка** или **Поиск вирусов**. Если вы выбрали задачу **Поиск вирусов**, Kaspersky Endpoint Security предложит задать область поиска. Помимо перечисленных задач, которые включены в поставку программы, в меню отображаются пользовательские задачи поиска вирусов (см. раздел «Создание задач поиска вирусов» на стр. 71), если они были созданы.

Рисунок 30. Задачи поиска вирусов

Информация о задачах, выполняющихся в текущий момент, отображается в левой части главного окна, а также в разделе **Выполняемые задачи** окна отчетов (см. раздел «Отчеты» на стр. 99). Информация о выполненных задачах представлена в разделе **Завершенные задачи** окна отчетов (см. рис. ниже).

Чтобы остановить выполнение задачи поиска вирусов, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  . Откроется окно отчетов Kaspersky Endpoint Security.

2. В разделе **Выполняемые задачи** (см. рис. ниже) выберите имя задачи поиска вирусов и нажмите на кнопку **Остановить**. Проверка будет остановлена до того момента, пока задача не будет запущена снова – вручную или по расписанию. Чтобы вновь запустить проверку, нажмите на кнопку **Запустить.** Откроется окно, в котором Kaspersky Endpoint Security предложит продолжить прерванную проверку или начать ее заново.

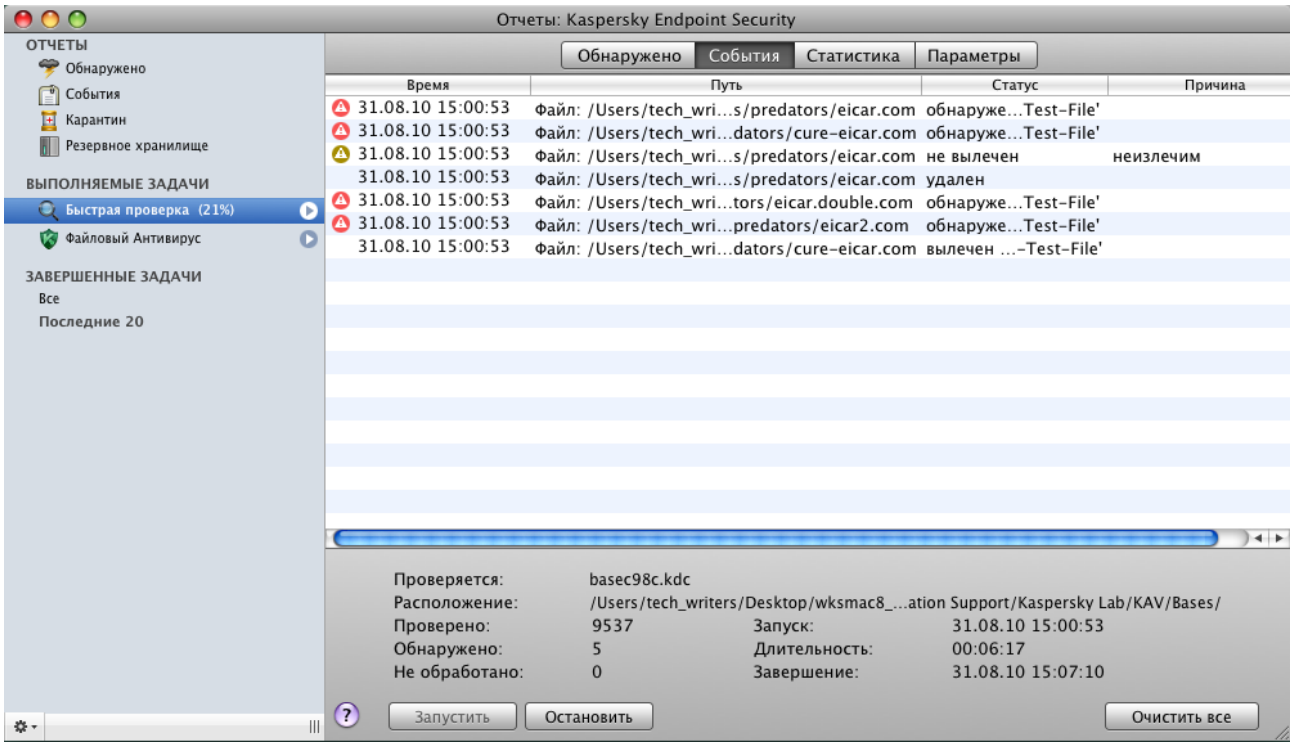


Рисунок 31. Окно отчетов. Поиск вирусов

СОЗДАНИЕ ЗАДАЧ ПОИСКА ВИРУСОВ

Для проверки объектов компьютера на вирусы вы можете использовать не только встроенные в Kaspersky Endpoint Security задачи поиска вирусов, но и создавать собственные задачи. Создание каждой новой задачи происходит на основе уже имеющихся задач.

Чтобы создать новую задачу поиска вирусов, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35).

2. Выберите закладку **Поиск вирусов** и в списке слева (см. рис. ниже) выберите задачу **Быстрая проверка** или **Полная проверка**, параметры которой наиболее приближены к вашим требованиям.

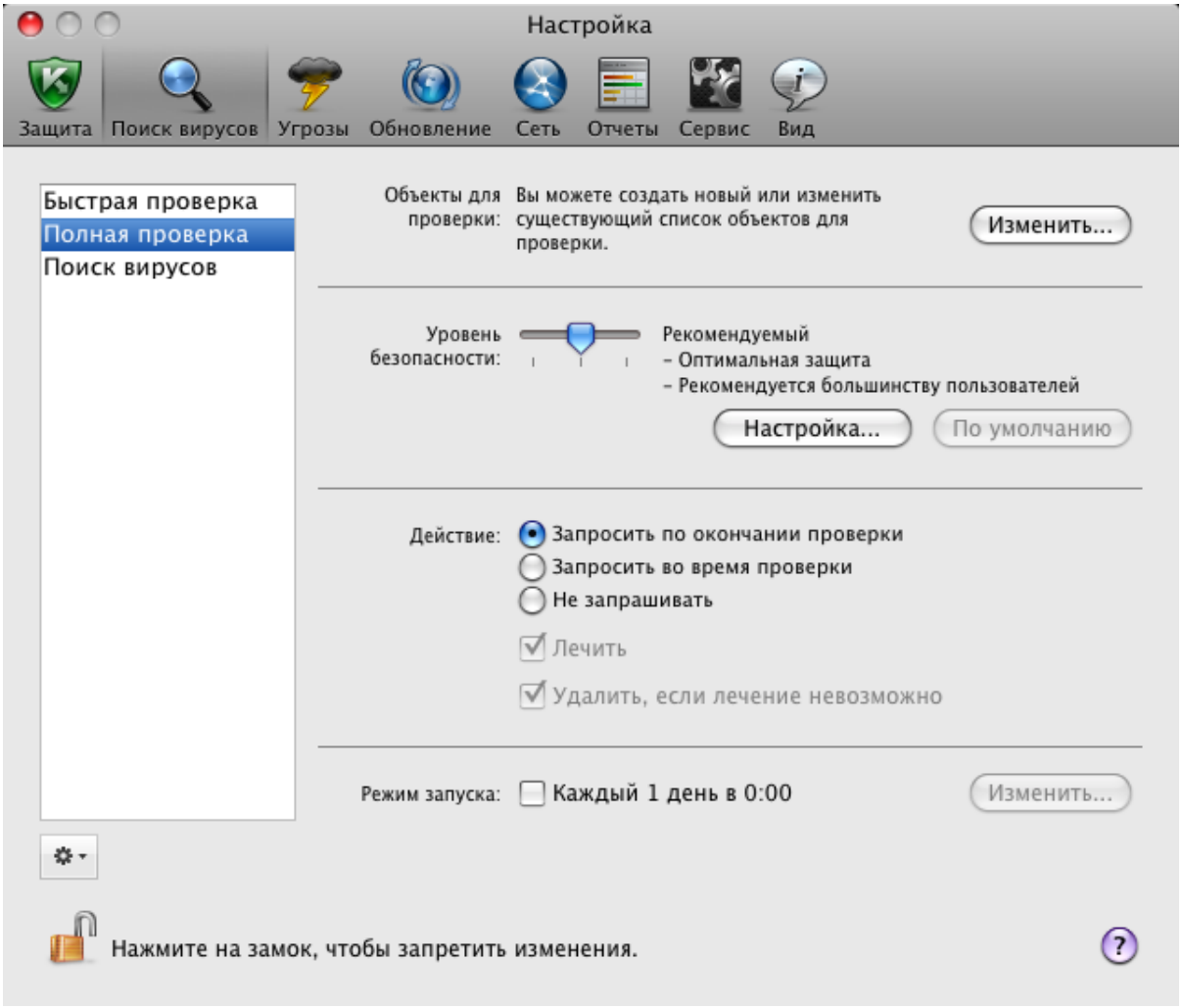


Рисунок 32. Окно настройки программы. Задача Полная проверка

3. Нажмите на кнопку  , расположенную под списком задач поиска вирусов, и в открывшемся меню выберите команду **Копировать**.

4. В открывшемся окне введите имя новой задачи и нажмите на кнопку **ОК**. В результате задача с указанным именем появится в списке задач.

Новая задача наследует все параметры задачи, на основе которой она была создана. Поэтому вам может потребоваться провести дополнительную настройку:

- изменить список объектов проверки (см. раздел «Формирование списка объектов проверки» на стр. 73);
- указать параметры (см. раздел «Настройка задач поиска вирусов» на стр. 75), с которыми будет выполняться задача;
- настроить расписание ее автоматического запуска (см. раздел «Настройка запуска задач поиска вирусов по расписанию» на стр. 79).

В дополнение к встроенным задачам поиска вирусов Kaspersky Endpoint Security позволяет создать не более шести пользовательских задач поиска.

Вы можете переименовывать и удалять задачи поиска.

Переименовать и удалить можно только те задачи поиска вирусов, которые созданы пользователем.

Чтобы переименовать созданную задачу, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35).
2. Выберите задачу в списке слева (см. рис. выше).
3. Нажмите на кнопку  , расположенную под списком задач проверки, и в открывшемся меню выберите команду **Переименовать**.
4. В открывшемся окне измените имя задачи и нажмите на кнопку **ОК**. Задача будет переименована.

Чтобы удалить созданную задачу, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35).
2. Выберите задачу в списке слева (см. рис. выше).
3. Нажмите на кнопку  , расположенную под списком задач проверки, и в открывшемся меню выберите команду **Удалить**. Подтвердите действие в открывшемся окне. Задача будет удалена из списка задач.

ФОРМИРОВАНИЕ СПИСКА ОБЪЕКТОВ ПРОВЕРКИ

Входящие в Kaspersky Endpoint Security задачи **Полная проверка** и **Быстрая проверка** уже имеют сформированные списки объектов для проверки. Задача **Полная проверка** позволяет выполнить проверку всех файлов, расположенных на всех жестких дисках компьютера. Выполняя задачу **Быстрая проверка**, Kaspersky Endpoint Security проверяет только уязвимые с точки зрения безопасности объекты: папки, содержащие файлы операционной системы и системные библиотеки.

Задача **Поиск вирусов** требует формирования списка объектов для проверки (выбора файла, папки, диска, сменного устройства).

*Чтобы ознакомиться со списком объектов для проверки при выполнении задач **Полная проверка** и **Быстрая проверка** или изменить его, выполните следующие действия:*

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Поиск вирусов**.
2. В списке слева выберите имя задачи: **Полная проверка** или **Быстрая проверка**.
3. Справа в блоке **Объекты для проверки** нажмите на кнопку **Изменить**. Откроется окно со списком объектов (см. рис. ниже). Отредактируйте список, если это необходимо.

   Вы можете выполнить следующие действия:

   - Добавить объект в список.

     Перетащите объект в окно или нажмите на кнопку  и выберите из раскрывающегося списка наиболее подходящий вам вариант (**Файл или папка**, **Все диски**, **Карантин** и т.д.). Если добавляемый объект содержит вложенные папки, которые также следует проверить, в открывшемся окне выбора файла установите флажок **Включая вложенные папки**. Если добавляемый объект содержит символические ссылки на другие объекты, требующие проверки, в открывшемся окне выбора файла установите флажок **Переходить по символическим ссылкам**.

- Изменить объект списка (доступно только для объектов, добавленных пользователем).

  Выберите объект и нажмите на кнопку **Изменить**. В открывшемся стандартном окне внесите необходимые изменения.

- Временно отключить проверку объекта списка.

  Выберите объект и снимите флажок рядом с ним. Задача поиска вирусов не будет выполняться для этого объекта до тех пор, пока флажок не будет вновь установлен.

- Удалить объект (доступно только для объектов, добавленных пользователем).

  Выберите объект и нажмите на кнопку  .

При создании пользовательских задач (см. раздел «Создание задач поиска вирусов» на стр. 71) список объектов для проверки формируется или изменяется аналогичным способом.

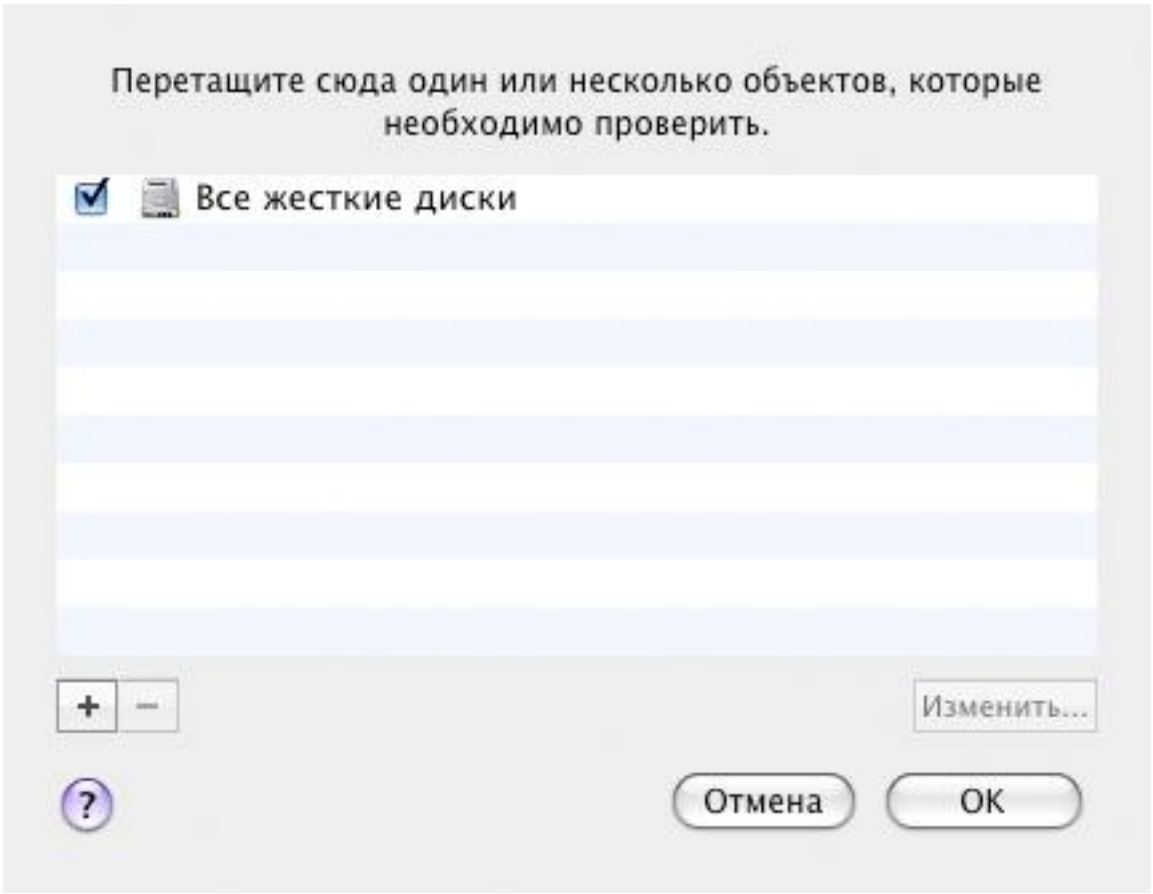


Рисунок 33. Формирование списка объектов проверки

*Чтобы выбрать один или несколько объектов для проверки при выполнении задачи **Поиск вирусов**, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .

2. В открывшемся меню выберите задачу **Поиск вирусов**. Откроется окно для формирования списка объектов (см. рис. выше). Отредактируйте список описанным выше способом.

НАСТРОЙКА ЗАДАЧ ПОИСКА ВИРУСОВ

Выполнение задач поиска вирусов на вашем компьютере определяется следующими параметрами:

- **Уровень безопасности**

  Уровень безопасности – это набор параметров, определяющих соотношение между тщательностью и скоростью проверки объектов на присутствие вирусов. Существует три предустановленных уровня безопасности (см. раздел «Выбор уровня безопасности» на стр. 75) с параметрами, разработанными специалистами «Лаборатории Касперского».

- **Действие над обнаруженным объектом**

  Действие (см. раздел «Выбор действия над объектами» на стр. 77) определяет поведение Kaspersky Endpoint Security при обнаружении зараженного или возможно зараженного объекта.

- **Режим запуска**

  Автоматический запуск задач поиска вирусов по заданному расписанию (см. раздел «Настройка запуска задач поиска вирусов по расписанию» на стр. 79) позволяет своевременно проверять ваш компьютер на вирусы. Доступно только для задач **Быстрая проверка**, **Полная проверка** и пользовательских задач.

- **Запуск задачи от имени пользователя**

  Запуск задачи от имени привилегированного пользователя (см. раздел «Запуск задач проверки от имени пользователя» на стр. 79) обеспечивает своевременность проверки вне зависимости от прав пользователя, работающего на компьютере в текущий момент. Доступно только для задач **Быстрая проверка**, **Полная проверка** и пользовательских задач.

Кроме того, вы можете устанавливать единые значения параметров **Уровень безопасности** и **Действие** над обнаруженным объектом для всех задач поиска вирусов (см. раздел «Назначение единых параметров проверки для всех задач поиска вирусов» на стр. 80).

ВЫБОР УРОВНЯ БЕЗОПАСНОСТИ

Каждая задача поиска вирусов обеспечивает проверку объектов на одном из следующих уровней:

- **Максимальная защита** – уровень, на котором осуществляется самая полная проверка всего компьютера или отдельного его диска, папки, файла. Мы рекомендуем использовать данный уровень, если вы подозреваете, что ваш компьютер заражен вирусом.

- **Рекомендуемый** – уровень, параметры которого рекомендованы экспертами «Лаборатории Касперского».

- **Максимальная скорость** – уровень, параметры которого позволяют вам комфортно работать с программами, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на данном уровне сокращен.

По умолчанию выполнение задач поиска вирусов осуществляется на **Рекомендуемом** уровне безопасности. Вы можете повысить или понизить тщательность проверки объектов, выбрав уровень **Максимальная защита** или **Максимальная скорость** соответственно, или изменив настройки текущего уровня.

Чтобы изменить уровень безопасности задачи поиска вирусов, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Поиск вирусов** (см. рис. ниже).

2. Выберите задачу в списке слева.

3. В блоке **Уровень безопасности** переместите ползунок по шкале. Регулируя уровень безопасности, вы определяете соотношение между скоростью выполнения проверки и количеством проверяемых файлов: чем меньше файлов подвергается анализу на присутствие вирусов, тем выше скорость проверки.

Если ни один из перечисленных уровней безопасности не соответствует вашим требованиям, выполните дополнительную настройку параметров защиты. Для этого рекомендуется выбрать наиболее близкий к вашим пожеланиям уровень безопасности в качестве базового и изменить его настройки. В этом случае название уровня безопасности изменится на **Пользовательский**.

Чтобы изменить параметры текущего уровня безопасности, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Поиск вирусов** (см. рис. ниже).
2. Выберите задачу в списке слева.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне отредактируйте параметры (см. раздел «Определение типов проверяемых объектов» на стр. 76) уровня безопасности и нажмите на кнопку **OK**, чтобы сохранить изменения.

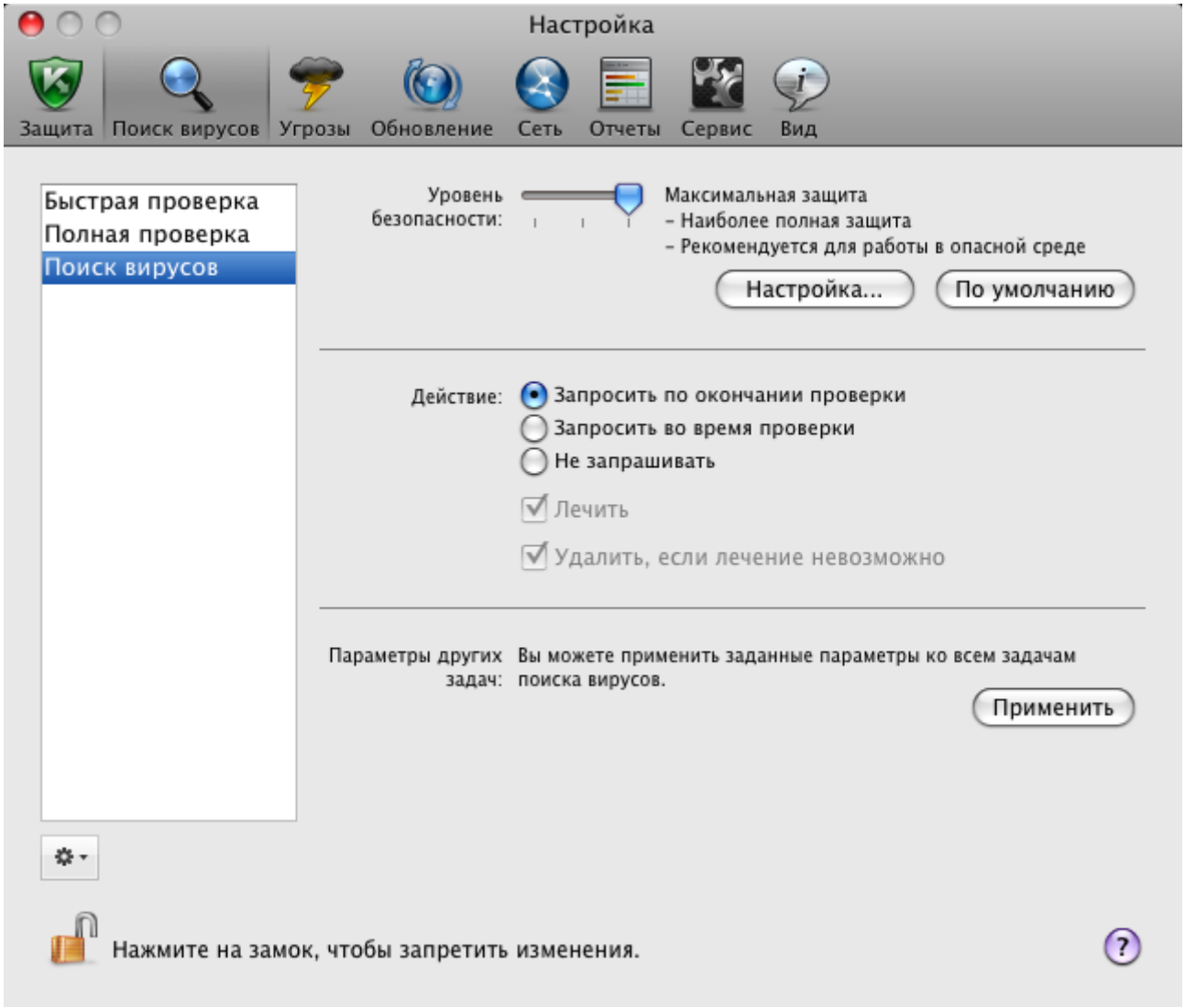


Рисунок 34. Окно настройки программы. Задача Поиск вирусов

Определение типов проверяемых объектов

Указывая тип проверяемых объектов, вы определяете формат и размер файлов, которые будут проверяться Kaspersky Endpoint Security при выполнении данной задачи.

Чтобы указать тип объектов, проверяемых при выполнении задачи поиска вирусов, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Поиск вирусов**.

2. Выберите задачу в списке слева.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**. В открывшемся окне (см. рис. ниже) настройте следующие параметры:

   - В блоке **Типы файлов** укажите формат файлов, которые будут проверяться Kaspersky Endpoint Security при выполнении задач поиска вирусов.
   - В блоке **Оптимизация** настройте производительность проверки и использование технологии проверки.
   - В блоке **Составные файлы** выберите, какие составные файлы необходимо анализировать на присутствие вирусов.
   - В блоке **Эвристический анализатор** настройте использование эвристического анализатора в задачах поиска вирусов.

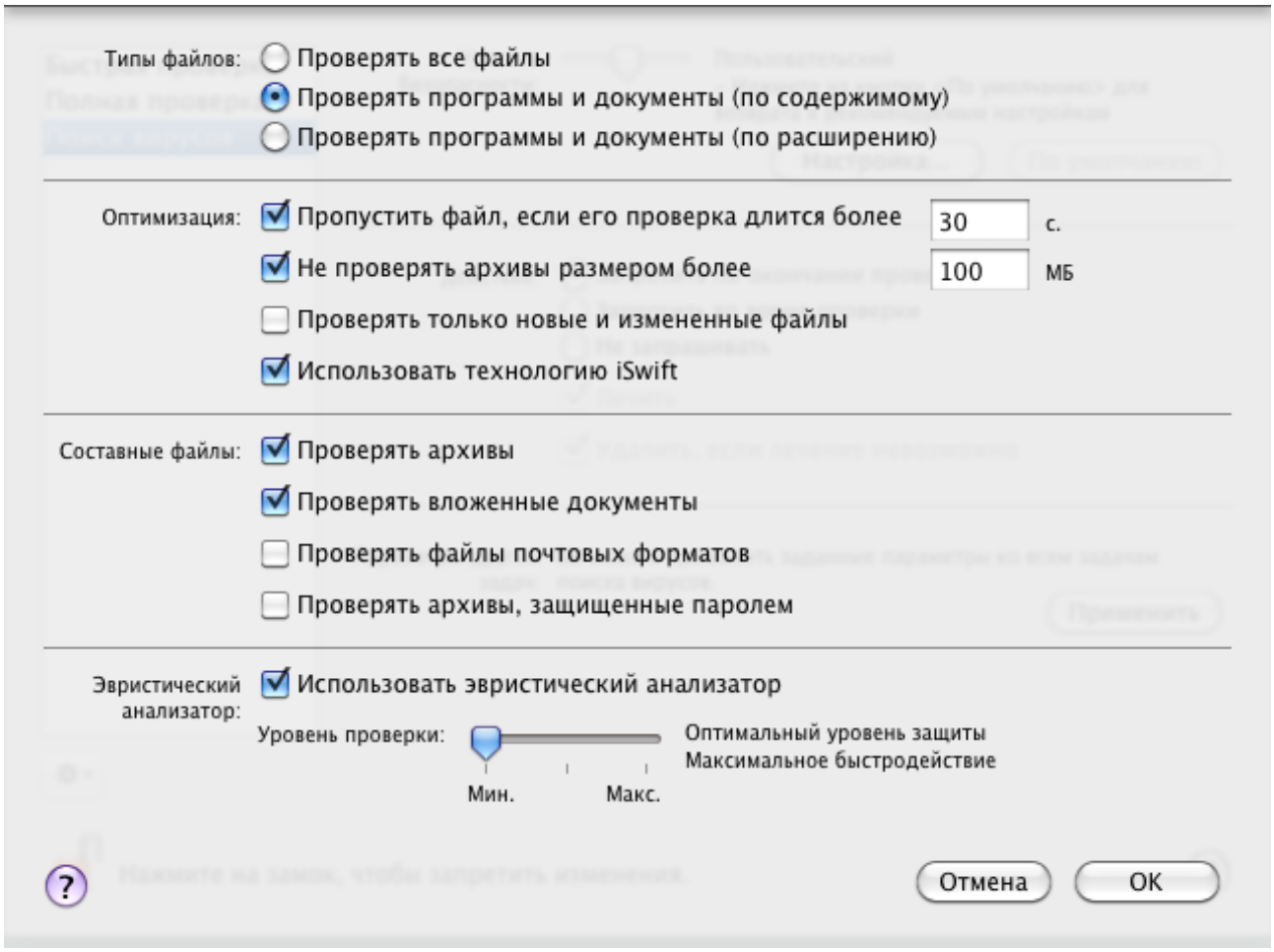


Рисунок 35. Поиск вирусов. Настройка параметров проверки

Выбор действия над объектами

Если в результате выполнения задачи поиска вирусов выясняется, что какой-либо объект заражен или возможно заражен, дальнейшее поведение Kaspersky Endpoint Security зависит от статуса объекта и выбранного действия.

По результатам проверки объект может быть идентифицирован следующим образом:

- как вредоносный, например, *вирус* или *троянская программа*;
- как *возможно зараженный*, когда в результате проверки однозначно невозможно определить, заражен объект или нет. Это означает, что в файле обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

По умолчанию все вредоносные объекты подвергаются лечению, а все возможно зараженные помещаются в хранилище карантина (см. раздел «Карантин» на стр. 94).

Чтобы выбрать действие, которое должен выполнить Kaspersky Endpoint Security при обнаружении зараженного или возможно зараженного объекта, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35), выберите закладку **Поиск вирусов** и имя задачи поиска вирусов в списке задач слева (см. рис. ниже).
2. В блоке **Действие** выберите действие Kaspersky Endpoint Security.

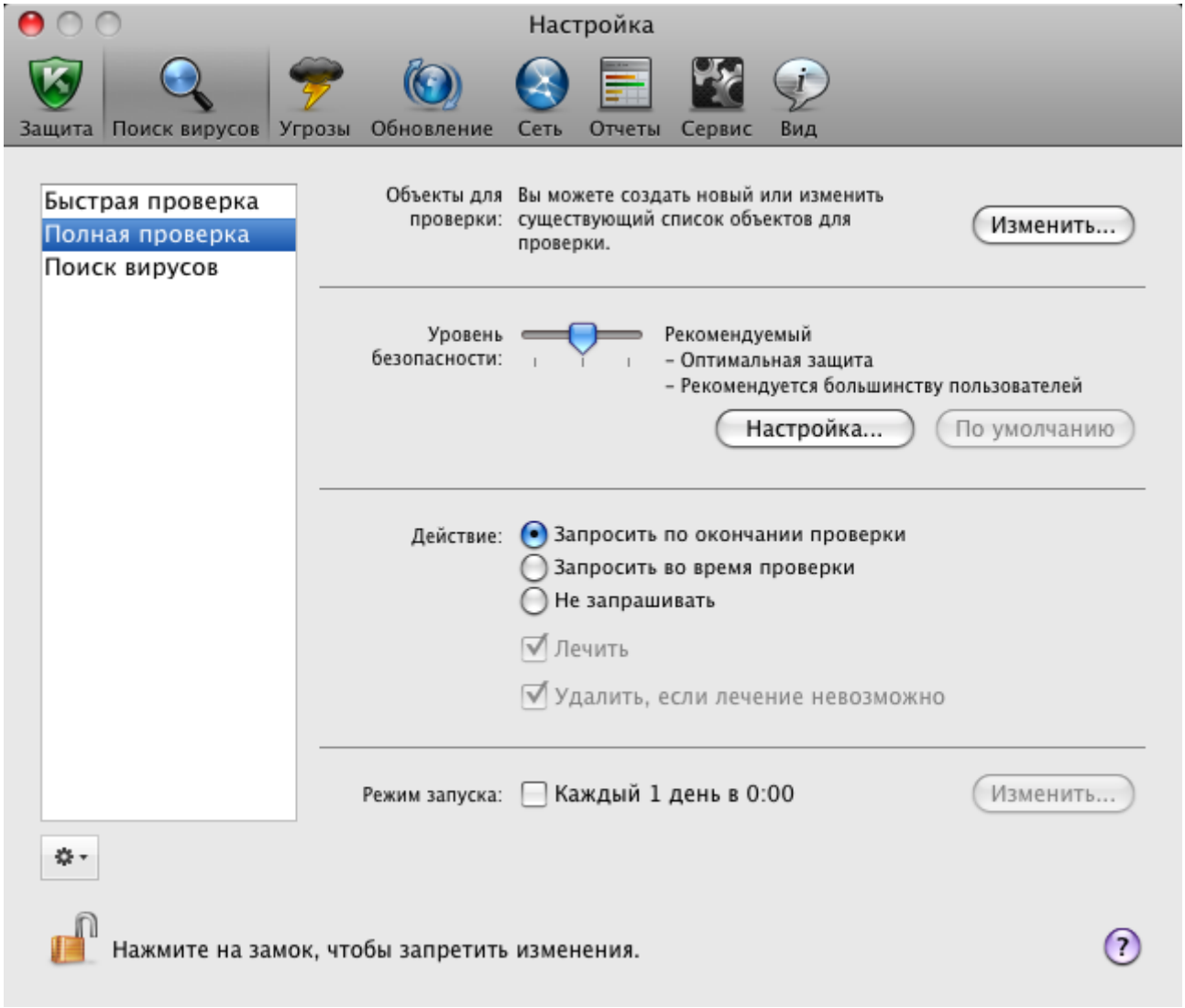


Рисунок 36. Окно настройки программы. Задача Полная проверка

Перед лечением или удалением объекта Kaspersky Endpoint Security создает его резервную копию и помещает ее в резервное хранилище (на стр. 97) на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

НАСТРОЙКА ЗАПУСКА ЗАДАЧ ПОИСКА ВИРУСОВ ПО РАСПИСАНИЮ

Все задачи поиска вирусов на вашем компьютере можно запускать вручную (см. раздел «Запуск / остановка задач поиска вирусов» на стр. 70). Кроме того, задачи **Быстрая проверка** и **Полная проверка** и задачи, созданные пользователем могут запускаться Kaspersky Endpoint Security по заранее сформированному расписанию.

*Чтобы настроить запуск задач **Быстрая проверка** и **Полная проверка**, а также пользовательских задач поиска вирусов по расписанию, выполните следующие действия:*

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Поиск вирусов.**

2. В списке слева выберите имя задачи поиска вирусов, а в блоке **Режим запуска** включите запуск задачи по расписанию. Нажмите на кнопку **Изменить**, чтобы настроить параметры запуска задачи.

3. В открывшемся окне (см. рис. ниже) установите, с какой частотой должна запускаться задача.

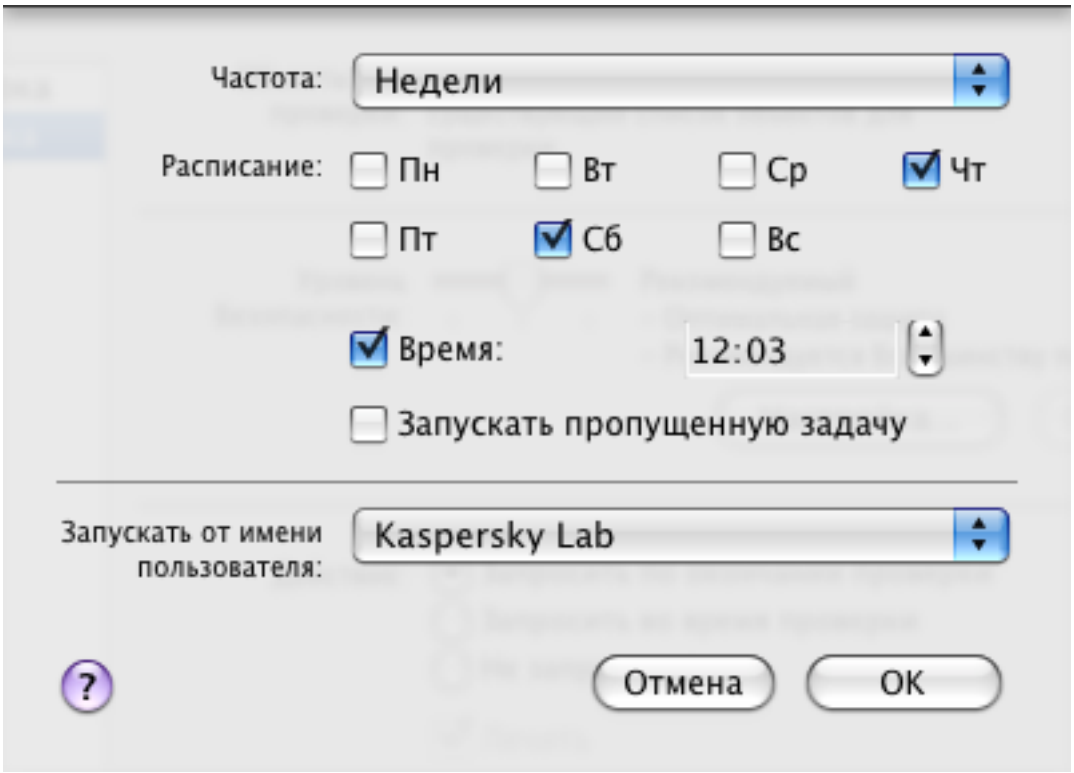


Рисунок 37. Настройка расписания запуска задачи поиска вирусов

ЗАПУСК ЗАДАЧ ПРОВЕРКИ ОТ ИМЕНИ ПОЛЬЗОВАТЕЛЯ

В программе реализована возможность запуска пользователем задач поиска вирусов от имени другой учетной записи. Это обеспечивает своевременность проверки компьютера вне зависимости от прав пользователя, работающего на компьютере в текущий момент. Так, например, во время проверки могут потребоваться права на доступ к проверяемому объекту. Используя данный сервис, вы можете настроить запуск задачи поиска вирусов от имени пользователя, обладающего такими привилегиями.

По умолчанию данный сервис отключен, и задачи запускаются от имени текущей учетной записи, под которой вы авторизованы в операционной системе.

Настроить запуск задач поиска вирусов от имени привилегированного пользователя вы можете только для задач **Быстрая проверка** и **Полная проверка**, а также для пользовательских задач поиска, созданных на их основе.

Чтобы задать учетную запись, от имени которой будут запускаться задачи поиска вирусов, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35), выберите закладку **Поиск вирусов**.

2. В списке слева выберите имя задачи поиска вирусов, а в блоке **Режим запуска** включите запуск задачи по расписанию. Нажмите на кнопку **Изменить**, чтобы настроить запуск задачи от имени пользователя.

3. В открывшемся окне (см. рис. ниже) в блоке **Запускать от имени пользователя** из раскрывающегося списка выберите учетную запись, от имени которой будет запускаться задача.

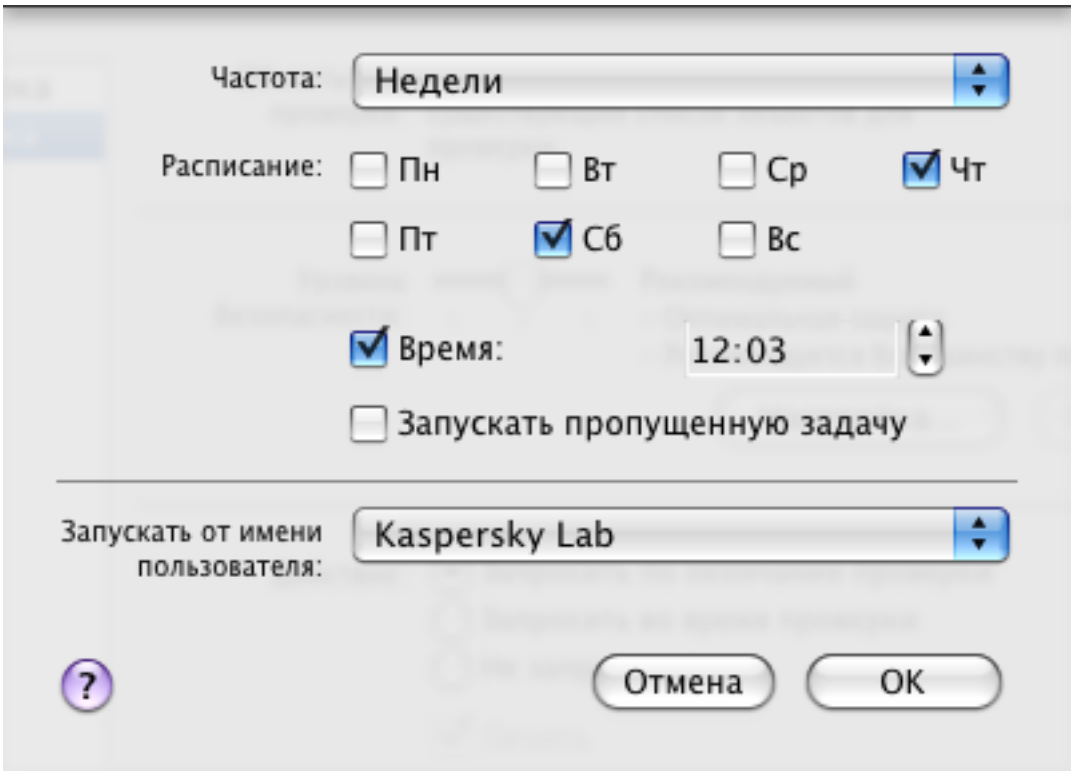


Рисунок 38. Настройка расписания запуска задачи поиска вирусов

Назначение единых параметров проверки для всех задач поиска вирусов

По умолчанию задачи поиска вирусов, входящие в поставку Kaspersky Endpoint Security, выполняются в соответствии с параметрами, рекомендованными экспертами «Лаборатории Касперского». Создаваемые на их основе пользовательские задачи поиска наследуют все установленные параметры. Вы можете не только изменить параметры (см. раздел «Настройка задач поиска вирусов» на стр. 75) каждой задачи поиска вирусов в отдельности, но и назначить единые параметры проверки для всех задач поиска вирусов. За основу будут взяты значения параметров **Уровень безопасности** и **Действие** задачи **Поиск вирусов**, предназначенной для проверки отдельного объекта.

Чтобы назначить единые параметры проверки для всех задач поиска вирусов, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Поиск вирусов**.

2. В списке слева выберите задачу **Поиск вирусов** (см. рис. ниже)**.**

3. Установите уровень безопасности (см. раздел «Выбор уровня безопасности» на стр. 75), наиболее близкий к вашим требованиям, отредактируйте его параметры (см. раздел «Определение типов

проверяемых объектов» на стр. 76) и выберите действие над зараженными или возможно зараженными объектами (см. раздел «Выбор действия над объектами» на стр. 77).

4. В блоке **Параметры других задач** нажмите на кнопку **Применить**. Kaspersky Endpoint Security применит значения параметров **Уровень безопасности** и **Действие** к другим задачам поиска вирусов, включая пользовательские.

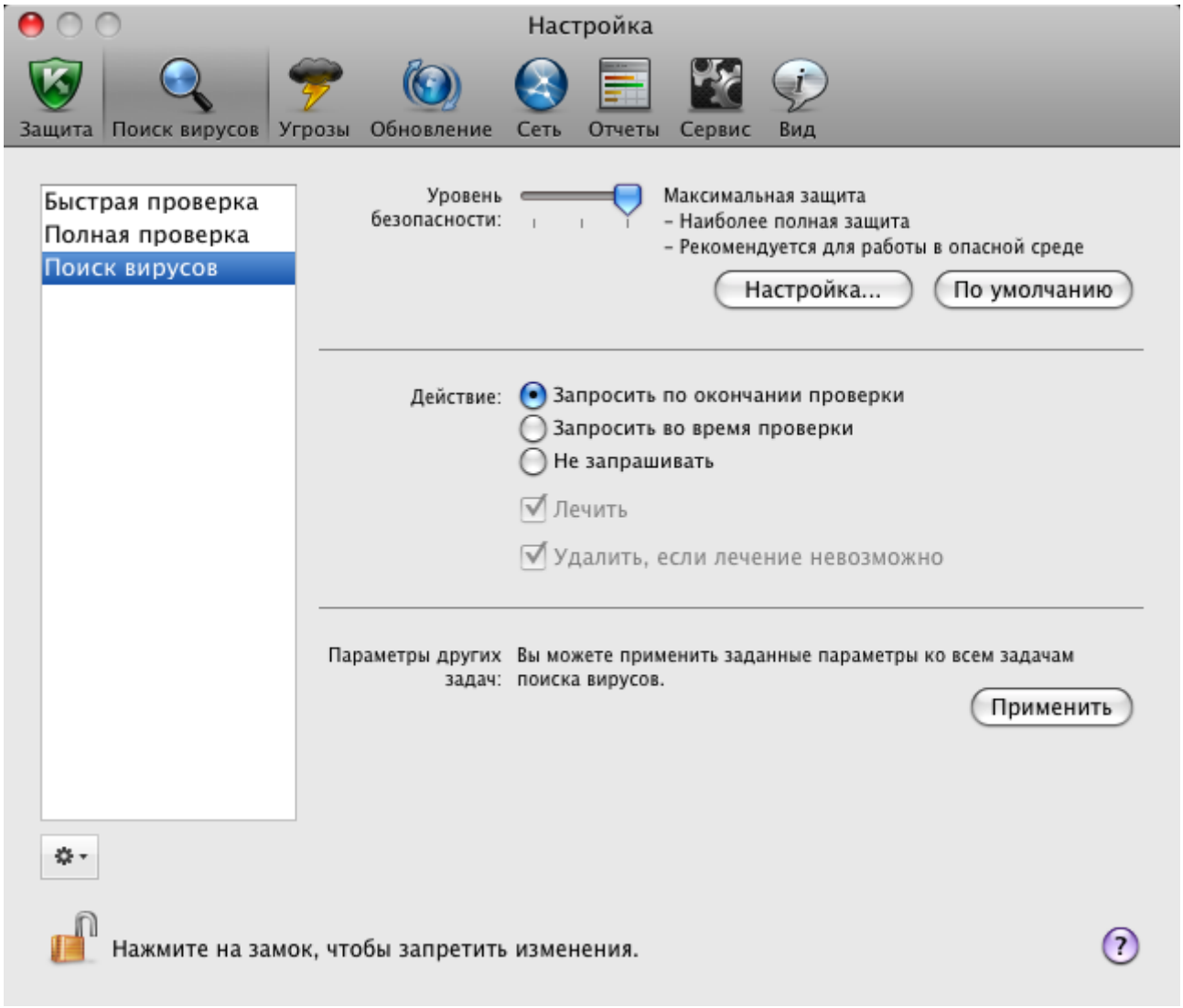


Рисунок 39. Окно настройки программы. Задача Поиск вирусов

ВОССТАНОВЛЕНИЕ ПАРАМЕТРОВ ПРОВЕРКИ ПО УМОЛЧАНИЮ

В любой момент вы можете вернуться к параметрам задач поиска вирусов по умолчанию. Они считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

➧ *Чтобы восстановить параметры проверки объектов на вирусы по умолчанию, выполните следующие действия:*

1. Откройте окно настройки программы (на стр. 35), выберите закладку **Поиск вирусов**, а затем имя нужной задачи в списке слева.

2. В блоке **Уровень безопасности** (см. рис. ниже) нажмите на кнопку **По умолчанию**. Параметры задачи вернутся к рекомендованным значениям.

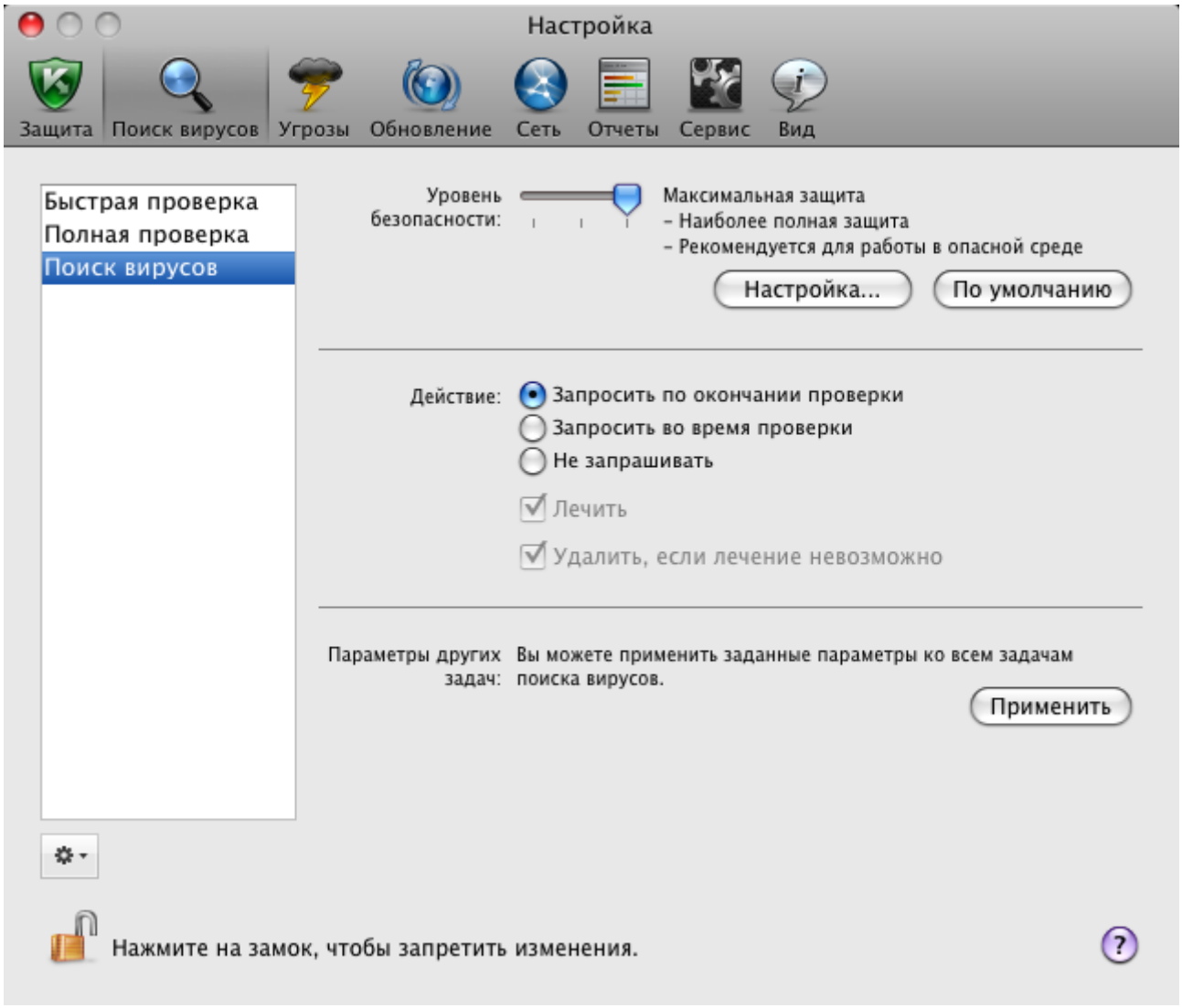


Рисунок 40. Окно настройки программы. Задача Поиск вирусов

СТАТИСТИКА ПОИСКА ВИРУСОВ

Краткая информация о выполнении каждой текущей задачи поиска вирусов (в процентах) представлена в главном окне программы (см. раздел «Главное окно программы» на стр. 34).

Также Kaspersky Endpoint Security предоставляет подробный отчет о выполнении задач поиска вирусов.

Чтобы просмотреть отчет о выполнении текущей задачи, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .

2. В разделе **Выполняемые задачи** открывшегося окна отчетов выберите имя нужной задачи.

Если задача поиска вирусов уже завершена, то сведения о результатах ее выполнения представлены в разделе **Завершенные задачи**.

В нижней части окна отчетов приводится информация о ходе выполнения текущей задачи или сводная статистика с результатами завершенной задачи поиска вирусов. Статистика включает в себя информацию о количестве проверенных объектов, о количестве обнаруженных вредоносных объектов и объектов, требующих обработки. Кроме того, приведены время начала проверки, ожидаемого завершения проверки и ее длительность.

Если в результате выполнения задачи возникли какие-то ошибки, запустите ее еще раз. Если повторная попытка выполнения проверки будет также завершена с ошибкой, обратитесь в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 156).

Подробная информация о выполнении задач поиска вирусов представлена в окне отчетов справа на следующих закладках:

- На закладке **Обнаружено** перечислены все опасные объекты, обнаруженные в процессе выполнения задачи. Для каждого объекта указано имя и путь к папке, в которой он хранится, а также статус, присвоенный этому объекту Kaspersky Endpoint Security. Если удалось точно установить, какой вредоносной программой поражен объект, ему присваивается статус *вирус*, *троянская программа* и т.д. Если тип вредоносного воздействия точно установить не удалось, объекту присваивается статус *возможно зараженный*. Рядом со статусом также указывается действие, выполненное над объектом (*обнаружен*, *вылечен*).

- На закладке **События** ведется полный список событий, возникших в ходе выполнения задачи поиска вирусов с указанием времени наступления события, его имени, статуса и причины возникновения. Событиям могут быть присвоены следующие статусы:

  - информационное событие (например: *объект не обработан: пропущен по типу*);

  - внимание (например: *обнаружен вирус*);

  - примечание (например: *архив защищен паролем*).

- На закладке **Статистика** приводится информация об общем количестве проверенных объектов, а в отдельных графах отражено, сколько объектов из общего числа проверенных являются архивами, сколько из них опасных объектов, сколько вылеченных, сколько помещенных на карантин и т.д.

- На закладке **Параметры** перечислены основные параметры, в соответствии с которыми выполняется задача поиска вирусов. Чтобы быстро перейти к настройке параметров поиска, нажмите на кнопку **Изменить параметры**.

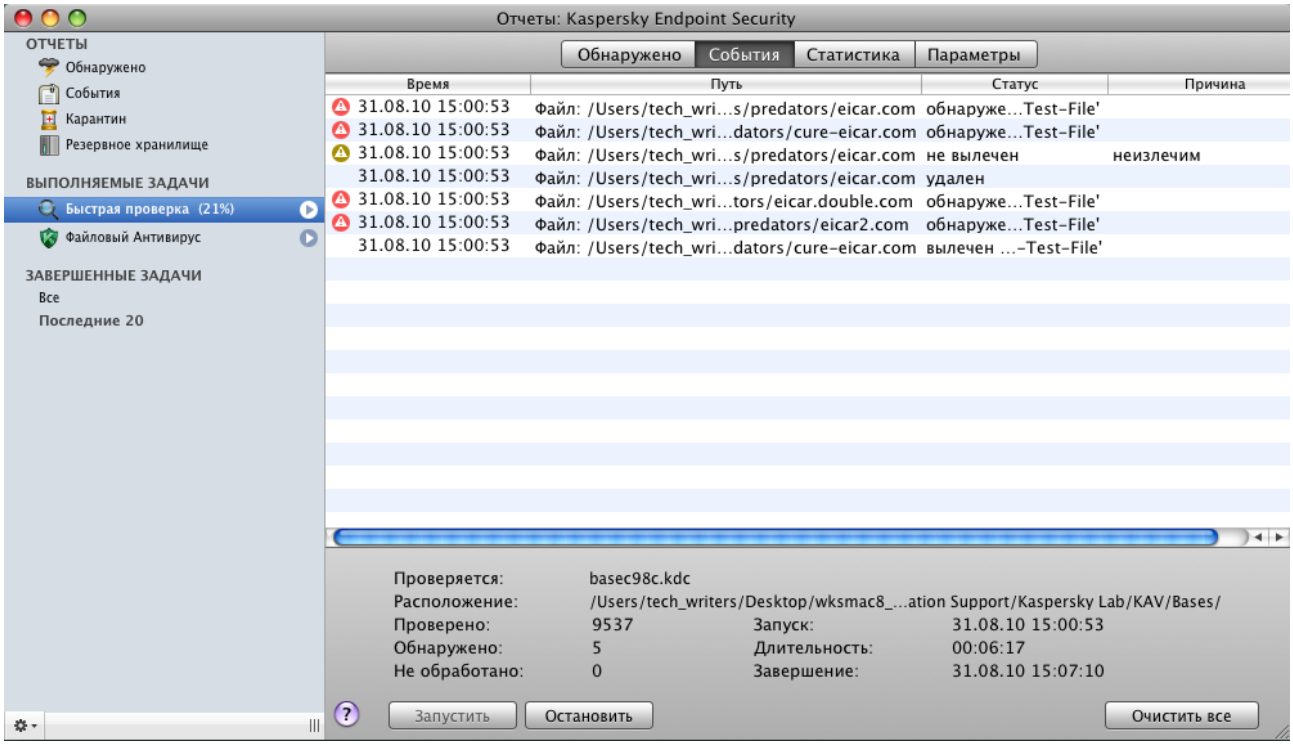


Рисунок 41. Окно отчетов. Поиск вирусов

Обновление программы

Поддержание антивирусных баз в актуальном состоянии – залог безопасности вашего компьютера. Каждый день в мире появляются новые вирусы, троянские и другие вредоносные программы, поэтому крайне важно быть уверенным в том, что ваша информация находится под надежной защитой.

Обновление Kaspersky Endpoint Security подразумевает загрузку и установку на ваш компьютер:

- **Антивирусных баз программы**

  Защита данных на компьютере обеспечивается с помощью антивирусных баз. Файловый Антивирус (на стр. 57) и задачи поиска вирусов (см. раздел «Поиск вирусов» на стр. 69) используют их для поиска и обезвреживания вредоносных объектов на вашем компьютере. Антивирусные базы ежечасно пополняются записями о новых угрозах и способах борьбы с ними, поэтому настоятельно рекомендуется их регулярно обновлять.

- **Модулей программы**

  Помимо баз вы можете обновлять и внутренние модули Kaspersky Endpoint Security. «Лаборатория Касперского» периодически выпускает пакеты обновлений.

Основными источниками обновлений Kaspersky Endpoint Security являются специальные серверы обновлений «Лаборатории Касперского» и Сервер администрирования Kaspersky Administration Kit.

Для успешной загрузки обновлений с серверов требуется подключение компьютера к интернету. Если выход в интернет осуществляется через прокси-сервер, произведите настройку параметров сети (см. раздел «Настройка параметров подключения к прокси-серверу» на стр. 92).

Если вам недоступны серверы обновлений «Лаборатории Касперского» (например, нет доступа к интернету), обратитесь в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу

технической поддержки» на стр. 156) для получения обновлений Kaspersky Endpoint Security на дисках в ZIP-формате.

Загрузка обновлений выполняется в одном из следующих режимов:

- *Автоматически*. Kaspersky Endpoint Security периодически проверяет наличие пакета обновлений в источнике обновлений. Частота проверки может увеличиваться во время вирусных эпидемий и уменьшаться при их отсутствии. Обнаружив свежие обновления, Kaspersky Endpoint Security скачивает их в фоновом режиме и устанавливает на компьютер. Такой режим используется по умолчанию.

- *По расписанию*. Обновление Kaspersky Endpoint Security производится автоматически в соответствии с установленным расписанием.

- *Вручную*. В этом случае вы самостоятельно запускаете обновление Kaspersky Endpoint Security.

Во время обновления модули программы и антивирусные базы на вашем компьютере сравниваются с доступными в данный момент в источнике обновлений. Если на вашем компьютере установлена последняя версия баз и модулей, в нижней части главного окна программы (см. раздел «Главное окно программы» на стр. 34) появится запись о том, что антивирусные базы находятся в актуальном состоянии. Если базы и модули отличаются от доступных в данный момент в источнике обновлений, на ваш компьютер будет установлена только недостающая часть обновлений. Базы и модули не копируются полностью, что позволяет увеличить скорость обновления и снизить объем сетевого трафика.

Перед обновлением баз и модулей Kaspersky Endpoint Security создает их резервную копию на тот случай, если возникнет необходимость вернуться к использованию предыдущей версии. Возможность отката (см. раздел «Откат последнего обновления» на стр. 86) полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

При повреждении баз Kaspersky Endpoint Security рекомендуется запустить задачу обновления, чтобы загрузить действительный набор баз для актуальной защиты.

Одновременно с обновлением Kaspersky Endpoint Security можно скопировать полученные обновления в локальный источник (см. раздел «Обновление из локального источника» на стр. 87). Данный сервис позволяет локально обновлять антивирусные базы Kaspersky Endpoint Security и модули, используемые программой, на других компьютерах для уменьшения интернет-трафика.

В ЭТОМ РАЗДЕЛЕ

ЗАПУСК ОБНОВЛЕНИЯ

Своевременное обновление Kaspersky Endpoint Security позволяет поддерживать защиту компьютера на должном уровне. Если обновление антивирусных баз и модулей программы не производится, информация на вашем компьютере подвергается серьезной опасности.

В нижней части главного окна программы (см. раздел «Главное окно программы» на стр. 34) представлена следующая информация об обновлении Kaspersky Endpoint Security: дата выпуска антивирусных баз, количество записей, которое содержат базы, установленные на вашем компьютере, а также данные об актуальности используемых баз. Число записей в базах отражает количество известных в настоящее время угроз, от которых защищен компьютер.

Во время работы с Kaspersky Endpoint Security в любой момент вы можете запустить обновление программы. Для этого в главном окне нажмите на кнопку . Подробная информация о выполнении этой задачи представлена в окне отчетов (см. раздел «Отчеты» на стр. 99).

Одновременно с получением обновлений с серверов «Лаборатории Касперского» или с Сервера администрирования Kaspersky Administration Kit будет произведено их копирование в локальный источник (см. раздел «Обновление из локального источника» на стр. 87), при условии, что данный сервис включен.

Откат последнего обновления

Каждый раз, когда вы запускаете обновление, Kaspersky Endpoint Security сначала создает резервную копию используемых антивирусных баз и модулей программы и только потом приступает к их обновлению. Такой порядок работы позволяет вам при необходимости вернуться к использованию предыдущей версии баз. Возможность отката обновления полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

При повреждении баз Kaspersky Endpoint Security рекомендуется запустить задачу обновления, чтобы загрузить действительный набор баз для актуальной защиты.

Чтобы вернуться к использованию предыдущей версии антивирусных баз, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Обновление** (см. рис. ниже).
2. В блоке **Откат обновления** нажмите на кнопку **Откат обновления**.

С результатами выполнения отката обновления можно ознакомиться в окне отчетов (см. раздел «Статистика обновления» на стр. 92).

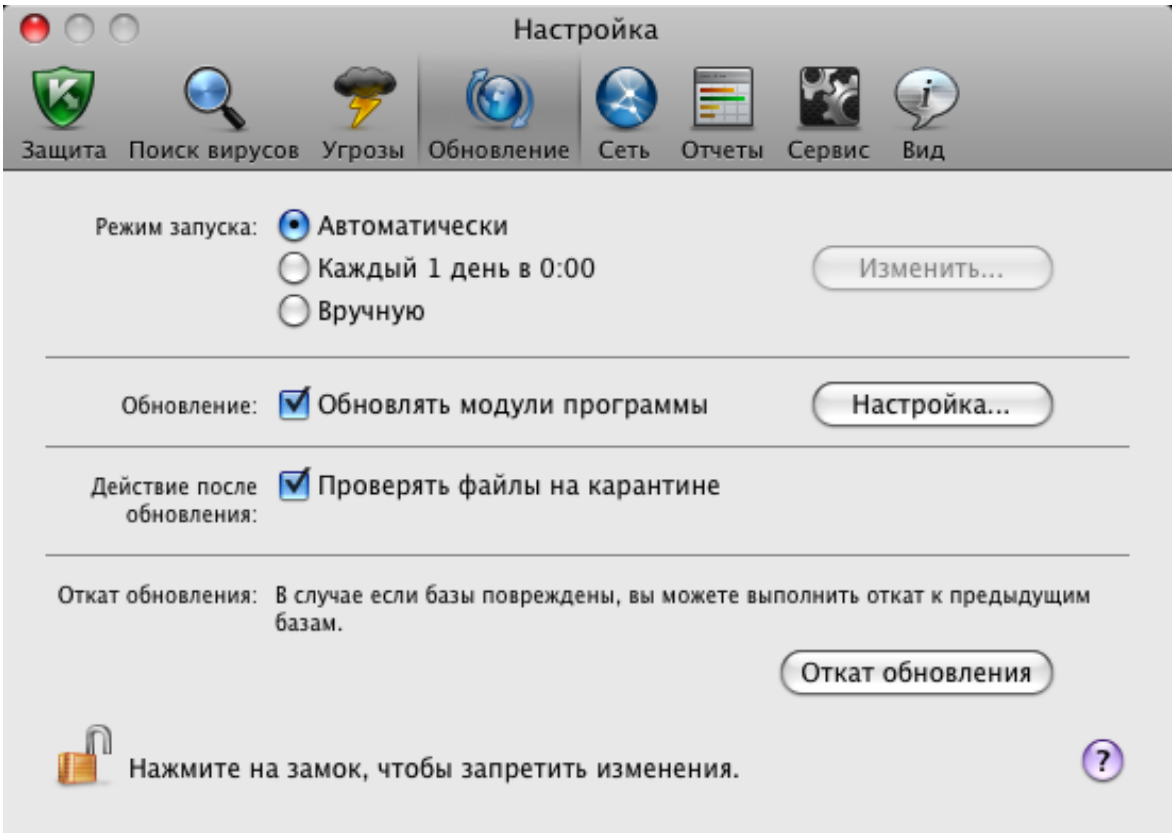


Рисунок 42. Окно настройки программы. Обновление

ОБНОВЛЕНИЕ ИЗ ЛОКАЛЬНОГО ИСТОЧНИКА

Если несколько компьютеров объединены в локальную сеть, нет необходимости получать обновления Kaspersky Endpoint Security на каждый из них отдельно, поскольку в этом случае значительно возрастает сетевой трафик. Вы можете использовать сервис копирования полученных обновлений, что позволит локально обновлять антивирусные базы Kaspersky Endpoint Security и модули, используемые программой, на других компьютерах, уменьшая тем самым интернет-трафик. Процедура получения обновлений будет организована следующим образом:

1. Один из компьютеров сети получает пакет обновлений Kaspersky Endpoint Security с серверов обновления «Лаборатории Касперского» в интернете, либо с Сервера администрирования Kaspersky Administration Kit, либо с другого веб-ресурса, содержащего актуальный набор обновлений программы. Полученные обновления сохраняются в папку общего доступа.

   Папка общего доступа должна быть создана заранее.

2. Другие компьютеры сети для получения обновлений обращаются к папке общего доступа, как к источнику обновлений.

Чтобы включить сервис копирования обновлений в локальный источник, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Обновление** (см. рис. ниже).

2. В блоке **Обновление** нажмите на кнопку **Настройка**.

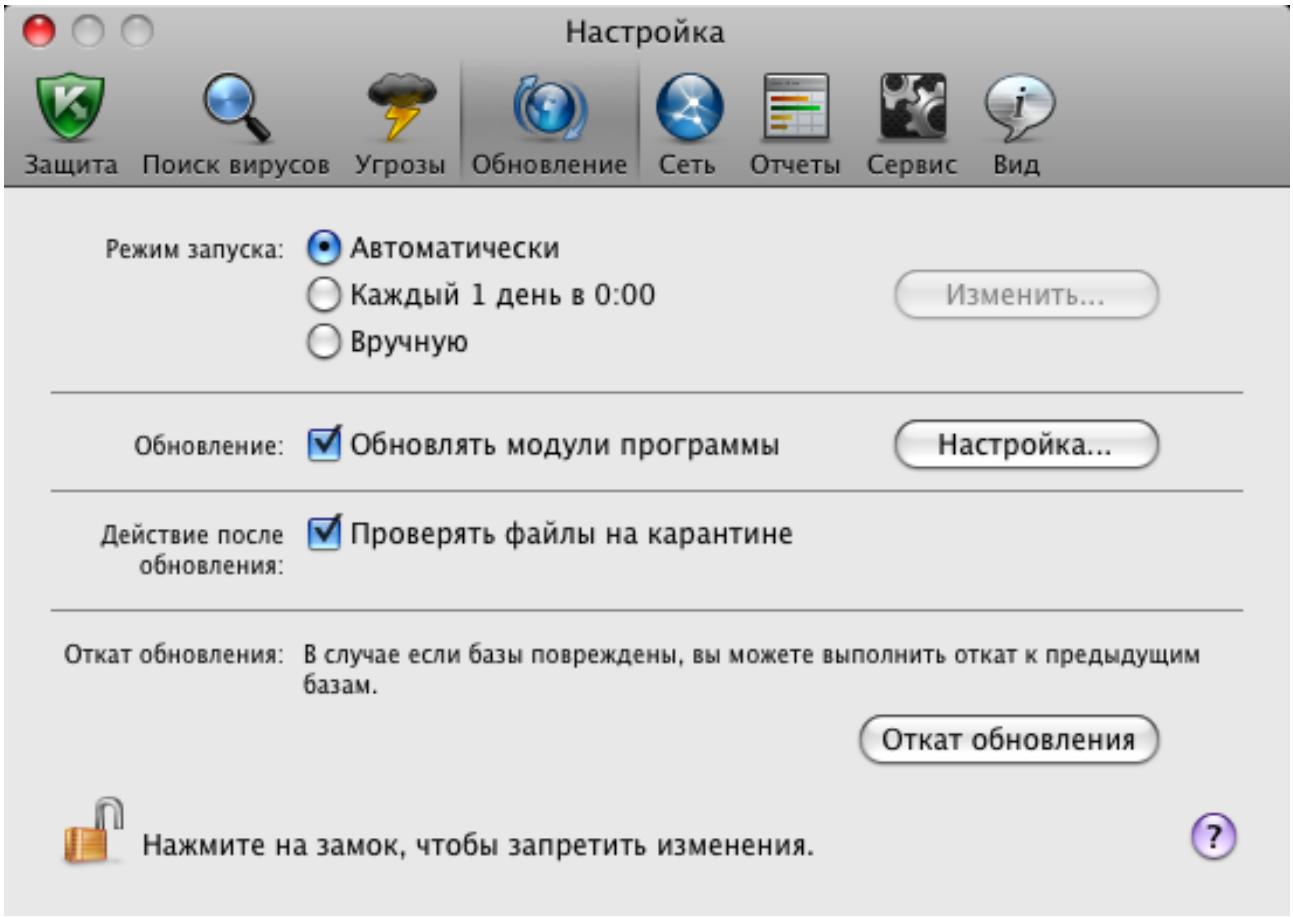


Рисунок 43. Окно настройки программы. Обновление

3. В открывшемся окне выберите закладку **Дополнительно** (см. рис. ниже). Установите флажок **Копировать в папку**, нажмите на кнопку **Выбрать**.

4. В открывшемся стандартном окне выберите папку общего доступа, в которую будут сохраняться получаемые обновления.

Kaspersky Endpoint Security получает с серверов «Лаборатории Касперского» или с Сервера администрирования Kaspersky Administration Kit только собственный пакет обновлений.

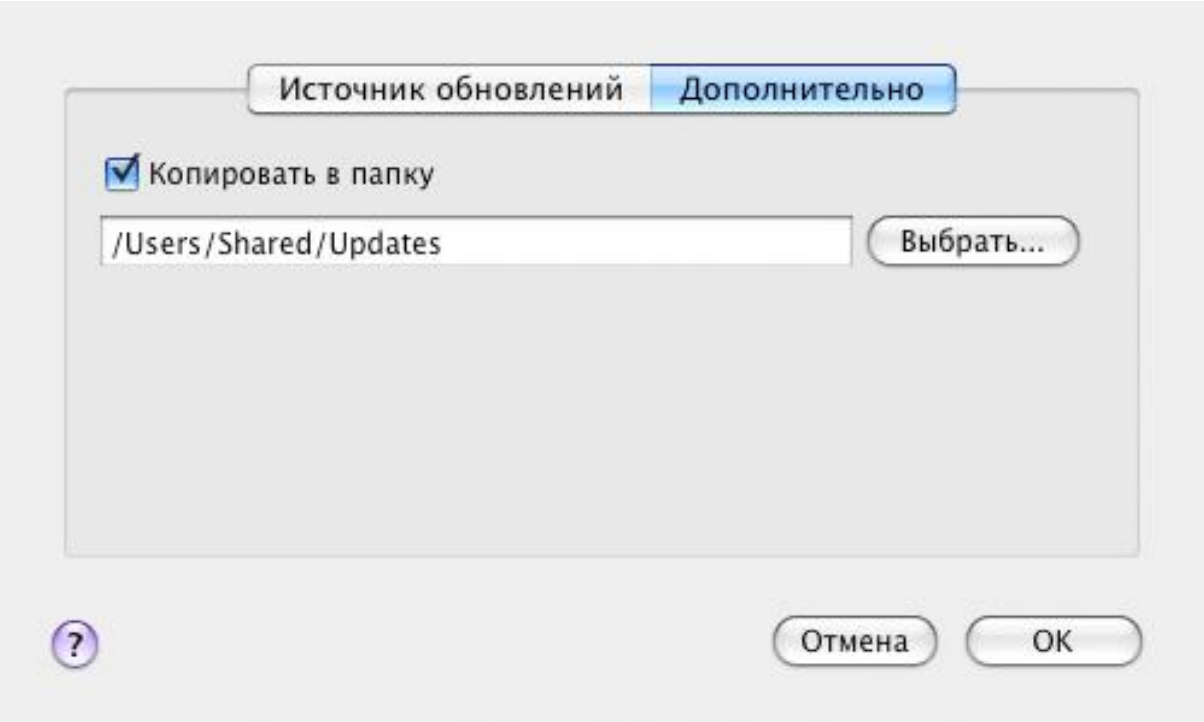


Рисунок 44. Настройка сервиса копирования обновлений

НАСТРОЙКА ОБНОВЛЕНИЯ

Обновление Kaspersky Endpoint Security выполняется в соответствии со следующими параметрами:

- **Режим запуска**

  Выбор режима запуска обновления определяет, каким образом будет производиться запуск обновления: автоматически (рекомендуется специалистами «Лаборатории Касперского»), вручную или по расписанию. При выборе последнего варианта требуется сформировать расписание запуска задачи обновления (см. раздел «Настройка запуска задач обновления по расписанию» на стр. 91).

- **Предмет обновления**

  Предмет обновления определяет, что именно будет обновляться: только антивирусные базы или базы и модули программы. Базы Kaspersky Endpoint Security обновляются всегда, а модули – только в том случае, если установлен соответствующий флажок (см. раздел «Выбор режима и предмета обновления» на стр. 89).

- **Источник обновлений**

  Источник обновлений – это ресурс, содержащий актуальные файлы антивирусных баз и модулей Kaspersky Endpoint Security. Источником обновлений могут быть HTTP- или FTP-серверы, локальные или сетевые папки.

- **Параметры сети**

  Для успешной загрузки обновлений с серверов обновлений «Лаборатории Касперского» или других источников обновлений, кроме локальных или сетевых папок, требуется подключение компьютера к интернету. Если выход в интернет осуществляется через прокси-сервер, требуется настроить параметры сети (см. раздел «Настройка параметров подключения к прокси-серверу» на стр. 92).

ВЫБОР РЕЖИМА И ПРЕДМЕТА ОБНОВЛЕНИЯ

Настраивая параметры обновления Kaspersky Endpoint Security, важно определить предмет и режим запуска обновления.

Чтобы выбрать режим запуска обновления, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Обновление** (см. рис. ниже).
2. В блоке **Режим запуска** выберите режим запуска задачи обновления.

Чтобы в процессе обновления программы на компьютер копировались и устанавливались не только антивирусные базы, но и модули программы, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35), выберите закладку **Обновление** (см. рис. ниже).
2. В блоке **Обновление** установите флажок **Обновлять модули программы**.

Если в ходе выполнения задачи обновления в источнике обновлений будут доступны и обновления модулей программы, Kaspersky Endpoint Security получит их и применит после перезагрузки компьютера. До перезагрузки полученные обновления модулей установлены не будут. Если следующее обновление программы станет доступно до перезагрузки компьютера и до установки обновлений модулей программы, полученных ранее, то будет произведено только обновление антивирусных баз.

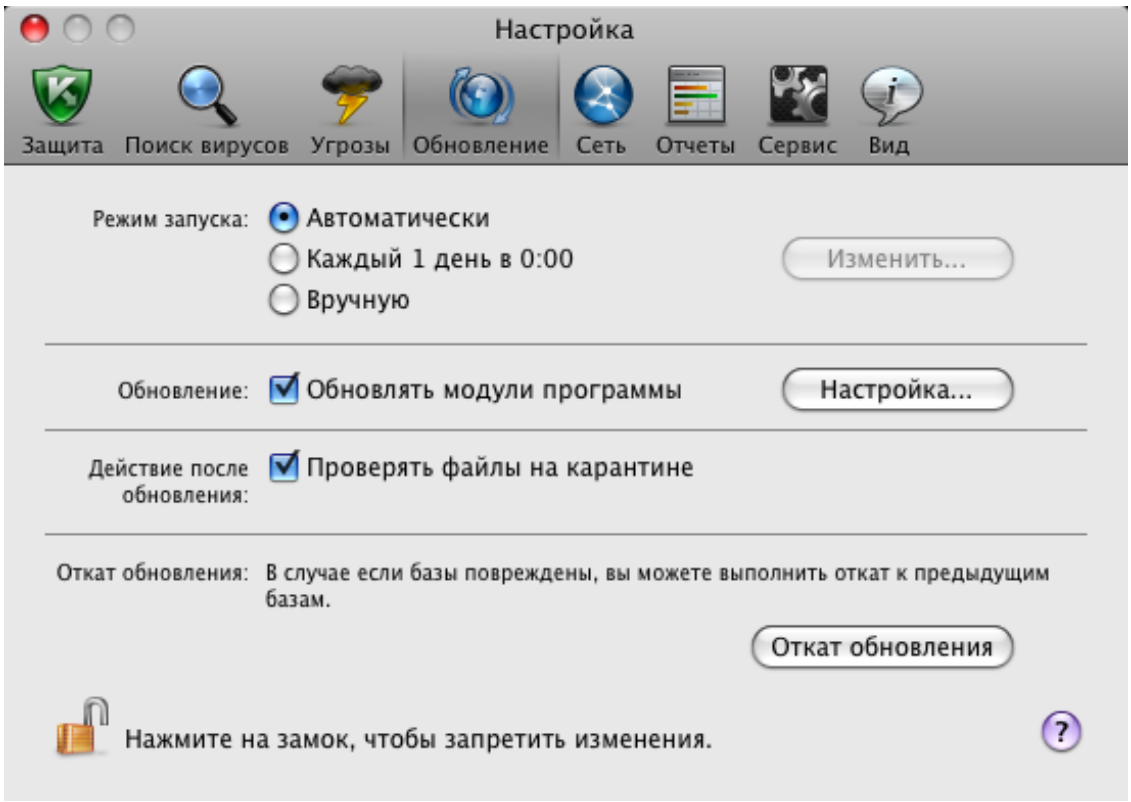


Рисунок 45. Окно настройки программы. Обновление

ВЫБОР ИСТОЧНИКА ОБНОВЛЕНИЙ

Источник обновлений – это ресурс, содержащий обновления антивирусных баз и внутренних модулей Kaspersky Endpoint Security. Источником обновления могут быть HTTP- или FTP-серверы, локальные или сетевые папки.

Основным источником для обновления программы являются серверы обновлений «Лаборатории Касперского». Это специальные интернет-сайты, на которые выкладываются обновления антивирусных баз и внутренних модулей для всех продуктов «Лаборатории Касперского». Сервер администрирования Kaspersky Administration Kit также является источником обновления Kaspersky Endpoint Security.

Если серверы обновлений «Лаборатории Касперского» вам недоступны (например, из-за отсутствия доступа в интернет), обратитесь в Службу технической поддержки «Лаборатории Касперского» для получения обновлений в ZIP-формате. Полученные обновления вы можете разместить как на некотором FTP-, HTTP-сайте, так и в локальной или сетевой папке.

При заказе обновлений на съемных дисках обязательно уточняйте, хотите ли вы получить обновления внутренних модулей Kaspersky Endpoint Security.

Чтобы выбрать источник обновлений Kaspersky Endpoint Security, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Обновление**.
2. В блоке **Обновление** нажмите на кнопку **Настройка**.
3. В открывшемся окне выберите закладку **Источник обновлений** (см. рис. ниже). Отредактируйте список источников обновлений, если это необходимо.

   По умолчанию список источников обновлений содержит только серверы обновлений «Лаборатории Касперского»и Сервер администрирования Kaspersky Administration Kit. Выполняя обновление, Kaspersky Endpoint Security обращается к данному списку, выбирает первый по порядку адрес сервера и пытается загрузить обновления с него. Если выполнить обновление с выбранного адреса невозможно, программа обращается к следующему по списку серверу и вновь пытается получить обновления. Перебор проводится до тех пор, пока процесс соединения не завершится успешно, или пока не будут опрошены все доступные источники обновлений. В следующий раз для получения обновлений программа будет обращаться в первую очередь к тому серверу, с которого обновления были успешно получены в предыдущий раз.

   Вы можете выполнить следующие действия:

   - Добавить новый источник обновлений в список.

     Нажмите на кнопку  и выберите из раскрывающегося списка наиболее подходящий вам вариант (**Путь** – для локальной или сетевой папки или **URL** – для HTTP- или FTP-сервера). В открывшемся окне укажите местоположение нового источника обновлений.

   - Изменить источник обновлений.

     Выберите источник обновлений в списке и нажмите на кнопку **Изменить**. В открывшемся окне внесите необходимые изменения.

     Обратите внимание, что серверы обновлений «Лаборатории Касперского» и Сервер администрирования Kaspersky Administration Kit являются источниками обновлений, недоступными для редактирования и удаления.

   - Временно отключить получение обновлений из источника.

     Выберите источник обновлений в списке и снимите флажок рядом с ним. Обновление Kaspersky Endpoint Security с этого источника не будет выполняться до тех пор, пока флажок не будет вновь установлен.

- Удалить источник обновлений.

  Выберите источник обновлений в списке и нажмите на кнопку [−].

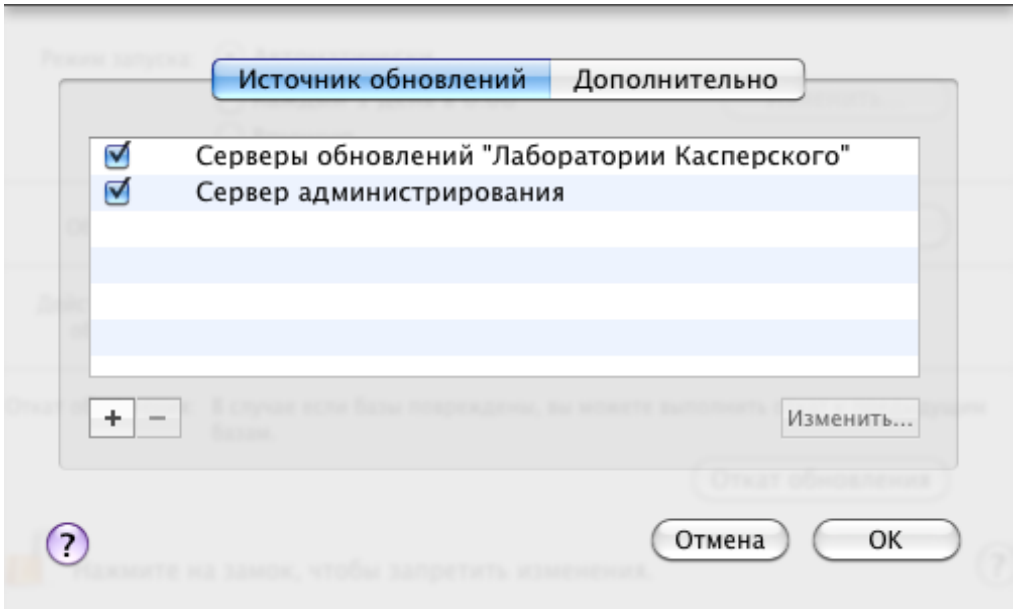


Рисунок 46. Выбор источника обновлений

НАСТРОЙКА ЗАПУСКА ЗАДАЧ ОБНОВЛЕНИЯ ПО РАСПИСАНИЮ

По умолчанию обновление Kaspersky Endpoint Security выполняется автоматически. Вы можете выбрать другой режим запуска задачи обновления: вручную или по установленному расписанию.

Чтобы настроить запуск задачи обновления Kaspersky Endpoint Security по расписанию, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Обновление**.
2. В блоке **Режим запуска** выберите вариант запуска обновления по расписанию и нажмите на кнопку **Изменить**.
3. В открывшемся окне (см. рис. ниже) установите частоту, с которой должно запускаться обновление программы.

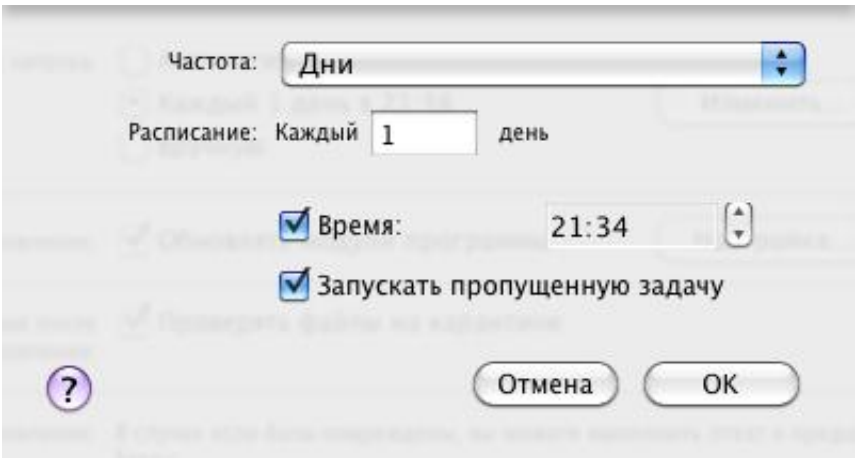


Рисунок 47. Настройка расписания запуска задачи обновления

Настройка параметров подключения к прокси-серверу

Если выход в интернет с компьютера осуществляется через прокси-сервер, настройте параметры подключения к нему. Kaspersky Endpoint Security использует данные параметры для обновления антивирусных баз и модулей.

Чтобы настроить параметры подключения к прокси-серверу, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Сеть** (см. рис. ниже).
2. В блоке **Основные** установите флажок **Использовать прокси-сервер**.
3. В блоке **Прокси-сервер** настройте параметры прокси-сервера.

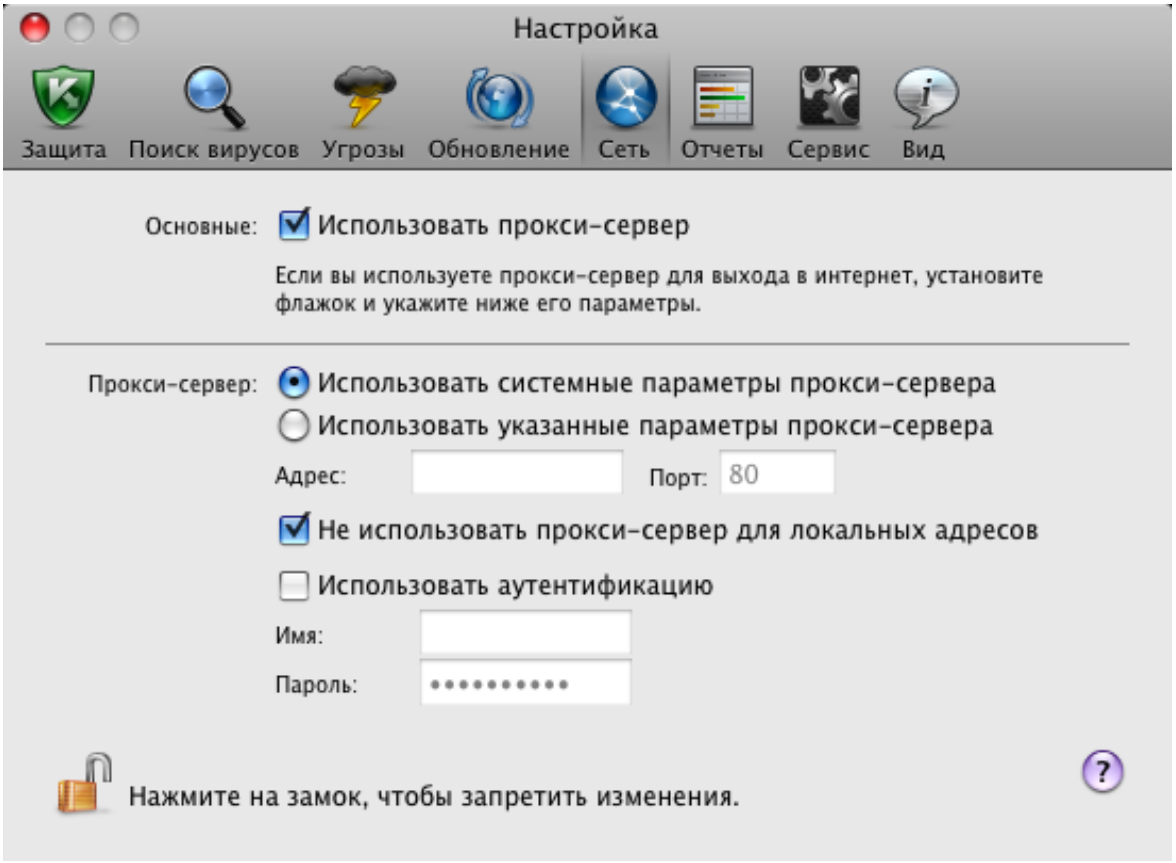


Рисунок 48. Окно настройки программы. Сеть

В случае обновления с FTP-сервера по умолчанию устанавливается соединение с сервером в пассивном режиме. При ошибке данного соединения выполняется попытка соединения в активном режиме.

По умолчанию время, отведенное на соединение с сервером обновлений, составляет одну минуту. Если соединение не было установлено, по истечении данного времени предпринимается попытка соединения со следующим источником обновлений из списка. Перебор проводится до тех пор, пока процесс соединения не завершится успешно, или пока не будут опрошены все доступные источники обновлений.

Статистика обновления

Краткая статистика текущей работы сервиса обновления (дата выпуска антивирусных баз, количество записей в базах, данные об актуальности используемых баз) представлена в нижней части главного окна программы (см. раздел «Главное окно программы» на стр. 34).

Если обновление Kaspersky Endpoint Security еще не проводилось, информация о дате последнего обновления отсутствует.

Также Kaspersky Endpoint Security предоставляет подробный отчет о выполнении задачи обновления.

Чтобы просмотреть отчет о выполнении текущей задачи, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  .
2. В разделе **Выполняемые задачи** открывшегося окна отчетов выберите задачу **Обновление**.

Сведения о результатах прошлых обновлений вы можете просмотреть в разделе **Завершенные задачи**.

В нижней части окна отчетов приводится информация о ходе выполнения текущей задачи обновления или сводная статистика с результатами завершенного обновления. Если обновление завершено успешно, статистика включает в себя информацию о размере скопированных и установленных обновлений, скорости, с которой производилось обновление, времени запуска и завершения обновления, а также о длительности выполнения задачи.

Если операцию произвести не удалось, необходимо проверить правильность настройки параметров обновления, сети, а также доступность источника обновлений. Запустите обновление еще раз. Если попытка будет также завершена с ошибкой, обратитесь в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 156).

Подробная информация о выполнении задачи обновления представлена в окне отчетов справа на следующих закладках:

- На закладке **События** последовательно перечислены все операции, выполненные в процессе обновления, с указанием имен обновляемых объектов, путей к папкам, в которых они хранятся и времени обращения к ним.
- На закладке **Параметры** перечислены основные параметры, в соответствии с которыми выполнялось обновление. Чтобы перейти к настройке параметров обновления, нажмите на кнопку **Изменить параметры**.

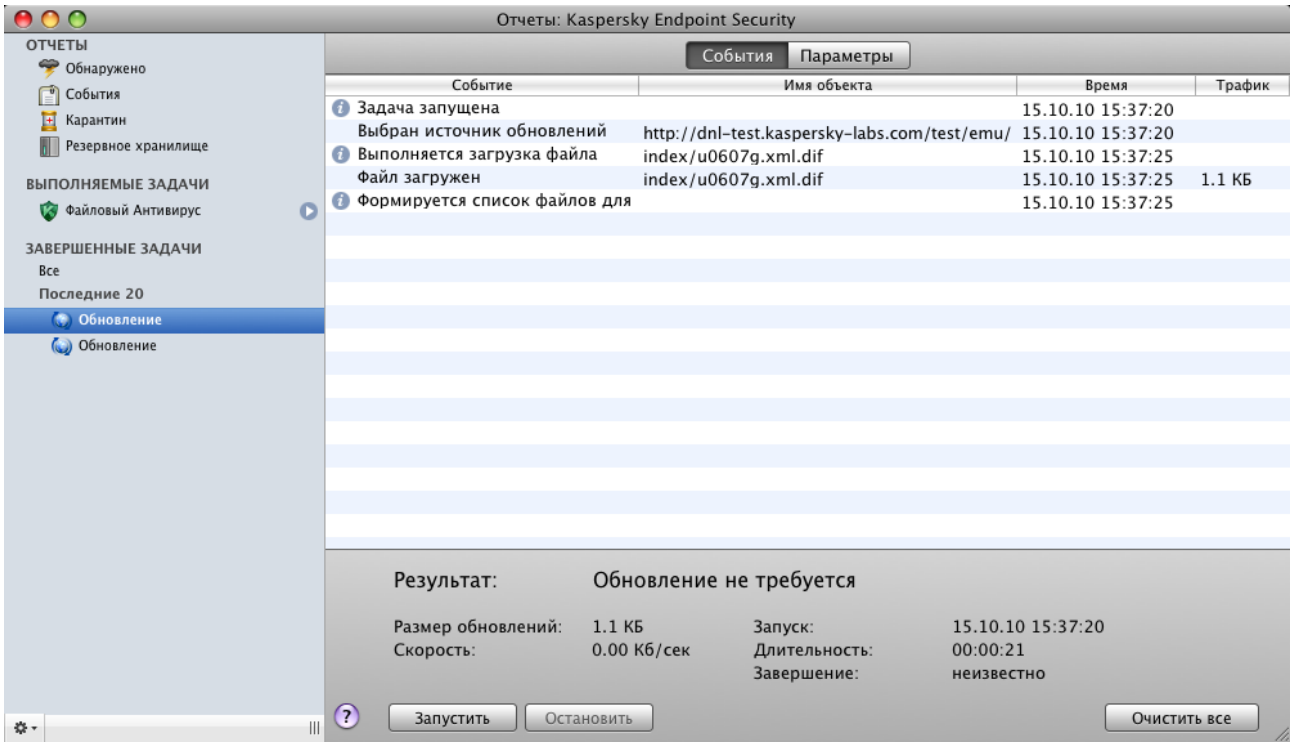


Рисунок 49. Окно отчетов. Обновление

Отчеты и хранилища

Kaspersky Endpoint Security позволяет помещать возможно зараженные объекты в хранилище карантина, создавать копии зараженных объектов в резервном хранилище перед лечением или удалением, а также формировать подробный отчет о работе каждого компонента программы.

В этом разделе

Карантин

Карантин – это специальное хранилище, в которое помещаются объекты, возможно зараженные вирусами.

Возможно зараженные объекты – это объекты, подозреваемые Kaspersky Endpoint Security на заражение вирусами или их модификациями. Статус *возможно зараженный* может быть присвоен объекту в следующих случаях:

- Код анализируемого объекта похож на известную угрозу, но частично изменен.

  Антивирусные базы Kaspersky Endpoint Security содержат те угрозы, которые на данный момент изучены специалистами «Лаборатории Касперского». Если в базах еще не содержится информация о модификикации вредоносной программы, то Kaspersky Endpoint Security отнесет объект, пораженный такой модификацией, к возможно зараженным объектам и укажет, на какую угрозу похоже это заражение.

- Код обнаруженного объекта по своей структуре напоминает вредоносную программу, однако базы Kaspersky Endpoint Security не содержат подобных записей.

  Вполне возможно, что это новый вид угроз, поэтому Kaspersky Endpoint Security относит такой объект к возможно зараженным объектам.

Возможно зараженный объект может быть обнаружен и помещен в хранилище карантина Файловым Антивирусом (см. раздел «Файловый Антивирус» на стр. 57), а также при выполнении задач поиска вирусов (см. раздел «Поиск вирусов» на стр. 69).

Кроме того, вы можете поместить объект в хранилище карантина вручную, нажав на кнопку **Карантин** в специальном уведомлении (см. раздел «Что делать при появлении уведомлений программы» на стр. 51), которое появляется на экране вашего компьютера при обнаружении возможно зараженного объекта.

Перемещая возможно зараженный объект в хранилище карантина, Kaspersky Endpoint Security удаляет его из текущей папки и сохраняет в папке карантина. Файлы на карантине хранятся в специальном формате и не представляют опасности для работы компьютера.

Просмотр содержимого хранилища карантина

Содержимое хранилища карантина можно просмотреть в разделе **Карантин** окна отчетов (см. рис. ниже).

Чтобы просмотреть содержимое хранилища карантина, выполните следующие действия:

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  . Откроется окно отчетов Kaspersky Endpoint Security.

2. В левой части окна отчетов выберите **Карантин**. В правой части окна будет представлено содержимое хранилища.

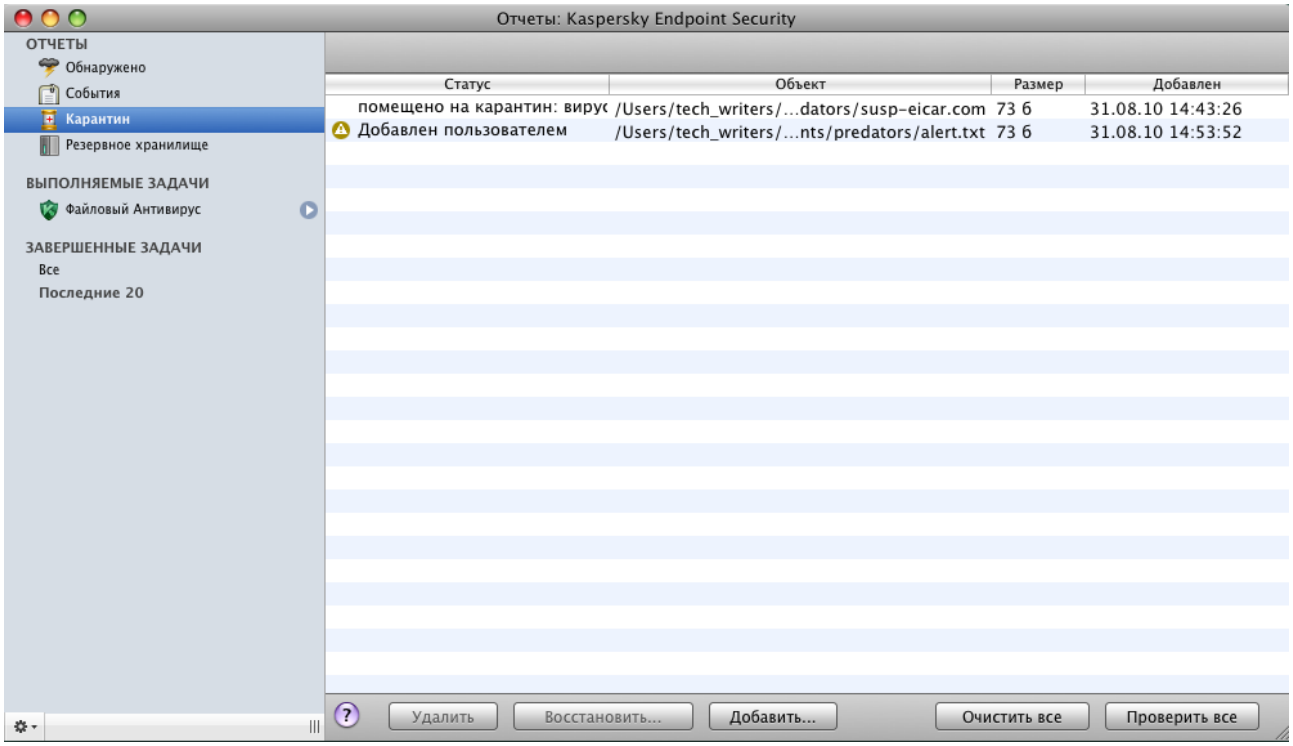


Рисунок 50. Окно отчетов. Хранилище карантина

ДЕЙСТВИЯ С ОБЪЕКТАМИ НА КАРАНТИНЕ

Kaspersky Endpoint Security позволяет совершать следующие действия с возможно зараженными объектами:

- Вручную переносить в хранилище карантина файлы, подозреваемые вами на присутствие вируса, но не обнаруженные Kaspersky Endpoint Security.

  Для этого в окне просмотра хранилища карантина (см. рис. ниже) нажмите на кнопку **Добавить** и в открывшемся стандартном окне выберите нужный файл. Он будет добавлен в список со статусом *добавлен пользователем*.

  Файл, помещенный на карантин вручную, может изменить статус, если он был проверен с использованием обновленных баз не ранее, чем через три дня с момента его первой проверки после помещения в хранилище карантина. Если ему будет присвоен статус *ложное срабатывание*, файл будет автоматически восстановлен. Если файл будет признан зараженным, он будет удален из карантина с помещением копии файла в резервное хранилище.

- Проверять и лечить все возможно зараженные объекты хранилища карантина с использованием текущей версии баз Kaspersky Endpoint Security.

  Для этого в окне просмотра хранилища карантина (см. рис. ниже) нажмите на кнопку **Проверить все**. В результате проверки и лечения любого объекта карантина его статус может измениться на *заражен*, *возможно заражен*, *ложное срабатывание*, *ок* и т. д.

Изменение статуса объектов, помещенных в хранилище карантина, происходит только после их проверки с использованием антивирусных баз, выпущенных не ранее, чем через три дня после помещения файла на карантин.

Присвоение объекту статуса *заражен* означает, что объект был идентифицирован как зараженный, но вылечить его не удалось. Kaspersky Endpoint Security удаляет такой объект из хранилища карантина, сохраняя его копию в резервном хранилище. Все объекты со статусом *ложное срабатывание* восстанавливаются в исходное местоположение.

По умолчанию Kaspersky Endpoint Security автоматически проверяет объекты хранилища карантина после каждого обновления (см. раздел «Проверка объектов карантина после обновления программы» на стр. 97).

- Восстанавливать файлы в папку, заданную пользователем, или папку, из которой они были перенесены в хранилище карантина (по умолчанию).

  Для восстановления объекта выберите его в окне просмотра хранилища карантина (см. рис. ниже) и нажмите на кнопку **Восстановить**. Подтвердите действие в открывшемся окне. При восстановлении объектов, помещенных на карантин из архивов, почтовых баз и файлов почтовых форматов необходимо дополнительно указать папку, в которую они будут восстанавливаться.

  Рекомендуем вам восстанавливать только объекты со статусом *ложное срабатывание*, *ок*, *вылечен*, поскольку восстановление объектов с другими статусами может привести к заражению вашего компьютера.

- Удалять любой объект хранилища карантина.

  Удаляйте только те объекты, которые невозможно вылечить. Чтобы удалить объект, выберите его в окне просмотра хранилища карантина (см. рис. ниже) и нажмите на кнопку **Удалить**. Чтобы полностью очистить содержимое хранилища карантина, нажмите на кнопку **Очистить все**. Также вы можете настроить автоматическое удаление наиболее старых объектов из карантина (см. раздел «Настройка параметров карантина и резервного хранилища» на стр. 102).

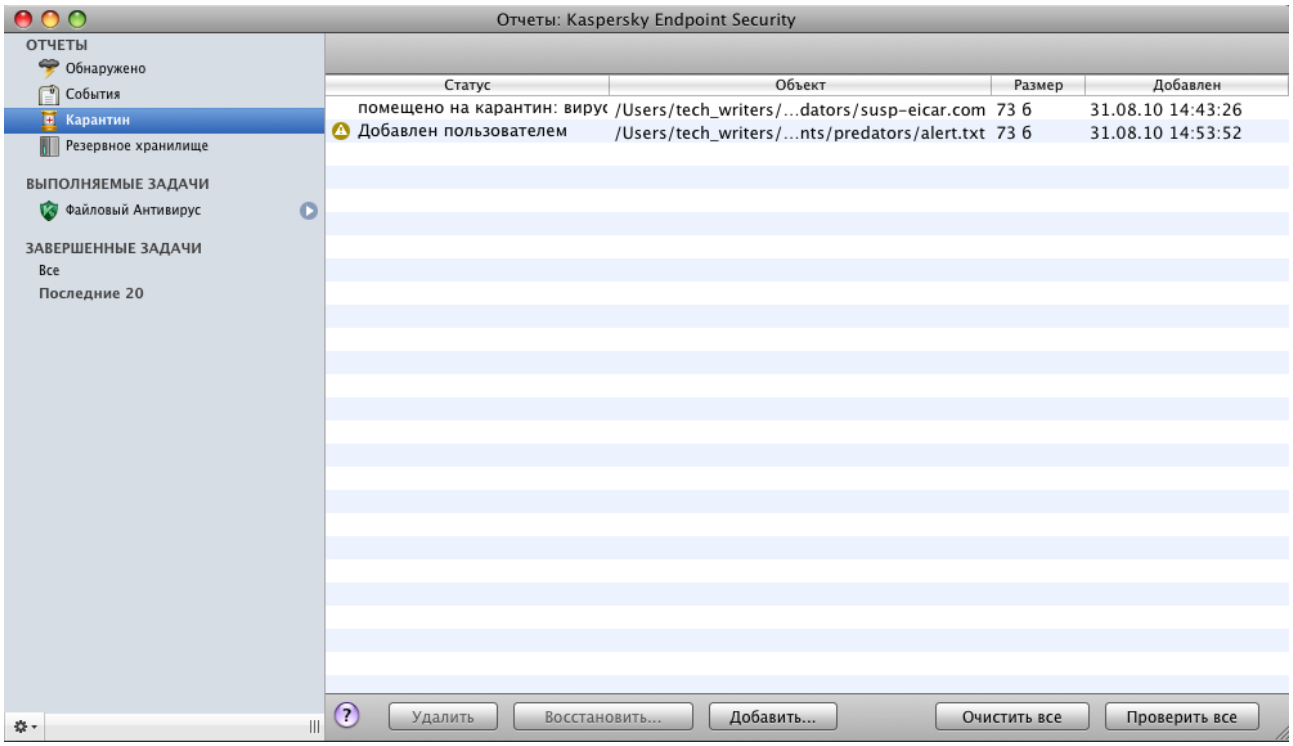


Рисунок 51. Окно отчетов. Хранилище карантина

ПРОВЕРКА ОБЪЕКТОВ КАРАНТИНА ПОСЛЕ ОБНОВЛЕНИЯ ПРОГРАММЫ

Каждый пакет обновления антивирусных баз программы содержит новые записи, позволяющие защищать ваш компьютер от недавно появившихся угроз. Специалисты «Лаборатории Касперского» рекомендуют вам сразу после обновления программы проверять возможно зараженные объекты, помещенные в хранилище карантина (см. раздел «Карантин» на стр. 94).

В хранилище карантина помещаются объекты, при проверке которых Файловым Антивирусом или при выполнении задачи поиска вирусов не удалось точно определить, какими вредоносными программами они поражены. Возможно, после обновления баз Kaspersky Endpoint Security сможет однозначно определить опасность и устранить проблему.

По умолчанию Kaspersky Endpoint Security проверяет объекты хранилища карантина после каждого обновления. Если после проверки у объекта сохраняется статус *возможно зараженный*, он остается в хранилище. Если статус меняется на *зараженный*, объект обрабатывается согласно выбранному действию; при этом он удаляется из карантина и его копия помещается в резервное хранилище (на стр. 97). Если по результатам проверки объект считается незараженным, и базы обновлялись не менее, чем три дня назад, объект восстанавливается из хранилища карантина в текущее местоположение. Если базы обновлялись менее трех дней назад, объект остается в хранилище карантина.

Kaspersky Endpoint Security не сможет проверить объекты хранилища карантина сразу после обновления баз, если в этот момент вы будете работать с хранилищем.

Проверку содержимого хранилища карантина после каждого обновления программы можно отключить, сняв соответствующий флажок на закладке **Обновление** окна настройки программы.

РЕЗЕРВНОЕ ХРАНИЛИЩЕ

Иногда в процессе лечения зараженных объектов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступной, можно попытаться восстановить исходный объект из его резервной копии.

Резервная копия – копия оригинального опасного объекта, которая создается при первом лечении или удалении данного объекта и хранится в резервном хранилище.

Резервное хранилище – это специальное хранилище, содержащее резервные копии обработанных или удаленных опасных объектов. Основная функция резервного хранилища – обеспечить возможность в любой момент восстановить исходный объект. Файлы в резервном хранилище хранятся в специальном формате и не представляют опасности для компьютера.

ПРОСМОТР СОДЕРЖИМОГО РЕЗЕРВНОГО ХРАНИЛИЩА

Содержимое резервного хранилища можно просмотреть в разделе **Резервное хранилище** окна отчетов (см. рис. ниже).

- *Чтобы просмотреть содержимое резервного хранилища, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 34) и нажмите на кнопку  . Откроется окно отчетов Kaspersky Endpoint Security.

2. В левой части окна отчетов выберите **Резервное хранилище**. В правой части окна будет представлено содержимое хранилища.

Для каждой резервной копии приведена следующая информация: полное имя объекта с указанием пути к исходному местоположению, время помещения в хранилище, статус объекта, присвоенный по результатам проверки, и его размер.

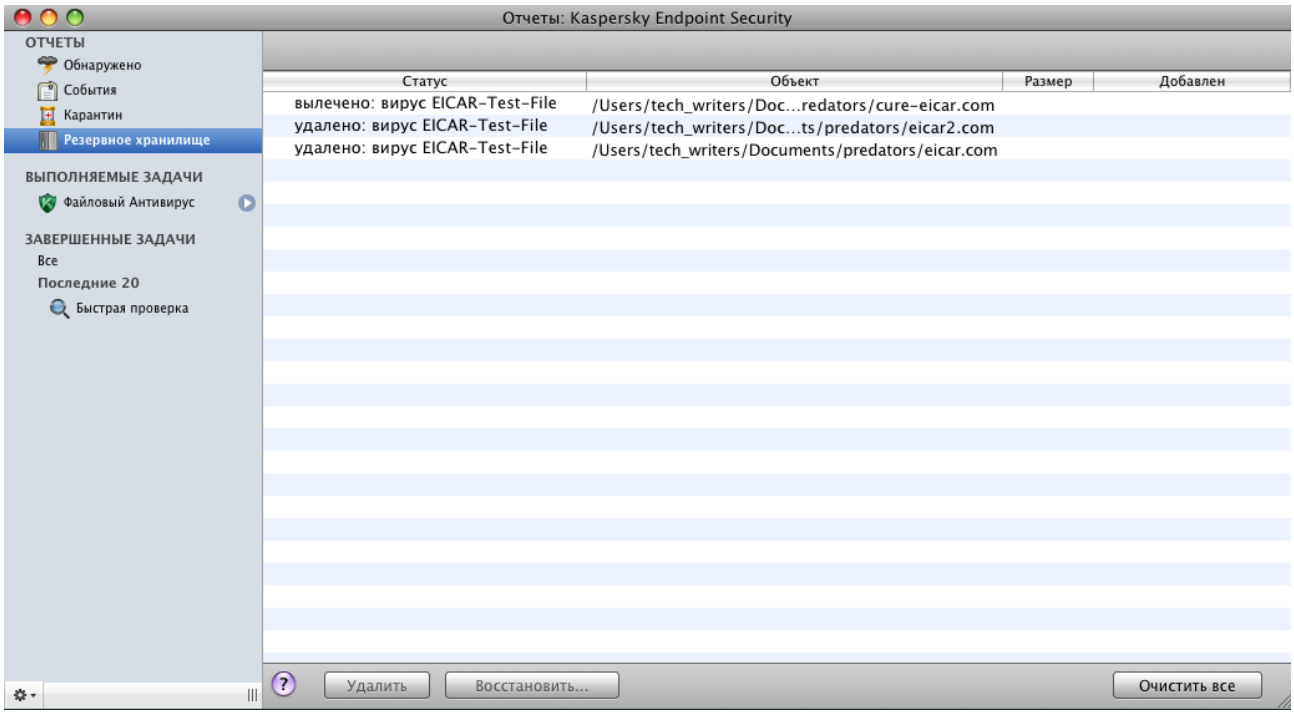


Рисунок 52. Окно отчетов. Резервное хранилище

Действия с резервными копиями

Kaspersky Endpoint Security позволяет совершать следующие действия с резервными копиями объектов:

- Восстанавливать выбранные резервные копии из резервного хранилища.

  Для этого в окне просмотра резервного хранилища (см. рис. ниже) выберите резервную копию необходимого объекта в списке и нажмите на кнопку **Восстановить**. Подтвердите действие в открывшемся окне. Объект будет восстановлен в исходное местоположение с тем же именем, которое было у него до лечения. Если в исходном местоположении уже находится объект с таким именем (данная ситуация возможна при восстановлении объекта, копия которого уже была создана перед лечением), на экран будет выведено соответствующее предупреждение. Вы можете изменить местоположение восстанавливаемого объекта или переименовать его.

  Рекомендуем сразу после восстановления проверить объект на вирусы. Возможно, с обновленными антивирусными базами его удастся вылечить без потери целостности.

  Не рекомендуется без крайней необходимости восстанавливать резервные копии объектов. Это может привести к заражению компьютера.

- Удалять резервные копии объектов из хранилища.

  Рекомендуем периодически просматривать хранилище и проводить его очистку. Чтобы удалить объекты, выберите их в окне просмотра резервного хранилища (см. рис. ниже) и нажмите на кнопку **Удалить**. Чтобы полностью очистить содержимое резервного хранилища, нажмите на кнопку **Очистить все**. Также вы можете настроить автоматическое удаление наиболее старых резервных копий из хранилища (см. раздел «Настройка параметров карантина и резервного хранилища» на стр. 102).

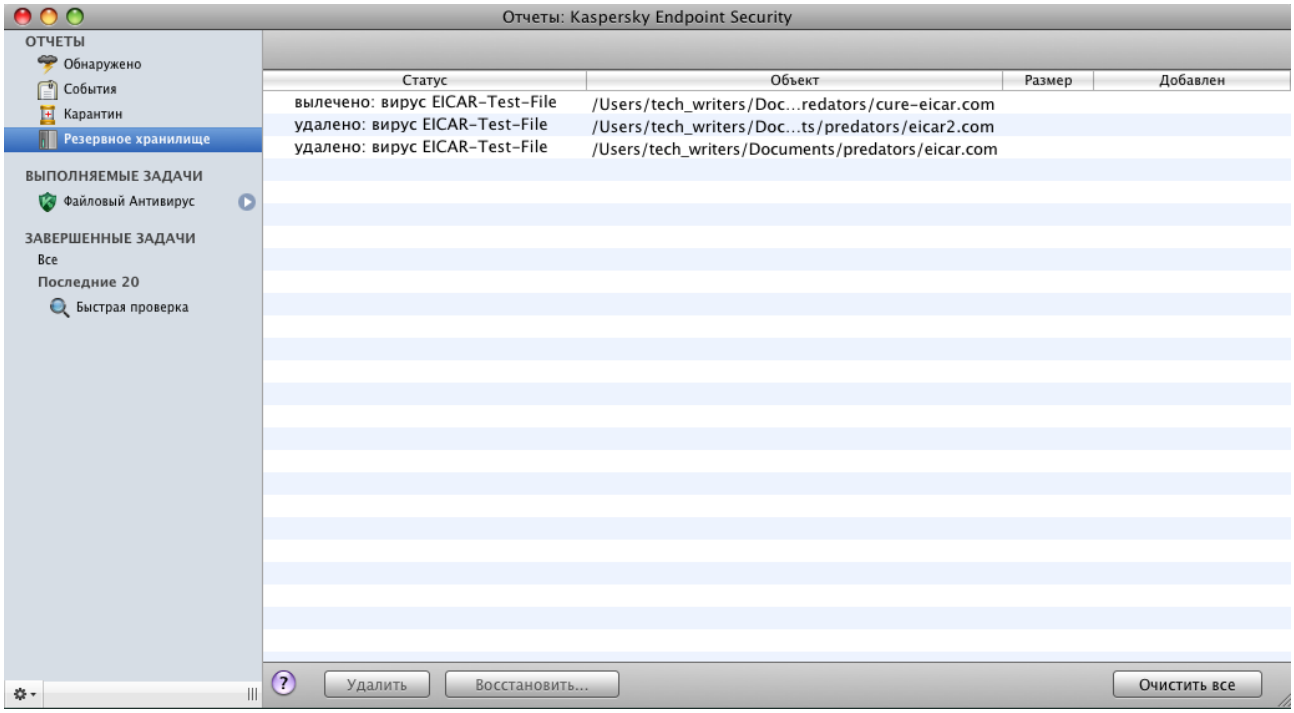


Рисунок 53. Окно отчетов. Резервное хранилище

Отчеты

Kaspersky Endpoint Security предоставляет возможность получения подробного отчета о результатах своей работы в целом с перечислением всех событий, которые возникли в работе программы. Кроме того, подробный отчет формируется отдельно для каждого компонента программы: Файлового Антивируса (см. раздел «Статистика защиты файлов» на стр. 67), задач поиска вирусов (см. раздел «Статистика поиска вирусов» на стр. 82) и обновления (см. раздел «Статистика обновления» на стр. 92).

Чтобы открыть окно отчетов,

откройте главное окно программы (на стр. 34) и нажмите на кнопку  .

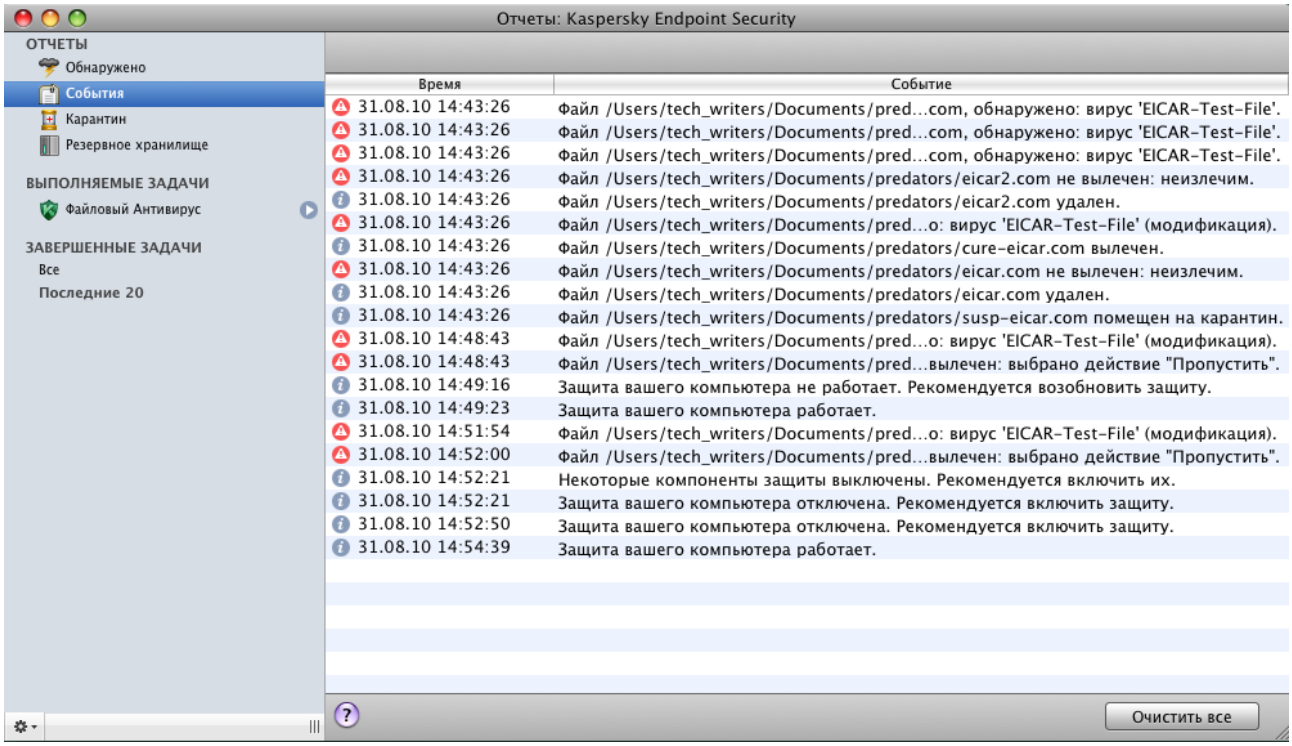


Рисунок 54. Окно отчетов Kaspersky Endpoint Security

Окно отчетов содержит следующие разделы:

- **Отчеты**. Статистические данные по обнаруженным опасным объектам, объектам, помещенным в хранилище карантина и в резервное хранилище, а также перечень событий, зафиксированных в работе программы. Вся статистика распределена на подразделы:

  - **Обнаружено**. Список всех опасных и подозрительных объектов, обнаруженных Файловым Антивирусом и задачами поиска вирусов. Для немедленного обезвреживания опасных объектов нажмите на кнопку **Лечить все**. Для удаления записей об обнаруженных объектах нажмите на кнопку **Очистить**. Обратите внимание, что при этом все обнаруженные опасные и подозрительные объекты останутся на вашем компьютере.

  - **События**. Список всех событий, зафиксированных в работе Kaspersky Endpoint Security. Для удаления информации из списка нажмите на кнопку **Очистить все**.

  - **Карантин**. Список объектов, помещенных в хранилище карантина (см. раздел «Карантин» на стр. 94).

  - **Резервное хранилище**. Список объектов, помещенных в резервное хранилище (на стр. 97).

- **Выполняемые задачи**. Список задач, которые выполняются Kaspersky Endpoint Security в данный момент. Если ни одна из задач не запущена и Файловый Антивирус отключен, список будет пуст.

- **Завершенные задачи**. Список завершенных задач. Вы можете просматривать все завершенные задачи или последние двадцать. Чтобы очистить список, нажмите на кнопку  в левом нижнем углу окна отчетов и выберите **Удалить все завершенные задачи**.

Из окна отчетов можно управлять работой Файлового Антивируса, а также задачами поиска вирусов и обновления: запускать и останавливать их. Для этого воспользуйтесь одноименными кнопками в окне отчетов конкретного компонента или задачи.

Kaspersky Endpoint Security позволяет сохранить отчет о своей работе в текстовом формате. Эта возможность может понадобиться в том случае, если в работе Файлового Антивируса или при выполнении другой задачи возникла ошибка, устранить которую самостоятельно вы не можете, и требуется помощь Службы технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 156). В этом случае отчет в текстовом формате необходимо отправить в Службу технической поддержки, чтобы наши специалисты могли детально изучить проблему и решить ее как можно скорее.

Чтобы экспортировать отчет о работе Kaspersky Endpoint Security в текстовый файл, выполните следующие действия:

1. В окне отчетов выберите необходимый отчет или задачу.

2. В левом нижнем углу окна отчетов нажмите на кнопку  , выберите команду **Экспортировать** и в открывшемся окне укажите имя файла и папку, в которую его следует сохранить.

НАСТРОЙКА ОТЧЕТОВ И ХРАНИЛИЩ

На закладке **Отчеты** окна настройки программы (см. раздел «Окно настройки программы» на стр. 35) вы можете настроить параметры формирования и хранения отчетов и максимальный срок хранения объектов в хранилище карантина и резервном хранилище.

НАСТРОЙКА ПАРАМЕТРОВ ОТЧЕТОВ

Чтобы настроить параметры формирования и хранения отчетов, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Отчеты** (см. рис. ниже).

2. В блоке **Отчеты** настройте следующие параметры:

   - Разрешить запись в отчет событий информационного характера.

     Как правило, такие события не важны для обеспечения защиты. Чтобы фиксировать их в отчете, установите флажок **Записывать некритические события**.

   - Сохранять в отчете только важные события, произошедшие при последнем запуске задачи.

     Это позволит сэкономить место на диске за счет уменьшения размера отчета. Если флажок **Хранить только текущие события** установлен, информация, представленная в отчете, будет обновляться при каждом перезапуске задачи: при этом важная информация (например, записи об обнаруженных вредоносных объектах) будет сохранена, а информация некритического характера – будет удалена.

   - Установить срок хранения отчетов.

По умолчанию срок хранения отчетов составляет 30 дней. По истечении этого времени отчеты удаляются. Вы можете изменить максимальный срок хранения или отменить это ограничение.

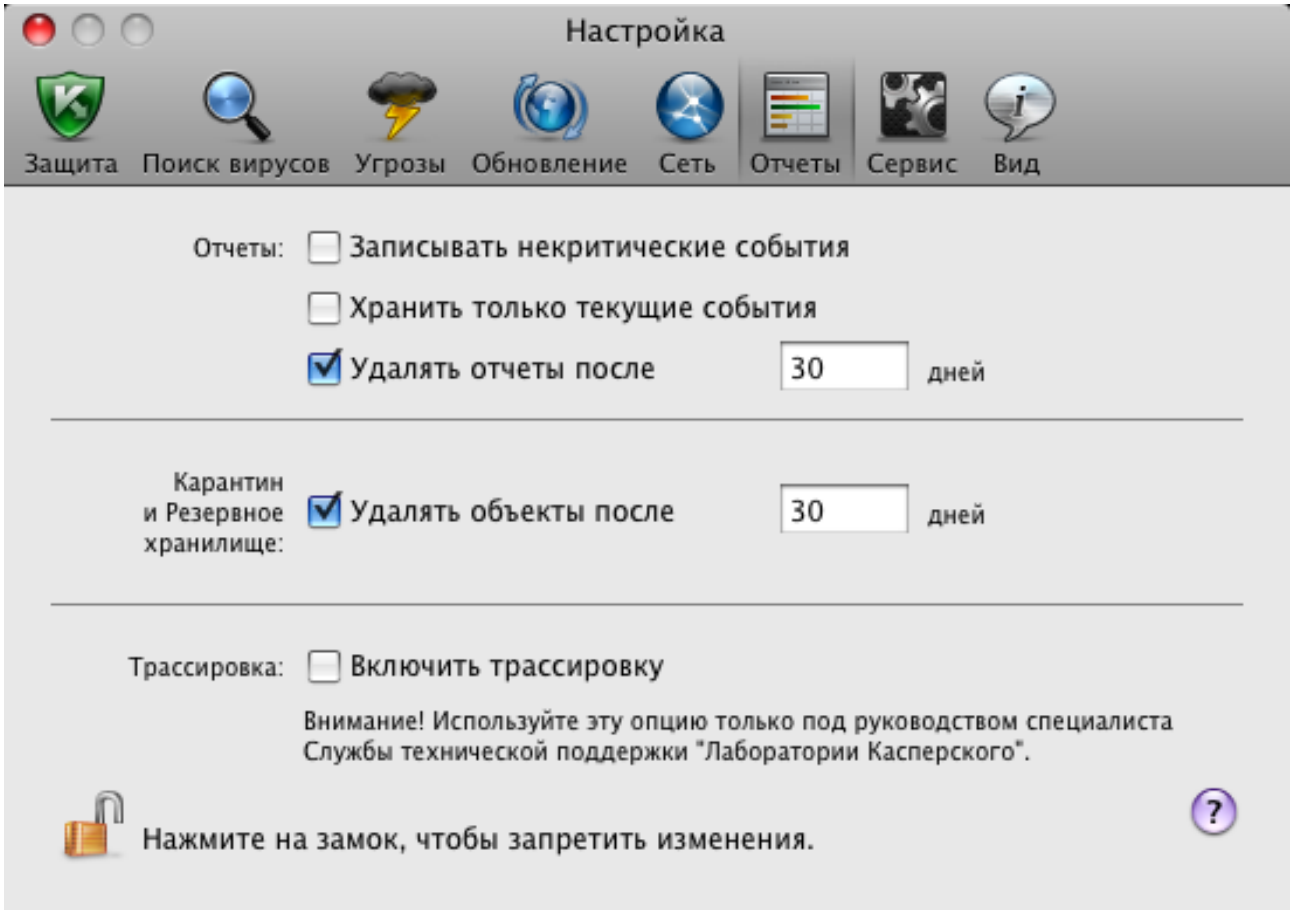


Рисунок 55. Окно настройки программы. Отчеты

Настройка параметров карантина и резервного хранилища

По умолчанию срок хранения объектов в хранилище карантина и резервном хранилище составляет 30 дней; по истечении этого срока объекты удаляются. Вы можете изменить максимальный срок хранения объектов в хранилищах или отменить такое ограничение совсем.

Чтобы настроить параметры хранения объектов в хранилищах, выполните следующие действия:

1. Откройте окно настройки программы (на стр. 35) и выберите закладку **Отчеты** (см. рис. ниже).

2. В блоке **Карантин и Резервное хранилище** установите флажок **Удалять объекты после** и укажите период, по истечении которого объекты, находящиеся в хранилищах, будут автоматически удалены.

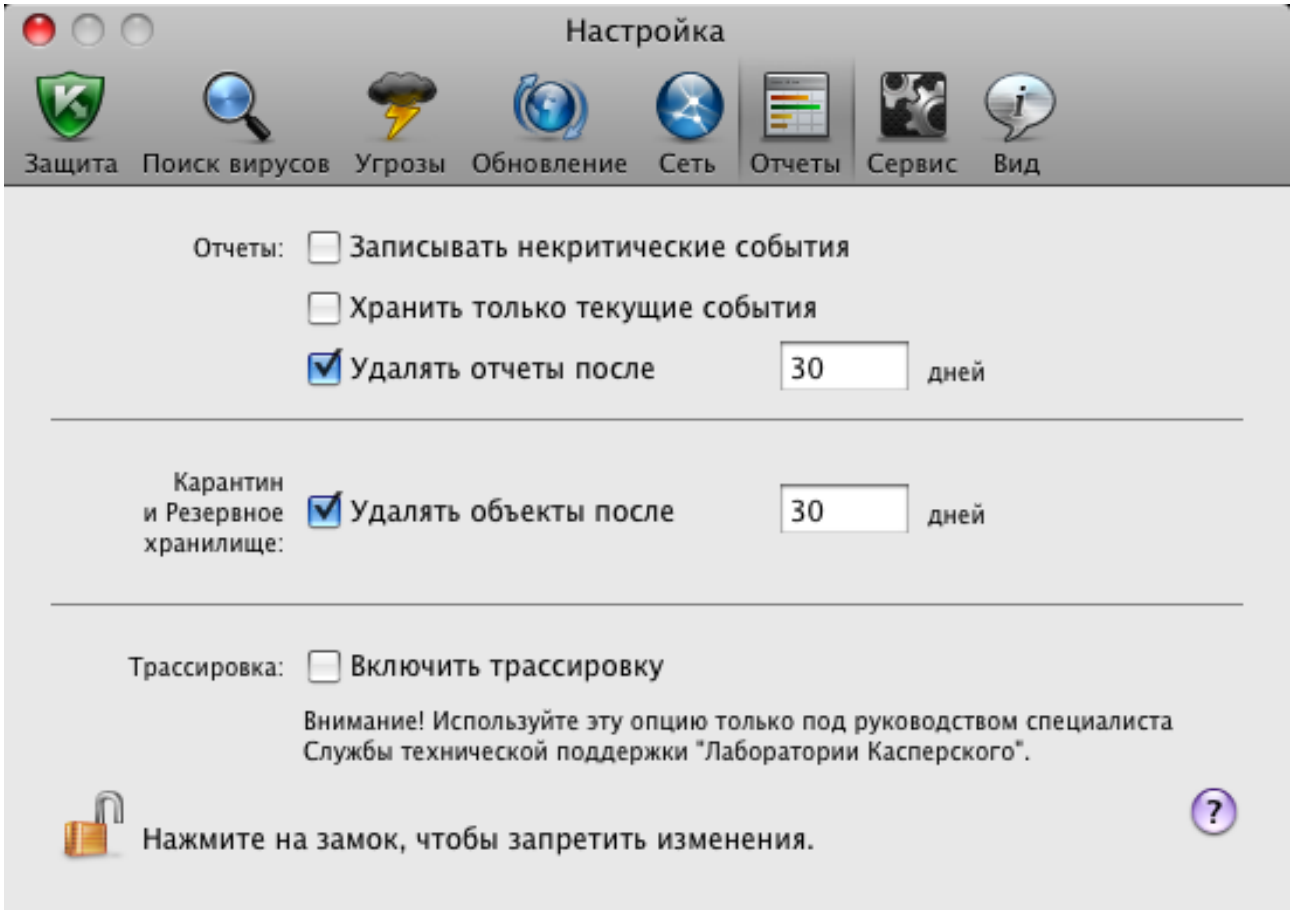


Рисунок 56. Окно настройки программы. Отчеты

РАБОТА С ПРОГРАММОЙ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете работать с Kaspersky Endpoint Security посредством командной строки.

Синтаксис командной строки:

```
kav <команда> [параметры]
```

В качестве <команды> может использоваться:

- **help –** помощь по синтаксису команды, вывод списка команд;
- **scan –** проверка объектов на присутствие вредоносных программ;
- **update –** запуск обновления программы;
- **rollback –** откат последнего произведенного обновления Kaspersky Endpoint Security (для выполнения команды требуются права администратора);
- **start –** запуск компонента или задачи;
- **stop –** остановка работы компонента или задачи (для выполнение команды требуются права администратора);
- **status –** вывод на экран текущего статуса компонента или задачи;
- **statistics –** вывод на экран статистики по работе компонента или задачи;
- **export –** экспорт параметров работы компонента или задачи;
- **import –** импорт параметров работы компонента или задачи (для выполнения команды требуются права администратора);
- **addkey –** активация программы с помощью файла ключа (для выполнения команды требуются права администратора);
- **exit –** завершение работы программы (для выполнения команды требуются права администратора).

Каждой команде соответствует собственный набор параметров.

В этом разделе

Просмотр справки

Для просмотра справки по синтаксису командной строки предусмотрена команда:

```
kav [ -? | help ]
```

Для получения справки по синтаксису конкретной команды вы можете воспользоваться одной из следующих команд:

```
kav <команда> -?
kav help <команда>
```

Проверка на вирусы

Командная строка запуска проверки некоторой области на вирусы имеет следующий общий вид:

```
kav scan [<объект проверки>] [<действие>] [<типы файлов>] [<исключения>] [<параметры отчета>] [<дополнительные параметры>]
```

Для поиска вирусов вы также можете воспользоваться сформированными в программе задачами, запустив нужную из командной строки (см. раздел «Запуск / остановка работы компонента или задачи» на стр. 109). При этом задача будет выполнена с параметрами, установленными в интерфейсе Kaspersky Endpoint Security.

Описание параметров

<объект проверки> – параметр задает перечень объектов, которые будут проверены на присутствие вредоносного кода. Параметр может включать несколько значений из представленного списка, разделенных пробелом:

<files> – список путей к файлам и / или папкам для проверки. Допускается ввод абсолютного или относительного пути. Разделительный символ для элемента списка – пробел. Замечания:

- если имя объекта или путь содержит пробел или специальные символы ($, &, @ и т.д.), оно должно быть заключено в одинарные кавычки или исключаемый символ должен быть отделен с левой стороны обратной косой чертой;
- если указана конкретная папка, проверяются все файлы и папки, содержащиеся в ней.

-all – полная проверка компьютера;

-remdrives – все съемные диски;

-fixdrives – все локальные диски;

-netdrives – все сетевые диски;

-quarantine – объекты, помещенные в хранилище карантина;

-@:<filelist.lst> – путь к файлу со списком объектов и папок, включаемых в проверку. Файл должен иметь текстовый формат, каждый объект проверки необходимо указывать с новой строки. Допускается ввод только абсолютного пути к файлу.

Если перечень объектов для проверки не указан, то Kaspersky Endpoint Security запустит задачу **Поиск вирусов** с параметрами, установленными в интерфейсе программы.

<действие> – параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению **-i8**. Возможны следующие значения:

-i0 – не совершать над объектом никаких действий, только фиксировать информацию о нем в отчете;

-i1 – лечить зараженные объекты, если лечение невозможно – пропускать;

-i2 – лечить зараженные объекты, если лечение невозможно – удалять; не удалять контейнеры, кроме контейнеров с исполняемым заголовком (sfx-архивы);

-i3 – лечить зараженные объекты, если лечение невозможно – удалять; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы;

-i4 – удалять зараженные объекты; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы;

-i8 – запрашивать действие у пользователя при обнаружении зараженного объекта. Данное действие используется по умолчанию;

-i9 – запрашивать действие у пользователя по окончании проверки.

<типы файлов> – параметр определяет типы файлов, которые будут подвергаться антивирусной проверке. По умолчанию, если параметр не задан, проверяются только заражаемые файлы по содержимому. Возможны следующие значения:

-fe – проверять только заражаемые файлы по расширению;

-fi – проверять только заражаемые файлы по содержимому (по умолчанию);

-fa – проверять все файлы.

<исключения> – параметр определяет объекты, исключаемые из проверки. Можно перечислить несколько параметров из следующего списка, разделив их пробелом:

-e:a – не проверять архивы;

-e:b – не проверять почтовые базы;

-e:m – не проверять почтовые сообщения в текстовом формате;

-e:<mask> – не проверять объекты по маске (см. раздел «Разрешенные маски исключений файлов» на стр. 160);

-e:<seconds> – пропускать объекты, которые проверяются дольше указанного времени в секундах;

-es:<size> – пропускать объекты, размер которых превышает указанное значение в мегабайтах.

<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного или относительного пути к файлу для сохранения отчета. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

-r:<report_file> – записывать в указанный файл отчета только важные события;

-ra:<report_file> – записывать в указанный файл отчета все события.

<дополнительные параметры> – параметры, определяющие использование технологий антивирусной проверки и файла настроек параметров:

-iSwift=<on|off> – включить / отключить использование технологии iSwift;

-c:<имя_конфигурационного_файла> – определяет путь к конфигурационному файлу, содержащему параметры работы программы при выполнении задач поиска вирусов. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, наряду со значениями уже указанными в командной строке, используются значения, установленные в интерфейсе программы.

Пример:

Запустить проверку папок ~/Documents, /Applications и файла my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Проверить объекты, список которых приведен в файле object2scan.txt. Использовать для работы конфигурационный файл scan_settings.txt. По результатам проверки сформировать отчет, в котором зафиксировать все события:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Пример конфигурационного файла:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

ОБНОВЛЕНИЕ ПРОГРАММЫ

Команда для обновления модулей и антивирусных баз программы имеет следующий синтаксис:

```
kav update [<источник_обновлений>] [-app=<on|off>] [<параметры_отчета>]
[<дополнительные_параметры>]
```

Описание параметров

<источник_обновлений> – HTTP-, FTP-сервер или сетевая или локальная папка для загрузки обновлений. Если путь не указан, источник обновлений будет взят из параметров сервиса обновления программы.

-app=<on|off> – включить / отключить обновление модулей программы.

<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события. Возможны следующие значения:

-r:<report_file> – записывать в указанный файл отчета только важные события;

-ra:<report_file> – записывать в указанный файл отчета все события.

<дополнительные параметры> – параметр, определяющий использование файла настроек параметров.

-c:<имя_конфигурационного_файла> – определяет путь к конфигурационному файлу, содержащему параметры работы программы при выполнении обновления. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.

Пример:

Обновить базы программы из источника по умолчанию, зафиксировав все события в отчете:

```
kav update -ra:avbases_upd.txt
```

Обновить модули Kaspersky Endpoint Security, используя параметры конфигурационного файла updateapp.ini:

```
kav update -app=on -c:updateapp.ini
```

Откат последнего обновления

Синтаксис команды:

```
kav rollback [<параметры_отчета>]
```

Для выполнения команды требуются права администратора.

Описание параметров

<параметры отчета> – параметр, определяющий формат отчета о результатах проверки. Допускается использование абсолютного и относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

-r:<report_file> – записывать в указанный файл отчета только важные события;

-ra:<report_file> – записывать в указанный файл отчета все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

Пример:

```
kav rollback -ra:rollback.txt
```

Запуск / остановка работы компонента или задачи

Синтаксис команды start:

```
kav start <профайл|имя_задачи> [<параметры_отчета>]
```

Синтаксис команды stop:

```
kav stop <профайл|имя_задачи>
```

Для выполнения команды stop требуются права администратора.

Описание параметров

<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного и относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события. Возможны следующие значения:

-r:<report_file> – записывать в указанный файл отчета только важные события;

-ra:<report_file> – записывать в указанный файл отчета все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

<профайл|имя_задачи> – указывается одно из следующих значений:

file_monitoring (fm) – Файловый Антивирус;

scan_my_computer (full) – задача полной проверки компьютера;

scan_objects – проверка объектов;

scan_quarantine – проверка хранилища карантина;

scan_critical_areas (quick) - задача быстрой проверки компьютера;

updater – задача обновления;

rollback – задача отката обновлений.

Также в качестве значения этого параметра можно указывать имя задачи поиска вирусов, созданной пользователем.

Компоненты и задачи, запущенные из командной строки, выполняются с параметрами, установленными в интерфейсе программы.

Пример:

Чтобы включить Файловый Антивирус, в командной строке введите:

```
kav start fm
```

Чтобы остановить задачу полной проверки, в командной строке введите:

```
kav stop scan_my_computer
```

СТАТИСТИКА РАБОТЫ КОМПОНЕНТА ИЛИ ЗАДАЧИ

Синтаксис команды status:

```
kav status [<профайл|имя_задачи>]
```

Синтаксис команды statistics:

```
kav statistics <профайл|имя_задачи>
```

Описание параметров

<профайл|имя_задачи> – указывается одно из значений, перечисленных для команды start / stop. (см. раздел «Запуск / остановка работы компонента или задачи» на стр. 109)

Если команда status запускается без указания значения параметра **<профайл|имя_задачи>**, то на экран выводится текущий статус всех задач и компонентов программы. Для команды statistics значение параметра **<профайл|имя_задачи>** должно быть указано обязательно.

ЭКСПОРТ ПАРАМЕТРОВ ЗАЩИТЫ

Синтаксис команды:

```
kav export <профайл|имя_задачи> <имя_файла>
```

Описание параметров

<профайл|имя_задачи> – указывается одно из значений, перечисленных для команды start / stop (см. раздел «Запуск / остановка работы компонента или задачи» на стр. 109).

<имя_файла> – путь к файлу, в который экспортируются параметры программы. Может быть указан абсолютный или относительный путь.

Пример:

```
kav export fm fm_settings.txt – текстовый формат
```

ИМПОРТ ПАРАМЕТРОВ ЗАЩИТЫ

Синтаксис команды:

```
kav import <имя_файла>
```

Для выполнения команды требуются права администратора.

Описание параметров

<имя_файла> – путь к файлу, из которого импортируются параметры программы. Может быть указан абсолютный или относительный путь.

Пример:

```
kav import settings.dat
```

АКТИВАЦИЯ ПРОГРАММЫ

Активацию Kaspersky Endpoint Security можно выполнить с использованием файла ключа.

Синтаксис команды:

```
kav addkey <имя_файла>
```

Для выполнения команды требуются права администратора.

Описание параметров

<имя_файла> – файл ключа к программе с расширением key.

Пример:

```
kav addkey 1AA111A1.key
```

ЗАВЕРШЕНИЕ РАБОТЫ ПРОГРАММЫ

Синтаксис команды:

```
kav exit
```

Для выполнения команды требуются права администратора.

КОДЫ ВОЗВРАТА КОМАНДНОЙ СТРОКИ

Общие коды могут быть возвращены любой командой командной строки. К кодам возврата задач относятся общие коды, а также коды, специфичные для конкретной задачи.

Общие коды возврата:

- 0 – операция выполнена успешно;
- 1 – неверное значение параметра;
- 2 – неизвестная ошибка;
- 3 – ошибка выполнения задачи;
- 4 – выполнение задачи отменено.

Коды возврата задач проверки на вирусы:

- 101 – все опасные объекты обработаны;
- 102 – обнаружены опасные объекты.

УПРАВЛЕНИЕ ПРОГРАММОЙ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit – это система централизованного решения основных административных задач по управлению системой безопасности компьютерной сети предприятия. Эта система построена на основе программ, входящих в состав Kaspersky Open Space Security. Kaspersky Administration Kit поддерживает работы во всех сетевых конфигурациях, использующих протокол TCP/IP.

Программа адресована администраторам корпоративных компьютерных сетей, а также сотрудникам, отвечающим за антивирусную защиту компьютеров в организациях.

Kaspersky Endpoint Security входит в группу продуктов «Лаборатории Касперского», управление которыми возможно через собственный интерфейс программы (на стр. 32), командную строку (см. раздел «Работа с программой из командной строки» на стр. 104), либо с помощью программы Kaspersky Administration Kit.

Доступ к управлению программой через Kaspersky Administration Kit обеспечивает Консоль администрирования (см. рис. ниже). Она представляет собой стандартный интерфейс, интегрированный в MMC, и позволяет администратору выполнять следующие функции:

- удаленно устанавливать Kaspersky Endpoint Security на компьютеры сети;
- удаленно настраивать Kaspersky Endpoint Security на компьютерах сети;
- обновлять антивирусные базы и модули программы и выполнять откат последнего обновления;
- запускать задачи поиска вирусов на компьютерах сети;
- удаленно активировать программу с использованием файла ключа;
- просматривать статистику и формировать отчеты о работе Kaspersky Endpoint Security на компьютерах сети.

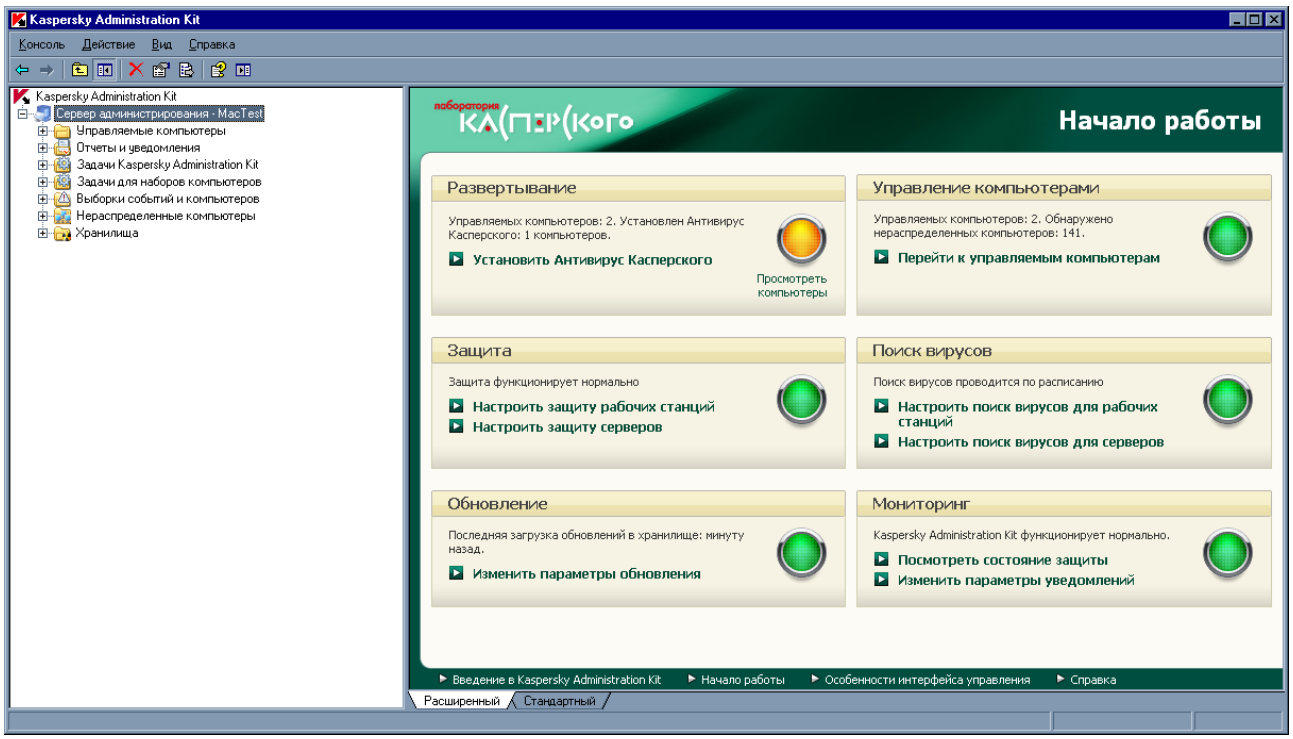


Рисунок 57. Консоль администрирования Kaspersky Administration Kit

Вид главного окна Kaspersky Administration Kit зависит от версии операционной системы, установленной на компьютере администратора.

Понятия и термины

При работе через Kaspersky Administration Kit управление Kaspersky Endpoint Security осуществляется через определение администратором параметров программы, политик и задач.

Именованное действие, выполняемое программой, называется *задачей*. В зависимости от выполняемых функций выделяют следующие типы задач:

- проверка на вирусы;
- обновление программы;
- откат последнего обновления;
- установка файла ключа.

Каждой задаче соответствует набор параметров работы программы. Набор параметров работы программы, общий для всех типов задач, составляет *параметры программы*. Параметры работы программы, специфичные для каждого типа задач, образуют *параметры задачи*. Параметры программы и параметры задач не пересекаются.

Особенностью централизованного управления является организация удаленных компьютеров сети в группы и управление ими через создание и определение групповых политик.

Политика – это набор параметров работы программы в группе, а также набор ограничений на переопределение этих параметров при настройке программы или настройке задачи на отдельном клиентском компьютере. Политика включает в себя параметры полной настройки всей функциональности программы, за исключением параметров, специфичных для конкретного типа задач. Примером таких специфичных параметров могут служить параметры расписания.

Таким образом, в политику входят параметры:

- общие для всех типов задач – параметры программы;
- общие для всех задач каждого типа – большая часть параметров задач.

Это означает, что политика для Kaspersky Endpoint Security, в число задач которого входят задачи защиты и поиска вирусов, включает все необходимые параметры настройки программы при выполнении обоих типов задач, но не включает, например, расписание запуска задач поиска вирусов и параметры, определяющие область проверки.

В этом разделе

ТИПИЧНАЯ СХЕМА РАЗВЕРТЫВАНИЯ

Для управления Kaspersky Endpoint Security через Kaspersky Administration Kit выполните следующие действия:

1. Разверните в сети Сервер администрирования;
2. Установите Консоль администрирования[2] и плагин управления Kaspersky Endpoint Security (см. раздел «Установка плагина управления Kaspersky Endpoint Security» на стр. 115) на рабочее место администратора Kaspersky Administration Kit.
3. На компьютеры Apple Macintosh установите Агент администрирования и Kaspersky Endpoint Security.
   - Установку Агента администрирования можно выполнить как локально (см. раздел «Локальная установка Агента администрирования» на стр. 115), так и удаленно, используя SSH-протокол (см. раздел «Установка Агента администрирования с использованием SSH-протокола» на стр. 116).
   - Установку Kaspersky Endpoint Security также можно выполнить локально (см. раздел «Установка программы» на стр. 20), удаленно, используя SSH-протокол (см. раздел «Установка программы с использованием SSH-протокола» на стр. 120) или удаленно через Kaspersky Administration Kit, используя предварительно созданный инсталляционный пакет (см. раздел «Установка программы через Kaspersky Administration Kit» на стр. 121).

Если на компьютерах пользователей уже установлен Антивирус Касперского для Mac, то его необходимо удалить с компьютера перед установкой Kaspersky Endpoint Security.

УСТАНОВКА ПО, НЕОБХОДИМОГО ДЛЯ УДАЛЕННОГО УПРАВЛЕНИЯ KASPERSKY ENDPOINT SECURITY

Для осуществления удаленного управления Kaspersky Endpoint Security через Kaspersky Administration Kit необходимо установить следующие программы:

- Плагин управления Kaspersky Endpoint Security – на рабочее место администратора Kaspersky Administration Kit, где уже установлена Консоль администрирования.
- Агент администрирования – на компьютеры Apple Macintosh корпоративной сети.

В ЭТОМ РАЗДЕЛЕ

[2] Подробнее смотрите Руководство по внедрению Kaspersky Administration Kit.

УСТАНОВКА ПЛАГИНА УПРАВЛЕНИЯ KASPERSKY ENDPOINT SECURITY

Перед установкой плагина управления Kaspersky Endpoint Security необходимо завершить работу Консоли администрирования на рабочем месте администратора Kaspersky Administration Kit.

Чтобы установить плагин управления Kaspersky Endpoint Security на рабочее место администратора, выполните следующие действия:

1. Откройте содержимое дистрибутива Kaspersky Endpoint Security. Для этого вставьте установочный диск в дисковод. В окне с содержимым дистрибутива откройте папку **AdminKit Deployment.**

   Если вы купили Kaspersky Endpoint Security в интернет-магазине, то на веб-сайте «Лаборатории Касперского» будет доступен для скачивания дистрибутив программы в формате ZIP. Распакуйте его и запустите dmg-файл, чтобы увидеть содержимое дистрибутива.

2. Откройте папку **AdminKit Console Plugin**, а в ней вложенную папку с версией программы на необходимом языке локализации.

3. Запустите исполняемый файл klcfginst.exe. Подождите пока будет выполнена установка программы.

По завершении установки плагин управления Kaspersky Endpoint Security будет добавлен в список установленных плагинов для управления программами[3].

ЛОКАЛЬНАЯ УСТАНОВКА АГЕНТА АДМИНИСТРИРОВАНИЯ

Чтобы выполнить локальную установку Агента администрирования на компьютер пользователя, выполните следующие действия:

1. Откройте содержимое дистрибутива Агента администрирования. Для этого вставьте установочный диск в дисковод.

   Если вы купили Kaspersky Endpoint Security в интернет-магазине, то на веб-сайте «Лаборатории Касперского» будет доступен для скачивания дистрибутив программы в формате ZIP. Распакуйте его и запустите dmg-файл, чтобы увидеть содержимое дистрибутива.

2. Запустите программу установки Агента администрирования. Для этого в окне с содержимым дистрибутива откройте установочный пакет **Kaspersky Network Agent**.

   Подтвердите запуск установки программы в окне запроса. Далее следуйте шагам программы установки, чтобы установить программу.

3. В окне **Введение** нажмите на кнопку **Продолжить**.

4. В окне **Информация** прочтите информацию об устанавливаемой программе.

   Убедитесь, что компьютер пользователя соответствует указанным системным требованиям. Чтобы распечатать информацию, нажмите на кнопку **Напечатать**. Для сохранения информации в текстовом файле нажмите на кнопку **Сохранить**. Для продолжения установки нажмите на кнопку **Продолжить**.

5. В окне **Лицензия** ознакомьтесь с текстом лицензионного соглашения об использовании Агента администрирования, которое заключается между вами и ЗАО «Лаборатория Касперского». Текст соглашения доступен на нескольких языках. Чтобы распечатать текст соглашения, нажмите на кнопку **Напечатать**. Для сохранения соглашения в текстовом файле нажмите на кнопку **Сохранить**.

[3] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.

Если вы согласны со всеми пунктами соглашения, нажмите на кнопку **Продолжить**. Откроется окно запроса подтверждения согласия с условиями лицензионного соглашения. Вы можете выполнить следующие действия:

- продолжить установку Агента администрирования, нажав на кнопку **Подтверждаю**;
- вернуться к тексту соглашения, нажав на кнопку **Прочитать лицензию**;
- прервать установку программы, нажав на кнопку **Не подтверждаю**.

6. В окне **Настройка** в поле **Сервер** укажите IP-адрес или DNS-имя сервера, на котором установлен Kaspersky Administration Kit, в поле **Порт** номер порта для незащищенного соединения с сервером и в поле **SSL порт** номер порта для соединения с сервером с использованием SSL.

   Если вы не хотите использовать SSL для соединения с сервером, снимите флажок **Использовать SSL**. Для продолжения установки нажмите на кнопку **Продолжить**.

7. В окне **Тип установки** изучите информацию о диске, на который будет устанавливаться программа.

   Чтобы установить программу, используя предлагаемые стандартные параметры установки, нажмите на кнопку **Установить** и введите пароль администратора для подтверждения.

   Чтобы выбрать другой диск для установки программы, нажмите на кнопку **Изменить размещение установки** и выберите другой диск, после чего нажмите на кнопку **Продолжить**.

   Диск для установки программы должен быть загрузочным. На диске должна быть установлена операционная система версии не ниже той, которая указана в системных требованиях (см. раздел «Аппаратные и программные требования к системе» на стр. 18).

   Дождитесь, пока программа установки Агента администрирования установит компоненты программы.

8. В окне **Сводка** прочтите информацию об окончании процесса установки и нажмите на кнопку **Закрыть** для завершения работы программы установки.

УСТАНОВКА АГЕНТА АДМИНИСТРИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ SSH-ПРОТОКОЛА

Перед установкой Агента администрирования на удаленный компьютер с использованием SSH-протокола убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Administration Kit развернут в сети предприятия[4].
- Консоль администрирования установлена на рабочее место администратора Kaspersky Administration Kit.
- Инсталляционный пакет Агента администрирования создан и хранится в папке общего доступа Сервера администрирования[5].

Чтобы выполнить установку Агента администрирования на удаленный компьютер с использованием SSH-протокола, выполните следующие действия:

1. Включите службу **Удаленный вход** на компьютере Apple Macintosh.

2. На рабочем месте администратора запустите SSH-клиент и соединитесь с удаленным компьютером Apple Macintosh.

[4] Подробнее смотрите Руководство по внедрению Kaspersky Administration Kit.
[5] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.

3. Подключите папку общего доступа Сервера администрирования в качестве сетевого диска на удаленном компьютере. Для этого в терминале SSH-клиента введите следующие команды:

   ```
   mkdir /Volumes/KLSHARE
   ```

   ```
   mount_smbfs //<admin_login>:<password>@<AK_server_address>/KLSHARE
   /Volumes/KLSHARE
   ```

   Описание параметров:

   - **<admin_login>** – имя учетной записи администратора Сервера администрирования;
   - **<password>** – пароль администратора Сервера администрирования;
   - **<AK_server_address>** – IP-адрес сервера, на котором установлен Kaspersky Administration Kit.

4. Запустите скрипт установки. Для этого в терминале SSH-клиента введите следующие команды:

   ```
   cd /Volumes/KLSHARE/Packages/<klnagent_package_folder>
   ```

   где **<klnagent_package_folder>** – папка, в которой хранится инсталляционный пакет Агента администрирования.

   ```
   sudo ./install.sh -r <сервер> [-s <действие>] [-p <номер порта>] [-l <номер SSL-порта>]
   ```

   Описание параметров:

   - **<действие>** – параметр, определяющий, будет ли использовано шифрование при соединении Агента администрирования с Сервером администрирования. Если указано значение 0, то будет использовано незащищенное соединение. Если указано значение 1, соединение будет осуществляться по SSL-протоколу (значение по умолчанию);
   - **<сервер>** – IP-адрес или DNS-имя сервера, на котором установлен Kaspersky Administration Kit;
   - **<номер порта>** – номер порта, по которому будет осуществляться незащищенное подключение к Серверу администрирования. По умолчанию используется 14000 порт;
   - **<номер SSL-порта>** – номер порта, по которому будет осуществляться защищенное подключение к Серверу администрирования с использованием SSL-протокола. По умолчанию это 13000 порт.

   Для выполнения команды требуются права администратора.

5. Отключите сетевой диск на удаленном компьютере. Для этого в терминале SSH-клиента введите следующую команду:

   ```
   umount /Volumes/KLSHARE
   ```

6. Проверьте работоспособность Агента администрирования на удаленном компьютере. Для этого в терминале SSH-клиента введите следующие команды:

   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   ```

   ```
   sudo ./klnagchk
   ```

   Если проверка прошла успешно, то Агент администрирования функционирует нормально.

ОБНОВЛЕНИЕ АГЕНТА АДМИНИСТРИРОВАНИЯ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Перед запуском обновления Агента администрирования, установленного на удаленном компьютере, убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Administration Kit развернут в сети предприятия[6].
- Консоль администрирования установлена на рабочее место администратора Kaspersky Administration Kit.
- Агент администрирования установлен на компьютер Apple Macintosh.
- Инсталляционный пакет для обновления Агента администрирования создан и хранится в папке общего доступа Сервера администрирования[7].

  В окне свойств инсталляционного пакета на закладке **Подключение** необходимо указать в поле **Адрес сервера** IP-адрес или DNS-имя Сервера администрирования, в поле **Номер порта** номер порта для незащищенного соединения с сервером и в поле **Номер SSL-порта** номер порта для соединения с сервером с использованием SSL. Если вы не хотите использовать SSL для соединения с сервером, снимите флажок **Использовать SSL-соединение**.
- Компьютер Apple Macintosh добавлен в группу **Управляемые компьютеры** Сервера администрирования (по желанию)[8].

Обновление Агента администрирования, установленного на удаленном компьютере, через Kaspersky Administration Kit осуществляется с помощью создания и последующего запуска задачи удаленной установки программы.

Чтобы создать задачу удаленной установки программы на удаленный компьютер через Kaspersky Administration Kit, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**, и выберите папку **Задачи для наборов компьютеров**.
3. В панели задач по ссылке **Создать новую задачу** запустите Мастер создания задачи. Следуйте его шагам, чтобы создать задачу удаленной установки.
4. В окне **Имя задачи** в поле **Имя** введите имя задачи и нажмите на кнопку **Далее**.
5. В окне **Тип задачи** выберите в списке задачу **Удаленная установка программы** для программы Kaspersky Administration Kit и нажмите на кнопку **Далее**.
6. В окне **Инсталляционный пакет** выберите в списке инсталляционный пакет для Агента администрирования и нажмите на кнопку **Далее**.
7. В окне **Метод установки** выберите вариант **Форсированная установка** в качестве метода удаленной установки и нажмите на кнопку **Далее**.
8. В окне **Параметры** нажмите на кнопку **Далее**.
9. В окне **Перезагрузка** выберите вариант **Не перезагружать компьютер** и нажмите на кнопку **Далее**.

Перезагружать компьютер после обновления Агента администрирования не требуется.

[6] Подробнее смотрите Руководство по внедрению Kaspersky Administration Kit.
[7] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.
[8] Подробнее смотрите Руководство администратора Kaspersky Administration Kit.

10. В окне **Перемещение компьютеров** выберите группу, в которую Kaspersky Administration Kit переместит компьютер пользователя после обновления Агента администрирования. Если перемещать компьютер в другую группу администрирования не требуется, выберите вариант **Не перемещать компьютеры**. Нажмите на кнопку **Далее**.

11. В окне **Способ выбора клиентских компьютеров** выберите тот вариант выбора компьютеров для установки программы, который наиболее вам подходит. Вы можете установить программу:

    - на основании данных, полученных в ходе опроса Windows-сети;
    - на основании адресов компьютеров, вводимых вручную.

    Нажмите на кнопку **Далее**.

12. В окне **Клиентские компьютеры** укажите компьютеры, для которых будет создана задача удаленной установки программы в соответствии с вариантом, выбранным на предыдущем шаге. Нажмите на кнопку **Далее**.

13. В окне **Учетная запись** нажмите на кнопку **Далее**.

14. В окне **Расписание запуска задачи** выберите режим запуска задачи: вручную или по установленному расписанию. Для этого выберите из раскрывающегося списка частоту, с которой должна запускаться задача и укажите время запуска задачи. Нажмите на кнопку **Далее**.

15. В последнем окне мастер проинформирует вас об успешном завершении процесса создания задачи. Нажмите на кнопку **Готово** для завершения работы мастера.

Созданная задача появится в дереве консоли в папке **Задачи для наборов компьютеров**.

Удаление Агента администрирования

Чтобы удалить Агент администрирования с компьютера, выполните следующие действия:

1. Откройте содержимое дистрибутива Агента администрирования. Для этого вставьте установочный диск в дисковод.

   Если вы купили Kaspersky Endpoint Security в интернет-магазине, то на веб-сайте «Лаборатории Касперского» будет доступен для скачивания дистрибутив программы в формате ZIP. Распакуйте его и запустите dmg-файл, чтобы увидеть содержимое дистрибутива.

2. Запустите программу удаления Агента администрирования. Для этого в окне с содержимым дистрибутива выберите **Удаление Kaspersky Network Agent**.

   Следуйте шагам программы удаления.

3. В окне **Введение** нажмите на кнопку **Продолжить**.

4. В окне **Информация** прочтите важную информацию. Для запуска процедуры удаления нажмите на кнопку **Удалить** и введите пароль администратора для подтверждения. Дождитесь, пока будет выполнено удаление программы.

5. В окне **Завершение** прочтите информацию об окончании процесса удаления и нажмите на кнопку **Готово** для завершения работы программы удаления.

УДАЛЕННАЯ УСТАНОВКА KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security можно установить на компьютер пользователя следующими способами:

- локально (см. раздел «Установка программы» на стр. 20);
- удаленно с использованием SSH-протокола (см. раздел «Установка программы с использованием SSH-протокола» на стр. 120);
- удаленно через Kaspersky Administration Kit (см. раздел «Установка программы через Kaspersky Administration Kit» на стр. 121).

В этом же разделе описано, как удалить программу с компьютера пользователя через Kaspersky Administration Kit (см. раздел «Удаление программы через Kaspersky Administration Kit» на стр. 122).

В ЭТОМ РАЗДЕЛЕ

УСТАНОВКА ПРОГРАММЫ С ИСПОЛЬЗОВАНИЕМ SSH-ПРОТОКОЛА

Перед установкой Kaspersky Endpoint Security на удаленный компьютер убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Administration Kit развернут в сети предприятия[9].
- Консоль администрирования установлена на рабочее место администратора Kaspersky Administration Kit.
- Инсталляционный пакет для программы Kaspersky Endpoint Security создан и хранится в папке общего доступа Сервера администрирования[10].
- Файл ключа для Kaspersky Endpoint Security хранится в папке общего доступа Сервера администрирования (по желанию).

Чтобы выполнить установку Kaspersky Endpoint Security на удаленный компьютер с использованием SSH-протокола, выполните следующие действия:

1. Включите службу **Удаленный вход** на компьютере Apple Macintosh.
2. На рабочем месте администратора запустите SSH-клиент и установите соединение с удаленным компьютером Apple Macintosh.
3. Подключите папку общего доступа Сервера администрирования в качестве сетевого диска на удаленном компьютере. Для этого в терминале SSH-клиента введите следующие команды:

```
mkdir /Volumes/KLSHARE

mount_smbfs //<admin_login>:<password>@<AK_server_address>/KLSHARE
/Volumes/KLSHARE
```

[9] Подробнее смотрите Руководство по внедрению Kaspersky Administration Kit.
[10] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.

Описание параметров:

- **<admin_login>** – имя учетной записи администратора Сервера администрирования;
- **<password>** – пароль администратора Сервера администрирования;
- **<AK_server_address>** – IP-адрес сервера, на котором установлен Kaspersky Administration Kit.

4. Запустите скрипт установки. Для этого в терминале SSH-клиента введите следующие команды:

```
cd /Volumes/KLSHARE/Packages/<kes_package_folder>
sudo ./install.sh
```

где **<kes_package_folder>** – папка, в которой хранится инсталляционный пакет для Kaspersky Endpoint Security.

Для выполнения команды требуются права администратора.

5. Отключите сетевой диск на удаленном компьютере. Для этого в терминале SSH-клиента введите следующую команду:

```
umount /Volumes/KLSHARE
```

УСТАНОВКА ПРОГРАММЫ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Перед установкой Kaspersky Endpoint Security на удаленный компьютер убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Administration Kit развернут в сети предприятия[11].
- Консоль администрирования установлена на рабочее место администратора Kaspersky Administration Kit.
- Агент администрирования установлен на компьютер Apple Macintosh.
- Инсталляционный пакет для программы Kaspersky Endpoint Security создан и хранится в папке общего доступа Сервера администрирования[12].
- Файл ключа для Kaspersky Endpoint Security хранится в папке общего доступа Сервера администрирования (по желанию).
- Компьютер Apple Macintosh добавлен в группу **Управляемые компьютеры** Сервера администрирования (по желанию)[13].

Установка Kaspersky Endpoint Security на удаленный компьютер через Kaspersky Administration Kit осуществляется с помощью создания и последующего запуска задачи удаленной установки программы.

Чтобы создать задачу удаленной установки Kaspersky Endpoint Security на удаленный компьютер через Kaspersky Administration Kit, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**, и выберите папку **Задачи для наборов компьютеров**.
3. В панели задач по ссылке **Создать новую задачу** запустите Мастер создания задачи. Следуйте его шагам, чтобы создать задачу удаленной установки Kaspersky Endpoint Security.
4. В окне **Имя задачи** в поле **Имя** введите имя задачи и нажмите на кнопку **Далее**.

[11] Подробнее смотрите Руководство по внедрению Kaspersky Administration Kit.
[12] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.
[13] Подробнее смотрите Руководство администратора Kaspersky Administration Kit.

5. В окне **Тип задачи** выберите в списке задачу **Удаленная установка программы** для программы Kaspersky Administration Kit и нажмите на кнопку **Далее**.

6. В окне **Инсталляционный пакет** выберите в списке инсталляционный пакет для программы Kaspersky Endpoint Security и нажмите на кнопку **Далее**.

7. В окне **Метод установки** выберите вариант **Форсированная установка** в качестве метода удаленной установки и нажмите на кнопку **Далее**.

8. В окне **Параметры** настройте параметры удаленной установки программы и нажмите на кнопку **Далее**.

9. В окне **Дополнительно** укажите дополнительный инсталляционный пакет для совместной установки программ, если это необходимо. Нажмите на кнопку **Далее**.

10. В окне **Перезагрузка** выберите вариант **Не перезагружать компьютер** и нажмите на кнопку **Далее**.

    Перезагружать компьютер после установки программы не требуется.

11. В окне **Способ выбора клиентских компьютеров** выберите тот вариант выбора компьютеров для установки программы, который наиболее вам подходит. Вы можете установить программу:

    - на основании данных, полученных в ходе опроса Windows-сети;
    - на основании адресов компьютеров, вводимых вручную.

    Нажмите на кнопку **Далее**.

12. В окне **Клиентские компьютеры** укажите компьютеры, для которых будет создана задача удаленной установки программы в соответствии с вариантом, выбранным на предыдущем шаге. Нажмите на кнопку **Далее**.

13. В окне **Учетная запись** нажмите на кнопку **Далее**.

14. В окне **Расписание запуска задачи** выберите режим запуска задачи: вручную или по установленному расписанию. Для этого выберите из раскрывающегося списка частоту, с которой должна запускаться задача и укажите время запуска задачи. Нажмите на кнопку **Далее**.

15. В последнем окне мастер проинформирует вас об успешном завершении процесса создания задачи. Нажмите на кнопку **Готово** для завершения работы мастера.

Созданная задача появится в дереве консоли в папке **Задачи для наборов компьютеров**.

УДАЛЕНИЕ ПРОГРАММЫ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Удаляя Kaspersky Endpoint Security с удаленного компьютера, вы подвергаете его серьезному риску заражения.

Перед удалением Kaspersky Endpoint Security с удаленного компьютера убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Administration Kit развернут в сети предприятия[14].
- Консоль администрирования установлена на рабочее место администратора Kaspersky Administration Kit.
- Агент администрирования и Kaspersky Endpoint Security установлены на компьютере Apple Macintosh.

Удаление Kaspersky Endpoint Security с клиентского компьютера через Kaspersky Administration Kit осуществляется с помощью создания и последующего запуска задачи удаленной деинсталляции программы.

[14] Подробнее смотрите Руководство по внедрению Kaspersky Administration Kit.

Чтобы создать задачу удаленной деинсталляции Kaspersky Endpoint Security с клиентского компьютера через Kaspersky Administration Kit, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**, и выберите папку **Задачи для наборов компьютеров**.
3. В панели задач по ссылке **Создать новую задачу** запустите Мастер создания задачи. Следуйте его шагам, чтобы создать задачу удаленной установки Kaspersky Endpoint Security.
4. В окне **Имя задачи** в поле **Имя** введите имя задачи и нажмите на кнопку **Далее**.
5. В окне **Тип задачи** выберите в списке программу Kaspersky Administration Kit и задачу **Удаленная деинсталляция программы** в папке **Дополнительно**. Нажмите на кнопку **Далее**.
6. В окне **Параметры** выберите в раскрывающемся списке программу **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Далее**.
7. В окне **Метод удаленной деинсталляции** выберите вариант **Форсированная деинсталляция** в качестве метода удаления программы и нажмите на кнопку **Далее**.
8. В окне **Параметры** настройте параметры удаленной деинсталляции программы и нажмите на кнопку **Далее**.
9. В окне **Перезагрузка** выберите вариант **Не перезагружать компьютер** и нажмите на кнопку **Далее**.

   Перезагружать компьютер после удаления Kaspersky Endpoint Security не требуется.

10. В окне **Клиентские компьютеры** укажите компьютеры, для которых будет создана задача удаленной деинсталляции программы. Нажмите на кнопку **Далее**.
11. В окне **Учетная запись** нажмите на кнопку **Далее**.
12. В окне **Расписание запуска задачи** выберите режим запуска задачи: вручную или по установленному расписанию. Для этого выберите из раскрывающегося списка частоту, с которой должна запускаться задача и укажите время запуска задачи. Нажмите на кнопку **Далее**.
13. В последнем окне мастер проинформирует вас об успешном завершении процесса создания задачи. Нажмите на кнопку **Готово** для завершения работы мастера.

Созданная задача появится в дереве консоли в папке **Задачи для наборов компьютеров**.

УПРАВЛЕНИЕ АГЕНТОМ АДМИНИСТРИРОВАНИЯ

Управление Агентом администрирования осуществляется с использованием командной строки на компьютере пользователя.

Kaspersky Administration Kit предоставляет возможность подключения клиентского компьютера к Серверу администрирования вручную с использованием утилиты klmover и проверки соединения клиентского компьютера с Сервером администрирования посредством утилиты klnagchk.

Также вы можете остановить работу Агента администрирования и запустить его вновь.

В этом разделе

Подключение клиентского компьютера к Серверу администрирования вручную. Утилита klmover

Чтобы подключить клиентский компьютер к Серверу администрирования,

на клиентском компьютере из командной строки запустите утилиту klmover, входящую в состав дистрибутива Агента администрирования.

После установки Агента администрирования данная утилита располагается в папке /Library/Application Support/Kaspersky Lab/klnagent/Binaries и при запуске из командной строки в зависимости от используемых параметров выполняет следующие действия:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в указанный файл или выводит их на экран.

Перед запуском утилиты перейдите в папку /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Синтаксис утилиты:

```
sudo ./klmover [-logfile <имя файла>] [-address <адрес сервера>] [-pn <номер порта>]
[-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent] [-
dupfix]
```

Для запуска утилиты требуются права администратора.

Описание параметров:

-logfile <имя файла> – записать результаты выполнения утилиты в указанный файл; если параметр не указан, результаты и сообщения об ошибках выводятся на экран.

-address <адрес сервера> – адрес Сервера администрирования для подключения; в качестве адреса может быть указан IP-адрес или DNS-имя сервера.

-pn <номер порта> – номер порта, по которому будет осуществляться незащищенное подключение к Серверу администрирования; по умолчанию используется порт 14000.

-ps <номер SSL-порта> – номер порта, по которому будет осуществляться защищенное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию номер порта 13000.

-nossl – использовать незащищенное подключение к Серверу администрирования; если ключ не указан, подключение Агента администрирования к серверу будет осуществляться по защищенному SSL-протоколу.

-cert <путь к файлу сертификата> – использовать указанный файл сертификата для аутентификации на новом Сервере администрирования. Если параметр не указан, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.

-silent – запустить утилиту на выполнение в неинтерактивном режиме.

-dupfix – данный параметр используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.

Рекомендуется запускать утилиту, указывая значения всех параметров.

Пример:

```
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001
```

Проверка соединения клиентского компьютера и Сервера администрирования вручную. Утилита klnagchk

Чтобы проверить соединение клиентского компьютера с Сервером администрирования,

на клиентском компьютере из командной строки запустите утилиту klnagchk, входящую в состав дистрибутива Агента администрирования.

После установки Агента администрирования данная утилита располагается в папке /Library/Application Support/Kaspersky Lab/klnagent/Binaries, и при запуске из командной строки в зависимости от используемых параметров выполняет следующие действия:

- выводит на экран или заносит в указанный файл значения параметров подключения установленного на клиентском компьютере Агента администрирования к Серверу администрирования;
- записывает в указанный файл статистику работы Агента администрирования (с момента последнего запуска данного компонента) и результаты выполнения утилиты, либо выводит информацию на экран;
- предпринимает попытку установить соединение Агента администрирования с Сервером администрирования;
- если соединение установить не удалось, посылает ICMP-пакет для проверки статуса компьютера, на котором установлен Сервер администрирования.

Перед запуском утилиты перейдите в папку /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Синтаксис утилиты:

```
sudo ./klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>]
[-restart]
```

Для запуска утилиты требуются права администратора.

Описание параметров

-logfile <имя файла> – записать значения параметров подключения Агента администрирования к Серверу администрирования и результаты выполнения утилиты в указанный файл; если параметр не указан, параметры подключения к серверу, результаты и сообщения об ошибках выводятся на экран.

-sp – отобразить пароль для аутентификации пользователя на прокси-сервере на экране или записать его в файл для логирования; параметр используется, если подключение к серверу администрирования осуществляется через прокси-сервер. По умолчанию не используется.

-savecert <имя файла> – сохранить сертификат для аутентификации на Сервере администрирования в указанном файле.

-restart – перезапустить Агент администрирования после завершения работы утилиты.

Пример:

```
sudo ./klnagchk -logfile klnagchk.log -sp
```

ЗАПУСК / ОСТАНОВКА АГЕНТА АДМИНИСТРИРОВАНИЯ НА КЛИЕНТСКОМ КОМПЬЮТЕРЕ

Вы можете остановить работу Агента администрирования и запустить его вновь на компьютере пользователя посредством командной строки.

- *Чтобы остановить работу Агента администрирования,*

  на клиентском компьютере из командной строки запустите утилиту launchctl с командой unload.

Синтаксис команды

```
launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

- *Чтобы запустить Агент администрирования,*

  на клиентском компьютере из командной строки запустите утилиту launchctl с командой load.

Синтаксис команды

```
launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Для остановки и запуска Агента администрирования требуются права администратора.

УПРАВЛЕНИЕ ПРОГРАММОЙ

Kaspersky Administration Kit предоставляет возможность удаленного управления запуском и остановкой Kaspersky Endpoint Security на отдельном клиентском компьютере, а также настройки общих параметров работы программы: включения и выключения защиты файловой системы компьютера, настройки отображения значка Kaspersky Endpoint Security, настройки параметров отчетов и хранилищ.

- *Чтобы перейти к настройке параметров работы программы, выполните следующие действия:*

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**.
3. В папке **Управляемые компьютеры** выберите папку с названием группы, в которую входит клиентский компьютер, а в ней выберите вложенную папку **Клиентские компьютеры**.
4. В панели результатов справа выберите компьютер, на котором установлена программа Kaspersky Endpoint Security.
5. В контекстном меню, открывающемся по правой клавише мыши, выберите пункт **Свойства**. Откроется окно свойств клиентского компьютера.
6. На закладке **Программы** (см. рис. ниже) в списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac**.

Под списком программ расположены кнопки управления:

- **События**. При нажатии на эту кнопку открывается окно **События**, в котором представлен список событий в работе программы, произошедших на клиентском компьютере и зарегистрированных на Сервере администрирования;
- **Статистика**. При нажатии на эту кнопку открывается окно **Статистика**, в котором вы можете просмотреть текущую статистическую информацию о работе программы;
- **Свойства**. При нажатии на эту кнопку открывается окно настройки параметров программы (см. раздел «Настройка параметров программы» на стр. 129).

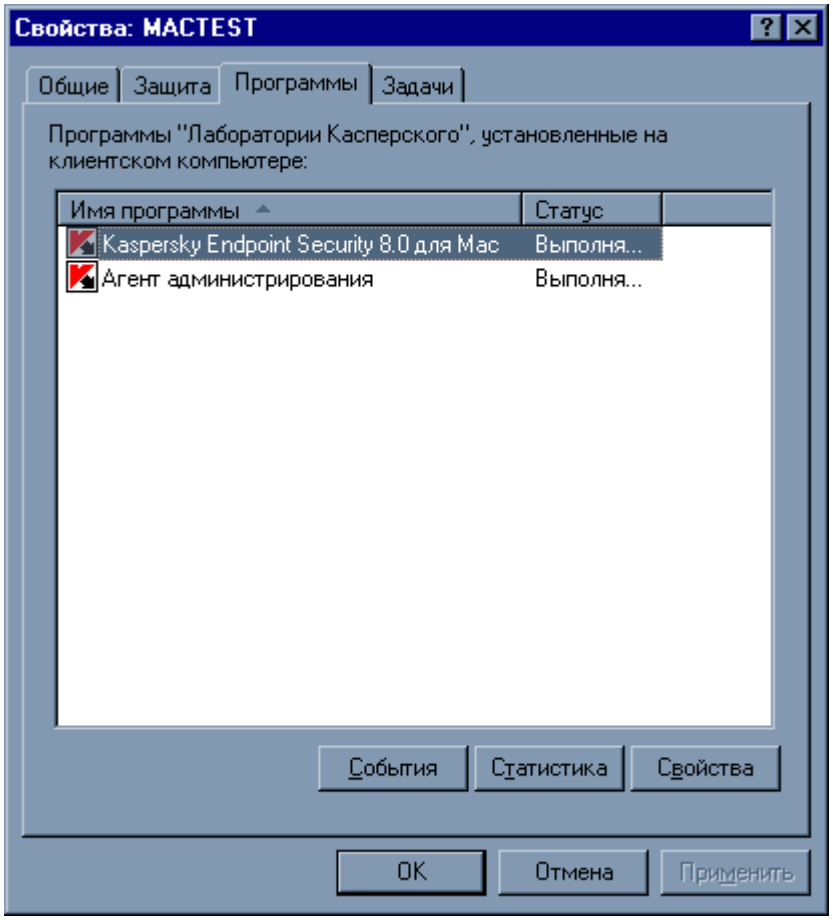


Рисунок 58. Окно свойств клиентского компьютера. Закладка Программы

В этом разделе

Запуск и остановка программы

Управление запуском и остановкой Kaspersky Endpoint Security на удаленном клиентском компьютере осуществляется на закладке **Общие** окна настройки параметров программы.

В верхней части окна приведены название программы, информация о ее версии, дата установки и последнего обновления, ее текущее состояние (выполняется или остановлена на локальном компьютере), а также информация о состоянии баз программы.

Чтобы остановить или запустить Kaspersky Endpoint Security на удаленном компьютере, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.

2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.

3. В открывшемся окне настройки параметров программы (см. рис. ниже) выберите закладку **Общие** и нажмите на кнопку **Остановить** для остановки программы или **Запустить** для ее запуска. Подождите пока Kaspersky Administration Kit выполнит действие на удаленном клиентском компьютере.

После остановки работы Kaspersky Endpoint Security на удаленном компьютере он продолжит работать в незащищенном режиме и может быть подвергнут риску заражения.

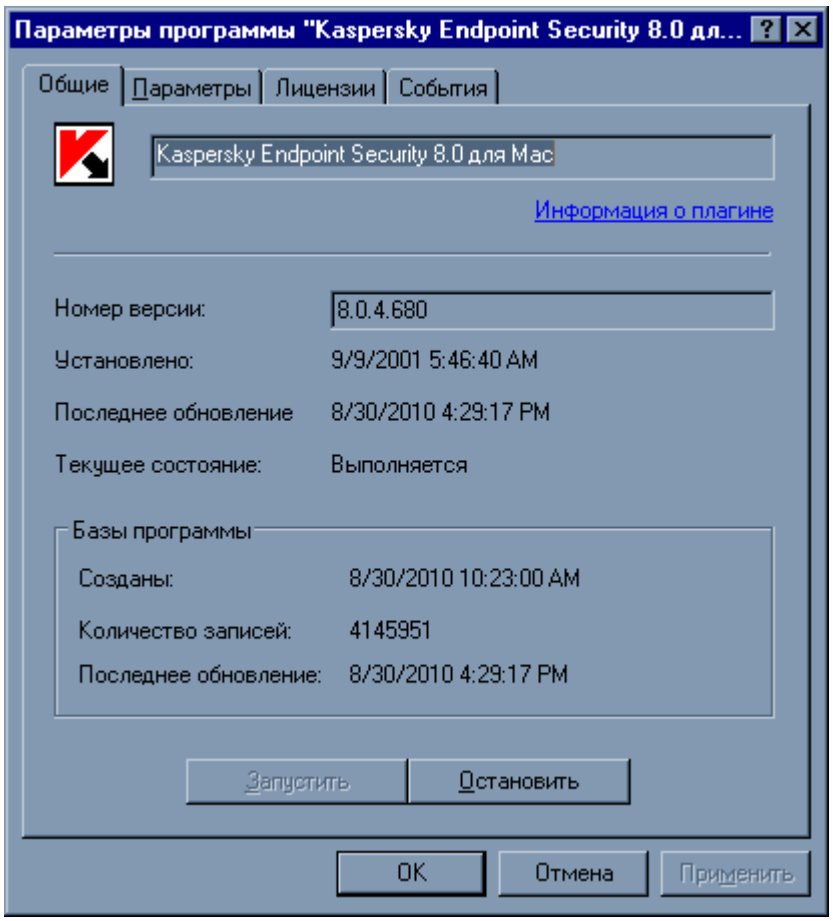


Рисунок 59. Окно настройки параметров программы. Закладка Общие

Настройка параметров программы

Просмотреть и изменить параметры работы программы на удаленном клиентском компьютере вы можете на закладке **Параметры** окна настройки параметров программы (см. рис. ниже).

Закладки **Лицензии** и **События** являются стандартными для программы Kaspersky Administration Kit[15].

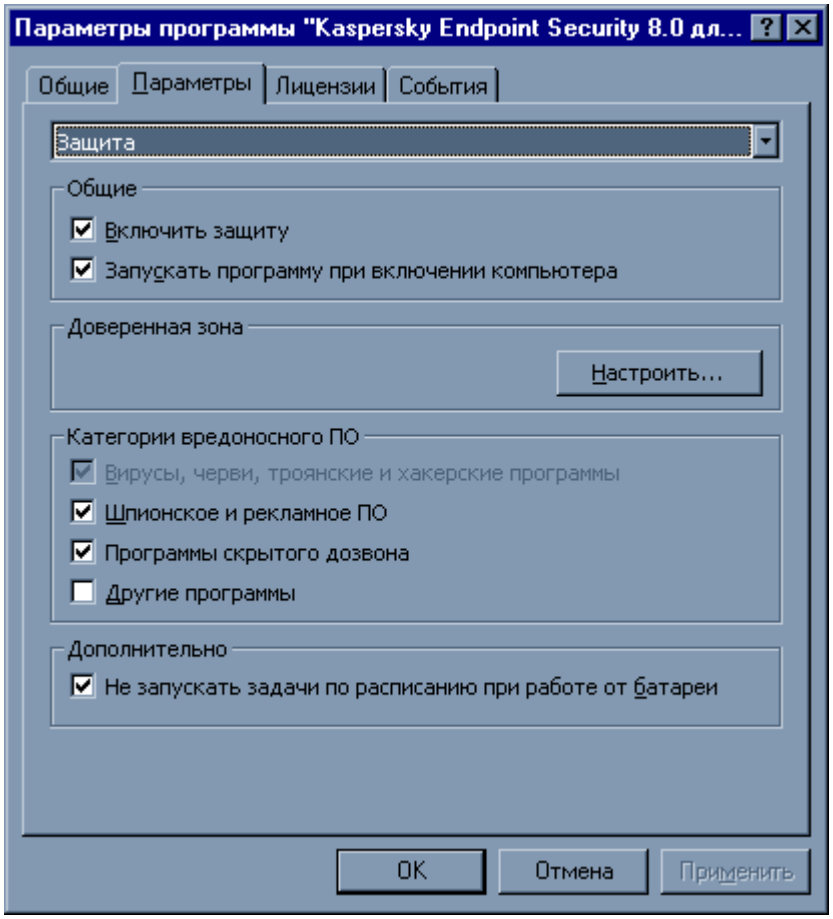


Рисунок 60. Окно настройки параметров программы. Закладка Параметры. Защита

Если для программы создана политика, в которой запрещено переопределение некоторых параметров, то их изменение при настройке параметров программы будет недоступно.

Включение и выключение защиты файлов

Специалисты «Лаборатории Касперского» настоятельно рекомендуют не отключать защиту, обеспечиваемую Файловым Антивирусом в режиме реального времени на удаленном компьютере, поскольку это может привести к его заражению и потере данных.

Чтобы выключить Файловый Антивирус на удаленном компьютере, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.

[15] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.

2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.

3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.

4. В раскрывающемся списке, расположенном в верхней части окна, выберите **Защита**.

5. В блоке **Общие** (см. рис. ниже) снимите флажок **Включить защиту** и нажмите на кнопку **Применить**.

Чтобы включить Файловый Антивирус на удаленном компьютере, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.

2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.

3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.

4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Защита**.

5. В блоке **Общие** (см. рис. ниже) установите флажок **Включить защиту** и нажмите на кнопку **Применить**.

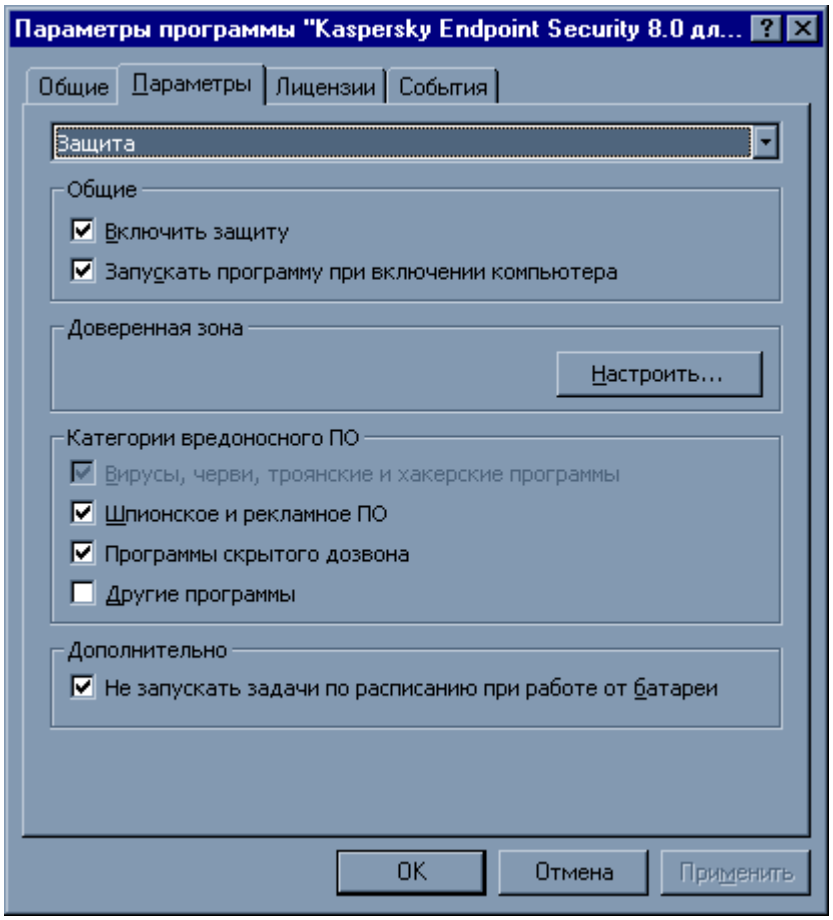


Рисунок 61. Окно настройки параметров программы. Закладка Параметры. Защита

См. также

Файловый Антивирус 57

Настройка автозапуска Kaspersky Endpoint Security

По умолчанию Kaspersky Endpoint Security запускается автоматически на удаленном компьютере при его включении или после перезагрузки операционной системы.

Чтобы выключить режим автозапуска Kaspersky Endpoint Security на удаленном компьютере, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.
2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.
3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.
4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Защита**.
5. В блоке **Общие** (см. рис. выше) снимите флажок **Запускать программу при включении компьютера** и нажмите на кнопку **Применить**.

Выключение режима автозапуска Kaspersky Endpoint Security на удаленном компьютере приведет к тому, что при следующем его включении или после перезагрузки операционной системы он будет работать в незащищенном режиме и может быть подвергнут риску заражения.

Формирование доверенной зоны

Чтобы создать новое правило исключения или просмотреть и изменить уже созданные правила исключения для Kaspersky Endpoint Security, установленного на удаленном компьютере, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.
2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.
3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.
4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Защита**.
5. В блоке **Доверенная зона** (см. рис. выше) нажмите на кнопку **Настроить**. Откроется окно **Доверенная зона** (см. рис. ниже) со списком объектов, которые Kaspersky Endpoint Security не будет контролировать в процессе своей работы.

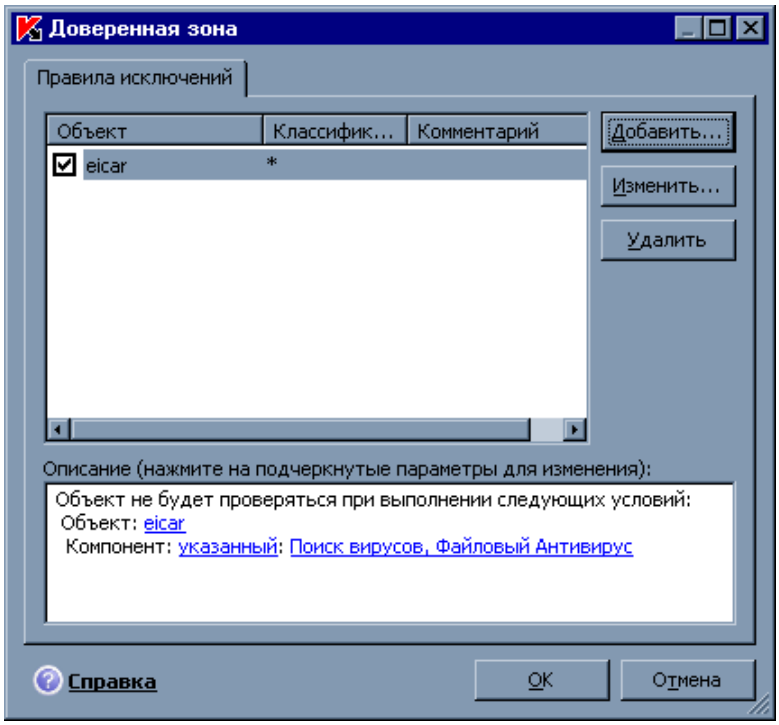


Рисунок 62. Окно Доверенная зона

Вы можете выполнить следующие действия:

- Создать новое правило исключения.

  Нажмите на кнопку **Добавить** и в открывшемся окне **Правило исключения** (см. рис. ниже) задайте его условия.

- Изменить уже созданное правило исключения.

  Выберите правило исключения в списке и нажмите на кнопку **Изменить**. В открывшемся окне **Правило исключения** внесите изменения в его условия.

- Временно отказаться от использования правила исключения.

  Выберите правило исключения в списке и снимите флажок рядом с ним. Правило исключения перестанет применяться до тех пор, пока флажок не будет вновь установлен.

- Удалить правило исключения.

  Выберите правило исключения в списке и нажмите на кнопку **Удалить**.

Создание правила исключения

В открывшемся окне **Правило исключения** задайте условия правила исключения соответствии со следующими параметрами:

- **Объект**. Установите флажок **Объект** в поле **Параметры**, если в качестве объекта исключения будет указан файл, папка или маска файла. Чтобы указать имя / маску имени объекта, по ссылке **Объект:** в поле **Описание** откройте окно **Имя объекта** и введите имя файла, папки или маску файла.

- **Классификация**. Установите флажок **Классификация** в поле **Параметры**, чтобы исключить из проверки объекты, исходя из типа угрозы, присвоенного согласно классификации Вирусной энциклопедии. Чтобы указать имя / маску угрозы, по ссылке **Классификация:** откройте окно **Классификация** и введите имя или маску угрозы, согласно классификации Вирусной энциклопедии.

- **Компонент**. Чтобы указать компоненты Kaspersky Endpoint Security, в работе которых должно быть использовано создаваемое правило, по ссылке **Компонент:** в поле **Описание** откройте окно **Исключающие компоненты / задачи** и установите флажки рядом с названиями компонентов: **Файловый Антивирус** или **Поиск вирусов**.

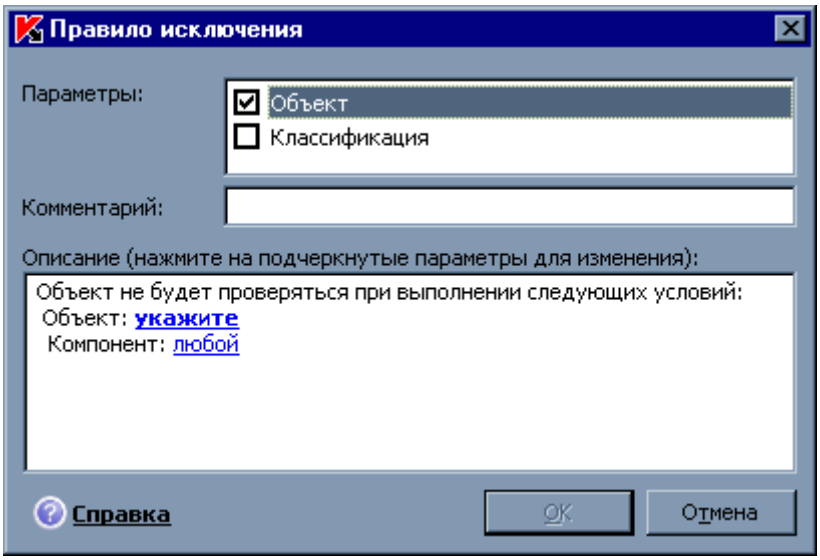


Рисунок 63. Окно Правило исключения

См. также

Формирование доверенной зоны 54

Выбор контролируемых вредоносных программ

Чтобы выбрать группы вредоносного программного обеспечения, от которых Kaspersky Endpoint Security будет защищать удаленный компьютер, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.
2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.
3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.
4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Защита**.
5. В блоке **Категории вредоносного ПО** (см. рис. ниже) установите флажок рядом с теми группами вредоносных программ, защиту от которых должен обеспечивать Kaspersky Endpoint Security.

Kaspersky Endpoint Security обеспечивает защиту компьютера от вирусов, червей, троянских и хакерских программ. Поэтому снять флажок рядом с этой группой невозможно. Специалисты «Лаборатории Касперского» не рекомендуют отключать контроль за шпионским, рекламным программным обеспечением и программами скрытого дозвона. Если Kaspersky Endpoint Security относит программу, которая, по вашему мнению, не является опасной, к категории нежелательных программ, рекомендуется настроить для нее правило исключения (см. раздел «Формирование доверенной зоны» на стр. 131).

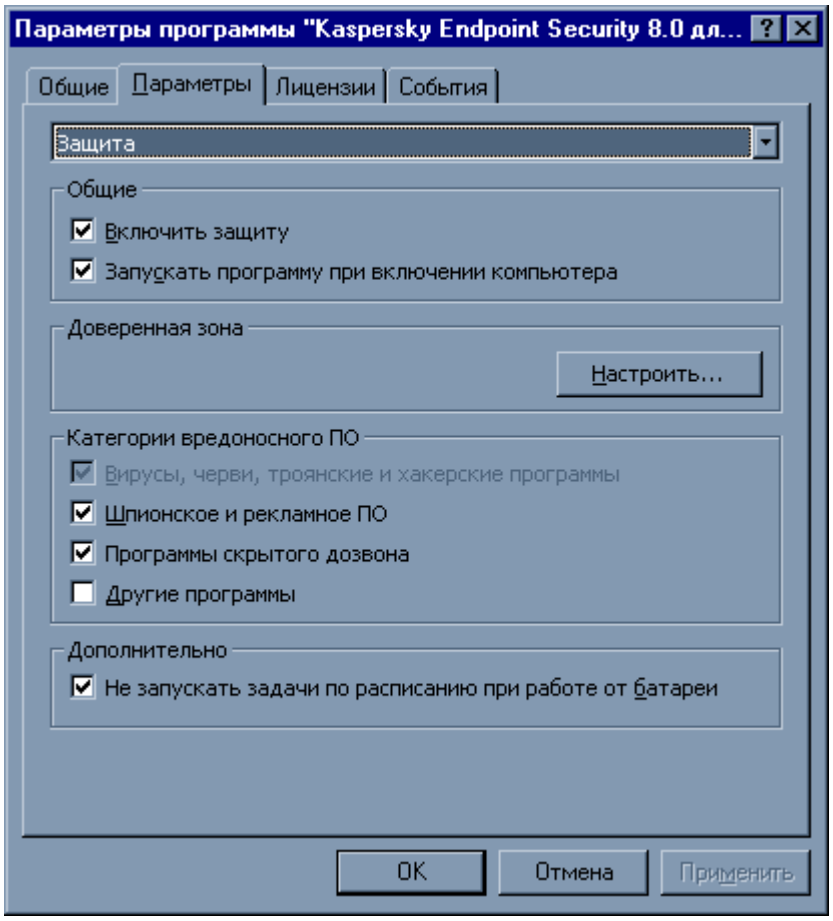


Рисунок 64. Окно настройки параметров программы. Закладка Параметры. Защита

См. также

Выбор контролируемых вредоносных программ 52

Настройка режима экономичного энергопотребления

По умолчанию Kaspersky Endpoint Security работает в режиме экономичного энергопотребления. В таком режиме задачи поиска вирусов, для которых установлено расписание их запуска, не будут запущены, если компьютер, на котором установлена программа работает от батареи.

Чтобы отключить режим экономичного энергопотребления на удаленном компьютере, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.
2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.
3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.
4. В раскрывающемся списке, расположенном в верхней части окна выберите элемент **Защита**.
5. В блоке **Дополнительно** (см. рис. выше) снимите флажок **Не запускать задачи по расписанию при работе от батареи**.

НАСТРОЙКА ПОЛУЧЕНИЯ УВЕДОМЛЕНИЙ

Чтобы настроить получение уведомления о событиях, возникающих на удаленном компьютере, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.

2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.

3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.

4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Взаимодействие с пользователем**.

5. В блоке **Уведомление о событиях** (см. рис. ниже) установите флажок **Включить уведомления о событиях** и перейдите к детальной настройке. Для этого нажмите на кнопку **Дополнительно**.

В открывшемся окне вы можете настроить следующие способы получения уведомлений о перечисленных событиях:

- *Всплывающее экранное сообщение*, содержащее информацию о возникшем событии.

  Чтобы использовать данный тип уведомления, в графе **Экран** установите флажок напротив события, о котором вы хотите быть уведомлены.

- *Звуковое оповещение*.

  Если вы хотите, чтобы уведомление сопровождалось звуковым сигналом, в графе **Звук** установите флажок напротив события.

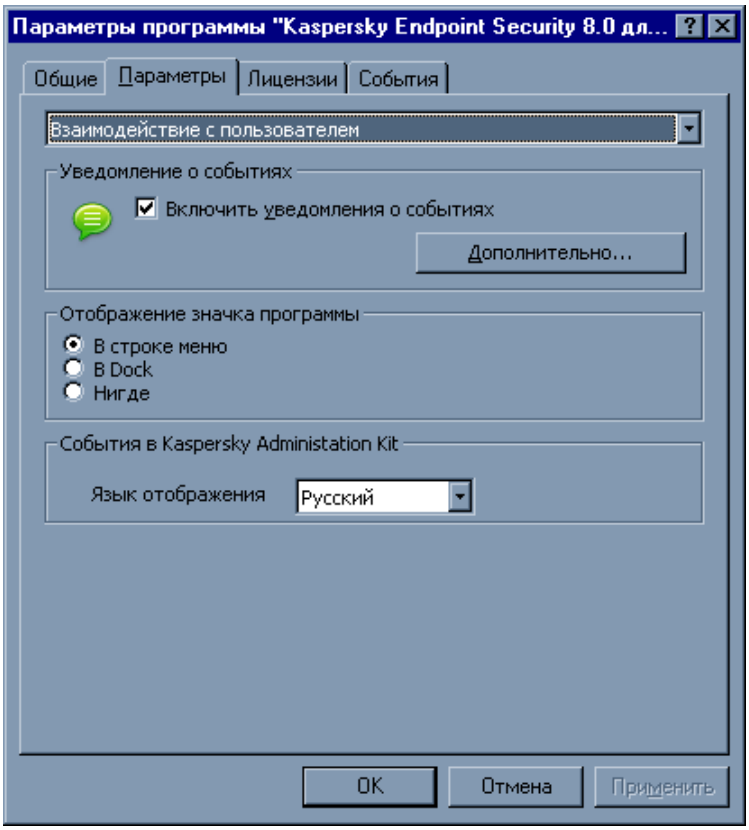


Рисунок 65. Окно настройки параметров программы. Закладка Параметры. Взаимодействие с пользователем

См. также

Окна уведомлений и всплывающие сообщения 37

Настройка отображения значка Kaspersky Endpoint Security

По умолчанию значок Kaspersky Endpoint Security располагается в строке меню. Вы можете изменить настройки программы так, чтобы значок программы отображался на удаленном компьютере в Dock или не отображался вообще.

- *Чтобы выбрать отображение значка программы на удаленном компьютере в панели быстрого запуска Dock, выполните следующие действия:*

  1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.
  2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.
  3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.
  4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Взаимодействие с пользователем**.
  5. В блоке **Отображение значка программы** (см. рис. выше) выберите вариант **В Dock**.

- *Чтобы отключить отображение значка программы на удаленном компьютере, выполните следующие действия:*

  1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.
  2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.
  3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.
  4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Взаимодействие с пользователем**.
  5. В блоке **Отображение значка программы** (см. рис. выше) выберите вариант **Нигде**.

Обратите внимание: изменение параметра вступит в силу только после перезапуска Kaspersky Endpoint Security.

См. также

Значок Kaspersky Endpoint Security 32

Настройка параметров отчетов

- *Чтобы настроить параметры формирования и хранения отчетов о работе Kaspersky Endpoint Security на удаленном компьютере, выполните следующие действия:*

  1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.

2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.

3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.

4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Отчеты и Хранилища**.

5. В блоке **Отчеты** (см. рис. ниже) настройте следующие параметры:

   - Разрешить запись в отчет событий информационного характера.

     Как правило, такие события не важны для обеспечения защиты. Чтобы фиксировать их в отчете, установите флажок **Записывать некритические события**.

   - Сохранять в отчете только важные события, произошедшие при последнем запуске задачи.

     Это позволит сэкономить место на диске за счет уменьшения размера отчета. Если флажок **Хранить только текущие события** установлен, информация, представленная в отчете, будет обновляться при каждом перезапуске задачи: при этом важная информация (например, записи об обнаруженных вредоносных объектах) будет сохранена, а информация некритического характера будет удалена.

   - Установить срок хранения отчетов.

     По умолчанию срок хранения отчетов составляет 30 дней. По истечении этого времени отчеты удаляются. Вы можете изменить максимальный срок хранения или отменить это ограничение.

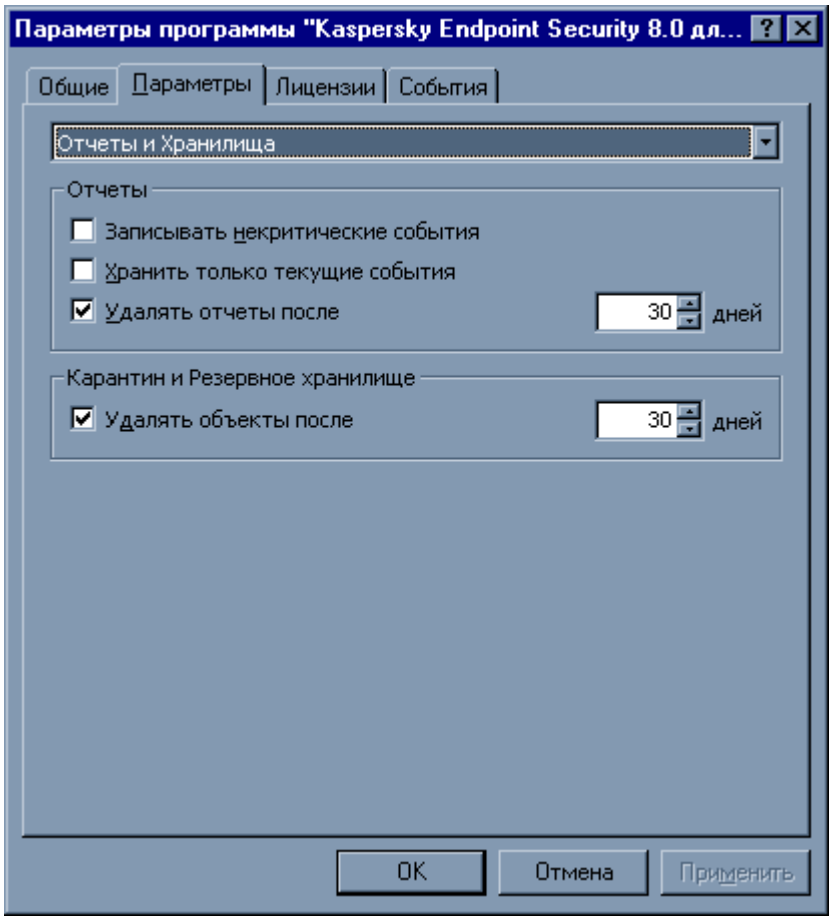


Рисунок 66. Окно настройки параметров программы. Закладка Параметры. Отчеты и Хранилища

НАСТРОЙКА ПАРАМЕТРОВ КАРАНТИНА И РЕЗЕРВНОГО ХРАНИЛИЩА

Вы можете определить максимальный срок хранения объектов в хранилище карантина и резервном хранилище на удаленном компьютере. По умолчанию срок хранения объектов составляет 30 дней; по истечении этого срока объекты удаляются. Вы можете изменить максимальный срок хранения объектов в хранилищах или отменить это ограничение.

Чтобы настроить параметры хранения объектов в хранилищах, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.
2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.
3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.
4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Отчеты и Хранилища**.
5. В блоке **Карантин и Резервное хранилище** (см. рис. выше) установите флажок **Удалять объекты после** и укажите период, по истечении которого объекты, находящиеся в хранилищах, будут автоматически удалены.

НАСТРОЙКА ПАРАМЕТРОВ ПОДКЛЮЧЕНИЯ К ПРОКСИ-СЕРВЕРУ

Если выход в интернет с удаленного клиентского компьютера осуществляется через прокси-сервер, настройте параметры подключения к нему. Kaspersky Endpoint Security использует данные параметры для обновления антивирусных баз и модулей.

Чтобы настроить параметры подключения удаленного компьютера к прокси-серверу, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Программы**.
2. В списке всех программ «Лаборатории Касперского», установленных на данном компьютере, выберите **Kaspersky Endpoint Security 8.0 для Mac** и нажмите на кнопку **Свойства**.
3. В открывшемся окне настройки параметров программы выберите закладку **Параметры**.
4. В раскрывающемся списке, расположенном в верхней части окна, выберите элемент **Настройка сети**.
5. Установите флажок **Использовать прокси-сервер** (см. рис. ниже) и настройте следующие параметры подключения к прокси-серверу:
   - использование Kaspersky Endpoint Security параметров прокси-сервера, указанных в системных настройках Mac OS X или заданных пользователем адреса прокси-сервера и порта;
   - возможность использования прокси-сервера при обновлении из локальной или сетевой папки;
   - параметры аутентификации для соединения с прокси-сервером.

В случае обновления с FTP-сервера по умолчанию устанавливается соединение с сервером в пассивном режиме. При ошибке данного соединения выполняется попытка соединения в активном режиме.

По умолчанию время, отведенное на соединение с сервером обновлений, составляет одну минуту. Если соединение не было установлено, по истечении данного времени предпринимается попытка соединения со следующим источником обновлений из списка. Перебор проводится до тех пор, пока процесс соединения не завершится успешно, или пока не будут опрошены все доступные источники обновлений.

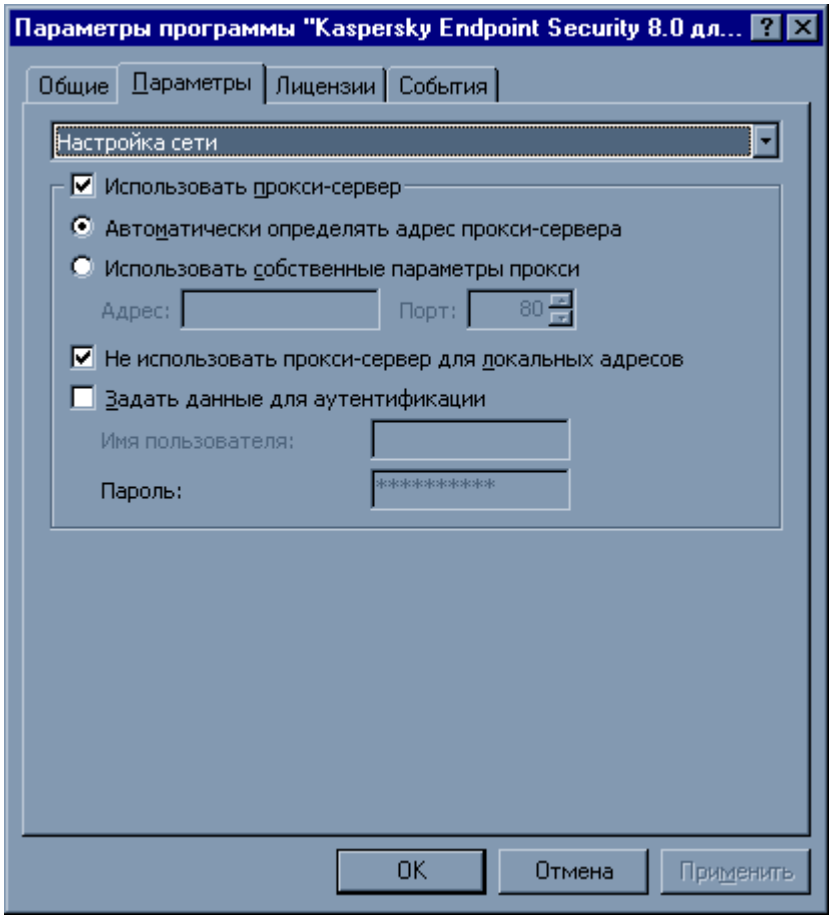


Рисунок 67. Окно настройки параметров программы. Закладка Параметры. Настройка сети

Управление задачами

В данном разделе приведена информация об управлении задачами для Kaspersky Endpoint Security[16].

При установке программы для каждого компьютера сети формируется набор системных задач. В этот список входят задачи защиты (Файловый Антивирус), ряд задач поиска вирусов (Полная проверка, Быстрая проверка) и задачи обновления (обновление баз и модулей программы, откат обновления).

Вы можете управлять запуском системных задач, настраивать их параметры. Удаление системных задач невозможно.

Можно также создавать пользовательские задачи, например, задачи поиска вирусов, обновления программы и отката обновления, задачу установки файла ключа.

[16] Подробнее смотрите Руководство администратора Kaspersky Administration Kit.

Над пользовательскими задачами вы можете выполнять следующие действия[17]:

- настраивать параметры задачи;
- отслеживать выполнение задачи;
- копировать и переносить задачи из одной группы в другую, а также удалять задачи при помощи контекстного меню;
- импортировать и экспортировать задачи.

Чтобы просмотреть список задач, сформированных для клиентского компьютера, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**.
3. В папке **Управляемые компьютеры** выберите папку с названием группы, в которую входит клиентский компьютер, а в ней выберите вложенную папку Клиентские компьютеры.
4. В панели результатов справа выберите компьютер, на котором установлена программа Kaspersky Endpoint Security.
5. В контекстном меню, открывающемся по правой клавише мыши, выберите пункт **Свойства**. Откроется окно свойств клиентского компьютера.
6. Выберите закладку **Задачи** (см. рис. ниже), чтобы просмотреть полный перечень задач, сформированных для данного клиентского компьютера.

   Под списком задач расположены кнопки управления:

   - **Добавить**. При нажатии на эту кнопку откроется Мастер создания задачи (на стр. 143). Вы можете создать новую задачу для программ «Лаборатории Касперского», установленных на этом компьютере.
   - **Удалить**. При нажатии на эту кнопку появляется окно запроса подтверждения действия, после чего выбранная в списке задача удаляется.
   - **Результаты**. При нажатии на эту кнопку открывается окно **Результаты выполнения задачи**.
   - **Свойства**. При нажатии на эту кнопку открывается окно свойств задачи. Вы можете просмотреть параметры задачи и внести изменения, если требуется.

[17] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.

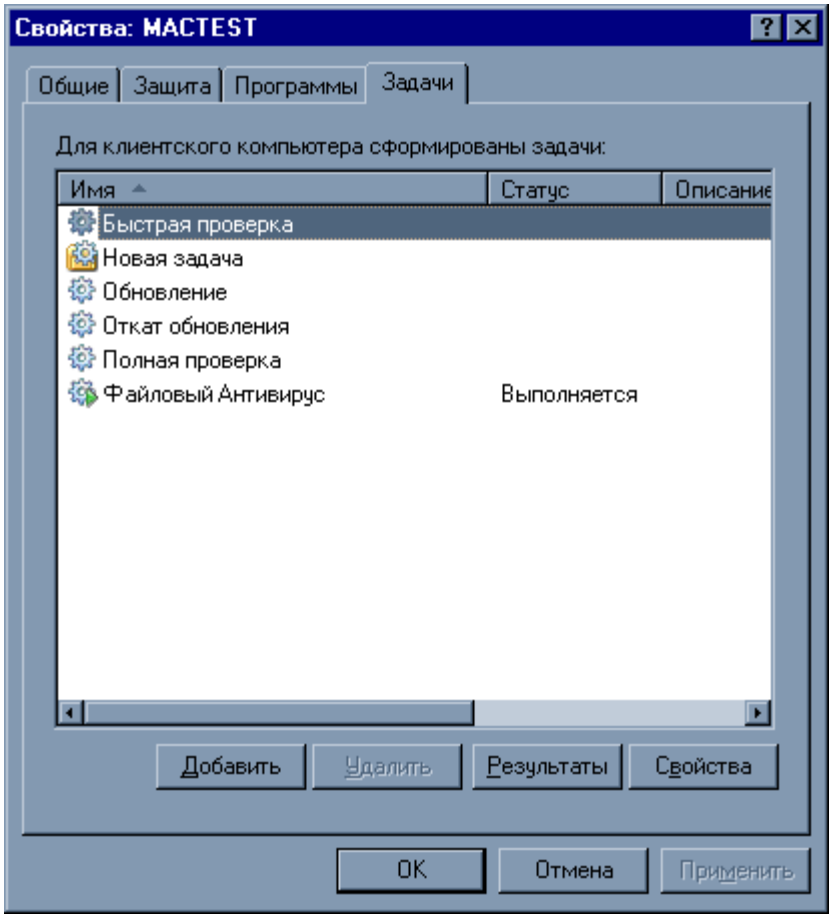


Рисунок 68. Окно свойств клиентского компьютера. Закладка Задачи

В этом разделе

Запуск и остановка задач

Запуск задач на удаленном компьютере выполняется только в том случае, если запущен Агент администрирования. При остановке работы Агента администрирования выполнение запущенных задач прекращается.

Запуск и остановка задач осуществляется автоматически (в соответствии с расписанием) или вручную (при помощи команд контекстного меню), а также из окна свойств задачи.

Чтобы запустить или остановить выполнение задачи вручную, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Задачи** (см. рис. выше).

2. Выберите нужную задачу в списке, затем в контекстном меню, открывающемся по правой клавише мыши, выберите необходимый пункт – **Запустить** или **Остановить**.

   или

   Выберите нужную задачу в списке и нажмите на кнопку **Свойства**. В открывшемся окне свойств задачи на закладке **Общие** при помощи соответствующих кнопок запустите или остановите выполнение задачи.

СОЗДАНИЕ ЗАДАЧ

При работе с Kaspersky Endpoint Security через Kaspersky Administration Kit вы можете создавать следующие типы задач:

- локальные задачи, определяемые для отдельного клиентского компьютера;
- групповые задачи, определяемые для клиентских компьютеров, входящих в группы администрирования;
- задачи для наборов компьютеров, определяемые для компьютеров вне групп администрирования;
- задачи Kaspersky Administration Kit – специфические задачи сервера обновления: задачи получения обновлений, задачи резервного копирования и задачи отправки отчетов.

Задачи для наборов компьютеров выполняются только для заданного набора компьютеров. Например, если в состав группы, для компьютеров которой сформирована задача удаленной установки, будут добавлены новые клиентские компьютеры, для них данная задача выполняться не будет. Необходимо создать новую задачу или внести соответствующие изменения в параметры уже существующей задачи.

Чтобы создать локальную задачу, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Задачи** (см. рис. выше).
2. Нажмите на кнопку **Добавить**. Откроется Мастер создания задачи (на стр. 143). Следуйте его шагам, чтобы создать новую задачу для клиентского компьютера.

Чтобы создать групповую задачу, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**.
3. В папке **Управляемые компьютеры** выберите папку с названием группы, для компьютеров которой вы хотите создать задачу, а в ней выберите вложенную папку **Групповые задачи**.
4. По ссылке **Создать новую задачу** в панели задач откройте Мастер создания задачи. Следуйте его шагам, чтобы создать новую групповую задачу. Информация об особенностях создания групповых задач представлена в Справочном руководстве Kaspersky Administration Kit.

Чтобы создать задачу для наборов компьютеров (задачу Kaspersky Administration Kit), выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Выберите папку **Задачи для наборов компьютеров** (**Задачи Kaspersky Administration Kit**).
3. По ссылке **Создать новую задачу** в панели задач откройте Мастер создания задачи. Следуйте его шагам, чтобы создать новую задачу для набора компьютеров или задачу Kaspersky Administration Kit. Информация об особенностях создания задач Kaspersky Administration Kit или задач для наборов компьютеров представлена в Справочном руководстве Kaspersky Administration Kit.

Мастер создания задачи

Создавать новые задачи для для программ «Лаборатории Касперского», установленных на отдельном клиентском компьютере, вы можете с помощью Мастера создания задачи.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Чтобы открыть Мастер создания задачи, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Задачи**.

2. Нажмите на кнопку **Добавить**.

Шаг 1. Ввод общих данных о задаче

В окне **Имя задачи** в поле **Имя** укажите имя создаваемой задачи.

Шаг 2. Выбор программы и типа задачи

В окне **Тип задачи** выберите программу «Лаборатории Касперского», для которой создается задача: **Kaspersky Endpoint Security 8.0 для Mac** или **Агент администрирования**, а затем тип создаваемой задачи. Для Kaspersky Endpoint Security можно создать задачи следующих типов:

- **Обновление** – задача получения и установки пакета обновлений для программы.
- **Откат обновления** – задача отката последнего произведенного обновления программы.
- **Поиск вирусов** – задача проверки на вирусы указанных пользователем областей.
- **Установка файла ключа** – задача установки файла ключа новой лицензии.

Для Агента администрирования возможно создание задачи **Смена Сервера администрирования**[18].

Шаг 3. Настройка параметров выбранного типа задачи

В зависимости от выбранного на предыдущем шаге типа задачи содержимое окна настройки параметров задачи может быть различным.

Поиск вирусов

В окне **Поиск вирусов** выполните следующие действия:

1. Сформируйте список объектов проверки для задачи поиска вирусов. Вы можете добавлять объекты в список и удалять их, если это необходимо. Нажмите на кнопку **Далее**, чтобы продолжить настройку.

2. Укажите действие, которое будет выполнять Kaspersky Endpoint Security при обнаружении зараженного или возможно зараженного объекта.

Обновление

В окне **Обновление** для задачи обновления антивирусных баз и модулей программы требуется указать источник, из которого будут загружены обновления. По умолчанию обновление выполняется с Сервера

[18] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.

администрирования и с серверов обновлений «Лаборатории Касперского». Отредактируйте список источников обновлений, если это необходимо.

Откат обновления

Задача отката обновления не имеет специфических настроек.

Установка файла ключа

В окне **Управление лицензиями** нажмите на кнопку **Обзор** и в открывшемся стандартном окне укажите путь к файлу ключа. Если файл ключа добавляется в качестве файла ключа для дополнительной лицензии, установите флажок **Добавить файл ключа как резервный**. Дополнительная лицензия вступает в силу по окончании срока действия используемой лицензии.

Информация об установленном файле ключа(номер ключа, его тип, а также дата окончания срока действия ключа) приводится ниже.

Смена Сервера администрирования.

В окне **Параметры** укажите параметры, которые Агент администрирования, установленный на клиентских компьютерах, будет использовать для подключения к новому Серверу администрирования.[19]

Шаг 4. Настройка расписания

В окне **Расписание запуска задачи** выберите режим запуска задачи: вручную или по установленному расписанию.

Для этого выберите из раскрывающегося списка частоту, с которой должна запускаться задача и укажите время запуска задачи.

Шаг 5. Завершение создания задачи

В последнем окне мастер проинформирует вас об успешном завершении процесса создания задачи. Нажмите на кнопку **Готово** для завершения работы мастера.

Настройка параметров задачи

Настройка параметров задачи Kaspersky Endpoint Security через интерфейс Kaspersky Administration Kit аналогична их настройке через локальный интерфейс программы. Исключение составляют параметры, которые настраиваются индивидуально для каждого пользователя, а также параметры, специфичные для Kaspersky Administration Kit: например, параметры, разрешающие (запрещающие) пользователю управлять локальной задачей поиска вирусов.

Если для программы создана политика, в которой запрещено переопределение некоторых параметров, их изменение при настройке задач будет недоступно.

Все закладки окна свойств задачи, кроме закладки **Параметры**, стандартны для программы Kaspersky Administration Kit[20]. Закладка **Параметры** содержит специфические параметры Kaspersky Endpoint Security, которые различаются в зависимости от выбранного типа задачи.

[19] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.
[20] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.

- *Чтобы перейти к просмотру и редактированию параметров локальной задачи, выполните следующие действия:*

  1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Задачи**.

  2. Выберите нужную задачу в списке и нажмите на кнопку **Свойства**. Откроется окно свойств задачи (см. рис. ниже).

- *Чтобы перейти к просмотру и настройке параметров групповых задач, выполните следующие действия:*

  1. Запустите Консоль администрирования Kaspersky Administration Kit.

  2. Разверните узел **Сервер администрирования**.

  3. В папке **Управляемые компьютеры** выберите папку с названием нужной группы, а в ней выберите вложенную папку **Групповые задачи**.

  4. В дереве консоли выберите нужную задачу для перехода к просмотру и редактированию ее свойств.

     В панели задач будет представлена сводная информация о задаче, а также ссылки для управления выполнением задачи и редактирования ее параметров. Информация об особенностях групповых задач содержится в Справочном руководстве Kaspersky Administration Kit.

- *Чтобы перейти к просмотру и настройке параметров задач для наборов компьютеров (задач Kaspersky Administration Kit), выполните следующие действия:*

  1. Запустите Консоль администрирования Kaspersky Administration Kit.

  2. Выберите папку **Задачи для наборов компьютеров** (**Задачи Kaspersky Administration Kit**).

  3. В дереве консоли выберите нужную задачу для перехода к просмотру и редактированию ее свойств.

     В панели задач будет представлена сводная информация о задаче, а также ссылки для управления выполнением задачи и редактирования ее параметров. Информация об особенностях задач Kaspersky Administration Kit и для наборов компьютеров содержится в Справочном руководстве Kaspersky Administration Kit.

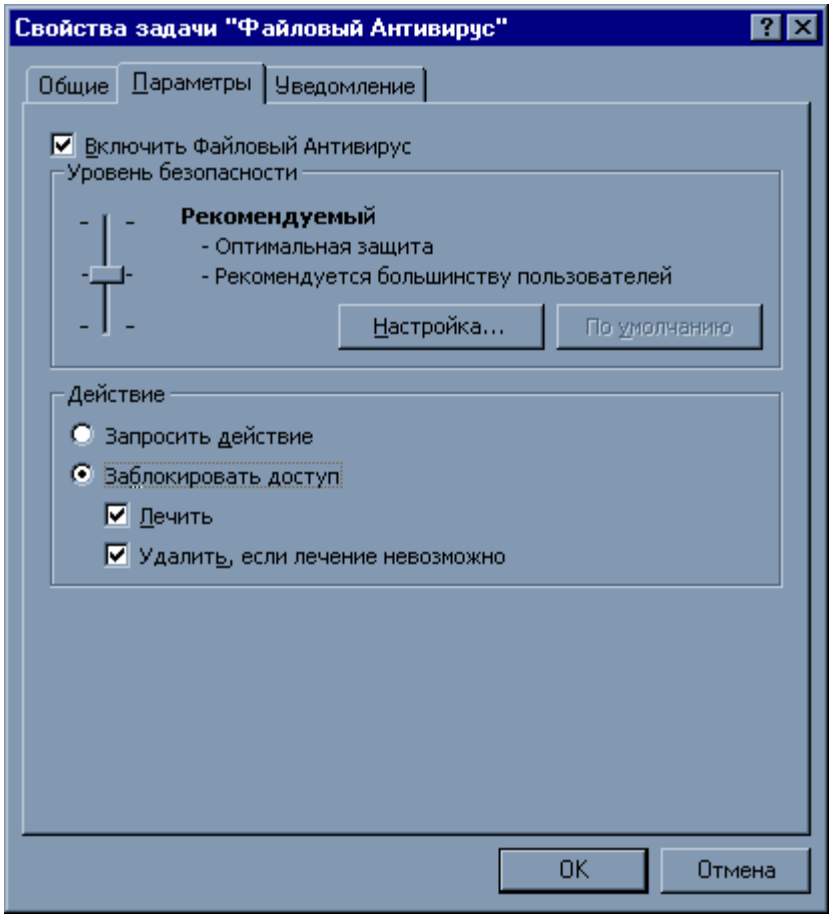


Рисунок 69. Окно Свойства задачи «Файловый Антивирус». Закладка Параметры

НАСТРОЙКА ФАЙЛОВОГО АНТИВИРУСА

Чтобы просмотреть и отредактировать параметры Файлового Антивируса, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Задачи**.

2. Выберите задачу **Файловый Антивирус** в списке и нажмите на кнопку **Свойства**.

3. В открывшемся окне свойств задачи на закладке **Параметры** (см. рис. выше) настройте следующие параметры:

   - Включите или выключите Файловый Антивирус на удаленном компьютере, используя соответствующий флажок.

   - В блоке **Уровень безопасности** выберите уровень защиты файловой системы удаленного компьютера, переместив ползунок по шкале или нажмите на кнопку **Настройка**, чтобы изменить параметры текущего уровня безопасности. В открывшемся окне **Настройка: Файловый Антивирус** (см. рис. ниже) отредактируйте параметры защиты файлов:

     - на закладке **Общие** укажите, объекты какого формата будут проверяться Kaspersky Endpoint Security на вирусы при открытии, исполнении и сохранении (блок **Типы файлов**), настройте производительность проверки и выберите технологию проверки (блок **Оптимизация**), выберите, какие составные файлы необходимо анализировать на присутствие вирусов и установите ограничение на проверку больших объектов (блок **Составные файлы**);

- на закладке **Область защиты** укажите диски или папки, которые должны контролироваться Файловым Антивирусом. По умолчанию включена защита всех объектов, расположенных на жестких, сменных и сетевых дисках, подключенных к компьютеру. Вы можете добавить объект для проверки, изменить объект списка, временно отключить проверку объекта списка или удалить объект;

- на закладке **Дополнительно** выберите режим срабатывания Файлового Антивируса (блок **Режим проверки**), включите приостановку работы Файлового Антивируса по расписанию и настройте параметры расписания (блок **Приостановка задачи**), настройте использование Файловым Антивирусом эвристического анализатора (блок **Эвристический анализатор**).

- В блоке **Действие** выберите действие, которое должен выполнить Файловый Антивирус при обнаружении зараженного или возможно зараженного объекта.

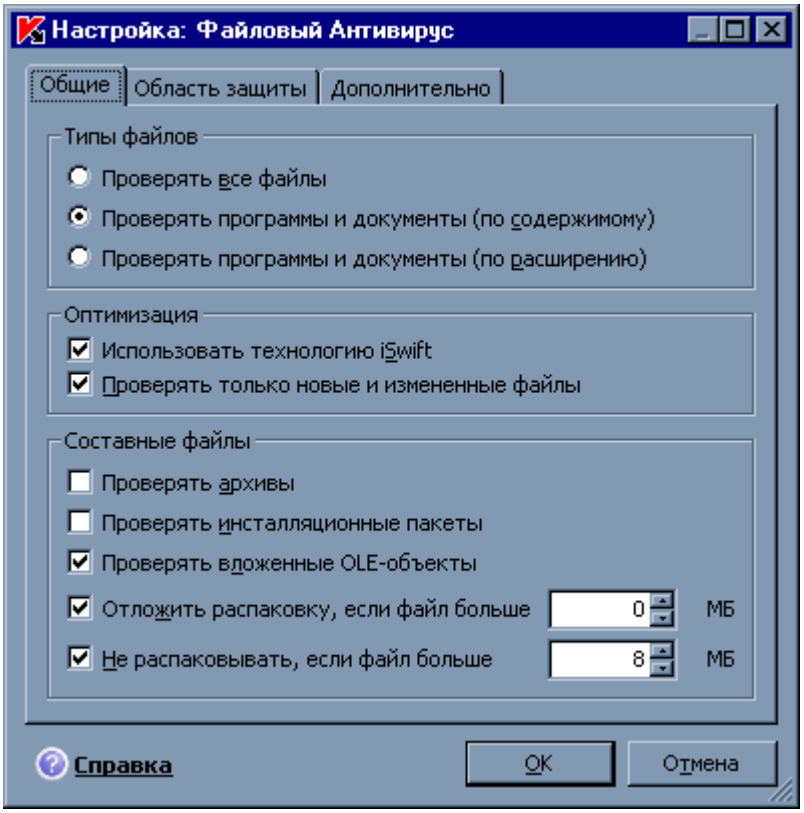


Рисунок 70. Окно Настройка: Файловый Антивирус

НАСТРОЙКА ЗАДАЧ ПОИСКА ВИРУСОВ

Чтобы просмотреть и отредактировать параметры задачи поиска вирусов, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Задачи**.

2. Выберите задачу поиска вирусов в списке и нажмите на кнопку **Свойства**.

3. В открывшемся окне свойств задачи на закладке **Параметры** (см. рис. ниже) настройте следующие параметры:

   - В блоке **Уровень безопасности** выберите уровень, на котором задача поиска вирусов будет осуществлять проверку объектов на удаленном компьютере, переместив ползунок по шкале или нажмите на кнопку **Настройка**, чтобы изменить параметры текущего уровня безопасности. В открывшемся окне (см. рис. ниже) отредактируйте параметры уровня безопасности:

- на закладке **Общие** укажите формат файлов, которые будут проверяться Kaspersky Endpoint Security при выполнении задач поиска вирусов (блок **Типы файлов**), настройте производительность проверки (блок **Оптимизация**), выберите, какие составные файлы необходимо анализировать на присутствие вирусов (блок **Составные файлы**);

- на закладке **Дополнительно** настройте использование технологии проверки и возможность возобновления остановленной задачи (блок **Дополнительные параметры**), также использование эвристического анализатора в задачах поиска вирусов (блок **Эвристический анализатор**).

- В блоке **Действие** выберите действие, которое должен выполнить Kaspersky Endpoint Security при обнаружении зараженного или возможно зараженного объекта;

- В блоке **Объекты проверки** укажите объекты, которые будут проверяться Kaspersky Endpoint Security при выполнении задачи. Вы можете добавить объект для проверки в список, временно отключить проверку объекта списка или удалить объект.

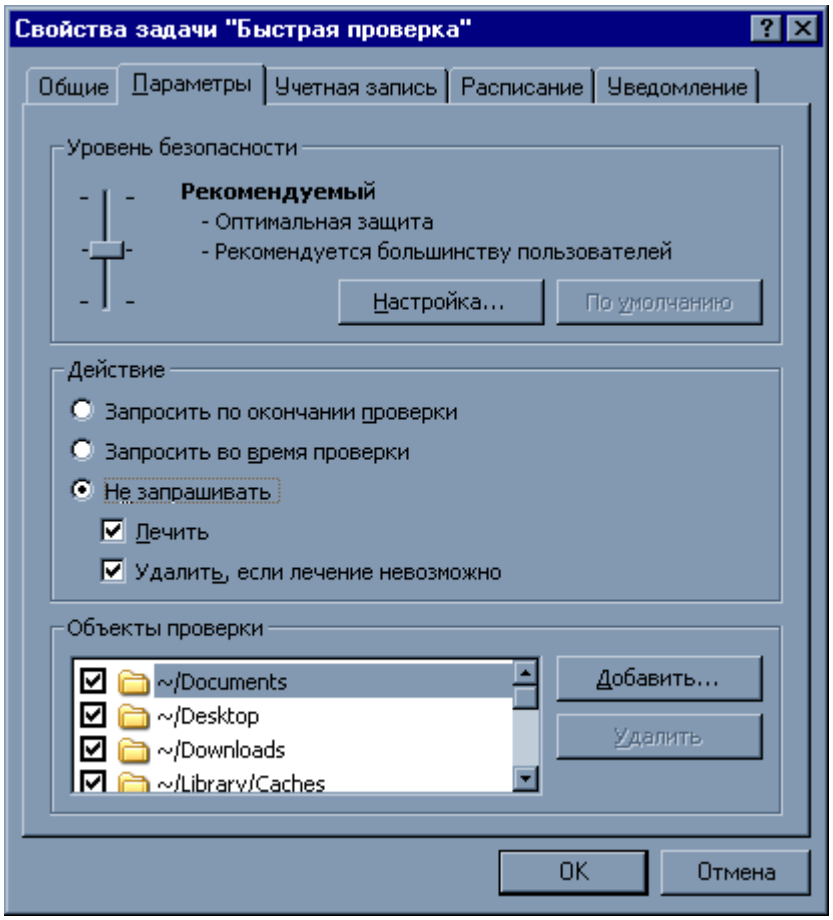


Рисунок 71. Окно Свойства задачи «Быстрая проверка». Закладка Параметры

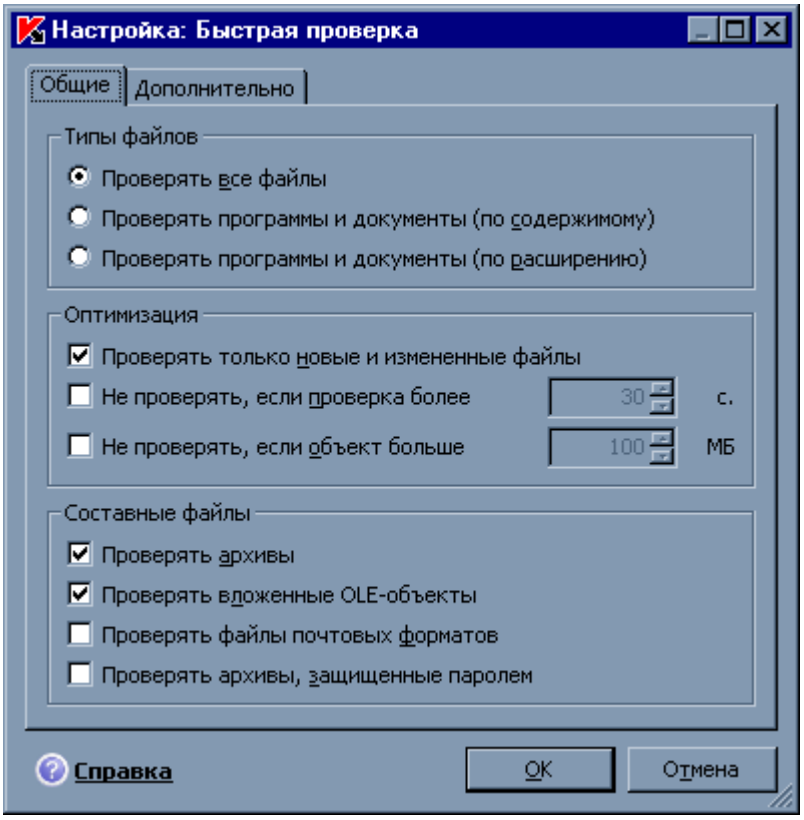


Рисунок 72. Окно Настройка: Быстрая проверка

НАСТРОЙКА ЗАДАЧИ ОБНОВЛЕНИЯ

Чтобы просмотреть и отредактировать параметры задачи обновления, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. раздел «Управление программой» на стр. 126) на закладке **Задачи**.

2. Выберите задачу обновления в списке и нажмите на кнопку **Свойства**.

3. В открывшемся окне свойств задачи на закладке **Параметры** (см. рис. ниже) настройте следующие параметры:

   - В блоке **Параметры обновления**, укажите должны ли в процессе обновления программы, копироваться и устанавливаться на удаленный компьютер не только антивирусные базы, но и модули программы. Для этого установите флажок **Обновлять модули программы**. Вы можете также выбрать источник обновлений и настроить копирование получаемых обновлений в локальный источник. Для этого нажмите на кнопку **Настройка**. Откроется окно **Настройка обновления** (см. рис. ниже), в котором вы можете выполнить следующие действия:

     - на закладке **Источник обновления** указать источник, из которого будут загружены обновления антивирусных баз и модулей программы. По умолчанию обновление выполняется с Сервера администрирования и с серверов обновлений «Лаборатории Касперского». Вы можете добавить новый источник обновлений в список, изменить источник обновлений, временно отключить получение обновлений из источника и удалить источник обновлений из списка;

     - на закладке **Дополнительно** включить сервис копирования обновлений в локальный источник и указать путь к папке общего доступа, в которую будут сохраняться получаемые обновления.

   - В блоке **Действия после обновления** укажите, должен ли Kaspersky Endpoint Security запускать проверку объектов, помещенных в хранилище карантина после обновления программы.

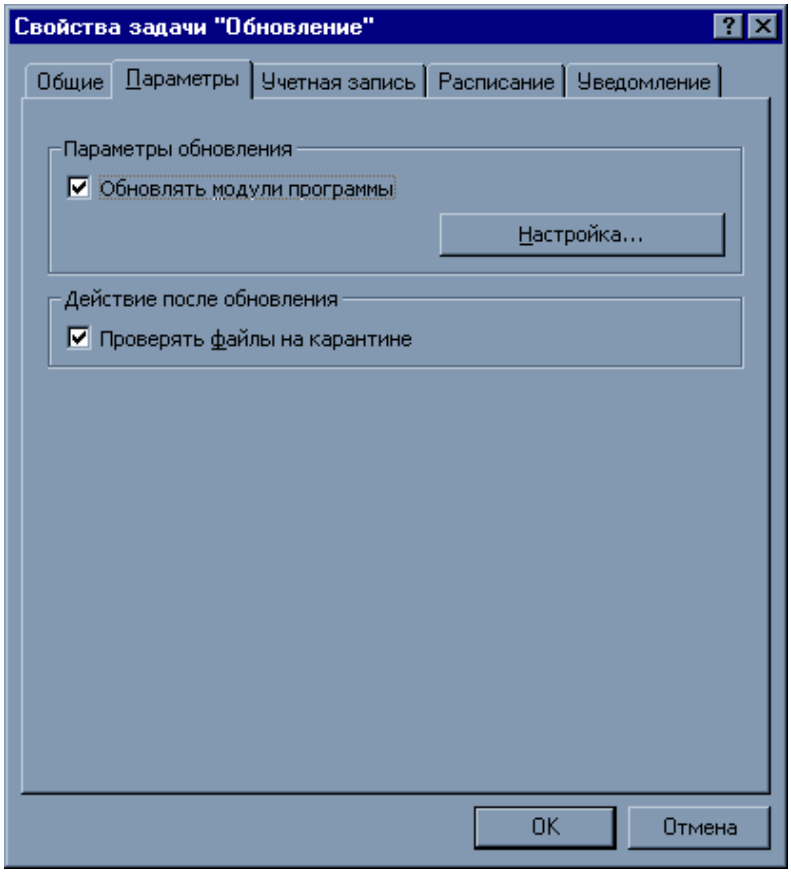


Рисунок 73. Окно Свойства задачи «Обновление». Закладка Параметры

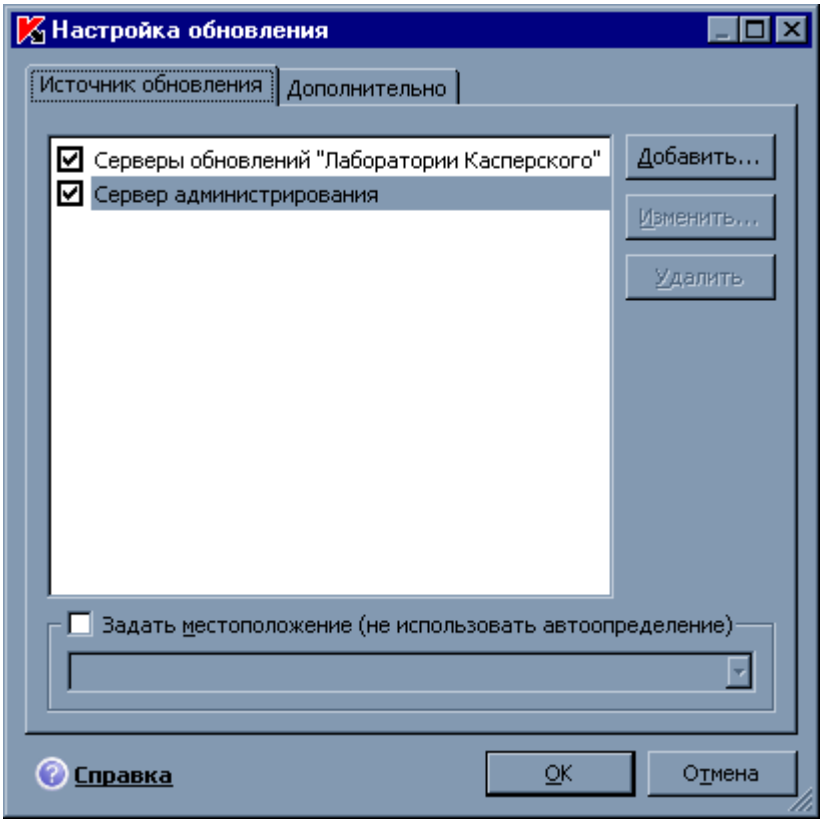


Рисунок 74. Окно Настройка обновления

Управление политиками

Определение политик позволяет распространять единые настройки параметров программы и задач на клиентские компьютеры, входящие в состав одной группы администрирования.

В данном разделе приведена информация о создании и настройке политик для Kaspersky Endpoint Security[21].

При создании и настройке политики вы можете налагать запрет на полное или частичное изменение ее параметров в политиках вложенных групп, параметрах задач и параметрах программы. Для этого нажмите на кнопку  . Для параметров, запрещенных к изменению, она должна принять вид  .

Над политиками можно выполнять следующие действия:

- создавать политики;
- настраивать параметры политик;
- копировать и переносить политики из одной группы в другую, а также удалять политики при помощи контекстного меню;
- импортировать и экспортировать параметры политик.

Чтобы открыть список политик, сформированных для Kaspersky Endpoint Security, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**.
3. В папке **Управляемые компьютеры** выберите папку с названием группы, в которую входит клиентский компьютер.
4. В выбранной группе выберите вложенную папку **Политики**. В дереве консоли будут представлены все созданные для этой группы политики.

В этом разделе

Создание политики

При работе с Kaspersky Endpoint Security через Kaspersky Administration Kit вы можете создавать политики для программы.

Чтобы создать политику, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**.

[21] Подробнее смотрите Руководство администратора Kaspersky Administration Kit.

3. В папке **Управляемые компьютеры** выберите папку с названием группы, в которую входит клиентский компьютер.

4. В выбранной группе выберите вложенную папку **Политики**. В дереве консоли будут представлены все созданные для этой группы политики.

5. По ссылке **Создать новую политику** в панели задач запустите Мастер создания политики (на стр. 152). Следуйте его шагам, чтобы создать новую политику для Kaspersky Endpoint Security.

МАСТЕР СОЗДАНИЯ ПОЛИТИКИ

Создавать новые политики, определяющие единые настройки параметров программы и задач для клиентских компьютеров, входящих в состав одной группы администрирования, вы можете с помощью Мастера создания политики.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

ШАГ 1. ВВОД ОБЩИХ ДАННЫХ О ПОЛИТИКЕ

В окне **Имя политики** в поле **Имя** укажите имя создаваемой политики.

ШАГ 2. ВЫБОР ПРОГРАММЫ

В окне **Программа** выберите программу «Лаборатории Касперского», для которой создается политика: **Kaspersky Endpoint Security 8.0 для Mac**.

ШАГ 3. ВЫБОР СТАТУСА ПОЛИТИКИ

В окне **Создание политики** выберите статус политики[22], который будет ей присвоен после создания. Политике можно присвоить следующие статусы:

- активная политика;
- неактивная политика;
- политика для мобильного пользователя.

В группе компьютеров для одной программы может быть создано несколько политик, но действующей (активной) может быть только одна из них.

ШАГ 4. НАСТРОЙКА ПАРАМЕТРОВ ЗАЩИТЫ

В окне **Защита** включите или выключите компоненты защиты, которые будут использоваться в политике.

По умолчанию все компоненты защиты включены. Чтобы отключить какой-либо из них, снимите флажок рядом с его названием. Для детальной настройки компонента защиты выберите его в списке и нажмите на кнопку **Настройка**.

[22] Подробнее смотрите Справочное руководство Kaspersky Administration Kit.

См. также

Шаг 5. Настройка параметров поиска вирусов

В окне **Поиск вирусов** настройте параметры по умолчанию, в соответствии с которыми будут выполняться задачи поиска вирусов.

См. также

Шаг 6. Настройка параметров обновления

В окне **Обновление** укажите параметры по умолчанию, с которыми будут выполняться задачи обновления программы.

См. также

Шаг 7. Настройка сети

В окне **Настройка сети** укажите параметры подключения к прокси-серверу.

Если вы не хотите использовать прокси-сервер для выхода в интернет во время обновления антивирусных баз и модулей программы, снимите флажок **Использовать прокси-сервер**.

Если флажок установлен, то возможна настройка следующих параметров подключения к прокси-серверу:

- использования Kaspersky Endpoint Security параметров прокси-сервера, указанных в системных настройках Mac OS X или заданных пользователем адреса прокси-сервера и порта;
- возможности использования прокси-сервера при обновлении из локальной или сетевой папки;
- параметров аутентификации для соединения с прокси-сервером.

См. также

Настройка параметров подключения к прокси-серверу 138

Шаг 8. Настройка параметров взаимодействия с пользователем

В окне **Взаимодействие с пользователем** укажите каким образом будет осуществляться взаимодействие пользователя с Kaspersky Endpoint Security на удаленном компьютере.

Вы можете настроить получение пользователем уведомлений и изменить отображение значка Kaspersky Endpoint Security на удаленном компьютере.

См. также

Настройка получения уведомлений 135

Настройка отображения значка Kaspersky Endpoint Security 136

Шаг 9. Настройка параметров отчетов и хранилищ

В окне **Отчеты и Хранилища** укажите параметры формирования и хранения отчетов, а также параметры хранения объектов в хранилище карантина и резервном хранилище.

См. также

Настройка параметров отчетов 136

Настройка параметров карантина и резервного хранилища 138

Шаг 10. Завершение создания политики

В последнем окне мастер проинформирует вас об успешном завершении процесса создания политики. Нажмите на кнопку **Готово** для завершения работы мастера.

Созданная политика появится в дереве консоли в папке **Политики** соответствующей группы администрирования.

Для созданной политики вы можете отредактировать ее параметры и установить ограничения на их изменения с помощью кнопок  и  для каждой группы настроек. Если установлен значок  , то пользователь на клиентском компьютере не сможет изменить настройки. Параметры, отмеченные значком  доступны для редактирования пользователем.

Политика будет распространена на клиентские компьютеры после первой синхронизации клиентов с Сервером администрирования.

Настройка параметров политики

Kaspersky Administration Kit позволяет вносить изменения в созданную политику, а также налагать запрет на изменение ее параметров в политиках вложенных групп, в параметрах программы и параметрах задач. Параметры политики можно редактировать в окне свойств политики на закладке **Настройка** (см. рис. ниже).

Все закладки окна свойств политики, кроме закладки **Настройка**, стандартны для программы Kaspersky Administration Kit[23].

Параметры политики для Kaspersky Endpoint Security включают в себя параметры программы (см. раздел «Настройка параметров программы» на стр. 129) и параметры задач (см. раздел «Настройка параметров задачи» на стр. 144).

Чтобы перейти к просмотру и настройке параметров политики, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Administration Kit.
2. Разверните узел **Сервер администрирования**.
3. В папке **Управляемые компьютеры** выберите папку с названием группы, в которую входит клиентский компьютер.
4. В выбранной группе выберите вложенную папку **Политики**. В дереве консоли будут представлены все созданные для этой группы политики.
5. Выберите в дереве консоли нужную политику для перехода к просмотру и редактированию ее свойств.

   В панели задач будет представлена сводная информация о политике и ссылки для управления статусом политики и редактирования ее параметров.

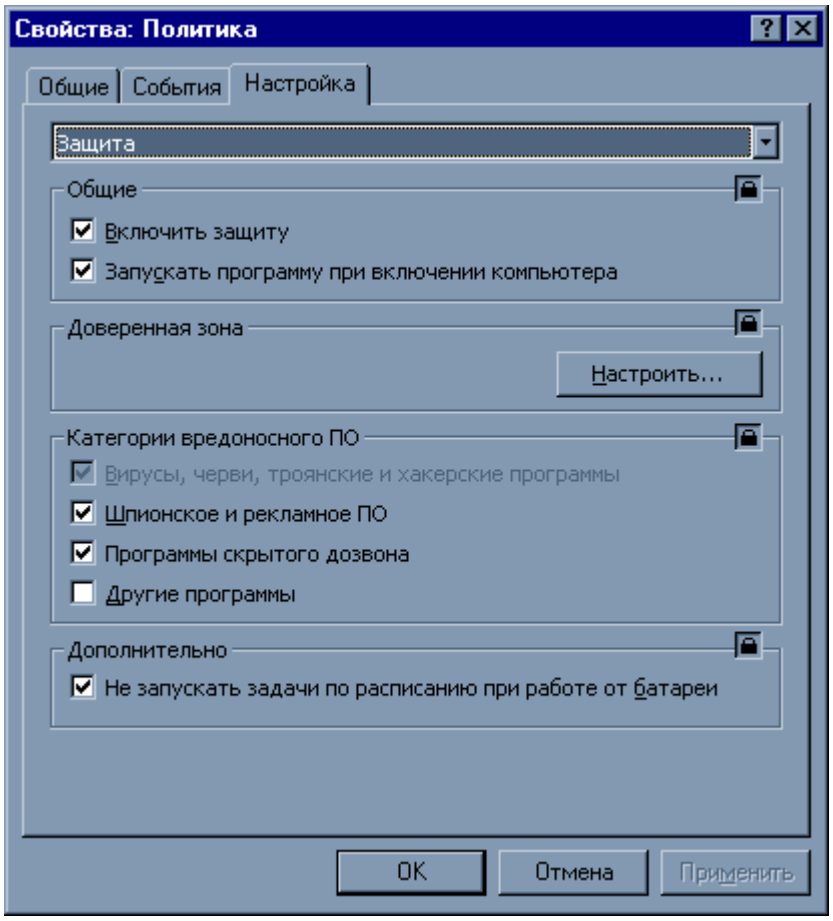


Рисунок 75. Окно свойств политики. Закладка Настройка

[23] Подробнее смотрите Руководство администратора Kaspersky Administration Kit.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Если вы приобрели Kaspersky Endpoint Security, информацию об этой программе можно получить от специалистов Службы технической поддержки по телефону или через интернет. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы, а если ваш компьютер был заражен, они помогут устранить последствия работы вредоносных программ.

Чтобы просмотреть информацию о способах получения поддержки по Kaspersky Endpoint Security,

откройте главное окно программы (на стр. 34) и нажмите на кнопку  .

Прежде чем обращаться в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами поддержки (http://support.kaspersky.ru/support/rules).

Если при использовании Kaspersky Endpoint Security у вас возникла проблема, прежде всего проверьте, не описан ли способ ее решения в документации, справке, в Базе знаний на веб-сайте Службы технической поддержки «Лаборатории Касперского» или на Форуме пользователей (см. раздел «Дополнительные источники информации» на стр. 15). Если вы не нашли решения вашей проблемы, рекомендуем обратиться в Службу технической поддержки «Лаборатории Касперского».

Обратите внимание, что для получения технической поддержки вы должны быть зарегистрированным пользователем коммерческой версии Kaspersky Endpoint Security. Поддержка пользователей пробных версий не осуществляется.

Если Kaspersky Endpoint Security активируется с помощью кода активации, регистрация пользователя будет выполнена Ассистентом активации (см. раздел «Активация Kaspersky Endpoint Security» на стр. 28).

Если вы активируете Kaspersky Endpoint Security с помощью файла ключа, пройдите процедуру регистрации непосредственно на веб-сайте Службы технической поддержки (http://www.kaspersky.ru/support).

Номер клиента и пароль, полученные при регистрации, необходимы для доступа к Персональному кабинету – личному разделу пользователя на веб-сайте Службы технической поддержки. В Персональном кабинете вы можете выполнять следующие действия:

- отправлять запрос в Службу поддержки без предварительного ввода регистрационной информации;
- переписываться со Службой поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени;
- просматривать полную историю ваших обращений в Службу поддержки;
- получать резервную копию файла ключа.

Электронный запрос в Службу технической поддержки

Для обращения в Службу технической поддержки откройте веб-форму системы обработки клиентских запросов Helpdesk (http://support.kaspersky.ru/helpdesk.html). На открывшейся веб-странице Службы технической поддержки войдите в свой Персональный кабинет и заполните форму запроса.

Запрос можно отправить на русском, английском, немецком, французском или испанском языках.

Отправляя электронный запрос, укажите в нем **номер клиента**, полученный при регистрации на веб-сайте Службы технической поддержки, и **пароль**.

В веб-форме запроса как можно подробнее опишите возникшую проблему. В обязательных для заполнения полях укажите:

- **Тип запроса**. Выберите тему, наиболее точно соответствующую возникшей проблеме, например «Проблема установки / удаления продукта» или «Проблема поиска / удаления вирусов». Если подходящей темы не найдется, выберите «Общий вопрос».
- **Название и номер версии программы**.
- **Текст запроса**. Как можно подробнее опишите возникшую проблему.
- **Номер клиента и пароль**. Введите номер клиента и пароль, которые вы получили при регистрации на веб-сайте Службы технической поддержки.
- **Электронный адрес**. По этому адресу специалисты Службы технической поддержки перешлют ответ на ваш запрос.

Вы получите ответ на свой запрос от специалиста Службы технической поддержки в своем Персональном кабинете и по электронному адресу, который вы указали в запросе.

Техническая поддержка по телефону

Если возникла неотложная проблема, вы можете позвонить в Службу технической поддержки в вашем городе. Перед обращением к сотрудникам русскоязычной (http://support.kaspersky.ru/support/support_local) или интернациональной (http://support.kaspersky.ru/support/international) технической поддержки, пожалуйста, соберите информацию (http://support.kaspersky.ru/support/details) о своем компьютере и установленной на нем антивирусной программе. Это позволит нашим специалистам быстрее помочь вам.

Создание файла трассировки

Во время работы Kaspersky Endpoint Security могут возникнуть сбои, причиной которых скорее всего является конфликт Kaspersky Endpoint Security с программным обеспечением, установленным на вашем компьютере. Для успешной диагностики и решения возникшей проблемы специалисты Службы технической поддержки «Лаборатории Касперского» могут попросить вас создать файл трассировки.

Чтобы создать файл трассировки, выполните следующие действия:

1. Откройте окно настройки программы и выберите закладку **Отчеты**.
2. В блоке **Трассировка** установите флажок **Включить трассировку**.
3. Перезапустите Kaspersky Endpoint Security, чтобы запустить процесс трассировки.

Используйте эту опцию только под руководством специалиста Службы технической поддержки «Лаборатории Касперского».

Файлы трассировки могут занимать значительный объем дискового пространства. По окончании работы с файлами трассировки рекомендуется выключить их создание, сняв флажок **Включить трассировку** на закладке **Отчеты** окна настройки программы. После этого перезапустите программу Kaspersky Endpoint Security.

ПРИЛОЖЕНИЯ

Этот раздел Руководства содержит справочную информацию о форматах проверяемых файлов и разрешенных масках исключения, используемых при настройке параметров Kaspersky Endpoint Security.

В ЭТОМ РАЗДЕЛЕ

Список объектов, проверяемых по расширению

Если при настройке Файлового Антивируса (см. раздел «Определение типов проверяемых файлов» на стр. 62) или задач поиска вирусов (см. раздел «Определение типов проверяемых объектов» на стр. 76) вы выбрали вариант **Проверять программы и документы (по расширению)**, то на вирусы будут проверяться объекты с приведенными ниже расширениями:

com – исполняемый файл программы Microsoft Windows размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив Microsoft Windows;

sys – системный файл Microsoft Windows;

prg – текст программы dBase, Clipper или Microsoft Visual FoxPro, программа пакета WAVmaker;

bin – бинарный файл Microsoft Windows;

bat – файл пакетного задания Microsoft Windows;

cmd – командный файл Microsoft Windows NT (аналогичен bat–файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки Microsoft Windows;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – программа Microsoft Windows, работающая в режиме разделения времени;

drv – драйвер некоторого устройства Microsoft Windows;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл Microsoft Windows с информацией о программе;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл инициализации Microsoft Windows;

cla – класс Java;

vbs – скрипт Visual Basic;

vbe – видеорасширение BIOS;

js, *jse* – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовая программа для Microsoft Internet Explorer;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

eml – почтовое сообщение Microsoft Outlook Express;

nws – новое почтовое сообщение Microsoft Outlook Express;

msg – почтовое сообщение Microsoft Mail;

plg – почтовое сообщение;

mbx – расширение для сохраненного письма Microsoft Office Outlook;

*doc** – документ Microsoft Office Word, например: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

*dot** – шаблон документа Microsoft Office Word, например, dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – программа баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave Flash;

jpg, *jpeg*, *png* – файл формата для хранения сжатых изображений;

emf – файл формата Enhanced Metafile. Следующее поколение метафайла операционной системы Microsoft Windows;

ico – файл значка объекта;

ov? – исполняемые файлы MS DOS;

x*l** – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документов, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

*pp** – документы и файлы Microsoft Office PowerPoint, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint 2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

*md** – документы и файлы Microsoft Office Access, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных и т.д.;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

Фактический формат файла может не совпадать с форматом, указанным в расширении файла.

Разрешенные маски исключений файлов

Рассмотрим примеры разрешенных масок, которые вы можете использовать при формировании списка исключаемых файлов:

1. Маски без путей к файлам:
   - ***.zip** – все файлы с расширением zip;
   - ***.zi?** – все файлы с расширением zi?, где вместо ? может использоваться любой один символ;
   - **test** – все файлы с именем test.
2. Маски с абсолютными путями к файлам:
   - **dir/*** или **/dir/** – все файлы в папке /dir/;
   - **/dir/*.zip** – все файлы с расширением zip в папке /dir/;
   - **/dir/*.zi?** – все файлы с расширением zi? в папке /dir/, где вместо ? может использоваться любой один символ;
   - **/dir/test** – все файлы с именем test в папке /dir/ и всех вложенных в нее папках.

3. Маски с относительными путями к файлам:

   - **dir/*** или **dir/** – все файлы во всех папках dir/;
   - **dir/*.zip** – все файлы с расширением zip во всех папках dir/;
   - **dir/*.zi?** – все файлы с расширением zi? во всех папках dir/, где вместо ? может использоваться любой один символ;
   - **dir/test** – все файлы с именем test во всех папках dir/ и всех вложенных в них папках.

Использовать маску исключения * допустимо только при указании типа исключаемой угрозы согласно Вирусной энциклопедии. В этом случае указанная угроза не будет обнаруживаться во всех объектах. Использование данной маски без указания типа угрозы равносильно отключению защиты.

Разрешенные маски исключений по классификации Вирусной энциклопедии

При добавлении в качестве исключения угрозы с определенным статусом по классификации Вирусной энциклопедии вы можете указать:

- Полное имя угрозы, как оно представлено в Вирусной энциклопедии на сайте www.securelist.com (http://www.securelist.com) (например, **not-a-virus:RiskWare.RemoteAdmin.RA.311** или **Flooder.Win32.Fuxx**).
- Имя угрозы по маске, например:
  - **not-a-virus*** – исключать из проверки легальные, но нежелательные программы, а также программы-шутки;
  - ***Riskware.*** – исключать из проверки все нежелательные программы типа Riskware;
  - ***RemoteAdmin.*** – исключать из проверки все версии программы удаленного администрирования.

Примеры названий угроз можно просмотреть в окне отчетов на закладке **Обнаружено**, в хранилище карантина и резервном хранилище, а также во всплывающих экранных сообщениях (см. раздел «Окна уведомлений и всплывающие сообщения» на стр. 37) об обнаружении опасных объектов.

ГЛОССАРИЙ ТЕРМИНОВ

О

OLE-объект

Присоединенный или встроенный в другой файл объект. Программа «Лаборатории Касперского» позволяет проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

А

Агент администрирования

Компонент программы Kaspersky Administration Kit, осуществляющий взаимодействие между Сервером администрирования и программами «Лаборатории Касперского», установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех Windows-программ из состава продуктов компании. Для Novell-, Unix- и Mac-программ «Лаборатории Касперского» существуют отдельные версии Агента администрирования.

Администратор Kaspersky Administration Kit

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Administration Kit.

Активация программы

Перевод программы в полнофункциональный режим. Для активации программы пользователю необходима лицензия.

Активная лицензия

Лицензия, используемая в данный временной период для работы программы «Лаборатории Касперского». Лицензия определяет срок действия полной функциональности и лицензионную политику в отношении программы. В программе не может быть больше одной лицензии со статусом «активная».

Архив

Файл, «содержащий» в себе один или несколько других объектов, которые в свою очередь также могут быть архивами.

Б

Базы

Базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие подробное описание всех существующих на текущий момент угроз компьютерной безопасности, способов их обнаружения и обезвреживания. Базы постоянно обновляются в «Лаборатории Касперского» по мере появления новых угроз.

Блокирование объекта

Запрет доступа к объекту со стороны внешних программ. Заблокированный объект не может быть прочитан, выполнен или изменен.

В

Возможно зараженный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Возможно зараженные файлы обнаруживаются с помощью эвристического анализатора.

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Г

Группа администрирования

Набор компьютеров, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ «Лаборатории Касперского». Компьютеры группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех входящих в ее состав клиентских компьютерах.

Групповая политика

см. Политика

Д

Дополнительная лицензия

Лицензия, добавленная для работы программы «Лаборатории Касперского», но не активированная. Дополнительная лицензия начинает действовать по окончании срока действия активной лицензии.

З

Задача для набора компьютеров

Задача, определенная для набора клиентских компьютеров из произвольных групп администрирования и выполняемая на них.

Зараженный объект

Объект, внутри которого содержится вредоносный код: при проверке объекта было обнаружено полное совпадение участка кода объекта с кодом известной угрозы. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами, поскольку это может привести к заражению вашего компьютера.

Защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект на чтение, запись и исполнение и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы или подозреваемые на наличие угрозы, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются, помещаются на карантин).

И

Исключение

Исключение – объект, исключаемый из проверки программой «Лаборатории Касперского». Исключать из проверки можно файлы определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по типу угрозы согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

К

Карантин

Определенная папка, куда помещаются все возможно зараженные объекты, обнаруженные во время проверки или в процессе функционирования постоянной защиты.

Клиент Сервера администрирования (Клиентский компьютер)

Компьютер, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые программы «Лаборатории Касперского».

Л

Лечение объектов

Способ обработки зараженных объектов, в результате которого происходит полное или частичное восстановление данных, либо принимается решение о невозможности лечения объектов. Лечение объектов выполняется на основе записей баз. В процессе лечения часть данных может быть потеряна.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой «Лаборатории Касперского» как зараженный ввиду того, что его код напоминает код вируса.

М

Максимальная защита

Уровень безопасности вашего компьютера, соответствующий максимально полной защите, которую может обеспечить программа. При таком уровне защиты на присутствие вирусов проверяются все файлы компьютера, сменных носителей и сетевых дисков, если таковые подключены к компьютеру.

Маска файла

Представление имени и расширения файла общими символами. Двумя основными символами, используемыми в масках файлов, являются ***** и **?** (где ***** – любое число любых символов, а **?** – любой один символ). При помощи данных знаков можно представить любой файл. Обратите внимание, что имя и расширение файла всегда пишутся через точку.

Н

Неизвестный вирус

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора, и таким объектам присваивается статус возможно зараженных.

О

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

Обновление баз

Одна из функций, выполняемых программой «Лаборатории Касперского», которая позволяет поддерживать защиту в актуальном состоянии. При этом происходит копирование баз с серверов обновлений «Лаборатории Касперского» на компьютер и автоматическое подключение их к программе.

Опасный объект

Объект, внутри которого содержится вирус. Не рекомендуется работать с такими объектами, поскольку это может привести к заражению компьютера. При обнаружении зараженного объекта рекомендуется лечить его с помощью программы «Лаборатории Касперского» или удалить, если лечение невозможно.

П

Пакет обновлений

Пакет файлов для обновления программного обеспечения, который копируется из интернета и устанавливается на вашем компьютере.

Подозрительный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Подозрительные объекты обнаруживаются при помощи эвристического анализатора.

Политика

Набор параметров работы программы в группе администрирования при управлении через Kaspersky Administration Kit. Для разных групп параметры работы программы могут быть различны. Для каждой программы определяется своя собственная политика. Политика включает в себя параметры полной настройки всей функциональности программы.

Потенциально заражаемый объект

Объект, который в силу своей структуры или формата может быть использован злоумышленниками в качестве «контейнера», для размещения и распространения вредоносного объекта. Как правило, это исполняемые файлы, например, с расширением com, exe, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Р

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их первым лечением или удалением.

Рекомендуемый уровень

Уровень безопасности, базирующийся на параметрах работы программы, рекомендуемых экспертами «Лаборатории Касперского» и обеспечивающих оптимальную защиту вашего компьютера. Данный уровень установлен для использования по умолчанию.

С

Сервер администрирования

Компонент программы Kaspersky Administration Kit, осуществляющий функции централизованного хранения информации об установленных в сети предприятия программах «Лаборатории Касперского» и управления ими.

Серверы обновлений «Лаборатории Касперского»

Список HTTP- и FTP-серверов «Лаборатории Касперского», с которых программа копирует базы и обновления модулей на ваш компьютер.

Сетевой порт

Параметр протоколов TCP и UDP, определяющий назначение пакетов данных в IP-формате, передаваемых на хост по сети и позволяющий различным программам, выполняемым на одном хосте, получать данные независимо друг от друга. Каждая программа обрабатывает данные, поступающие на определённый порт (иногда говорят, что программа «слушает» этот номер порта).

Обычно за некоторыми распространёнными сетевыми протоколами закреплены стандартные номера портов (например, веб-серверы обычно принимают данные по протоколу HTTP на TCP-порт 80), хотя в общем случае программа может использовать любой протокол на любом порте. Возможные значения: от 1 до 65535.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Т

Технология Growl

Универсальная система оповещения пользователя в операционной системе Mac OS X. Поддерживает настраиваемые стили уведомления: кроме всплывающих уведомлений присутствует возможность уведомления голосом, отправкой sms или e-mail.

Внешний вид уведомлений, выводимых с помощью Growl, может быть настроен из раздела **Другие** панели Системных настроек, куда Growl автоматически встраивается после установки.

Э

Эвристический анализатор

Технология обнаружения угроз, неопределяемых с помощью баз программ «Лаборатории Касперского». Позволяет находить объекты, которые подозреваются на заражение неизвестным вирусом или новой модификацией известного.

С помощью эвристического анализатора обнаруживаются до 92% новых угроз. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям.

Файлы, обнаруженные с помощью эвристического анализатора, признаются подозрительными.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» была основана в 1997 году. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

«Лаборатория Касперского» – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

«Лаборатория Касперского» сегодня – это более тысячи высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг «Лаборатории Касперского». Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие мировые разработчики используют в своих продуктах программное ядро Антивируса Касперского, например, такие как: Nokia ICG (США), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей технической поддержкой на нескольких языках.

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО «Лаборатория Касперского». Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки подозрительных объектов в архивированном виде) http://support.kaspersky.ru/virlab/helpdesk.html (для запросов вирусным аналитикам)

ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

Для создания программы использовался код сторонних производителей.

В ЭТОМ РАЗДЕЛЕ

Программный код

Для создания программы использовался программный код сторонних производителей.

В ЭТОМ РАЗДЕЛЕ

ADOBE ABI-SAFE CONTAINERS 1.0

BOOST 1.39.0

CURL 7.19.3

EXPAT 1.2

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FMT.H

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED «AS IS», WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

GROWL 1.1.5

Copyright (C) 2004, The Growl Project

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Growl nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS «AS IS» AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

For the purposes of this copyright and license, «Info-ZIP» is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided «as is», without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names «Info-ZIP» (or any variation thereof, including, but not limited to, different capitalizations), «Pocket UnZip,» «WiZ» or «MacZip» without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names «Info-ZIP,» «Zip,» «UnZip,» «UnZipSFX,» «WiZ,» «Pocket UnZip,» «Pocket Zip,» and «MacZip» for its own source and binary releases.

LIBPNG 1.2.8

Copyright (C) 2004, 2006-2009, Glenn Randers-Pehrson

LIBUTF

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED «AS IS», WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT ECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

LZMALIB 4.43

MD5.H

Copyright (C) 1999, Aladdin Enterprises

MD5.H

Copyright (C) 1990, RSA Data Security, Inc

License to copy and use this software is granted provided that it is identified as the «RSA Data Security, Inc. MD5 Message-Digest Algorithm» in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as «derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm» in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided «as is» without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

SHA1.C 1.2

STLPORT 5.2.1

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999-2003, Boris Fomitchev

This material is provided «as is», with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

TINYXML 2.5.3

Copyright (C) 2000-2006, Lee Thomason

ZLIB 1.0.8, 1.2.3

Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler

Средства разработки

Для создания программы использовались средства разработки, инструментарий и прочие средства сторонних производителей.

В этом разделе

GCC 4.0.1

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005 Free Software Foundation, Inc

---

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The «Program», below, refers to any such program or work, and a «work based on the Program» means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term «modification».) Each licensee is addressed as «you».

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and «any later version», you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM «AS IS» WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the «copyright» line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details

type `show w'. This is free software, and you are welcome

to redistribute it under certain conditions; type `show c'

for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a «copyright disclaimer» for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written

by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Другая информация

Дополнительная информация о стороннем коде.

Для проверки электронной цифровой подписи используется программная библиотека защиты информации (ПБЗИ) «Агава-С», разработанная ООО «Р-Альфа».

Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду («ПО с открытым исходным кодом»). Если такая лицензия предусматривает предоставление исходного кода пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса на адрес source@kaspersky.com или сопровождается с продуктом.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

А

Б

В

Г

Д

З

И

К

Л

О

П

Р

С

Т

У

Ф

Х